Code de Conduite des Fournisseurs d'Infrastructures Cloud relatif à la Protection des Données

9 Février 2021

Table des matières

Introduction

Les services de cloud computing offrent des avantages aux utilisateurs du secteur public et privé, notamment en termes d'économies de coûts, de flexibilité, d'efficacité, de sécurité et d'adaptabilité. Les clients qui souhaitent utiliser les services de cloud computing aux fins de traiter des données à caractère personnel doivent avant tout s'assurer que ce traitement soit effectué conformément aux dispositions de la législation européenne en matière de protection des données.

Il existe un grand nombre de fournisseurs de services cloud qui proposent une variété de modèles de cloud computing différents. C'est pourquoi les exigences de protection des données ne peuvent s'appliquer uniformément à l'ensemble de ces modèles de cloud. Le degré d'implication des fournisseurs de services de cloud computing dans le traitement des données à caractère personnel et l'étendue de leur contrôle sur le traitement de ces données, varient en fonction du type de services de cloud computing qui est proposé. Ainsi, les fournisseurs qui proposent plusieurs types de services de cloud computing endossent nécessairement des rôles et des responsabilités différents, notamment en ce qui concerne la protection des données et la sécurité des données.

Par exemple :

- Un fournisseur de Software-as-a-Service **(SaaS)** propose en principe une application logicielle spécifiquement conçue pour traiter des données à caractère personnel (ex. : un service par courriel, un logiciel PGI, des services marketing, etc.). Un fournisseur de SaaS a la capacité d'exercer plusieurs types de contrôles sur les données à caractère personnel qui sont traitées à l'aide de son SaaS et sur la manière dont ces données sont traitées. Par conséquent, il est en mesure de proposer à ses clients des services techniques et contractuels qui sont spécifiquement adaptés au SaaS qu'il propose et reflètent le degré de contrôle dont les fournisseurs SaaS disposent sur la conformité à la protection des données.

- Un fournisseur d'Infrastructure-as-a-Service **(IaaS),** fournit, quant à lui, uniquement du matériel informatique ou une infrastructure informatique virtualisée. Ses clients ont la possibilité de choisir comment ils souhaitent utiliser cette infrastructure. Par exemple, un client qui utilise une IaaS est libre de choisir les applications qu'il souhaite déployer sur cette infrastructure, les données qu'il souhaite traiter sur cette infrastructure, dans quels pays traiter les données et pour quelles finalités, et comment il souhaite protéger ces données. Comme indiqué à la Section 4.2, le Contrat de Services doit être rédigé de façon à refléter les caractéristiques des services d'infrastructure cloud utilisés par les clients. Cependant, étant donné que le client est le seul responsable du choix des données qu'il traite sur l'infrastructure, les fournisseurs IaaS ne sauront pas si, à un moment donné, leur infrastructure est utilisée ou non par les clients pour traiter des données à caractère personnel. Dans la mesure où une IaaS est conçue pour fournir des services automatisés à une échelle suffisante, les fournisseurs IaaS proposent des services standards à tous leurs clients. Ces services offrent des options standardisées aux clients, leur permettant de choisir le service qui correspond le mieux à leurs activités.

Le présent Code de Conduite **(Code)** se concentre sur les fournisseurs IaaS. Dans ce Code, les fournisseurs IaaS sont dénommés Fournisseurs de Services d'Infrastructures Cloud **(CISPs**, Cloud Infrastructure Services Providers**).** Le Code vise à aider les CISPs à s'assurer du respect des dispositions du RGPD et à aider les clients à déterminer si les services d'infrastructure cloud sont adaptés au traitement des données à caractère personnel qu'ils souhaitent effectuer. La nature très diverse des services d'infrastructure cloud - par rapport à d'autres types de services de cloud computing - suppose

nécessairement l'établissement d'un Code qui soit spécifiquement adapté aux IaaS.

Ce Code distinct fournira une meilleure compréhension des IaaS au sein de l'Union européenne en créant une transparence. Il contribuera ainsi à créer un environnement de confiance et à maintenir le degré le plus élevé de protection des données. Cet environnement sera bénéfique tant pour les Petites et Moyennes Entreprises (PME), que pour les clients et fournisseurs de cloud, et notamment pour les administrations publiques.

Le Code contient un ensemble d'exigences applicables aux CISPs en leur qualité de sous-traitant des données à la Section 4 (Exigences en matière de Protection des Données) et à la Section 5 (Exigences en matière de Transparence) (ensemble, les **Exigences du Code).** Ces exigences apportent des précisions et des éclaircissements sur la manière dont les CISPs respecteront leurs obligations prévues par le RGPD, sur les exigences en matière de transparence entre le CISP et le client et décrivent les normes minimales que les clients sont en droit d'attendre de CISPs qui respectent les dispositions du Code. Le Code permet de démontrer aux clients qu'un CISP a mis en place des mesures techniques et organisationnelles appropriées pour fournir des « garanties suffisantes » que le traitement répondra aux exigences du RGPD et s'assurera de la protection des droits des personnes concernées, en application de l'Art 28(1) du RGPD. Bien que dans un environnement IaaS, la responsabilité du respect de la protection des données soit partagée entre les clients et les CISPs, le Code n'impose aucune obligation aux clients.

De même, le Code inclut en Annexe A des pratiques et des obligations techniques et organisationnelles en matière de sécurité permettant aux CISPs, quelle que soit leur taille, de ne pas seulement renforcer leur niveau de sécurité en adoptant des meilleures pratiques en matière de sécurité, mais également de partager des normes de sécurité communes pour leurs offres IaaS. Ces normes aideront le client à déterminer s'il respecte ou non ses obligations aux termes de l'Article 25 du RGPD. Tandis que l'Annexe A fait référence à certaines pratiques visées dans les normes ISO/IEC 27001, 27017 et 27018, le Code n'a pas pour objet de répliquer ces normes de sécurité dans la mesure où la mise en œuvre et la certification de ces normes sont, en principe, difficilement abordables pour les CISPs de petite et moyenne taille. Le Code vise à définir des lignes directrices pragmatiques et clés en main que tous les CISPs peuvent utiliser pour garantir la conformité de leurs offres IaaS. La Check-list de Conformité incluse en Annexe B facilitera les efforts des CISPs pour respecter les Exigences du Code et adopter les mesures de sécurité pertinentes prévues par l'Annexe A. Le Code propose également une structure de gouvernance à la Section 7 (Gouvernance) pour soutenir la mise en œuvre, la gestion et l'évolution du Code.

Le Code est un instrument volontaire, qui permet à un CISP d'évaluer et de démontrer son adhésion aux Exigences du Code pour un ou plusieurs de ses services. Cette adhésion peut se manifester par (i) le processus d'auto-Évaluation, ou (ii) une Adhésion Contrôlée, comme indiqué à la Section 6.

Les CISPs qui ont démontré leur adhésion au Code peuvent utiliser la marque de conformité du Code.

Les clients sont invités à vérifier que les Exigences du Code, les autres assurances contractuelles fournies par le CISP, et leurs politiques internes sont conformes à leurs obligations au regard de la législation européenne applicable en matière de protection des données. Les clients ont la possibilité de vérifier l'adhésion d'un CISP au Code sur le site internet listant toutes les organisations ayant déclaré leur adhésion au présent Code (https://cispe.cloud) **(Registre Public CISPE).**

L'**Autorité de Contrôle Désignée** pour le Code est la Commission Nationale de l'Informatique et des Libertés (CNIL), qui a explicitement accepté cette désignation. CISPE

a identifié la CNIL comme l'Autorité de Contrôle Désignée en charge d'approuver le Code CISPE. Les membres de CISPE sont établis et actifs dans plusieurs États Membres de l'Union européenne, dont neuf membres ont leur siège en France et plusieurs autres disposent d'une clientèle active et opèrent des investissements en France. Les dirigeants de CISPE, notamment le Trésorier et le Président, possèdent des sociétés qui ont leurs sièges en France et sont basées à Paris. Il est important de noter que la CNIL a fortement contribué à l'élaboration du Code CISPE, en fournissant des analyses et recommandations sur ce Code pendant toute la durée du processus de rédaction, et a développé de ce fait une compréhension précieuse de l'industrie des infrastructures cloud et ses caractéristiques techniques. Cela la rend la mieux placée pour devenir l'Autorité de Contrôle compétente pour le Code CISPE.

L'élaboration du Code

Le Code CISPE a été préparé dans le cadre d'une initiative commune portée par les membres de CISPE, qui sont tous des CISPs au service de clients en Europe. CISPE a vocation à représenter les CISPs et elle se compose de représentants des CISPs de référence dans le secteur qui proposent des services dans de nombreux États Membres européens. CISPE compte parmi ses membres des PME ainsi que des grandes entreprises multinationales, dont chacun dispose d'une voix à l'Assemblée Générale. Une liste des membres de CISPE est disponible sur le site internet du CISPE à l'adresse suivante : https://cispe.cloud/

Dans le cadre du processus d'élaboration du Code CISPE, CISPE a créé la Task Force du Code de Conduite CISPE **(« CCTF »**, Code of Conduct Task Force) afin d'impliquer plusieurs acteurs dans l'élaboration du Code CISPE. La CCTF se compose de représentants des CISPs, de chercheurs universitaires, de représentants des clients, de Délégués à la Protection des Données et d'associations professionnelles. Les membres du CISPE ont également consulté plusieurs acteurs intéressés, notamment des clients, des experts en informatique cloud, la DG de la Justice de la Commission européenne, des représentants des Autorités de Contrôle européennes, le Groupe de Travail « Article 29 » et des organisations qui peuvent potentiellement devenir des organismes de contrôle en vertu du Code. Une synthèse des consultations des acteurs est présentée en Annexe E.

1 Structure du Code

Le présent Code est structuré comme suit :

- **Objet :** cette section décrit l'objet du Code au regard des règles instaurées par le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« **Règlement Général sur la Protection des Données** » ou « **RGPD** »).
- **Champ d'application :** cette section décrit le champ d'application du Code.
- **Exigences en matière de protection des données :** cette section décrit les droits et obligations substantiels des CISPs adhérents sur la base des principes fondamentaux du RGPD, comme les limitations de finalité, les droits des personnes concernées, les transferts, la sécurité, l'audit, la responsabilité, etc.
- **Exigences en matière de transparence :** cette section décrit comment les CISPs adhérents démontrent un niveau adéquat de sécurité des données à caractère personnel.
- **Adhésion :** cette section décrit les conditions applicables aux CISPs pour déclarer leur adhésion au Code.
- **Gouvernance :** cette section décrit comment le Code est géré, appliqué et révisé, y compris les rôles et obligations de ses organes de direction.

2 Objet

Ce Code vise à aider les clients à déterminer si le service d'infrastructure cloud qu'ils souhaitent utiliser est en adéquation avec les activités de traitement de données qu'ils envisagent d'effectuer. En fin de compte, l'objet de ce Code est d'aider les clients à choisir le service d'infrastructure cloud qui répond le mieux à leurs besoins spécifiques.

Une déclaration d'adhésion au Code par un CISP pour un service en particulier :

- Devrait instaurer une marque d'assurance et de confiance pour les clients que, pour ce service, le CISP se conforme à ses obligations en tant que sous-traitant en application des dispositions du RGPD; et
- Signifie que le CISP a consenti à être lié par les Exigences du Code pour ce service.

Les clients qui ont recours à un service d'infrastructure cloud sont encouragés à évaluer eux-mêmes leurs propres activités de traitement et leur conformité au regard des dispositions légales applicables, et notamment les législations en matière de protection des données comme le RGPD. Ce Code a vocation à aider les clients à réaliser ces évaluations, mais il ne doit pas s'y substituer.

Ce Code ne remplace pas un contrat signé entre le CISP et le client. Le CISP et son client sont libres de définir les modalités de prestation du service dans le Contrat de Services (défini à la Section 4.2) et de déterminer leurs responsabilités partagées. Avant de déclarer leur adhésion au Code, les CISPs doivent déterminer si le Contrat de Services qu'ils proposent aux nouveaux clients en rapport avec les services est contraire ou non aux Exigences du Code.

À l'heure actuelle, le Code ne constitue pas, en soi, un dispositif autorisant le transfert de données à caractère personnel en dehors de l'Espace économique européen (EEE). Lorsque des données à caractère personnel[1] sont transférées vers des pays non membres de l'EEE, il convient d'utiliser un mécanisme de transfert reconnu par le Chapitre V du RGPD.

Le Code ne doit pas être interprété comme un avis juridique. L'adhésion au Code ne constitue pas une garantie qu'un CISP ou un client se conforme aux dispositions du droit applicable, y compris au RGPD. Les CISPs et les clients sont invités à obtenir des conseils appropriés sur les dispositions légales applicables.

Le traitement effectué par les services d'infrastructure cloud est d'une nature très spécifique. Aussi, les CISPs et leurs clients bénéficient d'une vision plus détaillée des dispositions pertinentes du RGPD telles qu'elles s'appliquent dans ce contexte.

Le Code CISPE se concentre uniquement sur les caractéristiques spécifiques du traitement par les fournisseurs IaaS. Il tente d'apporter des éclaircissements sur la signification pratique du RGPD lorsque celui-ci est appliqué par des fournisseurs IaaS, et sur les mesures effectives que les CISPs envisagent d'adopter pour garantir leur conformité au RGPD. Ces éclaircissements permettent aux CISPs de saisir toute la mesure de leurs obligations au titre du RGPD, et de faciliter le respect des meilleures pratiques par les fournisseurs IaaS. Par ailleurs, la création d'un Organisme de Contrôle, chargé d'évaluer chaque année la conformité des CISPs, facilitera et contrôlera le respect par les CISPs des Exigences du Code et la transparence pour les clients. Les Exigences du Code énoncées dans le Code guident les Organismes de Contrôle dans leur évaluation et leur contrôle de la conformité des CISPs. Dans certains cas, il va au-delà des exigences du RGPD, notamment en ce qui concerne l'obligation des CISPs de laisser à leurs clients la possibilité de s'assurer que toutes leurs données sont traitées au sein de l'EEE.

Cela signifie que le Code peut appliquer plus spécifiquement le RGPD au traitement par les CISPs, et qu'il fournit une description des obligations applicables dans le cadre des services IaaS. Enfin, le Code permettra une meilleure transparence en ce qui concerne les responsabilités des CISPs et de leurs clients et il facilite la bonne application des obligations en matière de protection des données à ces types de services.

1 Il s'agit des données à caractère personnel qui sont traitées par une entité établie dans l'Union européenne ou en dehors de l'Union européenne, mais qui propose des biens ou des services à des résidents de l'UE ou qui contrôle le comportement de résidents de l'UE.

3 Champ d'application

Le Code comprend un ensemble d'exigences applicables aux CISPs en leur qualité de sous-traitant, notamment en ce qui concerne les mesures de sécurité. Ces exigences sont décrites à la Section 4 (Exigences en matière de Protection des Données) et à la Section 5 (Exigences en matière de Transparence). Ces exigences sont collectivement désignées, ci-après, les Exigences du Code.

Tout CISP peut déclarer son adhésion aux Exigences du Code pour un service d'infrastructure cloud si :

- le service concerné respecte les Exigences du Code ;
- au regard du service, le CISP se conforme à ses obligations de sous-traitant prévues par le RGPD; et
- le service offre au client la possibilité de choisir d'utiliser le service pour stocker et traiter ses données entièrement sur les territoires de l'EEE.

Un CISP peut décider de déclarer qu'une partie seulement (et non la totalité) de ses services d'infrastructure cloud respectent les Exigences du Code. Dans ce cas, il doit s'assurer que les clients potentiels sont informés, de manière explicite et non-équivoque, des services qui sont conformes aux Exigences du Code. Tout CISP qui déclare sa conformité aux dispositions du Code doit se conformer à l'ensemble des Exigences du Code pour chacun des services mentionnés dans sa déclaration.

Au regard de la législation européenne relative à la protection des données, il est essentiel d'identifier le responsable du traitement et les sous-traitants impliqués. Ces concepts sont expliqués à la Section 4 (Protection des Données) du présent Code.

Dans le cadre d'un service d'infrastructure cloud, le CISP agit en qualité de sous-traitant vis-à-vis du client (qui peut lui-même être un responsable du traitement ou un sous-traitant). Comme indiqué ci-dessous, le Code s'applique uniquement dans la mesure où le CISP agit en qualité de sous-traitant. Les Exigences du Code prévoient les principes que les CISPs sont tenus de respecter en tant que sous-traitants.

Les responsables du traitement et les sous-traitants ont des obligations légales à respecter en vertu du RGPD. Les obligations des responsables du traitement sont plus vastes que celles des sous-traitants ; les sous-traitants peuvent jouer un rôle de soutien dans l'exécution des obligations des responsables du traitement. Le Code s'emploie à prévoir les obligations des CISPs et à expliquer comment, en leur qualité de sous-traitant des données, ils peuvent aider leurs clients, qui sont eux-mêmes soit des responsables du traitement, soit des sous-traitants dans la chaîne logistique, à se conformer à leurs obligations.

En ce qui concerne les données à caractère personnel traitées au nom d'un client qui utilise un service d'infrastructure cloud **(Données Client),** le CISP n'est pas autorisé à (a) accéder à ces données ou à les utiliser sauf dans la mesure nécessaire pour fournir les services au client et assurer le maintien de ces services, ou (b) traiter ces données pour son propre compte, notamment à des fins de fouille de données (« data mining »), de profilage ou de prospection commerciale.

Le CISP peut agir en tant que responsable du traitement pour certaines données à caractère personnel utilisées par le CISP dans le but d'administrer le compte client. Il s'agit, par exemple, des informations relatives aux comptes (comme les noms d'utilisateur, les adresses électroniques et les données de facturation), que le client fournit au CISP au moment de la création ou lors de l'administration du compte client utilisé pour accéder au service proposé par le CISP.

Les dispositions du Code ne s'appliquent pas lorsque le CISP traite ces données en qualité de responsable du traitement.

Le Code a un champ d'application territorial transnational et il a vocation à s'appliquer dans tous les États membres de l'EEE. Les CISPs qui ne sont pas soumis aux dispositions du RGPD peuvent également décider, de leur plein gré, de se soumettre aux dispositions du Code. L'Annexe D contient une liste des Autorités de Contrôle compétentes dans tous les États membres de l'EEE.

Bien que le Code s'appuie principalement sur le RGPD, les CISPs reconnaissent également qu'ils seront fréquemment soumis aux exigences de sécurité et aux obligations de notification d'incidents imposées par la Directive (UE) 2016/1148 relative aux Réseaux et Systèmes d'information, telle qu'elle est transposée dans la législation des États Membres. Ces obligations viennent compléter et étoffer les exigences similaires prévues par le RGPD qui sont visées par le présent Code.

4 Exigences en matière de protection des données

En application de l'Article 4 du RGPD, (a) le « responsable du traitement » est la partie qui « *détermine les finalités et les moyens du traitement »,* et (b) le « sous-traitant » est la partie qui *« traite des données à caractère personnel pour le compte du responsable du traitement ».*

Les CISPs fournissent des infrastructures cloud en libre-service et à la demande. C'est le client qui décide si et comment utiliser cette infrastructure, et qui détermine si des données à caractère personnel sont chargées sur l'infrastructure cloud et, si tel est le cas, comment ces données sont « traitées ».

Si le client décide de stocker ou traiter d'une autre manière des données à caractère personnel en ayant recours aux services d'un CISP, et s'il définit les finalités du traitement et les moyens utilisés pour ce traitement, le CISP agira en tant que sous-traitant du client et le client sera le responsable du traitement.

Par exemple :

- Les services d'infrastructure cloud tels que les services de serveurs virtuels sont dépourvus de contenu et de données. En principe, ils offrent au client la possibilité de déployer sur un serveur virtuel ou sur une infrastructure cloud les applications créées par le client et les données destinées à être stockées uniquement par le CISP, sans aucune autre interaction de sa part.

- Un service de serveur dédié est un autre type de service d'infrastructure cloud, mais il s'agit d'un serveur entièrement dédié à un client. Le serveur est déployé et hébergé par le CISP qui, par exemple, remplacera les pièces défectueuses du matériel informatique, relancera le serveur et assurera la maintenance du réseau. Toutefois, les applications et les données sont déployées par le client.

Le CISP peut également agir en tant qu'autre sous-traitant. C'est le cas lorsque le client traite des données à caractère personnel, en qualité de sous-traitant, sur le service fourni par le CISP pour le compte et sous les instructions d'un tiers, en tant que responsable du traitement. En principe, ce cas de figure se présente lorsque le client du CISP fournit un service applicatif à son propre client final (ex. : SaaS). Dans ce scénario, le CISP est un autre sous-traitant, le client du CISP est un sous-traitant et le tiers est le responsable du traitement.

Comme il est indiqué à la Section 3 (Champ d'application), un CISP peut agir en tant que responsable du traitement dans le cadre de ses propres activités de traitement (ex. : pour certaines données à caractère personnel fournies par le client au CISP à des fins de gestion). Le Code ne s'applique pas lorsque le CISP traite ces données en qualité de responsable du traitement, il s'applique uniquement pour décrire et clarifier les engagements du CISP lorsque celui-ci agit en tant que sous-traitant.

Objet de la présente section du Code relatif aux Exigences en matière de Protection des Données

La présente Section 4 (Exigences en matière de Protection des Données) a pour objet de clarifier le rôle du CISP en tant que sous-traitant ou autre sous-traitant en vertu du RGPD dans le cadre de la prestation de services d'infrastructure cloud.

Le Code poursuit cet objectif de la manière suivante :

(a) en identifiant des exigences pour les sous-traitants au regard du RGPD (l'**Exigence du RGPD)** sur la base des obligations sous-jacentes établies par le RGPD ; et

(b) en appliquant l'Exigence du RGPD dans le contexte de services d'infrastructure cloud, en attribuant la responsabilité pour ces exigences entre le CISP et le client, et en définissant des obligations spécifiques pour le CISP en conformité avec les dispositions du Code (l'**Obligation du CISP);**

Au travers de cette approche, le Code fournit aux CISPs à la fois une interprétation et une application de l'Exigence du RGPD, ce qui permet au client d'avoir une vision plus claire de ce qu'il peut s'attendre à recevoir et d'exiger un niveau élevé de conformité de la part du CISP. En plus d'adhérer au Code, les CISPs et les clients doivent tenir compte de toutes les exigences imposées par les législations européennes et nationales applicables en matière de protection des données dans leur prestation et utilisation des services d'infrastructure cloud, respectivement.

L'un des objectifs principaux du Code consiste à répondre aux obligations clés des CISPs imposées par le RGPD. Le Code sera examiné et actualisé dans la mesure nécessaire pour refléter l'évolution de la législation européenne applicable en matière de protection des données conformément à la section 7 (Gouvernance) (y compris tout élément spécifique contraignant pouvant être imposé par les Autorités de Contrôle compétentes concernant le RGPD).

Note explicative concernant l'interprétation

Dans les Exigences du Code énoncées ci-après, toute référence à « raisonnable » s'entend, dans ce contexte, à ce qui est objectivement raisonnable au vu des circonstances compte tenu du contexte entre le CISP et le(s) client(s) concerné(s).

4.1 Licéité du traitement de données à caractère personnel

Exigence du RGPD :

Le **responsable du traitement** doit s'assurer que les données à caractère personnel sont « *traitées de manière licite* » (Art 5(1)(a) du RGPD). Le traitement est considéré comme licite uniquement dans certaines conditions. À moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis, le **sous-traitant** ne traite les données à caractère personnel « *que sur instruction documentée du responsable du traitement* » (Art 28(3)(a) du RGPD et Art 29 du RGPD).

Obligation du CISP :

Le CISP traite uniquement les données à caractère personnel sur instruction du client. Le Contrat de Services et l'utilisation par le client des caractéristiques et fonctionnalités qui sont mises à sa disposition par le CISP dans le cadre du service constituent les instructions complètes et définitives du client au CISP en rapport avec le traitement de données à caractère personnel. Le Contrat de Services décrit les paramètres du service et du traitement que le CISP est ainsi en droit d'effectuer : les caractéristiques et fonctionnalités et tous les services de support disponibles permettent au client de fournir des instructions complémentaires au CISP. Par exemple, le client peut utiliser les outils de configuration du service pour déterminer comment certains aspects sont configurés. Ces nouvelles instructions doivent s'inscrire dans les paramètres généraux de la Description du Service. Si le CISP est tenu en vertu du droit de l'Union ou le droit d'un État membre à traiter des données à caractère personnel, le sous-traitant devra se conformer à cette obligation. Dans ce cas, le RGPD dispose que le CISP doit informer le client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

Explication :

Les CISPs n'exercent aucun contrôle sur le contenu que le client décide de charger sur le service (que ce contenu contienne des données à caractère personnel ou non). Les CISPs ne jouent aucun rôle dans la prise de décisions qui consistent à déterminer si le client utilise ou non un service d'infrastructure cloud pour traiter des données à caractère personnel et pour quelle finalité. En conséquence, les CISPs ne peuvent pas affirmer avec certitude s'il existe ou non une base juridique pour le traitement. À ce titre, leur responsabilité consiste à (a) se conformer aux instructions du client telles qu'elles sont décrites dans le Contrat de Services et (b) fournir des informations sur le service conformément à la Section 5 (Exigences en matière de Transparence) du Code.

4.2 Conditions générales contractuelles des services du CISP Exigence du RGPD :

> « *Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement* » (Art 28(3) du RGPD).

Obligation du CISP :

Un contrat entre le CISP et le Client doit définir les caractéristiques du service et les modalités de sa prestation ainsi que les droits et obligations respectifs du CISP et du client (le **Contrat de Services**) tels qu'indiqués aux paragraphes (a) et (b) ci-dessous. Le CISP doit s'assurer d'être lié juridiquement par le Contrat de Services vis-à-vis du client. Le CISP n'est pas autorisé à traiter les Données Client sans avoir au préalable établi un Contrat de Services.

Explication :

Les CISPs fournissent des infrastructures cloud. Les clients sont libres de choisir comment ils souhaitent utiliser cette infrastructure et ils peuvent également décider à tout moment de modifier la manière dont ils utilisent cette infrastructure cloud et la finalité de cette utilisation. Le Contrat de Services doit fournir des descriptions appropriées, sans inhiber la flexibilité accordée au client pour déterminer la façon dont il souhaite utiliser l'infrastructure.

(a) Description du traitement

Pour rendre les caractéristiques des services d'infrastructure cloud plus accessibles et pour éviter de modifier le Contrat de Services ou de conclure un nouveau Contrat de Services à chaque fois que le client ou un utilisateur final du client décide de modifier sa façon d'utiliser le service, la description du traitement dans le Contrat de Services doit être libellée de façon à refléter les caractéristiques des services d'infrastructure cloud utilisées par le client.

Pour plus de flexibilité, les Contrats de Service peuvent fournir une description générique du traitement au moyen des services d'infrastructure cloud, par exemple, « le calcul, le stockage et la diffusion de contenu sur le réseau du CISP » et s'appuyer sur la documentation, notamment les descriptions des services ou les guides de l'utilisateur pour plus de détails. Les activités de traitement exécutées par le CISP dans le cadre de sa prestation du service doivent clairement apparaître dans cette documentation, par exemple, au travers d'une description détaillée du service.

(b) Contenu du Contrat de Services

Le Contrat de Services doit faire l'objet d'un écrit (y compris sous forme électronique) et avoir force exécutoire entre le CISP et le client. Le Contrat de Services doit stipuler les obligations du sous-traitant telles qu'elles sont énoncées à l'Article 28(3) du RGPD et doit contenir, au minimum, des clauses qui satisfont les obligations exprimées comme s'appliquant au CISP, notamment les :

- Exigences du CISP en vertu de la Section 4.1 (Licéité du traitement des Données à Caractère Personnel) (Art 28(3)(a) du RGPD) ;
- Exigences du CISP en vertu de la Section (Sécurité) (Art 28(3)(c) du RGPD) ;
- Exigences du CISP en vertu de la Section 4.4 (Transfert des données à caractère

personnel vers des pays tiers) ;

- Exigences du CISP en vertu de la Section 4.5 (Sous-traitance) (Art 28(2) et (4) du RGPD) ;
- Exigences du CISP en vertu de la Section 4.6 (Démonstration de la conformité) (Art 28(3)(h) du RGPD) ;
- Exigences du CISP en vertu de la Section 4.7 (Droits des personnes concernées) (Art 28(3)(e) du RGPD) ;
- Exigences du CISP en vertu de la Section 4.8 (Personnel du CISP) (Art 28(3)(b) du RGPD) ;
- Exigences du CISP en vertu de la Section 4.9 (Violation des données) (Art 28(3)(a) et (f) du RGPD) ;
- Exigences du CISP en vertu de la Section 4.10 (Suppression ou renvoi des données à caractère personnel) (Art 28(3)(g) du RGPD) ; et
- Exigences du CISP en vertu de la Section 5 (Transparence).

(c) Forme du Contrat de Services

Le Contrat de Services doit faire l'objet d'un écrit, y compris sous forme électronique, mais il peut revêtir plusieurs formes, y compris :

- un contrat unique ;
- un ensemble de documents tel un contrat-type de services et les annexes s'y rattachant (contrats de sous-traitance, contrats de niveau de service, conditions d'utilisation des services, politiques de sécurité, etc.) ; ou
- des conditions générales en ligne.

4.3 Sécurité

Exigence du RGPD :

> *« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le* ***responsable du traitement et le sous-traitant*** *mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* » (Art 32(1) du RGPD).

Obligation du CISP :

(a) Mesures de sécurité

Le CISP doit mettre en œuvre et maintenir des mesures techniques et organisationnelles appropriées pour les centres de données, serveurs, équipement réseau du CISP et héberger les systèmes logiciels qu'il contrôle et qui sont utilisés pour fournir le service du CISP (le **Réseau du CISP).**

L'Annexe A du Code (Responsabilités en matière de Sécurité) définit les standards minimums de sécurité et contient les responsabilités en matière de sécurité que le CISP doit respecter pour qu'un service adhère au Code. Les mesures techniques et organisationnelles mises en place par le CISP doivent : (a) être conçues pour aider les clients à protéger leurs données à caractère personnel contre le traitement non autorisé et

la perte, l'accès ou la communication, de manière accidentelle ou illicite, et (b) viser chacune des obligations du CISP en matière de sécurité décrites en Annexe A (Responsabilités en matière de Sécurité).

Les CISPs doivent s'employer activement à s'assurer ce que les mesures de sécurité qu'ils mettent en œuvre n'empêchent pas les clients de déployer leurs meilleures pratiques en matière de sécurité. Par exemple, les clients doivent pouvoir effectuer le chiffrement de leurs données à caractère personnel en toute sécurité.

Explication :

Les services d'infrastructure cloud sont généralement agnostiques quant au contenu. Ils offrent les mêmes mesures techniques et organisationnelles et le même niveau de sécurité à tous les clients, que ces derniers traitent ou non des données à caractère personnel, et sans tenir compte de la nature, de la portée, du contexte et de la finalité du traitement que le client qui utilise le service envisage d'effectuer. Le CISP peut proposer des options types pour permettre au client de sélectionner d'autres mesures à appliquer. Par exemple, les CISPs fourniront les informations disponibles sur toutes les améliorations apportées aux fonctionnalités afin que le client, lorsqu'il traite des catégories particulières de données, puisse sélectionner d'autres options de sécurité pour satisfaire les exigences applicables au traitement de ces données. Il appartient au client d'adopter, après en avoir évalué les risques, des mesures techniques et organisationnelles pour sécuriser les données, en sélectionnant les options appropriées qui sont mises à sa disposition par le CISP. Le CISP, quant à lui, est responsable de la mise en œuvre des mesures techniques et organisationnelles applicables pour chaque option standardisée.

La sécurité et la conformité, y compris la configuration technique de l'environnement, est partagée entre le CISP et le client. Ce partage peut libérer le client de la charge opérationnelle qui pèse sur lui car le CISP opère, gère et contrôle les composants du système d'exploitation *hôte (host)* et de la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles le service fonctionne. Le client assume la responsabilité et la gestion du système d'exploitation *invité (guest)* (y compris les mises à jour et les patchs de sécurité), d'autres logiciels applicatifs, ainsi que la configuration des mesures de sécurité du CISP conformément au Contrat de Services. L'Annexe A (Responsabilités en matière de Sécurité) définit les responsabilités du CISP et du client en matière de sécurité dans le cadre d'infrastructure cloud. Les contrôles spécifiques des mesures de sécurité et de protection des données mises en place par le CISP et le client seront décrits dans chaque Contrat de Services.

Il est essentiel d'opérer une distinction entre :

- la sécurité de l'infrastructure fournie par le CISP sur laquelle les données sont traitées ; et
- la sécurité des données qui sont traitées.

Sécurité de l'infrastructure

Le CISP assume la responsabilité de la protection de l'infrastructure qui exécute tous les services proposés dans le cadre du service d'infrastructure cloud. Cette infrastructure se compose du matériel informatique, du Logiciel d'Exploitation Hôte (si celui-ci s'applique au service proposé), de la mise en réseau et des installations qui permettent d'exécuter les services d'infrastructure cloud. Par exemple, le CISP assure le déploiement, le fonctionnement et la sécurité de tout équipement physique

utilisé pour fournir le service d'infrastructure cloud. L'Annexe A (Responsabilités en matière de Sécurité) fournit plus de détails sur l'étendue de ces responsabilités.

Le CISP doit installer un mécanisme permettant de filtrer les flux de données, comme un pare-feu, autour du périmètre de l'infrastructure cloud dans son ensemble et/ou un pare-feu pour isoler l'instance de service qui est déployée.

S'il existe des mécanismes de filtre (tel qu'un pare-feu) pour protéger l'infrastructure du CISP, il appartient au CISP de les configurer.

La mise à disposition ou non d'un pare-feu pour chaque instance de service dépendra du service. Certains services ne peuvent pas disposer de pare-feux pour une instance spécifique. Dans ce cas, le client devra appliquer son propre pare-feu pour l'instance spécifique.

Sécurité des données traitées

Dans le cadre de l'utilisation d'un service d'infrastructure cloud par un client, certains aspects clés de la sécurité relèvent de la responsabilité du client (et non pas de la responsabilité du CISP).

Dans le contexte de services cloud pris dans leur ensemble, la responsabilité du client varie en fonction des services qu'il choisit. Le choix du/des services par le client détermine les travaux de configuration que le client doit accomplir au regard de ses responsabilités en matière de sécurité.

Dans une IaaS, le client est tenu d'exécuter toutes les tâches de configuration et de gestion de la sécurité, par exemple, si un client déploie un service d'infrastructure cloud, il doit assurer la gestion du système d'exploitation invité (y compris les mises à jour et patchs de sécurité), de tout logiciel applicatif ou tous équipements qu'il a installés pour ce service, ainsi que la configuration du pare-feu fourni par le CISP pour chaque instance. Par ailleurs, le client est responsable de la sécurité des données en transit et de ses identifiants de connexion, et de la gestion des autorisations qu'il accorde aux membres de son personnel qui utilisent le service. L'Annexe A (Responsabilités en matière de Sécurité) fournit plus de détails sur l'étendue de ces responsabilités. Les CISPs doivent garantir la transparence entre les CISPs et les clients en ce qui concerne leurs obligations en matière de sécurité, par exemple, en fournissant des informations sur les paramètres par défaut qu'un client peut être tenu de configurer. Comme indiqué à la section 5.1 du Code, le Contrat de Services doit prévoir un partage des responsabilités entre le CISP et le Client pour la sécurité du service.

Les CISPs ont la responsabilité de mettre à la disposition des clients les informations relatives à la sécurité des données en rapport avec les services. Les CISPs doivent également désigner un point de contact au sein du CISP chargé de répondre aux questions des clients concernant la protection des données ou sécurité du service (cf. Section 5 (Exigences en matière de Transparence). Cela doit permettre aux clients d'examiner : (a) les responsabilités en matière de sécurité du CISP décrites en Annexe A, (b) les informations communiquées par le CISP concernant la sécurité des données en rapport avec les services (cf. Section 5 (Exigences en matière de Transparence) ci-dessous), (c) la configuration du service d'infrastructure cloud choisie par le client et l'utilisation des fonctionnalités et contrôles mis à disposition pour ce service, et (d) les mesures de sécurité que le client mettra en place en ce qui concerne les aspects de la sécurité relevant de sa responsabilité, et obtenir l'assurance que ces mesures, prises dans leur ensemble, fournissent un niveau approprié de sécurité pour le traitement que le client effectuera en utilisant ce service. Cette assurance s'obtient en déterminant la nature, la portée, le contexte et les finalités du traitement envisagé par le client, que seul le client connaitra avec

suffisamment de détails.

(b) <u>Programme sur la sécurité de l'information</u>

Le CISP doit établir un programme sur la sécurité de l'information dans le but de : (a) identifier les risques raisonnablement prévisibles pour la sécurité du Réseau du CISP, et (b) minimiser les risques de sécurité, notamment en procédant régulièrement à des analyses de risque et des tests.

Le CISP doit désigner un ou plusieurs membres de son personnel pour coordonner et être responsable du programme sur la sécurité de l'information.

(c) <u>Évaluation permanente</u>

Le CISP doit procéder à des examens réguliers de la sécurité du Réseau du CISP et de l'adéquation de son programme sur la sécurité de l'information. Le CISP peut décider de revoir son programme sur la sécurité de l'information au regard d'un ou plusieurs standards de sécurité du secteur (par exemple la série de standards ISO 27000) ou de l'état de l'art. Le CISP doit évaluer en permanence la sécurité du Réseau du CISP afin de déterminer si des mesures de sécurité supplémentaires ou différentes sont nécessaires pour faire face aux nouveaux risques de sécurité ou en fonction des résultats qu'il a obtenus à l'issue de ses propres examens périodiques.

Le CISP peut être amené à modifier de temps à autres les normes de sécurité sur la base desquelles son programme sur la sécurité de l'information peut être évalué, mais il doit au moins continuer, pendant toute la durée du Contrat de Services, d'assurer le même niveau de sécurité que celui qui est décrit dans ses normes de sécurité à la date de prise d'effet du Contrat de Services.

Le CISP doit notifier au client tout changement qu'il considère objectivement comme ayant une incidence sur la portée de son programme sur la sécurité de l'information ou sur les mesures techniques et organisationnelles de sécurité relevant de sa responsabilité à la date de prise d'effet du Contrat de Services. Cette notification doit avoir lieu avant la modification des normes de sécurité du CISP, sauf si le CISP peut démontrer que cette modification doit être effectuée de toute urgence pour résoudre une vulnérabilité de sécurité. Le client aura la possibilité de vérifier l'incidence de ces modifications conformément à la Section 4.6 du Code.

4.4 Transfert des données à caractère personnel vers des pays tiers

<u>Exigence du RGPD :</u>

« *Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans* » le Chapitre V du RGPD *« sont respectées* ***par le responsable du traitement et le sous-traitant*** [...] » (Art 44 du RGPD).

« Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre. » (Art. 48 du RGPD)

<u>Obligation du CISP :</u>

(a) Localisation

Le service du CISP offre au client la possibilité de choisir d'utiliser le service pour stocker et traiter ses données exclusivement sur les territoires de l'EEE, évitant ainsi l'application des dispositions du RGPD régissant le transfert de données à caractère personnel vers des pays tiers.

(b) Information

Le CISP doit fournir au client des informations sur la région et le pays dans lequel ses données sont stockées et traitées par ou au nom du CISP (que ces données soient ou non stockées et traitées exclusivement sur les territoires de l'EEE, ou dans un pays tiers). Si le CISP sous-traite une partie du traitement auprès d'autres sous-traitants, il doit également communiquer les informations mentionnées à la Section 4.5 ci-dessous.

Pour des raisons de sécurité, seule une localisation générale (une ville ou partie d'une ville ou d'une région) doit être communiquée. Cette description générale doit au moins permettre au client qui utilise le service d'identifier l'État membre de l'UE dont le client relève pour effectuer ses activités de traitement.

Le CISP doit communiquer à l'Autorité de Contrôle compétente l'adresse exacte du lieu des installations concernées, si cette information est requise par l'Autorité de Contrôle compétente pour satisfaire ses obligations au regard de la législation européenne en matière de protection des données. Compte tenu de la nature sensible de cette information et des risques pour la sécurité que cela pourrait engendrer si elle était rendue publique, le CISP peut demander à l'Autorité de Contrôle compétente de tenir compte du caractère sensible de cette information chaque fois qu'elle sera amenée à la communiquer.

Pour les services qui peuvent être exécutés indifféremment en plusieurs endroits différents du Réseau du CISP, les CISPs doivent rendre ces informations facilement accessibles au client (par exemple sur le site internet du CISP) et permettre au client de choisir la(s) localisation(s) au sein du Réseau du CISP dans laquelle/lesquels leurs données seront traitées. Comme indiqué ci-dessus, les CISPs doivent fournir à leurs clients la possibilité de choisir d'utiliser le service exclusivement sur les territoires de l'EEE. Si un client choisit de ne pas utiliser le service exclusivement sur les territoires de l'EEE, la décision du CISP d'autoriser ou non les clients à sélectionner les pays (hors EEE) dans lesquels leurs données seront stockées et traitées dépendra du service proposé par le CISP.

(c) Niveau de protection

Tout transfert de données à caractère personnel vers un pays situé en dehors de l'EEE pour la fourniture des services du CISP, y compris l'accès à partir d'un pays tiers situé en dehors de l'EEE, ne peut se faire que sur instruction du client au CISP.

Le CISP doit aider les clients, en tant qu'exportateurs, à se conformer à leurs obligations du chapitre V du RGPD pour le transfert licite de données à caractère personnel vers le pays concerné, y compris les transferts en vertu d'une décision d'adéquation alors en vigueur (par exemple, actuellement, vers la Suisse, Israël et autres) (Art 45 du RGPD) ou soumis à des garanties appropriées (telles que, actuellement, les règles d'entreprise contraignantes ou les clauses contractuelles types de protection des données adoptées par la Commission (Art 46 du RGPD)), si :

(i) le client transfère des données depuis l'EEE pour les stocker en utilisant le service du CISP, y compris lorsque les données sont transférées afin de fournir des services de « sauvegarde » aux centres de données de l'EEE en cas d'évènement de force majeure ou de continuité du CISP, dans tout pays situé en dehors de l'EEE qui n'est pas reconnu par la Commission européenne comme offrant un niveau de protection adéquat des données à caractère personnel ; ou

(ii) le client a choisi d'autoriser le CISP, sur ses instructions, à accéder aux données stockées en utilisant le service du CISP au sein de l'EEE à partir du pays mentionné au point (i) ci-dessus.

Le Contrat de Service entre le CISP et le client doit préciser les circonstances dans lesquelles il peut y avoir un transfert de données en dehors de l'EEE sur instruction du client (y compris la fourniture d'instructions via les outils de configuration du CISP et les API pour les services du CISP) ainsi que la délimitation des responsabilités entre le client (en tant qu'exportateur) et le CISP (en tant qu'importateur) concernant ce transfert.

En outre, le CISP doit fournir au client les informations appropriées, notamment sur le lieu du traitement concerné, afin de permettre au client de vérifier au cas par cas, avant tout transfert, si la législation ou la pratique du pays tiers concerné assure le niveau de protection des données requis dans l'EEE, de manière à déterminer si les garanties fournies par les garanties appropriées choisies peuvent être en pratique respectées.

Si tel n'est pas le cas, la responsabilité d'identifier et de mettre en œuvre les mesures supplémentaires en plus des garanties appropriées concernées pour assurer aux données transférées un niveau de protection essentiellement équivalent à celui prévu dans l'EEE repose sur le client, si nécessaire avec l'aide du CISP (en tant qu'importateur de données). Le Comité Européen de la Protection des Données a publié une recommandation [insérer le lien] sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE qui peut aider le CISP dans l'évaluation du pays tiers et dans l'identification des mesures supplémentaires appropriées.

Aucun transfert de données à caractère personnel vers un pays hors de l'EEE ne sera initié par le CISP dans le cadre de la fourniture des services, si le CISP n'a pas reçu les instructions du client pour le faire.

Le CISP vérifie au cas par cas, avant tout transfert ou toute divulgation de données à caractère personnel en réponse à un jugement d'une juridiction ou à une décision d'une autorité administrative d'un pays tiers, que ce jugement ou cette décision peut être reconnu ou exécuté sur la base d'un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, afin de garantir la légalité de ce transfert ou de cette divulgation. Si tel n'est pas le cas, et sans préjudice d'autres motifs de transfert en vertu du chapitre V du RGPD, le CISP doit définir et mettre en œuvre des mesures visant à garantir que tout transfert ou divulgation non autorisé par le droit de l'Union soit refusé au pays tiers demandeur.

Explication :

Le RGPD limite le transfert de données à caractère personnel vers des pays situés en dehors de l'EEE ou des organisations internationales sans garanties appropriées.

Dans le cadre des services d'infrastructure cloud, les transferts de données à caractère personnel en dehors de l'UE peuvent survenir, par exemple, lorsque :

- le client a consenti à ce que les données soient stockées en dehors de l'UE et le CISP utilise des centres de données situés en dehors de l'EEE pour fournir les services ; ou
- le CISP possède des centres de données en dehors de l'EEE et les données sont transférées vers ces sites dans le but de fournir des services de « sauvegarde » aux centres de données de l'EEE en cas de force majeure ou

d'évènement de continuité.

Pour se conformer au RGPD, les transferts limités de données à caractère personnel doivent être fondés sur une « décision d'adéquation » ou couverts par des garanties appropriées.

Décisions d'adéquation : La Commission européenne a constaté que le cadre juridique en place dans un pays, un territoire, un secteur ou une organisation internationale spécifique assure un niveau de protection « adéquat » des droits et libertés des personnes au regard de leurs données à caractère personnel. Si un transfert est fondé sur une décision d'adéquation, le transfert peut avoir lieu. Une liste actualisée des pays qui assurent un niveau de protection adéquat est publiée sur le site internet de la protection des données de la Commission européenne.

Garanties : En l'absence de décision d'adéquation pour le pays, le territoire ou le secteur concerné par le transfert limité, les transferts doivent faire l'objet de garanties appropriées. Les garanties reconnues par le RGPD incluent :

Garantie	Description
1. Un instrument juridiquement contraignant et exécutoire entre les autorités et les organismes publics	Une autorité ou un organe publique/public peut transférer des données à un(e) autre autorité ou organe publique/public, si un contrat signé ou un autre instrument juridique qui est juridiquement contraignant et exécutoire a été établi et contient des droits opposables et des voies de droit effectives pour les personnes dont les données à caractère personnel ont été transférées. Cette garantie n'est pas applicable si la partie qui transfère ou qui reçoit est un organisme ou une personne physique privé(e). Il est donc peu probable que cette garantie soit appropriée pour les CISPs.
2. Règles d'entreprise contraignantes	Les Règles d'Entreprise Contraignantes sont des codes de conduite internes établis au sein d'un groupe d'entreprises multinational. Les Règles d'Entreprise Contraignantes doivent être soumises à l'approbation d'une Autorité de Contrôle dans un pays de l'EEE où un CISP est implanté. Un CISP peut effectuer un transfert si la partie qui transfère les données et la partie qui les reçoit ont toutes deux signé le document des Règles d'Entreprise Contraignantes concernant les transferts de données à caractère personnel d' entités du groupe situées dans un territoire de l'EEE vers des entités du groupe situées en dehors de l'EEE.

3. Clauses types de protection des données	Les clauses contractuelles types ou « clauses types » sont des clauses de protection des données adoptées par la Commission européenne en application de la Directive 95/46/CE. Il existe deux ensembles de clauses contractuelles types pour les transferts entre un responsable du traitement et un responsable du traitement, et deux ensembles pour les transferts entre un responsable du traitement et un sous-traitant. Ces clauses imposent des obligations contractuelles à l'exportateur des données et à l'importateur des données, et confèrent des droits aux personnes dont les données à caractère personnel sont transférées. Un CISP peut effectuer un transfert limité si la partie qui transfère les données et la partie qui les reçoit ont toutes deux adhéré à ces clauses contractuelles types. Les clauses types de protection des données constituent la garantie la plus fréquemment utilisée par les CISPs et probablement la plus appropriée.
4. Clauses types de protection des données Adoptées par une Autorité de Contrôle et approuvées par la Commission	En principe, un CISP peut effectuer un transfert s'il signe un contrat contenant des clauses types de protection des données adoptées par l'Autorité de Contrôle compétente et approuvées par la Commission européenne. À ce jour, aucune Autorité de Contrôle n'a adopté de clauses types de protection des données.
5. Un code de conduite approuvé	En principe, un transfert est possible si le bénéficiaire a adhéré à un code de conduite qui a été approuvé par une Autorité de Contrôle. Ce code de conduite doit contenir des garanties appropriées pour protéger les droits des personnes dont les données à caractère personnel sont transférées, et qui peuvent être directement appliquées. À ce jour, aucun code de conduite approuvé n'est utilisé comme outil de transfert. Pour lever toute ambiguïté, à l'heure actuelle, le Code CISPE n'a pas vocation à servir de garantie pour les transferts transfrontaliers de données à caractère personnel.
6. Un mécanisme de certification approuvé	En principe, un transfert est possible si le bénéficiaire possède une certification, en vertu d'un mécanisme approuvé par une Autorité de Contrôle. Ce mécanisme de certification doit contenir des garanties appropriées pour protéger les droits des personnes dont les données à caractère personnel sont transférées, et qui peuvent être directement appliquées. À ce jour, aucun mécanisme de certification approuvé n'est utilisé.

Dans un arrêt du 16 juillet 2020, Data Protection Commissioner contre Facebook Ireland LTD, et Maximillian Schrems, C- 311/18, la Cour de justice de l'Union européenne a examiné la validité des clauses contractuelles types de la Commission européenne (décision 2010/87/CE) et les a jugées valides. En particulier, la Cour a déclaré que les clauses contractuelles types prévoient des mécanismes efficaces qui, en pratique, garantissent que le transfert de données à caractère personnel vers un

pays tiers est suspendu ou interdit lorsque le destinataire du transfert ne respecte pas ces clauses ou n'est pas en mesure de les respecter. Néanmoins, la Cour a précisé qu'en raison de leur nature contractuelle, les clauses contractuelles types ne peuvent pas lier les autorités publiques de pays tiers, puisqu'elles ne sont pas parties au contrat. En conséquence, les exportateurs de données, le cas échéant en collaboration avec l'importateur de données, doivent vérifier, au cas par cas et en tenant compte des circonstances du transfert, si le droit ou la pratique du pays tiers de destination empêche de respecter les engagements des clauses contractuelles types et, le cas échéant, compléter ceux-ci par des mesures supplémentaires afin d'assurer aux données transférées un niveau de protection essentiellement équivalent à celui de l'EEE. Si l'exportateur de données n'est pas en mesure de prendre les mesures supplémentaires appropriées pour garantir un niveau de protection essentiellement équivalent au droit de l'EEE, l'exportateur de données ou, à défaut, l'autorité de contrôle compétente, sont tenus de suspendre ou de mettre fin au transfert de données à caractère personnel vers le pays tiers concerné. La position établie par la Cour s'applique à toutes les garanties appropriées de l'article 46 du RGPD.

Transferts ou divulgations non autorisés par le droit de l'Union : Conformément à l'article 48 du RGPD, la demande d'un pays tiers de transférer ou de divulguer des données à caractère personnel ne rend pas, en tant que tel, un transfert ou une divulgation licite au regard du RGPD. Une demande émanant d'une juridiction ou d'une autorité d'un pays tiers ne constitue pas en soi un motif légal pour un tel transfert ou une telle divulgation. Un jugement d'une juridiction et toute décision d'une autorité administrative d'un pays tiers demandant à un responsable du traitement ou à un sous-traitant de transférer ou de divulguer des données à caractère personnel ne peuvent être reconnus ou exécutés que s'ils sont fondés sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du chapitre V du RGPD.

En l'absence d'un tel cadre fourni par un accord international ou d'une autre base juridique prévu par le RGPD, ainsi que d'un motif de transfert en vertu du chapitre V du RGPD, les prestataires de services soumis au droit de l'UE ne peuvent légalement fonder la divulgation et le transfert de données à caractère personnel sur de telles demandes.

4.5 Sous-traitance

<u>Exigence du RGPD</u> :

« Le sous-traitant ne recrute pas un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du responsable du traitement. Dans le cas d'une autorisation écrite générale, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements ». (Art 28(2) du RGPD).

« Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes

obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant […] sont imposées […] Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations ». (Art 28(4) du RGPD).

Obligation du CISP :

(a) Consentement

Le CISP doit obtenir l'autorisation du client avant d'autoriser un autre sous-traitant à traiter des Données Client. Cette autorisation peut être soit :

Spécifique : dans ce cas, le CISP doit informer le client par écrit, y compris de manière électronique, des sous-traitants spécifiques qu'il envisage de recruter. Le CISP pourra recruter le sous-traitant qu'il a sélectionné pour traiter des Données Client uniquement si le responsable du traitement y consent ; ou

Générale : dans ce cas, le consentement du client peut être donné de manière générale dans le cadre du Contrat de Services. En particulier, le Contrat de Services doit définir les situations et les conditions dans lesquelles le CISP peut recruter d'autres sous-traitants pour exécuter des activités de traitement spécifiques au nom du client sans qu'il soit nécessaire d'obtenir l'autorisation de ce dernier.

Dans les deux cas, le CISP doit informer le client par écrit (ou par voie électronique) des changements prévus concernant ses autres sous-traitants, dans un délai raisonnable avant le changement envisagé pour permettre au client d'examiner ce changement et de s'opposer au sous-traitant. Si le client émet des objections concernant un autre sous-traitant, le client peut, à son gré, résilier le Contrat de Services avec effet immédiat au moyen d'un préavis écrit ou, en cas d'accord du client et du CISP, mettre immédiatement fin au service ou à la partie du service qui est fournie par l'autre sous-traitant recruté par le CISP.

(b) Information

Le CISP doit dresser une liste à jour des autres sous-traitants qui traitent des Données Client. Cette liste doit indiquer la localisation de l'autre sous-traitant et elle doit être facilement accessible pour le client au moment de l'acceptation du Contrat de Services et pendant toute sa durée de validité. Cette liste actualisée doit être mise à la disposition du client au moyen d'un lien URL, ou sinon par écrit à la demande du client. Seule une localisation générale (un pays ou une zone régionale spécifique) doit être communiquée. Cette description générale doit au moins permettre au client qui utilise le service d'identifier l'État membre de l'UE dont le client relève pour effectuer ses activités de traitement.

Avant d'autoriser le nouveau sous-traitant à accéder aux Données Client :

(i) si le CISP obtient l'autorisation générale du client pour recruter d'autres sous-traitants, il doit communiquer au client : l'identité et la localisation générale (un pays ou une zone régionale spécifique) de ce nouveau sous-traitant ; le droit pour le client de s'opposer à ce nouveau sous-traitant (comme il est indiqué ci-dessus au point (a)) ; et le délai dont le client dispose pour exercer son droit d'opposition. Ce délai doit donner au client un délai raisonnable pour examiner le changement.

(ii) si le CISP obtient une autorisation spécifique pour recruter d'autres sous-traitants, il doit communiquer au client l'identité et la localisation générale (un pays ou une zone régionale spécifique) de ce nouveau sous-traitant et obtenir l'autorisation spécifique du client avant de recruter ce sous-traitant.

Bien que la localisation du traitement des données puisse varier en fonction du service choisi par le client et de la manière dont le client configure ce service, le client peut demander au CISP de lui communiquer des informations pertinentes sur les autres sous-traitants impliqués et sur la façon dont ils traitent les Données Client (y compris la localisation).

(c) Modalités de sous-traitance

Le CISP doit imposer à son sous-traitant des obligations contractuelles de protection des données équivalentes à celles mentionnées dans le Contrat de Services entre le CISP et le client.

Le CISP doit définir des modalités de fonctionnement concernant son autre sous-traitant afin de fournir un niveau identique ou supérieur de protection que le niveau de protection des données défini dans le Contrat de Services. Le CISP doit pouvoir démontrer au client au moyen de preuves documentaires appropriées qu'il a pris de telles mesures.

Le CISP doit limiter le traitement des Données Client par son autre sous-traitant dans la mesure strictement nécessaire pour fournir ou maintenir les services.

Le CISP demeure pleinement responsable devant le client du respect de ses obligations de protection des données et de l'exécution par l'autre sous-traitant de ces obligations de protection des données qui lui incombent en vertu du Contrat de Services.

Nonobstant les termes des paragraphes (a) – (c) ci-dessus, les CISPs sont libres de recourir à des sous-traitants ou des fournisseurs qui ne traitent pas des Données Client (comme les fournisseurs d'énergie, les fournisseurs d'équipement, de transport, les prestataires de services techniques, les Opérateurs IP, les transitaires, les vendeurs de matériel informatique, etc.) pour exécuter les obligations du CISP en vertu du Contrat de Services sans avoir à en informer ou à obtenir l'autorisation du client, **étant précisé que** les mesures de sécurité applicables mentionnées à la Section 4.3 et en Annexe A (Responsabilités en matière de Sécurité) doivent être mises en place par le CISP pour s'assurer que ces sous-traitants, fournisseurs ou autres prestataires tiers ne puissent pas accéder aux Données Client ou traiter ces données.

4.6 Démonstration du la conformité

Exigence du RGPD :

> *« Le sous-traitant [...] met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits » (Art 28(3)(h) du RGPD).*

Obligation du CISP :

Pour permettre au client d'exercer ses droits en vertu de l'Article 28(3)(h) du RGPD, le CISP doit : (i) communiquer au client les informations et la documentation appropriées telles qu'elles sont décrites à la Section 4.6(a) et (ii) soumettre ses installations de traitement des données à des audits réalisés par un tiers indépendant comme indiqué à la Section 4.6(b).

(a) Information

Les CISPs doivent respecter les Exigences en matière de Transparence énoncées à la Section 5 et doivent communiquer les informations nécessaires concernant les contrôles de sécurité mis en place pour les services proposés aux clients afin que les clients

comprennent ces contrôles de sécurité et puissent raisonnablement vérifier que le CISP respecte les obligations de sécurité définies dans le Contrat de Services.

Si ces informations ne sont pas confidentielles ou sensibles, il doit les communiquer aux clients au moyen d'un processus simple (ex. : sur le site internet du CISP). Si ces informations sont confidentielles, le CISP doit les mettre à la disposition des clients sur demande, mais en ayant au préalable demandé au client de signer un accord de confidentialité. Cet accord de confidentialité permettra au CISP de s'assurer que l'accès aux informations confidentielles est limité au client et que le client ne peut pas divulguer ces informations sans l'accord préalable écrit du CISP. L'accord de confidentialité ne doit pas empêcher le client de communiquer avec son Autorité de Contrôle lorsque cette communication est obligatoire. Nonobstant l'obligation de communiquer les informations concernant la sécurité en application de la Section 5, le CISP peut, à son entière discrétion, décider de ne pas divulguer certaines informations hautement sensibles concernant la sécurité (ex. : des informations qui, si elles sont disponibles, porteraient atteinte à la sécurité des services qui sont fournis par le CISP).

Lorsque ces informations sont considérées comme étant trop sensibles pour être communiquées, le CISP doit exposer la situation au client, si cela est nécessaire pour que le client comprenne les mesures de sécurité adoptées par le CISP.

Le tableau ci-dessous fournit des exemples d'informations hautement sensibles en matière de sécurité qu'un CISP peut décider de ne pas communiquer :

Exemples d'informations hautement sensibles concernant la sécurité qu'un CISP peut choisir de ne pas communiquer :
• L'identité et la localisation du personnel en charge des opérations de sécurité • Les résultats détaillés des tests d'intrusion réalisés en interne • Le modèle de menace, dès lors que le partage d'un modèle complet risque de porter gravement atteinte à la sécurité de l'infrastructure du CISP • Le code source des services lorsque l'accès au code source ne permettrait pas d'améliorer de manière significative la sécurité du client

Les CISPs peuvent demander aux clients de payer des frais supplémentaires pour ces informations ou peuvent choisir de fournir ces informations sans frais supplémentaires. Les frais supplémentaires doivent être raisonnables, fondés sur les coûts, proportionnés aux efforts fournis pour communiquer ces informations, et ils ne doivent pas être utilisés pour empêcher les clients d'évaluer la conformité du CISP dans le cadre de l'Article 28 du RGPD. Les CISPs doivent indiquer clairement aux clients les informations qui peuvent leur être communiquées sans frais supplémentaires, et celles qui sont uniquement disponibles moyennant des frais supplémentaires. Le tableau ci-dessous fournit quelques exemples d'informations pour lesquelles des frais supplémentaires sont généralement demandés.

Exemples de services qui impliquent généralement des frais supplémentaires :

- La communication des rapports d'audit, y compris le rapport d'audit spécifique demandé par le client, qui ne sont généralement pas transmis par le CISP
- L'assistance interne ou externe (ex. : conseillers/auditeurs en sécurité) fournie pour toute activité d'inspection requise par le client (s'il y a lieu)
- La participation à des réunions, des ateliers ou des tests sur la sécurité requis par le client
- Les réponses aux enquêtes, questionnaires et entretiens de sécurité requis par les clients

Le CISP peut publier sur son site internet les dernières informations concernant la disponibilité des services et/ou des mises à jour concernant les dispositifs de sécurité et de conformité en rapport avec le service. Le service concerné peut, en fonction de sa nature et ses fonctionnalités, offrir au client un accès aux rapports et journaux lui permettant de vérifier la conformité.

Le CISP doit mettre en place un dispositif (gratuit ou moyennant une contrepartie raisonnable) pour les clients qui ont des questions concernant la protection des données ou les mesures de sécurité en rapport avec le service, leur permettant de se mettre en contact avec le personnel du CISP correspondant ou le représentant désigné par le CISP pour traiter ces questions. Ces dispositifs doivent aider le client à exécuter ses obligations en qualité de responsable du traitement et doivent être appropriés et proportionnés au service d'infrastructure cloud en question. Ces dispositifs peuvent prendre la forme de numéros de téléphone, adresses électroniques, systèmes de chat, ou toute autre méthode permettant au client d'établir une communication avec le représentant du CISP. L'accès aux Données Client ou la connaissance de ces données n'est pas nécessaire pour respecter cette obligation. Le CISP doit également s'engager sur les délais de réponse, conformément aux accords définis dans le Contrat de Services.

(b) <u>Audit</u>

Outre les exigences d'information mentionnées ci-dessus, le CISP peut faire appel à des auditeurs indépendants pour vérifier l'adéquation des contrôles de sécurité et de protection des données applicables au service.

Si le CISP le propose, ces audits :

- doivent être réalisés conformément à une norme de sécurité reconnue (y compris, notamment, la norme ISO 27001, 27017, 27018) ;
- doivent être réalisés périodiquement selon les instructions fournies par la norme applicable ;
- doivent être réalisés par des professionnels de la sécurité, tiers indépendants, qualifiés pour réaliser cet audit (sur la base d'une certification ou d'une expérience reconnue) et dont la compétence est reconnue sur le marché ; et
- doivent aboutir à la rédaction d'un rapport d'audit.

À la demande écrite du client, le CISP peut lui remettre une copie intégrale de ce rapport d'audit afin que le client, l'auditeur du client et les Autorités de Contrôle dont le client relève puissent examiner et vérifier que le CISP se conforme aux obligations de sécurité et de protection des données qui lui incombent en vertu du Contrat de Services. Ce rapport doit

être daté de moins de 12 mois. Le CISP peut décider de facturer des frais supplémentaires au client, comme indiqué à la Section 4.6(b) ci-dessus, pour la délivrance du rapport d'audit.

Ce rapport constituera des informations confidentielles du CISP. Avant de transmettre ce rapport au client, le CISP peut au préalable lui demander de signer un accord de confidentialité. Cet accord de confidentialité permettra au CISP de s'assurer que l'accès aux informations confidentielles est limité au client et que le client ne peut pas divulguer ces informations sans l'accord préalable écrit du CISP. Cet accord de confidentialité ne doit pas empêcher le client de communiquer avec son Autorité de Contrôle lorsque cette communication est obligatoire, par exemple une demande formelle d'informations sur des questions qui sont nécessaires pour fournir des preuves concernant une plainte selon laquelle le RGPD n'est pas respecté.

Le client peut également demander à recevoir le rapport annuel produit par l'Organisme de Contrôle du CISP conformément à la Section 7.2 (a) du Code. Compte tenu de la nature des services d'infrastructure cloud et des risques inhérents aux environnements multi-locataires (*multi-tenant*), le rapport annuel et les audits externes (y compris les rapports, attestations et/ou certifications en résultant) servent à démontrer que le CISP (en tant que sous-traitant) respecte les dispositions de l'Article 28(3)(h) du RGPD.

Si les informations communiquées par le CISP (y compris les informations fournies au titre de la Section 4.6(a) ci-dessus et dans le rapport annuel préparé par l'Organisme de Contrôle dans le cadre de sa mission décrite à la Section 7.2(a)) ne sont pas suffisantes pour vérifier que le respect par le CISP de ses obligations en vertu du RGPD telles qu'elles sont décrites dans les Exigences du Code, alors le client peut choisir d'exercer droits en vertu de l'Article 28(3)(h) du RGPD comme suit :

- le client peut demander par écrit au CISP que l'Organisme de Contrôle procède à une vérification, dans la mesure strictement nécessaire pour démontrer la conformité du CISP aux Exigences du Code, dès lors que celle-ci n'a pas déjà été démontrée (notamment en vertu de tout rapport déjà préparé par l'Organisme de Contrôle dans le cadre de sa mission décrite à la Section 7.2(a)) ;

- le CISP doit autoriser l'Organisme de Contrôle à effectuer cette vérification ;

- au vu des risques de sécurité potentiels pour les autres clients et pour le service en général, l'accès direct aux sites ou aux systèmes du CISP par l'Organisme de Contrôle doit être autorisé uniquement s'il n'existe aucun autre moyen raisonnable de démontrer la conformité du CISP, et s'il est exécuté dans des conditions contrôlées (convenues d'un commun accord entre le CISP et l'Organisme de Contrôle) qui perturbent le moins possible le CISP, n'entrainent pas de risque pour la sécurité et la continuité du service aux autres clients, et ne font pas en sorte que le CISP enfreigne une obligation ou un devoir légal qu'il pourrait avoir ; et

- une fois cette vérification effectuée, l'Organisme de Contrôle doit produire un rapport qui sera remis au client, mais qui sera traité comme des informations confidentielles du CISP et de la même manière que tout rapport d'audit décrit ci-dessus.

Le rapport produit par l'Organisme de Contrôle, dès lors qu'il révèle un cas de non-conformité au Code :

- peut être cité dans toute réclamation faite par un client à propos de la conformité des services aux dispositions du Code, selon la Procédure de Réclamation décrite à la Section 7.2(a) ci-après ; et

- sera utilisé par l'Organisme de Contrôle pour imposer des sanctions appropriées conformément à la Section 7.2(b) ci-dessous.

Les informations communiquées au client en vertu de la Section 4.6(a) ci-dessus (le rapport annuel fourni par l'Organisme de Contrôle du CISP, les rapports d'audit externes et les certifications délivrées par le CISP, ainsi que le rapport de vérification complémentaire produit par l'Organisme de Contrôle) ne limitent aucun des droits conférés en vertu de l'Article 28(3)(h du RGPD. Lorsque les informations communiquées par le CISP en vertu de la Section 4.6 ne suffisent pas à démontrer la conformité du CISP selon les dispositions de l'Article 28(3)(h), le client peut demander au CISP d'accomplir toutes les autres démarches nécessaires pour prouver sa conformité. Ces démarches peuvent impliquer d'autres demandes auprès de l'Organisme de Contrôle. Si la réponse du CISP ou de l'Organisme de Contrôle ne suffit pas à démontrer que le CISP respecte les obligations qui lui incombent en vertu de l'Article 28 du RGPD, le client peut demander des informations complémentaires au CISP au travers d'un nouvel audit, y compris des inspections, par un auditeur sélectionné par le client à partir d'une liste d'auditeurs agréés fournie par le CISP à l'avance. Cet audit sera mené de la façon la moins intrusive possible pour le CISP pour vérifier la conformité avec ses obligations en vertu de l'Article 28 du RGPD et il sera soumis à (i) des contrôles raisonnables déterminés par le CISP afin d'éviter les risques pour les autres clients ou le CISP, notamment un contrôle de la sécurité des installations du CISP et le maintien de la continuité des opérations ; (ii) l'acceptation par le client de modalités visant à protéger les informations confidentielles du CISP ; et (iii) l'obligation du client de payer les frais raisonnables de l'audit. Le client et le CISP discuteront de bonne foi et s'accorderont sur la portée des activités de l'audit avant de réaliser cet audit.

Pour les besoins du paragraphe ci-dessus, on entend par « auditeur » un tiers indépendant, professionnel de la sécurité, qui est qualifié pour effectuer un tel audit (sur la base d'une certification ou d'une expérience reconnue) et reconnu sur le marché comme ayant la compétence pour le faire.

Explication :

Les services d'infrastructure cloud sont des environnements multi-locataires (*multi-tenant)*. Cela signifie que les données de pratiquement tous les clients du CISP peuvent être hébergées dans les mêmes locaux ou installations. L'accès physique aux installations du CISP par un seul client ou tiers pose un risque de sécurité pour tous les autres clients du CISP dont les données sont hébergées dans ces mêmes locaux ou installations. Ce risque peut être contrôlé si, lorsque cela est possible, au lieu d'un audit sur site, le client utilise les informations fournies par le CISP, ou obtenues dans le cadre de l'inspection de l'Organisme de Contrôle, pour vérifier si le CISP a respecté les obligations de sécurité et de protection des données prévues dans le Contrat de Services.

4.7 Droits des personnes concernées

Exigence du RGPD :

« Tient compte de la nature du traitement », le ***sous-traitant*** *« aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits [...] » (Art 28(3)(e) du RGPD).*

Les droits des personnes concernées en vertu du chapitre III du RGPD sont le droit à la transparence des informations (Art. 12, Art. 13 et Art. 14), le droit d'accès (Art. 15), le droit de rectification (Art. 16), le droit à l'effacement (Art. 17), le droit à la limitation du traitement (Art. 18), le droit à la notification en ce qui concerne la rectification ou l'effacement de données ou la limitation du traitement (Art 19), le droit à la portabilité des données (Art. 20), le droit d'opposition (Art. 21) et les droits concernant la décision individuelle automatisée, y compris le profilage (Art. 22).

Obligation du CISP :

Le CISP doit offrir au client la possibilité de rectifier, d'effacer, de limiter, d'accéder ou de porter (dans un format structuré, couramment utilisé et lisible par machine) les Données Client dans le cadre du service ou de concevoir et déployer leurs propres solutions en utilisant le service.

Le client peut utiliser cette capacité pour s'acquitter de ses obligations en répondant aux demandes des personnes concernées. Le CISP fournit une explication sur la manière dont ces capacités seront fournies au client dans le cadre des informations requises en vertu de la Section 5 (Transparence). Les informations fournies en vertu de la Section 5 (Transparence) permettront également au client de respecter ses propres obligations en matière de transparence vis-à-vis des personnes concernées.

Explication :

Offrir au client la possibilité de rectifier, d'effacer, de limiter, d'accéder ou de porter les Donnés Client, est censé être la limite de ce qu'un CISP peut faire pour soutenir les demandes des personnes concernées, bien que le CISP et le client aient la possibilité de définir d'autres responsabilités entre eux. En effet, il appartient au client (et non au CISP) de gérer les données qu'il traite en utilisant le service. Par conséquent, le CISP ne connaît pas les données clients qui sont chargées sur le service et, en particulier, l'identité des personnes concernées auxquelles les données à caractère personnel traitées se rapportent.

4.8 Personnel du CISP

Exigence du RGPD :

« Le sous-traitant [...] veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité » (Art 28(3)(b) du RGPD).

Obligation du CISP :

(a) Confidentialité :

Le CISP doit imposer des obligations contractuelles appropriées stipulant que les membres du personnel du CISP qui sont autorisés à accéder aux Données Client doivent préserver la confidentialité de ces données.

(b) Contrôles d'accès :

Le CISP doit mettre en œuvre et maintenir des contrôles et des politiques d'accès afin de limiter son personnel traitant les Données Client au personnel du CISP qui a besoin de traiter les Données Client pour fournir les services au client. Le CISP doit sélectionner les contrôles d'accès appropriés, à savoir : (i) limiter l'accès physique aux installations du centre de données au personnel autorisé ; (ii) limiter l'accès technique aux logiciels et réseaux hôtes au personnel autorisé; (iii) enregistrer les accès du personnel du CISP aux Données Client. Dès que le personnel du CISP n'a plus besoin de traiter les Données Client, le CISP doit supprimer ces privilèges d'accès dans les meilleurs délais.

Explication :

Le personnel du CISP peut avoir besoin d'accéder aux Données Client pour exécuter les services. Dans ce cas, l'accès sera uniquement autorisé en tant que de besoin pour gérer le service. Les membres du personnel qui n'ont pas besoin

d'accéder aux Données Client pour gérer le service seront soumis à des contrôles d'accès appropriés destinés à leur interdire tout accès.

4.9 Violation des données

Exigence du RGPD :

*« Le **sous-traitant** notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance ». (Art 33(2) du RGPD).*

*« **[Le sous-traitant]** aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant » (Art 28(3)(f) du RGPD).*

Obligation du CISP :

(a) Politique de gestion des incidents

Le CISP doit établir une politique de gestion des incidents qui décrit les procédures à suivre pour identifier les violations de données à caractère personnel dont il a connaissance, et y répondre.

Cette politique doit contenir :

- des lignes directrices sur la façon de traiter les incidents, et déterminer qui est responsable de la gestion des incidents au sein du CISP ;
- des lignes directrices concernant les aspects constitutifs d'une violation de données à caractère personnel au regard du RGPD, et des directives permettant de déterminer les types d'incidents qui doivent être notifiés au client en fonction de leur impact potentiel sur les Données Client ;
- une obligation de mener des enquêtes rapides dès lors qu'un CISP prend connaissance d'une violation de données présumée afin de déterminer si une violation a eu lieu, et quelles Données Client peuvent être affectées ;
- une procédure visant à mettre en œuvre des activités de remédiation afin de minimiser l'impact d'une violation de données, et de corriger les vulnérabilités engendrées par les incidents de sécurité ;
- une procédure pour notifier le client dans les meilleurs délais dès lors qu'un CISP a obtenu l'assurance qu'une violation de données a eu lieu en rapport avec les Données Client de ce client ;
- un classement des incidents par type de gravité, et des délais indicatifs pour les principales mesures d'investigation, ainsi que la notification planifiée du/des client(s) (le cas échéant), en fonction de la gravité de l'incident ;
- des mesures d'escalade, au sein même de la gouvernance du CISP, pour intervenir en cas d'incident ;
- une spécification des informations qu'il convient de mettre à la disposition du client à la suite d'une violation de données ; et
- une procédure visant à coopérer avec le client lorsque ce dernier informe le CISP d'une violation de données, notamment en communiquant au client toutes les informations préliminaires disponibles pour l'aider à respecter ses obligations prévues par l'Article 33(1) du RGPD.

(b) Notification d'une violation de sécurité

Portée et délai de la notification

Si le CISP prend connaissance de la destruction, la perte ou l'altération, ou de la divulgation non autorisée de Données Client, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite, sur l'équipement ou les installations du CISP, le CISP en informera le client dans les meilleurs délais.

Contenu de la notice

La notice doit, dans la mesure où le CISP a connaissance de ces informations en sa qualité de sous-traitant : (i) décrire la nature de la violation de sécurité, (ii) décrire les conséquences de la violation, (iii) décrire les mesures prises ou que le CISP propose de prendre pour remédier à l'incident et (iv) communiquer le nom et les coordonnées d'un point de contact au sein du CISP. Un modèle de notification de violation de sécurité est présenté en Annexe F. Les CISPs n'ont pas l'obligation d'utiliser ce modèle, mais il donne un exemple du format à utiliser et du type d'informations qu'un CISP peut mentionner dans une notification de violation de sécurité adressée à un client. Le Comité Européen de la Protection des Données a publié des lignes directrices sur la notification de violations de données à caractère personnel en vertu du RGPD, qui pourraient aider les CISPs à définir leur politique et leurs modèles pour les violations de sécurité. Ces lignes directrices sont accessibles à l'adresse suivante :

https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

4.10 Suppression ou renvoi de données à caractère personnel

Exigence du RGPD :

> ***« [Le sous-traitant]*** *selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel »* (Art 28(3)(g) du RGPD).

Obligation du CISP :

Le CISP doit donner au client la possibilité de récupérer et de supprimer toutes les Données Client. Le client peut utiliser cette option à tout moment pour récupérer ou supprimer des Données Client.

Selon le type de service, le CISP peut offrir au client la possibilité de récupérer et de supprimer des Données Client (a) dans le cadre du service, ou (b) en autorisant les clients à concevoir et déployer leurs propres solutions de suppression et d'extraction en utilisant le service. Le CISP doit inclure dans les informations requises en vertu de la Section 5 (Transparence), un paragraphe qui explique comment ces options seront mises à disposition du client. À tout moment, le CISP doit suivre les instructions fournies par le client en ce qui concerne l'extraction ou la suppression des Données Client.

En l'absence d'instruction du client, le CISP doit, par défaut, supprimer les Données Client dans un délai raisonnable après l'expiration ou la résiliation du service.

> **Explication :**
>
> Le CISP ne supprime pas les données d'un client, ni ne prend la décision de le faire au nom de ce client. Par conséquent, il appartient au client de gérer la suppression et l'extraction de ses données sur le service, en tenant compte des procédures mises en place après la résiliation ou l'expiration du Contrat de Services, en utilisant

l'option proposée par le CISP bien que le CISP et le client aient la possibilité de définir d'autres responsabilités entre eux.

4.11 Registres des activités de traitement

Exigence du RGPD :

« Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement. Ce registre comporte toutes les informations suivantes :

(a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;

(b) les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

(c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées ;

(d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1.. » (Art 30(2) du RGPD).

« Les registres…se présentent sous une forme écrite y compris la forme électronique. » (Art 30(3) du *RGPD*)

« *Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'autorité de contrôle sur demande »* (Art 30(4) du RGPD)

Obligation du CISP :

Le CISP doit tenir un registre écrit (y compris sous forme électronique) des activités de traitement qu'il effectue pour le compte de ses clients qui sont des responsables du traitement, comprenant :

- le nom et les coordonnées du client ;
- les catégories de traitements effectués par le client (ces catégories peuvent être décrites en référence aux services fournis par le CISP) ;
- si le CISP a mis en œuvre ou met à la disposition du client un mécanisme de transfert reconnu en vertu du Chapitre V du RGPD ; et
- une description générale des mesures de sécurité mises en place (par exemple, les mesures adoptées pour se conformer à l'Annexe A).

Le CISP doit mettre ce registre à la disposition d'une Autorité de Contrôle sur demande.

Explication :

Compte tenu de la nature de l'IaaS, seul le client aura une visibilité et pourra exercer un contrôle sur les catégories de traitement spécifiques. Le CISP tiendra des registres des services utilisés par ses clients conformément aux dispositions du

RGPD ; toutefois, seul le client possède une visibilité sur les détails spécifiques des données à caractère personnel qu'il choisit de traiter en utilisant ces services (et il a l'obligation de tenir des registres en application de l'Article 30(1) du RGPD).

De même, le CISP aura probablement besoin de tenir un registre distinct de ses activités de traitement conformément à l'Article 30.1 du RGPD lorsqu'il agit en qualité de responsable du traitement, notamment dans le cadre de ses propres registres ou de ses systèmes de gestion du client. Cependant, étant donné que le Code met l'accent sur les obligations des CISPs en tant que sous-traitants, cette obligation qui incombe spécifiquement aux responsables du traitement n'entre pas dans le champ d'application matériel du Code.

5 Exigences en matière de Transparence

Les clients doivent pouvoir évaluer de manière fiable les risques pour la sécurité et l'analyse d'impact relative à la protection des données, en ce qui concerne les données à caractère personnel traitées sur les services d'infrastructure cloud.

Le CISP doit aider le client à atteindre cet objectif en garantissant la transparence des mesures de sécurité mises en œuvre par le CISP pour ses services. Pour garantir un niveau adéquat de transparence, le CISP doit se conformer à la Section 4.6 du Code, « Démonstration de la conformité » et aux dispositions de l'Article 28(3)(h) du RGPD, et il doit, au moins fournir les informations suivantes aux clients :

1. Un Contrat de Services qui prévoit un partage des responsabilités entre le CISP et le Client pour la sécurité du service.
2. Une déclaration de haut niveau sur les objectifs et les normes de sécurité qui s'appliquent au service concernant au moins la Confidentialité, la Disponibilité et l'Intégrité.
3. Des informations concernant la conception et la gestion du service pour aider les clients à comprendre les menaces et vulnérabilités potentielles liées à leur utilisation du service.
4. Des informations à l'appui des processus de gestion du risque, le modèle de menaces envisagé et les critères de gestion du risque du CISP pour le service.
5. Des informations concernant les mesures de sécurité mises en place par le CISP pour le service.
6. La documentation relative au système de gestion de la sécurité de l'information du CISP.
7. Des informations concernant le fonctionnement du service qui permettent au client de i) rectifier, effacer, limiter, accéder ou porter des Données Client (conformément à la Section 4.7) ; et ii) récupérer et supprimer des Données Client (conformément à la Section 4.10).

Le CISP doit également, seul ou conjointement avec d'autres prestataires (internes ou externes) nommer un point de contact pour la protection des données ou un Délégué à la Protection des Données, conformément aux exigences du RGPD ou aux dispositions légales applicables (le Groupe de Travail « Article 29 » a publié des Lignes Directrices concernant les Délégués à la Protection des Données qui peuvent aider les CISPs dans cette évaluation. Ces lignes directrices sont accessibles à l'adresse suivante https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048). Si un CISP n'est pas tenu de désigner un point de contact pour la protection des données ou un Délégué à la Protection des Données, il doit tout de même affecter un point de contact interne pour traiter les demandes des clients concernant la protection des données ou les questions de sécurité relatives au service, en utilisant le mécanisme décrit à la Section 4.6(a).

Les paragraphes ci-dessous décrivent les étapes que le CISP doit suivre pour garantir un niveau adéquat de transparence pour chaque service déclaré comme étant conforme aux dispositions du Code.

Le CISP peut atteindre ces objectifs en établissant un système de gestion de la sécurité de l'information qui couvre ces 7 objectifs (tels qu'ils sont définis aux paragraphes 5.1 à 5.7 ci-dessous). Le Code encourage les CISPs à mettre en place des systèmes de gestion de la sécurité de l'information de haute technologie sur la base d'un ou plusieurs standards

reconnus dans le secteur. À l'exception des exigences spécifiquement applicables au Contrat de Services, le CISP peut décider de communiquer aux clients les informations visées dans la présente Section 5 (Exigences en matière de Transparence) en :

- fournissant des informations sur les pratiques de sécurité et de contrôle du CISP ; et/ou
- obtenant des certifications délivrées par des organismes du secteur et/ou des attestations délivrées par des tiers indépendants ; et/ou
- délivrant des certificats, rapports et autres documents directement aux clients.

Si le CISP considère que ces informations sont confidentielles, le CISP doit les mettre à la disposition du client sur demande, mais en ayant au préalable demandé au client de signer un accord de confidentialité. Cet accord de confidentialité permettra au CISP de s'assurer que l'accès aux informations confidentielles est limité au client et que le client ne peut pas divulguer ces informations sans l'accord préalable écrit du CISP. L'accord de confidentialité ne doit pas empêcher le client de communiquer avec son Autorité de Contrôle lorsque cette communication est obligatoire.

5.1 Un Contrat de Services qui prévoit une répartition des responsabilités entre le CISP et le Client pour la sécurité du service

Le Contrat de Services doit définir les responsabilités en matière de sécurité du CISP et du client pour la durée dudit contrat. Nonobstant les dispositions du droit de l'Union et du droit des États Membres qui s'appliquent au CISP, le client, en tant que responsable du traitement, demeure en principe responsable de tous les aspects de sécurité des données relevant de sa responsabilité en qualité de responsable du traitement, qui ne sont pas couverts par le Contrat de Services.

Outre le Contrat de Services, le CISP peut choisir de rendre accessible toute autre documentation concernant le service qui décrit la répartition des responsabilités en matière de sécurité entre le CISP et le client. Par exemple, le CISP peut fournir une matrice décrivant les responsabilités des deux parties sur la base du contrôle partagé de l'environnement informatique et des contrôles lors de l'utilisation du service.

5.2 Une déclaration de haut niveau sur les objectifs de sécurité et les normes applicables au service

Le CISP doit déclarer (a) les objectifs que les mesures de sécurité qu'il a mises en place pour le service sont censées atteindre, et le cas échéant (b) les standards que le CISP s'engage à suivre pour la mise en œuvre de ces mesures de sécurité. Reportez-vous à l'Annexe A (Responsabilités en matière de Sécurité) pour en savoir plus.

Le CISP peut être amené à modifier ses normes de sécurité, mais il doit au moins continuer d'assurer le même niveau de sécurité que celui qui est décrit dans ses normes de sécurité applicables à la date de prise d'effet du Contrat de Services.

Le CISP doit informer les clients lorsqu'un service d'infrastructure cloud a vocation à aider les clients à respecter une norme reconnue ou une disposition légale applicable à un type de traitement spécifique (ex : le traitement des données concernant la santé). Cette information peut être communiquée aux clients dans le Contrat de Services, dans un descriptif du service et/ou via le site internet du CISP ou tout autre support public disponible.

5.3 Informations concernant la conception et la gestion du service

Le CISP doit transmettre au client des informations sur l'infrastructure disponible et sur la façon dont elle est utilisée pour fournir le service (à savoir les installations, le réseau, le matériel informatique et le logiciel opérationnel qui soutiennent la fourniture et l'utilisation

des services).

Ces informations peuvent inclure, par exemple :

- L'architecture de haut niveau de l'infrastructure
- La localisation générale des dispositifs d'hébergement du CISP pertinents pour le client
- La configuration du matériel informatique, le cas échéant
- L'autre sous-traitant autorisé par le CISP à accéder aux Données Client
- Les dispositifs de sécurité du service
- Les options qui sont proposées au client pour renforcer la sécurité du service

5.4 Informations à l'appui des processus de gestion du risque et des critères du CISP

Le CISP doit fournir aux clients des informations confirmant l'existence et le caractère adéquat du programme de gestion du risque mis en place par le CISP, y compris le modèle de menaces et les critères de gestion du risque qu'il a envisagés, pour aider les clients à intégrer les procédures de contrôle du CISP dans leurs propres cadres de gestion du risque. Ces informations concernent, par exemple, les évaluations du risque internes et/ou externes réalisées ou mandatées par le CISP et couvertes dans un ou plusieurs rapports d'audit.

Le Code encourage le CISP à suivre une méthode d'évaluation du risque sur la base des standards de référence, notamment ISO/CEI 27005, OCTAVE ou EBIOS.

5.5 Des informations concernant les mesures de sécurité mises en place par le CISP pour le service

Le CISP doit fournir toutes les informations nécessaires concernant les mesures de sécurité adoptées pour les services proposés aux clients, afin d'aider les clients à comprendre les dispositifs contrôles mis en place pour le service qu'ils utilisent et comment ces dispositifs de contrôle ont été approuvés.

Ces informations visent à permettre aux clients de déterminer s'ils peuvent utiliser et configurer les services afin d'assurer un niveau de sécurité approprié pour le traitement que le client envisage d'effectuer en ayant recours au service.

Le CISP doit, en particulier, décrire :

- les procédures de sécurité physique et opérationnelle pour l'infrastructure du réseau et du serveur sous la supervision du CISP ; et
- les dispositifs de sécurité et de contrôle que les clients peuvent utiliser et configurer sur le service (sur chacun desquels le CISP doit maintenir un mode sécurisé par défaut).

Ces informations doivent inclure, par exemple, des informations concernant :

- la sécurité physique et environnementale ;
- la sécurité du réseau ;
- des contrôles logiques ou physiques pour garantir l'isolement des données du client, comme la segmentation réseau des principes de stockage des données ;

- la gestion de la continuité de l'exploitation ;
- la gestion des changements ; et
- les dispositifs de sécurité des comptes.

5.6 La documentation relative au système de gestion de la sécurité de l'information du CISP

Les CISPs doivent communiquer les informations nécessaires concernant le système de gestion de la sécurité de l'information mis en place pour les services proposés aux clients afin que les clients puissent raisonnablement vérifier la conformité du CISP avec les obligations de sécurité définies dans le Contrat de Services et décrites à la Section 4.6 (Protection des Données ; Démonstration de la conformité) du présent Code.

5.7 Informations concernant le fonctionnement du service qui permettent au client de i) rectifier, effacer, limiter, accéder ou transférer des Données Client ; et ii) récupérer et supprimer des Données Client.

Le CISP doit communiquer au client des informations sur les capacités dont il dispose pour lui permettre de :

- rectifier, effacer, limiter, accéder ou porter des Données Client conformément à la Section 4.7 du présent Code (Droits des personnes concernées) ; et
- récupérer et supprimer des Données Client conformément à la Section 4.10 du présent Code (Suppression ou renvoi de données à caractère personnel).

6 Adhésion

Un CISP qui déclare son adhésion au Code doit respecter toutes les Exigences du Code pour les services couverts par sa déclaration et pourra ensuite utiliser la Marque (telle que définie à la Section 6.4 ci-après). Les CISPs ne peuvent pas respecter une partie seulement des Exigences du Code ou se soustraire à certaines dispositions des Exigences du Code.

Les CISPs qui ont déclaré leur adhésion au Code doivent également s'engager à se soumettre aux règles de la Section 7 (Gouvernance). Si un CISP refuse de se soumettre aux Exigences du Code, il sera soumis aux mesures d'exécution décrites à la Section 7 (Gouvernance). Le respect de la Section 7 par un CISP est sans préjudice des sanctions possibles imposées par les Autorités de Contrôle compétentes en vertu de la législation européenne applicable en matière de protection des données.

6.1 Déclarer un service comme étant conforme aux dispositions du Code

Il existe deux procédures possibles pour déclarer un service comme étant conforme aux dispositions du Code : l'Autoévaluation et l'Adhésion Contrôlée :

(a) Autoévaluation

En ce qui concerne l'Autoévaluation, un CISP doit réaliser une autoévaluation de son service par rapport aux Exigences du Code et présenter au Secrétariat :

- sa Déclaration d'Adhésion ; et
- une Liste de Contrôle de la Conformité complète conformément aux indications fournies en Annexe B du Code, et toute pièce justificative.

D'autres informations concernant les documents à délivrer figurent à la Section 6.2 ci-après.

Une fois la documentation remise, le Secrétariat doit en étudier le contenu. (Pour lever toute ambigüité, le Secrétariat exerce une fonction administrative, et doit uniquement confirmer que la documentation est complète. Seul un Organisme de Contrôle est habilité à évaluer la conformité d'un service au Code).

Dans un délai de 40 jours après réception de la documentation, le Secrétariat doit indiquer au CISP si celle-ci est complète ou non. Si la documentation est incomplète, le Secrétariat peut demander au CISP de lui fournir le(s) document(s) manquant(s) ou les informations complémentaires requises pour compléter son dossier.

Si la documentation est complète, le Secrétariat doit consigner la Déclaration d'Adhésion dans le Registre Public CISPE dans un délai de 10 jours ouvrés après avoir signifié son acceptation au CISP. Le Registre Public CISPE indiquera clairement que le service concerné n'a pas encore été évalué et approuvé par un Organisme de Contrôle et le service sera décrit comme « Candidat au Code » jusqu'à ce qu'un Organisme de Contrôle ait achevé son Examen Initial et confirmé que ce service respecte les dispositions du Code conformément à la Section 6.3 ci-après.

Les CISPs qui ont choisi la procédure d'Autoévaluation doivent :

uniquement consigner le service ayant fait l'objet d'une autoévaluation dans le Registre Public CISPE en tant que « Candidat au Code », pour une période de 12 mois maximum après la date de consignation de la Déclaration d'Adhésion dans le Registre Public CISPE ; et

s'assurer que l'Organisme de Contrôle qu'ils ont désigné examine et vérifie que le service est conforme aux dispositions du Code dans un délai de 12 mois après la date de consignation.

Une fois que l'Organisme de Contrôle a évalué la conformité du service au Code dans le cadre de son Examen Initial, s'il confirme que le service est conforme aux dispositions du Code, le CISP doit remettre une confirmation écrite délivrée par son Organisme de Contrôle indiquant que le service est conforme au Code. Une fois que le Secrétariat a reçu cette confirmation écrite, le service du CISP doit avoir le même statut que si le CISP avait suivi la procédure d'Adhésion Contrôlée décrite ci-dessous :

  - il peut utiliser la Marque de Conformité, conformément aux indications de la Section 6.2 ci-après ; et
  - le Registre Public CISPE doit être actualisé et indiquer que le service du CISP a désormais été évalué et approuvé par son Organisme de Contrôle,

- si le service est jugé comme étant non conforme aux dispositions du Code, ledit service et la Déclaration d'Adhésion du CISP doivent être supprimés du Registre Public CISPE.

La procédure d'Autoévaluation est une procédure provisoire. Le(s) service(s) du CISP ne doit/doivent pas être réputé(s) conforme(s) aux dispositions du Code tant qu'il(s) n'a/n'ont pas été évalué(s) et approuvé(s) par son Organisme de Contrôle. La procédure d'Autoévaluation vise à faciliter la participation des PME au Code, à accorder aux CISPs un délai supplémentaire pour se familiariser avec la procédure et les exigences du Code, à conclure un contrat avec un Organisme de Contrôle et à organiser les ressources internes pertinentes pour faciliter l'adhésion continue au Code.

(b) <u>Adhésion Contrôlée</u>

Dans la procédure d'Adhésion Contrôlée, un CISP doit au préalable soumettre le service concerné à l'Organisme de Contrôle pour évaluation et vérification, et présenter au Secrétariat:

- sa Déclaration d'Adhésion ;
- une Check-list de Conformité complète conformément aux indications fournies en Annexe B du Code, et toute pièce justificative ; et
- une confirmation écrite délivrée par son Organisme de Contrôle indiquant que le service du CISP est conforme aux dispositions du Code.

D'autres informations concernant les documents à délivrer figurent à la Section 6.2 ci-après.

Une fois la documentation remise, le Secrétariat doit en étudier le contenu. (Pour lever toute ambigüité, le Secrétariat exerce une fonction administrative, et doit uniquement confirmer que la documentation est complète. Seul un Organisme de Contrôle est habilité à évaluer la conformité d'un service au Code).

Dans un délai de 40 jours après réception de la documentation, le Secrétariat doit indiquer au CISP si celle-ci est complète ou non. Si la documentation est incomplète, le Secrétariat peut demander au CISP de lui fournir le(s) document(s) manquant(s) ou les informations complémentaires requises pour compléter son dossier.

Si la documentation est complète, le Secrétariat doit consigner la Déclaration d'Adhésion dans le Registre Public CISPE dans un délai de 10 jours ouvrés après avoir signifié son acceptation au CISP.

Une fois que la Déclaration d'Adhésion est consignée dans le Registre Public CISPE :

- le CISP est autorisé à utiliser cette Déclaration d'Adhésion et la Marque de Conformité appropriée, conformément aux indications de la Section 6.4 ci-après, exclusivement pour les services couverts par cette déclaration et tant qu'elle demeure valable et soumise aux mesures d'exécution visées à la Section 7.2 (Contrôle, Réclamations et Mesures d'Exécution) ; et

- si un changement au niveau du service nécessite de mettre à jour le matériel mentionné dans la Déclaration d'Adhésion actuelle du CISP, alors (i) le CISP doit immédiatement en informer le Secrétariat et l'Organisme de Contrôle ; (ii) coopérer avec le Secrétariat pour opérer les mises à jour du matériel en question ; et (iii) respecter toute obligation imposée par l'Organisme de Contrôle de soumettre ces mises à jour à une nouvelle évaluation.

6.2 Documentation

(a) Déclarations d'Adhésion

L'Annexe C présente un modèle de Déclaration d'Adhésion sous sa forme actuelle. Ce modèle peut être actualisé par la CCTF si besoin. Le Secrétariat doit publier et conserver une version actualisée de la Déclaration d'Adhésion sur le Registre Public CISPE. En soumettant sa Déclaration d'Adhésion, le CISP confirme que le service est conforme aux Exigences du Code. L'Organisme de Contrôle désigné par le CISP est chargé de contrôler et d'évaluer si le CISP respecte les dispositions du Code, telles qu'indiquées ci-dessus pour la Déclaration d'Adhésion initiale et dans la Section 7.2 ci-après pour l'évaluation continue.

(b) Check-list de Conformité et pièces justificatives

La Check-list de Conformité est présentée en Annexe B. Cette liste énonce les Exigences du Code et les lignes directrices sur les démarches à accomplir pour respecter les Exigences du Code et sur la manière de mettre en œuvre les pratiques techniques et organisationnelles en matière de sécurité décrites en Annexe A.

Lorsqu'ils soumettent leur Check-list de Conformité complétée, les CISPs sont invités à inclure les pièces justificatives.. Par exemple : le Contrat de Services dans sa version actuelle ; les politiques et procédures internes du CISP ; des exemples de contrats avec le personnel, les sous-traitants etc. du CISP ; des informations relatives aux services du CISP ; des informations concernant les pratiques de sécurité et de contrôle du CISP ; et/ou certifications délivrées par des organismes du secteur et/ou des attestations délivrées par des tiers indépendants, sont autant de documents qui permettent d'appuyer la Check-list de Conformité d'un CISP et qui peuvent être utilisés, à l'entière discrétion de l'Organisme de Contrôle, pour évaluer la conformité aux dispositions du Code. L'Organisme de Contrôle est en droit de demander au CISP tout autre document qu'il juge nécessaire pour vérifier si le CISP respecte les Exigences du Code.

(c) Confirmation écrite délivrée par l'Organisme de Contrôle

Un CISP qui choisit la procédure d'Adhésion Contrôlée doit remettre une confirmation écrite indiquant que son service a été évalué et vérifié par son Organisme de Contrôle. Cette confirmation peut prendre la forme d'une lettre ou tout autre document signé préparé par l'Organisme de Contrôle.

6.3 Renouvellement et examen

Pour les CISPs qui choisissent la procédure d'Autoévaluation, l'Organisme de Contrôle doit évaluer et vérifier que le service est conforme aux dispositions du Code dans un délai de 12

mois après la date de consignation de la Déclaration d'Adhésion dans le Registre Public CISPE. Pour les CISPs qui choisissent la procédure d'Adhésion Contrôlée, l'Organisme de Contrôle procédera à l'évaluation et à la vérification du service avant de consigner la Déclaration d'Adhésion du CISP dans le Registre Public. Dans les deux cas, l'Organisme de Contrôle recevra la Déclaration d'Adhésion et la Check-list de Conformité sur lesquelles il doit s'appuyer pour effectuer son évaluation et sa vérification, et l'Organisme de Contrôle utilisera la même approche pour procéder à son évaluation. L'Organisme de Contrôle est en droit de demander au CISP toute autre information qu'il juge nécessaire pour évaluer la conformité aux dispositions du Code.

Dans l'un ou l'autre des cas, il s'agit de l'« **Examen Initial** » de l'Organisme de Contrôle. Pour lever toute ambigüité, l'évaluation, la vérification et l'examen permanent de la conformité aux dispositions du Code seront effectués pour *chaque service* qui est déclaré comme étant conforme aux dispositions du Code. Si le CISP propose plusieurs services qui sont déclarés conformes aux dispositions du Code, l'Organisme de Contrôle doit évaluer chacun de ces services.

Après l'Examen Initial, l'évaluation par l'Organisme de Contrôle doit avoir lieu chaque année, conformément à la Section 7.2(a) du Code. Pour s'assurer que ces examens reflètent les cycles d'audit annuel existants du CISP, le second examen doit avoir lieu dans les 18 mois qui suivent la date de l'Examen Initial. Par la suite, des examens annuels doivent être réalisés dans les 12 mois après la date d'anniversaire de l'examen annuel précédent.

Pour réaliser ces examens, l'Organisme de Contrôle doit utiliser les documents pertinents existants qui sont mis à sa disposition (y compris les documents utilisés pour appuyer la Déclaration d'Adhésion du CISP), mais l'Organisme de Contrôle peut exiger un nouvel examen si les documents existants ne permettent pas de vérifier l'adhésion du CISP au Code .

Au moins deux semaines avant la date de chaque examen annuel, le CISP doit remettre au Secrétariat et à l'Organisme de Contrôle : une version actualisée de la Déclaration d'Adhésion ; ou, dans l'hypothèse où ni le service couvert par la Déclaration d'Adhésion initiale, ni le Code, n'a été modifié de manière substantielle depuis sa délivrance, une confirmation écrite de l'exactitude des renseignements mentionnés dans la Déclaration d'Adhésion et des pièces justificatives communiquées au moment de sa délivrance. Une Déclaration d'Adhésion est valable uniquement pour une durée de trois ans. Au-delà de ce délai, le CISP doit soumettre une nouvelle Déclaration d'Adhésion.

L'Organisme de Contrôle doit renouveler son approbation du respect par le CISP des dispositions du Code chaque année dans le cadre de son examen annuel : Un examen annuel n'implique pas nécessairement un audit complet du respect des dispositions du Code. Les examens annuels se dérouleront de la manière suivante :

- Lors du premier examen annuel après l'Examen Initial, ou le dernier cycle d'audit, l'Organisme de Contrôle examinera la conformité aux exigences du Code visées à la Section 4 du Code, à l'exception de la Section 4.3 ;

- Lors du second examen annuel après l'Examen Initial ou le dernier cycle d'audit, l'Organisme de Contrôle examinera la conformité aux exigences du Code visées à la Section 4.3 du Code ;

- Lors du troisième examen annuel après l'Examen Initial, ou le dernier cycle d'audit, l'Organisme de Contrôle examinera la conformité aux exigences du Code visées à la Section 5 du Code.

Cependant, l'Organisme de Contrôle doit au moins réaliser un examen complet de la conformité du service au Code dans les cas suivants :

- après que le service ou le code ait subi des modifications substantielles ; ou,

- en l'absence de modifications substantielles du service ou du Code, une fois tous les trois ans.

Outre ce qui précède, durant chaque cycle d'audit de trois ans, l'Organisme de Contrôle doit procéder à un audit complet du respect des dispositions du Code :

Si le Code a subi des modifications substantielles, CISPE doit spécifier un délai raisonnable durant lequel le CISP doit apporter toutes les mises à jour nécessaires pour s'assurer que ses services respectent les nouvelles Exigences du Code, après quoi le CISP devra présenter une nouvelle Déclaration d'Adhésion ou une Déclaration d'Adhésion révisée, une nouvelle Check-list de Conformité ou une version révisée de celle-ci, ainsi que toutes les pièces justificatives, indiquant dans quelle mesure les services du CISP respectent les nouvelles Exigences du Code. Le délai spécifié par CISPE tiendra compte des modifications pertinentes apportées au Code mais, en tout état de cause, il n'excédera pas six mois.

On entend par modifications substantielles du service, les modifications qui pourraient avoir un impact sur la conformité du service au Code. Par exemple, les modifications apportées à la conception et la mise en œuvre des services. La CCTF peut être amenée à publier à l'avenir d'autres lignes directrices sur les caractéristiques d'une « modification substantielle » au sens entendu par le Code, reflétant les observations formulées par les Organismes de Contrôle concernant les aspects qui ont un impact substantiel sur leur évaluation de la conformité.

Tous les trois ans, l'Organisme de Contrôle doit rédiger un rapport d'audit pour le service du CISP et doit communiquer ce rapport à CISPE. Ce rapport d'audit doit comprendre une description de la méthodologie, du résultat, de l'analyse, des conclusions et des recommandations de l'audit ou tout constat équivalent compatible avec l'état de l'art en matière d'évaluation de la conformité, comme dans le cadre d'un audit réalisé selon la norme ISO 27001.

6.4 Marque

La CCTF doit établir une Marque de Conformité à utiliser comme un symbole, face au public, de l'adhésion d'un service aux Exigences du Code (la Marque). La Marque doit être approuvée par le Comité Exécutif.

Les CISPs qui optent pour l'auto-Évaluation ne sont pas autorisés à utiliser la Marque de Conformité tant que l'Organisme de Contrôle n'a pas achevé son Examen Initial et vérifié que le CISP respecte les dispositions du Code. Cette pratique vise à renforcer la transparence pour les clients et à opérer une distinction entre les services des CISPs qui : (a) entrent dans le champ de la procédure d'auto-Évaluation, et (b) ont obtenu l'approbation de l'Organisme de Contrôle.

La CCTF doit établir des lignes directrices pour l'utilisation de la Marque par les CISPs **(Lignes Directrices pour l'Utilisation des Marques) et procéder à un examen régulier de ces lignes directrices.** Le Secrétariat doit publier et conserver une version actualisée des Lignes Directrices pour l'Utilisation des Marques de Conformité sur le Registre Public CISPE. Les Lignes Directrices pour l'Utilisation des Marques doivent au minimum prévoir les dispositions suivantes :

- L'obligation que la Marque soit appliquée uniquement aux services que l'Organisme de Contrôle a spécifiquement confirmé comme étant conformes aux dispositions du Code lors de son Examen Initial

- L'obligation que la Marque soit utilisée d'une manière claire et qu'elle ne risque pas d'induire en erreur les intervenants sur le marché en ce qui concerne l'adhésion réelle

des CISPs

- Le droit du CISPE de suspendre ou mettre fin à l'utilisation de la Marque si un CISP a utilisé cette Marque sans respecter les exigences prévues par les Lignes Directrices pour l'Utilisation des Marques

- La suspension des droits d'utilisation de la Marque en cas de suspension de l'adhésion des CISPs à l'égard d'un service, et résiliation des droits d'utilisation de la Marque en cas d'exclusion de l'adhésion des CISPs à l'égard d'un service

Une fois que la Déclaration d'Adhésion du CISP a été consignée dans le Registre Public CISPE, le CISP est autorisé à utiliser la Marque tant que sa Déclaration d'Adhésion demeure valable et à condition que le CISP utilise la Marque : (a) exclusivement pour les services couverts par sa Déclaration d'Adhésion, et (b) conformément aux Lignes Directrices pour l'Utilisation des Marques de Conformité. Si le CISP propose des services d'infrastructure cloud différents et si tous les services du CISP ne sont pas couverts par une Déclaration d'Adhésion, le CISP doit veiller à ce que les Marques qu'il utilise identifient, de manière non équivoque, les services spécifiquement couverts par sa Déclaration d'Adhésion.

Pour lever toute ambigüité, l'affichage de la Marque de Conformité ne se substitue pas au respect du RGPD et ne présume pas du respect des dispositions d'un code de conduite assorti d'engagements juridiquement contraignants et exécutoires en application de l'Art 46 du RGPD.

Le Secrétariat enverra une communication à la CNIL deux fois par an en qualité d'Autorité de Contrôle Désignée en vertu du Code, identifiant les nouveaux services des CISPs qui ont été déclarés par un Organisme de Contrôle comme étant conformes aux dispositions du Code pendant la période de six mois concernée et qui sont autorisés à utiliser la Marque de Conformité.

7 Gouvernance

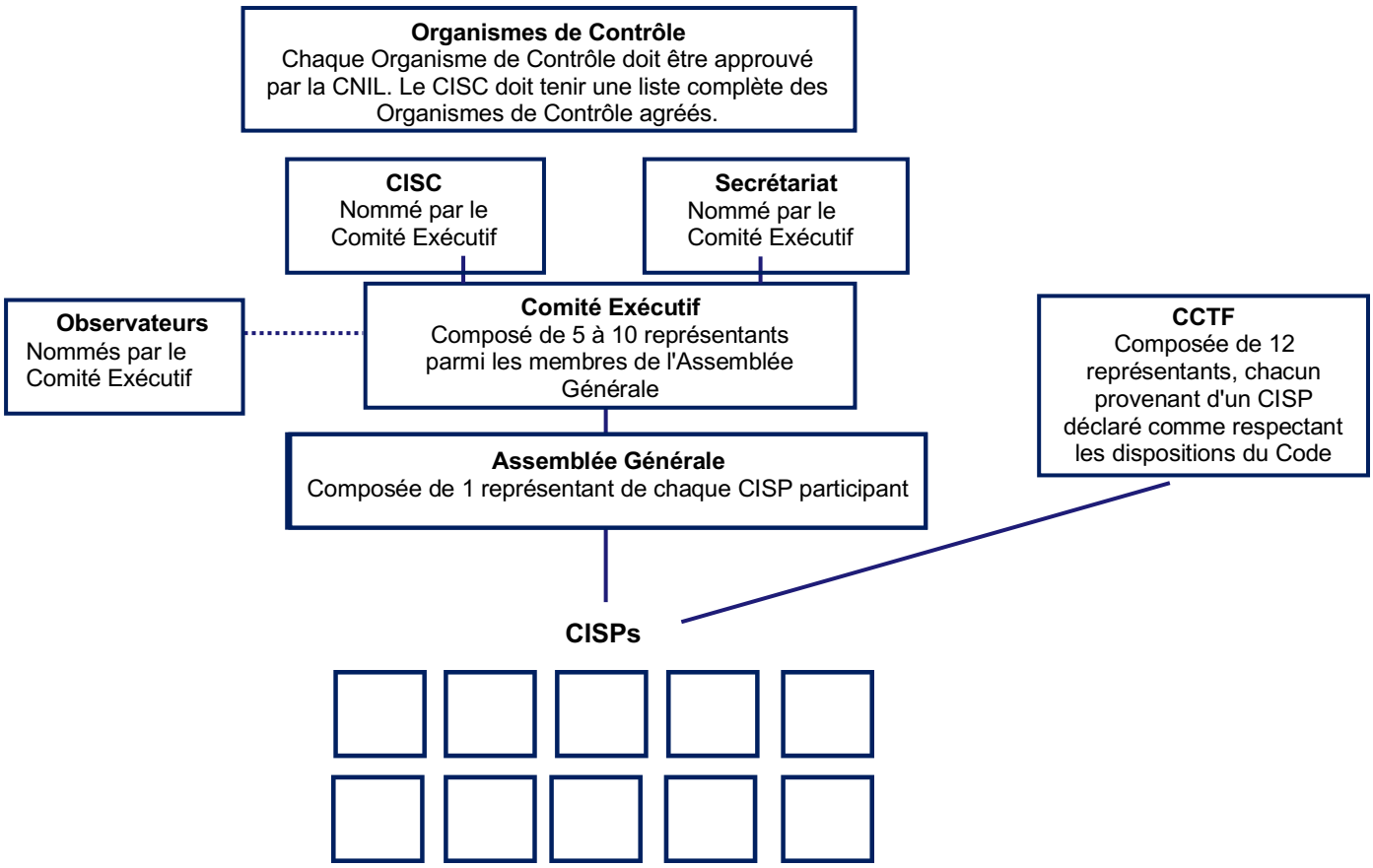
7.1 Structure de gouvernance

L'Association des fournisseurs européens d'infrastructures Cloud **(CISPE)** est responsable de la gouvernance du Code. Le tableau et l'organigramme ci-dessous donnent un aperçu de la structure actuelle du CISPE, y compris ses principaux organes, la composition de ces organes et de leurs principales responsabilités.

Assemblée Générale
Représentation : Chaque organisation participante peut nommer un représentant avec droit de vote à l'Assemblée Générale. Il n'y a pas de limite quant au nombre d'organisations participantes. **Éligibilité :** Pour être éligible à l'Assemblée Générale, une organisation doit (a) fournir un service d'infrastructure cloud à des clients établis dans des territoires de l'EEE, (b) ce service doit offrir aux clients la possibilité de choisir d'utiliser le service pour stocker et traiter leurs données exclusivement dans l'EEE, et (c) proposer au moins un service déclaré comme étant conforme aux dispositions du Code par son Organisme de Contrôle (i) avant sa participation à l'Assemblée Générale si le CISP choisit la procédure d'Adhésion Contrôlée, ou (ii) dans un délai d'un an après sa participation à l'Assemblée Générale, si le CISP choisit la procédure d'Autoévaluation. **Principales responsabilités** : Désigner des représentants du Comité Exécutif ; au moins 10% des membres agissant conjointement peuvent soumettre des propositions de modification du Code au Comité Exécutif ; approuver les modifications du Code.
Comité Exécutif
Représentation : Entre 5 et 10 représentants, chacun étant un membre différent de l'Assemblée Générale. Les représentants du Comité sont élus par l'Assemblée Générale. **Éligibilité :** Pour pouvoir présenter un candidat à l'élection du Comité Exécutif, chaque membre doit (a) être un membre fondateur ou (b) à la fois (i) générer une part significative de ses revenus de services d'infrastructure cloud, et (ii) posséder ou exercer un contrôle effectif sur l'infrastructure informatique cloud physique sous-jacente à ces services d'infrastructure cloud. **Principales responsabilités** : Approbation : (a) admission de nouveaux membres à l'Assemblée Générale, (b) Marques, (c) lignes directrices d'adhésion au Code, et (d) examens et modifications du Code. Désignation : (a) représentants de la CCTF sans droit de vote, (b) Membres du CISC, (c) le Secrétariat, et (d) les Observateurs.
Task Force du Code de Conduite (« CCTF »)
Représentation : Chaque organisation (qu'elle soit membre de l'Assemblée Générale ou non) qui propose au moins un service déclaré comme respectant les dispositions du Code peut nommer un représentant avec droit de vote à la CCTF. La CCTF compte **au maximum douze (12) membres** possédant (i) une expertise dans le domaine de l'informatique cloud et/ou de la protection des données, et/ou (ii) une bonne maîtrise des « business models » de l'informatique cloud. Chaque membre de l'Assemblée Générale et du Comité Exécutif peut nommer des représentants sans droit de vote à la CCTF (ex. : universitaires ou experts, représentants d'associations d'utilisateurs de services d'infrastructures informatiques cloud, des représentants de la Commission européenne). Un tiers (y compris un client final) qui souhaite désigner un représentant sans droit de vote doit envoyer une demande écrite au Comité Exécutif pour obtenir une invitation. **Éligibilité :** Les représentants doivent justifier : (a) d'une expertise dans le domaine de l'informatique cloud et/ou de la protection des données, et/ou (b) d'une bonne maîtrise des « business models » de l'informatique cloud. **Principales responsabilités** : Examiner le Code au regard de l'évolution de la législation européenne applicable en matière de protection des données ; proposer des modifications du Code au Comité Exécutif ; établir des lignes directrices d'adhésion au Code ; exprimer un avis non contraignant sur les propositions de modification du Code présentées par le Comité Exécutif, recommander des auditeurs, des normes et des mécanismes de certification appropriés pour démontrer que les entités respectent le Code ; établir des Marques et développer des lignes directrice pour l'utilisation des marques de conformité.
Comité de Surveillance Indépendant du Code (« CISC »)
Représentation : Trois membres nommés par le Comité Exécutif. **Éligibilité :** Experts indépendants ayant reçu une formation universitaire, technique ou juridique. Ces experts doivent avoir l'expérience nécessaire pour engager le contact avec les Autorités de Contrôle, les entreprises et les personnes concernées. **Principales responsabilités** : Tenir la liste des organisations autorisées par la CNIL à agir en tant qu'Organismes de Contrôle ; prêter assistance aux Organismes de Contrôle dans le contrôle de l'application de la Procédure de Réclamation ; prêter assistance aux Organismes de Contrôle dans la bonne application du Code ; examiner régulièrement le fonctionnement du Code au travers d'ateliers avec les Organismes de Contrôle.
Organisme de Contrôle
Représentation : Nommé à partir d'une liste de CISP conservée par le CISC. **Éligibilité :** Cf. ci-dessous

Principales responsabilités : contrôler la conformité des CISPs aux dispositions du Code ; examiner les réclamations concernant la non-conformité des services par rapport au Code ; prendre des mesures d'exécution à l'encontre de tout CISP qui ne respecte le Code ; signaler toute préoccupation concernant le fonctionnement du Code à une Autorité de Contrôle compétente.	
Secrétariat **Représentation** : Nommé par le Comité Exécutif. **Principales responsabilités** : Examiner les déclarations d'adhésion au Code ; publier des informations sur le Registre Public CISPE et maintenir à jour ces informations ; assurer l'administration quotidienne du CISPE.	**Observateurs** Le Comité Exécutif peut inviter des représentants non-membres de l'Assemblée Générale à y participer en tant qu'observateurs sans droit de vote.

Organigramme de la structure



7.2 Contrôle, Réclamations et Mesures d'Exécution

(a) Structure du Contrôle et Organismes de Contrôle

Le contrôle du Code est structuré comme suit :

- Tous les Organismes de Contrôle doivent être agréés par la CNIL en sa qualité d'Autorité de Contrôle Désignée.
- Le CISC doit tenir une liste des organisations qui ont été agréées par la CNIL. Ces organisations peuvent être nommées par les CISPs pour agir en qualité d'Organisme de Contrôle ;
- L'Organisme de Contrôle est chargé de s'assurer du contrôle obligatoire de la conformité des CISPs avec le Code. Chaque CISP doit sélectionner un Organisme de Contrôle à partir de la liste tenue par le CISC ;
- Une Procédure de Réclamations doit être établie conformément aux principes énoncés ci-après ; et
- Le CISC doit prêter assistance aux Organismes de Contrôle pour garantir la bonne application du Code par chaque Organisme de Contrôle, et contrôler l'application de la Procédure de Réclamation.

Comité de Surveillance Indépendant du Code (« CISC »)

Le CISC doit examiner régulièrement la bonne mise en œuvre du Code, y compris la Check-list de Conformité, et émettre des recommandations à la CCTF et au Comité Exécutif sur les éventuelles modifications qu'il convient d'apporter au Code.

Le CISC doit dresser et tenir une liste d'organisations tiers indépendantes possédant les compétences requises pour être sélectionnées comme Organisme de Contrôle par les CISPs car elles sont dûment agréées par l'Autorité de Contrôle compétente. Ces organisations doivent démontrer :

a) qu'elles possèdent un niveau d'expertise approprié au regard de l'objet du Code et de l'environnement cloud. Un Organisme de Contrôle peut faire valoir ces compétences en démontrant : (i) son expérience en matière de certification selon les standards de référence tels que ISO 27001, 27017 et 27018 ou d'autres standards équivalents ; ou (ii) toute autre expérience équivalente en matière d'audit de la sécurité de l'information ou de la protection des données à caractère personnel;

b) qu'elles sont des Organismes de Contrôle agréés par la CNIL agissant en qualité d'Autorité de Contrôle désignée ;

c) qu'elles agissent en toute indépendance au regard de l'objet du Code à la satisfaction d'une Autorité de Contrôle compétente ;

d) qu'elles ont établi des procédures leur permettant d'évaluer l'éligibilité du CISP concerné à appliquer le Code, de contrôler le respect des dispositions du Code par le CISP et d'examiner périodiquement les activités des CISPs. Un Organisme de Contrôle peut prouver qu'il a mis en place ces procédures en démontrant : (i) l'existence de procédures de certification selon les standards de référence tels que ISO/IEC 27001, 27017 et 27018 ou d'autres standards équivalents ; ou (ii) toute autre expérience équivalente en matière d'audit de la sécurité de l'information ou de la protection des données à caractère personnel ;

e) qu'elles ont établi des procédures et des structures pour traiter les réclamations relatives aux violations du Code ou à la manière dont le code a été ou est appliqué par un CISP comme il est indiqué ci-après ;

f) que les procédures et les structures mentionnées au paragraphe e) ci-dessus ont été établies et qu'elles sont transparentes et accessibles aux personnes concernées et au public ; et

g) pour la satisfaction d'une Autorité de Contrôle compétente, que leurs tâches et missions n'entraînent pas de conflits d'intérêt.

Pour lever toute ambigüité, l'éligibilité d'un Organisme de Contrôle est déterminée par la procédure d'accréditation de l'Autorité de Contrôle Désignée. Les critères visés ci-dessus ont vocation à indiquer l'indépendance, l'expérience et les qualifications attendues des Organismes de Contrôle par CISPE lui-même. Cependant, en cas de divergence entre les critères susvisés et les critères d'accréditation de la CNIL pour les Organismes de Contrôle, ces derniers prévaudront.

La liste des Organismes de Contrôle doit être publiée et maintenue sur le Registre Public CISPE. Seules les organisations qui ont obtenu une accréditation d'une Autorité de Contrôle désignée peuvent figurer dans le Registre Public CISPE.

Le CISC doit communiquer avec les Organismes de Contrôle et leur prêter assistance pour s'assurer que chacun applique les dispositions de Code de façon cohérente. Il doit organiser les ateliers annuels et encourager les Organismes de Contrôle à y participer pour discuter de chacun de leur Rapport d'Audit Annuel (cf. Section 7.2(c)), y compris les difficultés pratiques auxquelles les Organismes de Contrôle ont été confrontés en examinant l'application des dispositions du Code (les « **Ateliers des Organismes de Contrôle »**). Après chaque Atelier d'un Organisme de Contrôle, le CISC doit communiquer les résultats de ces ateliers, notamment les meilleures pratiques adoptées, et des exemples des décisions d'exécution prises par les Organismes de Contrôle, y compris les conflits potentiels et les mesures identifiées pour y remédier. Ces documents d'orientation doivent être distribués aux nouveaux et aux existants Organismes de Contrôle pour faciliter la bonne application du Code.

Si nécessaire, le CISC fournira des conseils aux Organismes de Contrôle, de manière spontanée, ou en réponse à une demande d'un Organe de Contrôle. Ces conseils n'ont pas vocation à s'imposer à l'Organisme de Contrôle, mais ils visent à aider l'Organisme de Contrôle dans son application des dispositions du Code et à maintenir une certaine cohérence entre les approches utilisées par les Organismes de Contrôle.

Le CISC se compose de 3 experts indépendants ayant reçu une formation universitaire, technique ou juridique (les **Membres du CISC**). Les Membres du CISC doivent avoir l'expérience nécessaire pour engager le contact avec les Autorités de Contrôle, les entreprises et les personnes concernées. Les Membres du CISC sont nommés par le Comité Exécutif du CISPE pour une durée fixe de trois ans. Les Membres du CISC ne doivent pas avoir conclu d'accords de conseil avec un CISP, et ne peuvent pas être membres du Comité Exécutif du CISPE. Le Comité Exécutif examine en permanence l'expertise et la performance des Membres du CISC et remplace ces membres dès lors qu'ils ne satisfont plus aux exigences mentionnées ci-dessus.

Chaque Membre du CISC doit s'interdire d'agir d'une manière qui peut, ou pourrait, générer un risque de conflit d'intérêt direct ou indirect ou être en contradiction avec les intérêts du Code. Si un Membre du CISC, ou le Comité Exécutif, prend connaissance de l'existence d'un conflit d'intérêt, le Membre du CISC doit se récuser du CISC, et le Comité doit désigner un remplaçant. Si le Comité Exécutif a connaissance d'un tel conflit, le Comité Exécutif doit demander au Membre du CISC de se récuser. Si le Membre du CISC refuse de se récuser lui-même, le Comité Exécutif le récusera. Tout Membre du CISPE peut à tout moment

contacter le Comité Exécutif s'il a des soupçons de conflit d'intérêt de la part d'un Membre du CISC.

Le Secrétaire Général du CISPE joue un rôle d'observateur général en ce qui concerne le respect des activités du CISC, et il exerce les tâches administratives dans le cadre des activités du CISC et des Organismes de Contrôle dans le respect des dispositions du Code.

Organismes de Contrôle, contrôle proactif

L'Article 40(4) du RGPD dispose qu'un organisme qui répond aux critères de l'Article 41(1) du RGPD, est tenu de procéder au contrôle obligatoire du respect des dispositions du Code par les CISPs qui s'engagent à l'appliquer et à y adhérer.

Chaque CISP qui s'engage à appliquer le Code est contrôlé par l'Organisme de Contrôle qu'il a lui-même sélectionné pour vérifier qu'il respecte les dispositions du Code. L'Organisme de Contrôle est sélectionné par le CISP parmi la liste tenue par le CISC. Le CISP doit être libre de sélectionner un Organisme de Contrôle à partir de la liste tenue par le CISC. Il appartient à l'Organisme de Contrôle d'accepter ou non d'agir en cette qualité pour un CISP. Le CISP doit rémunérer son Organisme de Contrôle pour toutes les activités qu'il exerce en rapport avec le contrôle de la conformité du CISP aux dispositions du Code, et la gestion des réclamations formées à l'encontre de ce CISP. Chaque Organisme de Contrôle doit être agréé par la CNIL, et la rémunération versée par le CISP à l'Organisme de Contrôle ne doit pas entraver l'indépendance et l'efficacité de l'Organisme de Contrôle. Dans l'hypothèse où un CISP ne peut pas nommer un Organisme de Contrôle en raison du refus de ce dernier fondé sur des critères objectifs, le CISC organisera une médiation entre le CISP et l'Organisme de Contrôle afin qu'ils trouvent une solution à leurs problèmes potentiels. En cas d'échec de cette médiation, le CISC demandera à un autre Organisme de Contrôle mentionné sur sa liste de prêter assistance au CISP ou s'efforcera d'ajouter d'autres Organismes de Contrôle à cette liste qui seraient susceptibles d'agir en qualité d'Organisme de Contrôle pour le CISP. Si à l'issue de cette procédure, aucun Organisme de Contrôle n'accepte la mission d'agir en qualité d'Organisme de Contrôle pour le CISP, le CISC demandera conseil à l'Autorité de Contrôle compétente.

L'Organisme de Contrôle est chargé d'évaluer que chacun des CISPs qu'il contrôle respecte les dispositions du Code. Cette évaluation doit être effectuée par une équipe d'experts qui (collectivement) est capable de démontrer les compétences techniques et juridiques du CISP.

Cette expertise technique peut se justifier, entre autres, comme suit :

- au moins trois ans d'expérience dans le domaine de la sécurité de l'information, y compris l'obtention des certifications de sécurité appropriées (ex : ISO/IEC 27001 Lead Auditor, Certified Information Systems Auditor (CISA) de l'ISACA, Certified Information Security Manager (CISM) de l'ISACA) ; ou

- une formation dans le domaine de la sécurité de l'information complétée par au moins une année d'expérience dans ce domaine.

L'expertise juridique peut se justifier, entre autres, comme suit :

- au moins deux ans d'expérience confirmée dans le domaine de la protection des données et de la vie privée et l'obtention des certifications requises (ex : IAPP CIPP/E), ou

- une formation en droit accompagnée de la certification requise en matière de protection des données (ex : CIPP/E).

L'évaluation de la conformité aux dispositions du Code comprend deux aspects : l'évaluation des mesures de sécurité techniques et opérationnelles et l'évaluation des

autres exigences du Code en matière de protection des données et de transparence :

1. **Évaluation des mesures de sécurité techniques et organisationnelles :** L'Annexe A (Responsabilités en matière de Sécurité) décrit les responsabilités en matière de sécurité qui incombent aux CISPs. Si le CISP adopte des mesures appropriées pour s'acquitter de ces responsabilités et si ces mesures sont jugées conformes à la norme ISO/IEC 27001/27018 (ou un standard de référence équivalent), alors le CISP sera réputé avoir mis en œuvre les mesures de sécurité techniques et organisationnelles qui satisfont aux exigences du Code. Pour les CISPs qui ne possèdent pas l'accréditation ISO/IEC 27001/ ISO/IEC 27018, une évaluation sera effectuée par rapport aux Exigences du Code définies à l'Annexe B au moyen d'une méthodologie d'évaluation définie établie par l'Organisme de Contrôle.

2. Évaluation des autres exigences du Code en matière de protection des données et de transparence : Le Code impose des exigences aux CISPs en matière de protection des données et de transparence décrites aux Sections 4 et 5.

La méthode utilisée pour contrôler le respect (i) des exigences en matière de protection des données et de transparence du Code et (ii) des mesures techniques et organisationnelles en matière de sécurité de l'Annexe A s'appuiera sur le cadre de contrôle de l'Annexe B du Code, qui utilise des méthodologies d'évaluation similaires à ISO/IEC 27001/ISO/IEC 27018, ou des standards de référence équivalents.

Conformément aux indications de la Section 6, la première évaluation de la conformité aux dispositions du Code effectuée par l'Organisme de Contrôle aura lieu avant que le CISP ne délivre sa Déclaration d'Adhésion, ou dans l'année qui suit sa délivrance, selon la procédure d'adhésion choisie par le CISP. Par la suite, l'Organisme de Contrôle contrôlera le respect de chaque CISP sur une base annuelle. Après chaque évaluation, l'Organisme de Contrôle doit produire un rapport qui synthétise ses conclusions concernant la conformité du CISP **(« Rapport »)** et doit remettre ce Rapport au CISP et à CISPE. Si le Rapport atteste que le CISP a respecté les dispositions du Code, CISPE doit confirmer la Déclaration d'Adhésion du CISP en application de la Section 6.

Si le Rapport démontre que le CISP n'a pas respecté les dispositions du Code, l'Organisme de Contrôle doit s'appuyer sur la Matrice d'Exécution décrite au paragraphe 7.2(b) ci-dessous pour déterminer les sanctions appropriées.

Toutes les décisions prises par un Organisme de Contrôle doivent être documentées. Cela inclura, la décision elle-même, les circonstances dans lesquelles elle a été prise et l'exposé des motifs à l'origine de cette décision, y compris tous les aspects relatifs à l'interprétation du Code. Les Organismes de Contrôle peuvent demander le soutien du CISC à tout moment en ce qui concerne les questions d'interprétation du Code.

Les CISPs doivent coopérer avec leur Organisme de Contrôle et lui fournir toutes les informations que ce dernier estime raisonnablement nécessaires pour exécuter ses missions en vertu du Code.

Procédure de Réclamation

Les réclamations introduites par un client, une personne concernée ou tout autre CISP à propos de la conformité des services couverts par la Déclaration d'Adhésion aux Exigences du Code d'un CISP seront traitées comme suit :

(a) Les réclamations doivent avant tout être soumises à l'Organisme de Contrôle et à CISPE pour alléger les tâches administratives. Si la réclamation n'est adressée qu'à CISPE, CISPE transmet ensuite ces réclamations à l'Organisme de Contrôle compétent pour examen : CISPE n'exerce aucun pouvoir de discrétion en ce qui concerne le choix des réclamations à

transmettre à un Organisme de Contrôle. Si la réclamation n'est adressée qu'à l'Organisme de Contrôle, celui-ci doit envoyer une copie de cette réclamation à CISPE pour des raisons de suivi ;

(b) L'Organisme de Contrôle enquête sur les services et/ou mesures spécifiques qui sont présumés avoir été enfreints dans la réclamation, en utilisant ses propres processus d'enquête, puis prend sa décision ;

(c) L'Organisme de Contrôle doit communiquer sa décision sur la réclamation au Comité Exécutif, y compris les détails de toute mesure d'exécution prise à l'encontre du CISP en cause ;

(d) Les mesures d'exécution doivent être prises conformément à la Matrice d'Exécution décrite au paragraphe (b) ci-après.

Le Comité Exécutif du CISPE doit remettre au CISC une copie de toutes les réclamations reçues et de tous les rapports transmis par les Organismes de Contrôle, mais le CISC ne jouera aucun rôle dans la décision relative aux réclamations individuelles. Le CISC doit contrôler le fonctionnement de la Procédure de Réclamation et fournir un rapport annuel au Comité Exécutif du CISPE sur les réclamations reçues et sur la manière dont elles ont été traitées. Le rapport doit décrire, par exemple, les statistiques relatives au nombre de réclamations soumises et les principaux thèmes émergents concernant les types de réclamations déposées. Le CISC doit également coopérer avec les Organismes de Contrôle pour s'assurer que chacun d'eux applique les dispositions du Code de façon cohérente conformément au paragraphe (c) ci-après, et conformément aux principes suivants à l'égard d'une réclamation en particulier :

- L'Organisme de Contrôle peut demander conseil à l'égard de toute question relative à l'interprétation du Code, si cela est nécessaire pour traiter une réclamation, sans se reporter aux faits qui entourent spécifiquement cette réclamation
- Le CISC est en droit de communiquer à l'Organisme de Contrôle des informations générales concernant le traitement de dossiers analogues dans le contexte d'autres examens ou du traitement d'autres réclamations par les Organismes de Contrôle. Dans l'hypothèse où aucun dossier analogue n'existe, le CISC peut, si cela s'avère nécessaire, donner un avis général et non contraignant, sans se reporter aux faits spécifiques de la réclamation
- Seul l'Organisme de Contrôle est autorisé à prendre une décision sur chaque réclamation individuelle.

(b) <u>Mesures d'Exécution</u>

Si l'Organisme de Contrôle détermine dans la préparation de sa réponse à une réclamation, ou dans la préparation d'un Rapport annuel concernant un CISP, qu'il nécessite des documents ou des clarifications complémentaires, il peut demander des renseignements complémentaires au CISP. Le CISP doit répondre à cette demande de renseignements complémentaires dans le délai raisonnable spécifié par l'Organisme de Contrôle dans sa demande.

Si l'Organisme de Contrôle détermine dans sa réponse à une réclamation, ou dans un Rapport annuel concernant un CISP, que ce CISP n'a pas respecté les Exigences du Code, alors l'Organisme de Contrôle utilisera la Matrice d'Exécution ci-dessous pour déterminer les mesures de sanction appropriées :

Matrice d'Exécution :

Étape	Situation	Sanction
1. Premier Avertissement Écrit	L'Organisme de Contrôle constate que le CISP n'a pas respecté certaines exigences du Code.	L'Organisme de Contrôle adresse au CISP un avertissement écrit (par courrier ou sous forme électronique) avec accusé de réception, Indiquant que : • les exigences qui n'ont pas été respectées et les conclusions détaillées de l'Organisme de Contrôle à cet égard ; • les mesures correctives à prendre par le le CISP; et • que les mesures correctives doivent être prises dans un délai de 60 jours après réception de l'avertissement écrit ou un constat de non-conformité sera publié, (le « **Premier Avertissement Écrit »**). Dans un délai de 60 jours après réception du Premier Avertissement Écrit, le CISP doit : (i) se soumettre à un nouvel examen par l'Organisme de Contrôle pour déterminer s'il a respecté les exigences en question ; ou (ii) soumettre un exposé écrit à l'Organisme de Contrôle contenant d'autres éléments de preuve, ou arguments écrits en réponse qui, s'ils sont jugés recevables, démontreraient sa conformité. Si, à la suite de ce nouvel examen : a) l'Organisme de Contrôle conclut que le CISP a réparé son manquement, ou constate sur la base d'autres déclarations que le CISP a respecté les exigences du Code, le dossier sera clos. b) b) l'Organisme de Contrôle conclut que le CISP n'a pas réparé son manquement, l'Organisme de Contrôle doit prendre les mesures décrites à l'Étape 2.
2. Second Avertissement Écrit et publication du non-respect	L'Organisme de Contrôle constate que le CISP n'a pas respecté les exigences du Code dans un délai de 60 jours après réception du Premier Avertissement Écrit.	L'Organisme de Contrôle adresse au CISP un second avertissement écrit (par courrier ou sous forme électronique) avec accusé de réception, indiquant : • les dispositions du Code qui ne sont toujours pas respectées et des précisions sur les mesures correctives qui, à ce jour, demeurent inadéquates ; • les mesures correctives que le CISP doit adopter ; et • qu'un constat de non-conformité sera publié ; et • que les mesures correctives doivent être

		prises dans un délai de 30 jours après réception du second avertissement écrit, à défaut de quoi la Déclaration d'Adhésion du CISP sera suspendue, (le « **Second Avertissement Écrit** »**).** Après la délivrance du Second Avertissement Écrit, l'Organisme de Contrôle doit remettre au Comité Exécutif du CISPE une déclaration écrite expliquant que le CISP n'a pas respecté les exigences du Code et qu'il dispose d'un délai de 30 jours pour réparer son manquement. CISPE doit publier cette déclaration sur son site internet. Au plus tard 30 jours après réception du Second Avertissement Écrit, le CISP doit se soumettre à un nouvel examen par l'Organisme de Contrôle pour déterminer s'il a respecté les exigences en question. Si, après ce nouvel examen : a) l'Organisme de Contrôle détermine que le CISP a réparé son manquement, le dossier sera clos et un avis de clôture sera publié sur le site internet du CISPE. b) l'Organisme de Contrôle conclut que le CISP n'a pas réparé son manquement, l'Organisme de Contrôle prend les mesures décrites à l'Étape 3.
3. Suspension de la Déclaration d'Adhésion d'un CISP	L'Organisme de Contrôle constate que le CISP n'a pas respecté les exigences du Code dans un délai de 30 jours après réception du Second Avertissement Écrit.	L'Organisme de Contrôle informe par écrit le Comité Exécutif du CISPE que la Déclaration d'Adhésion du CISPE doit être suspendue. Cette suspension est effective jusqu'à ce que le CISP puisse démontrer à l'Organisme de Contrôle qu'il a remédié au manquement concerné.

4. Exclusion du service d'un CISP du Code	En cas de violation grave ou persistante des dispositions du Code, l'Organisme de Contrôle peut décider d'exclure du Code le service d'un CISP.	L'Organisme de Contrôle informe par écrit le Comité Exécutif du CISPE que le service du CISP a été exclu du Code. La Déclaration d'Adhésion du CISP et les documents à l'appui cesseront immédiatement de faire effet.

Dans chaque cas, l'Organisme de Contrôle doit indiquer la sanction qu'il convient d'imposer au CISP dans un rapport écrit.

Dans l'hypothèse où la Déclaration d'Adhésion du CISP doit être suspendue ou le service du CISP doit être exclu du Code, l'Organisme de Contrôle doit en informer par écrit le Comité Exécutif de CISPE et le Comité Exécutif de CISPE veillera à ce que la suspension ou l'exclusion soit mise en œuvre. Le Comité Exécutif du CISPE transmettra les avis de sanction au CISC.

Lorsque la Déclaration d'Adhésion d'un CISP est suspendue ou lorsque le service d'un CISP est exclu du Code :

- le Secrétariat doit, dans les meilleurs délais, supprimer du Registre Public CISPE le(s) service(s) affectés mentionnés dans la Déclaration d'Adhésion du CISP et informer l'Autorité de Contrôle Désignée pour le Code de cette suspension ou exclusion ;
- l'Organisme de Contrôle doit aviser par écrit le CISP que sa Déclaration d'Adhésion sera suspendue, ou que le service sera exclu du Code dans un délai de 7 jours ouvrés et que le CISP doit cesser d'utiliser la Marque de Conformité associée au service affecté au plus tard 7 jours ouvrés après réception de cet avis ; et
- le CISP doit cesser d'utiliser la Marque de Conformité associée au service affecté au plus tard 7 jours ouvrés après réception de l'avis de l'Organisme de Contrôle. CISPE est le propriétaire de la Marque de Conformité et toute utilisation de cette Marque sans son autorisation sera considérée comme une contrefaçon de marque. CISPE prendra les mesures nécessaires pour faire valoir cette utilisation abusive de la Marque de Conformité.

En cas de suspension, ces mesures doivent s'appliquer jusqu'à ce que la suspension soit levée. Lorsque la Déclaration d'Adhésion d'un CISP est suspendue, le CISP est effectivement exclu du Code jusqu'à ce qu'il répare son manquement et que l'Organisme de Contrôle vérifie que le manquement ait bien été réparé.

Dans le cas d'une exclusion, la Déclaration d'Adhésion concernée cesse définitivement de faire effet. Après l'exclusion du service d'un CISP, le CISP peut de nouveau soumettre ce service au Code. Dans ce cas, il doit former une nouvelle demande en utilisant la procédure d'adhésion définie à la Section 6. Le CISP doit indiquer dans sa nouvelle Déclaration d'Adhésion que ce service a déjà fait l'objet d'une exclusion du Code.

Les mesures d'exécution susvisées sont :

- le seul et unique recours en cas de non-respect des Exigences du Code

par un CISP ;

- sans préjudice des droits du client en vertu de la législation européenne applicable en matière de protection des données ou en application des stipulations du Contrat de Services ; et

- sans préjudice du droit du CISP de contester la décision de l'Organisme de Contrôle par tous les moyens dont il peut se prévaloir en vertu du droit.

Le droit pour un client d'introduire une réclamation ne peut, à lui seul, conférer au client des droits ou recours directs à l'encontre du CISP ou du CISPE en vertu du Code ou en relation avec celui-ci. CISPE décline toute responsabilité quant au respect des dispositions du Code par un CISP. CISPE ne sera pas non plus responsable vis-à-vis d'une partie d'un quelconque motif pour agir ou de toute théorie de responsabilité en cas de pertes ou de dommages causés par un acte ou une omission du CISPE ou d'un CISP en rapport avec le Code.

Lorsqu'un Organisme de Contrôle émet un Second Avertissement Écrit, ou lorsque la Déclaration d'Adhésion d'un CISP est suspendue ou lorsque le service d'un CISP est exclu du Code, l'Organisme de Contrôle doit en rendre compte à la CNIL, en sa qualité d'Autorité de Contrôle compétente. Ces comptes rendus doivent contenir des informations sur la non-conformité des CISPs, sur l'absence de mise en œuvre par le CISP des mesures correctives requises par l'Organisme de Contrôle, et sur les actions adoptées en réponse par l'Organisme de Contrôle. Dans l'hypothèse où, après la délivrance d'un Second Avertissement Écrit, l'Organisme de Contrôle constate que le CISP a réparé son manquement, l'Organisme de Contrôle avisera la CNIL de la clôture du dossier.

(c) Rapports de suivi

Pour faciliter l'élaboration du Code et rendre son examen plus efficace, l'Organisme de Contrôle doit soumettre un Rapport de Suivi Annuel au Comité Exécutif de CISPE et à la CNIL, en sa qualité d'Autorité de Contrôle Désignée. Ce Rapport de Suivi Annuel décrira en détail les dispositifs de contrôle et les méthodes d'audit appliqués par l'Organisme de Contrôle, les statistiques relatives au résultat des réclamations qu'il a traitées et des examens qu'il a réalisés (y compris le nombre de premiers avertissements écrits qu'il a remis aux CISPs), ainsi que les difficultés pratiques auxquelles il a été confronté en examinant l'application des dispositions du Code par les CISPs placés sous son contrôle (par exemple, les difficultés à évaluer comment un CISP met en œuvre les exigences de l'Annexe A).

Tous les trois ans (à moins que le CISC et les Organismes de Contrôle en décident autrement), le CISC doit procéder à une analyse pour évaluer les Rapports de Suivi Annuels de chaque Organisme de Contrôle et s'assurer qu'ils s'alignent de façon cohérente sur l'évaluation des meilleures pratiques et l'application des exigences du Code. Il doit également émettre des recommandations appropriées aux Organismes de Contrôle pour renforcer cette cohérence.

7.3 Révision du Code

(a) Révision du Code

La CCTF continuera de réviser le Code au fur et à mesure de l'évolution de la législation européenne applicable en matière de protection des données et, en particulier, au regard de l'interprétation du RGPD après son entrée en vigueur.

La CCTF a vocation à effectuer une révision complète du Code tous les deux ans pour refléter les développements juridiques et technologiques ainsi que l'évolution des standards de référence. Par exemple, la CCTF doit prendre en compte l'évolution des meilleures pratiques en s'appuyant sur les certifications adoptées sur le marché du cloud, telles que

la norme ISO/IEC 27701, ou d'autres nouveaux standards.

Le Comité Exécutif peut demander à la CCTF de procéder à une révision spécifique du Code, en lui adressant une demande conjointe par au moins deux membres du Comité Exécutif. Le Comité Exécutif peut entamer cette révision de sa propre initiative ou à la demande de :

- au moins 10% des membres de l'Assemblée Générale ;
- un Organisme de Contrôle ;
- une Autorité de Contrôle compétente agissant en sa qualité officielle ; ou
- une association représentant les intérêts des utilisateurs de services d'infrastructure cloud agissant en sa qualité officielle.

Toutes les propositions de modification du Code doivent être examinées et considérées rapidement.

(b) Modifications du Code

Après un examen, la CCTF peut soumettre au Comité Exécutif des propositions de modification du Code. Ces modifications doivent être adoptées par CISPE avant de devenir effectives.

Pour être adoptée par CISPE, une modification du Code doit être :

- présentée au Comité Exécutif et à l'Assemblée Générale ;
- approuvée par le Comité Exécutif ; et
- adoptée par une résolution spéciale de l'Assemblée Générale.

Avant l'adoption par CISPE, le Comité Exécutif doit soumettre les modifications ou développements du Code à l'Autorité de Contrôle Désignée pour approbation. En outre, le Comité Exécutif peut également décider de soumettre une modification du Code à l'examen et l'observation de l'association qui représente les intérêts des utilisateurs de services d'infrastructure cloud.

Dans les meilleurs délais après qu'une modification du Code ait été adoptée par CISPE, le Secrétariat doit publier une version actualisée du Code sur le Registre Public CISPE.

Les CISPs ont l'obligation de renouveler ou reconfirmer leurs Déclarations d'Adhésion dans l'année qui suit la publication de la version actualisée du Code sur le Registre Public CISPE. Un CISP qui démontre que son service respecte les Exigences du Code au moyen de la délivrance d'une approbation existante d'un Organisme de Contrôle et d'une Check-list de Conformité, ainsi que de sa Déclaration d'Adhésion, peut s'appuyer sur l'approbation existante et sur la Check-list de Conformité pour prouver que son service respecte la version actualisée du Code, sans avoir à se soumettre à un nouvel audit, ou à un audit séparé, dans le but d'obtenir une nouvelle approbation ou un nouveau rapport, à condition que l'approbation existante et la Check-list de Conformité prouvent que le service du CISP respecte les exigences de la version actualisée du Code.

Annexe A – Pratiques techniques et organisationnelles en matière de sécurité et obligations en matière de sécurité

Introduction

La présente Annexe définit un ensemble minimum de pratiques techniques et organisationnelles en matière de sécurité et les responsabilités en matière de sécurité que le CISP doit prendre en compte pour définir et adopter un ensemble de mesures visant à protéger les données à caractère personnel contre le traitement non autorisé et la perte, l'accès ou la divulgation, de manière accidentelle ou illicite. Les services du CISP qui sont déclarés comme étant conformes aux dispositions du Code doivent respecter ces pratiques et responsabilités, documenter les mesures adoptées et seront soumis à l'examen de l'Organisme de Contrôle. Des exemples spécifiques des mesures que le CISP doit adopter pour s'acquitter de ses responsabilités en matière de sécurité figurent dans les tableaux à la fin de chaque paragraphe. Ces exemples sont fournis à titre d'illustration uniquement et n'ont pas de caractère normatif ou exécutoire. Les mesures, techniques et contrôles spécifiques qu'un CISP peut mettre en œuvre pour s'acquitter de ses responsabilités en matière de sécurité varieront en fonction de la taille et de la complexité de chaque CISP, et ces mesures de sécurité sont susceptibles d'être ajustées au fil du temps pour suivre les évolutions techniques. Cependant, un CISP qui adhère aux dispositions du présent Code de Conduite est invité à se fonder sur la norme ISO/IEC 27002 comme document d'orientation pour mettre en œuvre les contrôles de sécurité de l'information généralement admis. Les CISPs qui sont accrédités ISO/IEC 27001 / ISO/IEC 27018 / ISO/IEC 27017, ou tout standard de référence équivalent, seront réputés respecter les exigences de la présente Annexe A. Le Code reconnaît que les nouveaux standards de référence pourront s'appliquer, compte tenu de l'évolution du marché, et le Code sera révisé de temps à autre pour fournir d'autres lignes directrices sur les normes de sécurité applicables qu'il convient de prendre en compte. Les exemples de contrôles ISO qui seraient susceptibles de respecter les exigences prévues par la présente Annexe A sont exposés ci-après.

(1) Gestion de la Sécurité des Informations

(a) Responsabilités du CISP

Le CISP doit avoir une direction et un soutien clairs au niveau de la direction pour la sécurité du service.

Le CISP doit mettre en place un ensemble de politiques sur la sécurité de l'information approuvées par la direction qui régissent la sécurité du service.

Le CISP doit mettre en œuvre un système de gestion de la sécurité de l'information ou un dispositif équivalent. Le champ d'application du système de gestion de la sécurité de l'information doit couvrir le service.

Le CISP doit désigner un ou plusieurs membres de son personnel pour coordonner et assumer la responsabilité du système de gestion de la sécurité de l'information.

(b) Responsabilités du client

Le client devrait désigner un point de contact pour les questions de sécurité en rapport avec son utilisation du service d'infrastructure cloud.

Le client devrait procéder à une évaluation du risque pour déterminer si le service d'infrastructure cloud est en adéquation avec les activités de traitement de données que le client souhaite exécuter sur la base de la législation européenne applicable en matière de protection des données.

(c) Exemples de mesures que le CISP peut adopter

Le tableau ci-dessous dresse une liste des exemples de mesures qu'un CISP peut adopter pour s'acquitter de ses responsabilités en ce qui concerne la gestion de la sécurité de l'information :

Exemples :
• S'assurer que les politiques et procédures sur la sécurité de l'information couvrent, au minimum : (a) la portée et les limites du programme sur la sécurité de l'information, y compris l'activité, l'organisation, les emplacements, les actifs et la technologie ; (b) les politiques d'utilisation qui définissent un usage approprié des technologies importantes comme les appareils mobiles, la technologie sans fil, les e-mails et internet ; et (c) les tâches et missions de gestion et de mise en œuvre des politiques sur la sécurité de l'information. • S'assurer que le cadre de la politique sur la sécurité de l'information du CISP couvre, au minimum, les aspects suivants : (a) gestion d'actifs ; (b) ressources humaines ; (c) contrôles d'accès ; (d) sécurité physique et environnementale ; (e) cycle de vie du développement d'un système ; (f) gestion des incidents ; (g) continuité de l'exploitation ; (h) conformité ; et (i) utilisation d'un appareil mobile. • Communiquer les politiques sur la sécurité de l'information à tous les membres du personnel du CISP (y compris les fournisseurs et partenaires commerciaux), ainsi que les mises à jour régulières. • Développer des procédures opérationnelles visant à orienter l'exploitation des systèmes et des services dans l'environnement du CISP, le cas échéant.

(d) Exigences ISO correspondantes

Les CISPs qui adhèrent aux dispositions du Code sont invités à prendre en compte les contrôles ISO énumérés ci-dessous lors de la mise en œuvre de leurs mesures de sécurité. Un CISP qui a vérifié le respect de ces normes peut s'appuyer sur cette vérification pour démontrer le respect de l'exigence prévue par le présent paragraphe (1) de l'Annexe A.

Contrôles ISO pertinents :

- ISO/IEC 27001 : A.5
- ISO/IEC 27017 : 5
- ISO/IEC 27018 : 5

(2) Sécurité des Ressources Humaines

(a) Responsabilités du CISP

Le CISP doit mettre en place une structure organisationnelle pour gérer la mise en œuvre de la sécurité de l'information dans les services qu'il propose, avec une définition claire des rôles et responsabilités.

Le CISP doit créer une organisation pour la sécurité de l'information gérée par son personnel de sécurité et dirigée par le Responsable de la Sécurité de l'Information (CISO) ou toute personne occupant un poste équivalent. L'organisation de la sécurité du CISP doit établir et maintenir des politiques et procédures officielles visant à définir des normes d'accès logique au système et à l'infrastructure hébergés par le CISP. Ces politiques identifient également des responsabilités fonctionnelles pour l'administration de l'accès logique et de la sécurité. Le CISP assure la formation de ses employés et prestataires à ces politiques et procédures.

Des procédures doivent être mises en place pour ajouter, modifier ou désactiver les comptes utilisateurs des employés et prestataires du CISP, le cas échéant, et pour examiner ces comptes de façon périodique. Par ailleurs, la configuration de mots de passe complexes pour l'authentification des utilisateurs sur les systèmes du CISP est gérée conformément à la politique de mot de passe du CISP qui doit s'aligner sur la norme en vigueur en matière de mot de passe, notamment en ce qui concerne la complexité minimale, la longueur, l'historique du mot de passe, le blocage en cas d'échecs d'authentification répétés ou l'authentification multi-facteurs.

Les demandes de modification d'accès doivent être enregistrées au moyen d'un outil de gestion des autorisations, sur un journal d'audit, ou tout dispositif équivalent. Le CISP doit appliquer le principe de moindre privilège, en accordant aux utilisateurs un accès strictement nécessaire pour mener à bien leurs missions. Les comptes utilisateurs sont conçus pour fournir un accès minimum. Tout accès au-delà de ces moindres privilèges requiert une autorisation préalable.

(b) Responsabilités du client

Le client est seul responsable de son personnel et des tiers qui accèdent aux services d'infrastructure cloud proposés aux clients, ou qui utilisent ces services (y compris, sans s'y limiter, les prestataires, agents ou utilisateurs finaux), et de la formation de son personnel ou des tiers qui accèdent aux services d'infrastructure cloud ou qui utilisent ces services.

(c) Exemples de mesures que le CISP peut adopter

Le tableau ci-dessous dresse une liste des exemples de mesures qu'un CISP peut adopter pour s'acquitter de ses responsabilités en ce qui concerne la sécurité des ressources humaines :

Exemples :

- S'assurer que le conseil d'administration du CISP soit tenu informé des incidents, des menaces et du statut des dispositifs d'amélioration de la sécurité.

- Mettre en place un programme de sensibilisation aux questions de sécurité pour les membres du personnel du CISP afin de s'assurer qu'ils adoptent les bons comportements et possèdent les compétences nécessaires pour garantir la sécurité du CISP.

- Mettre à jour le programme de sensibilisation aux questions de sécurité du CISP pour faire face aux nouvelles technologies, aux menaces, aux normes, au respect de la vie privée et à la protection des données et aux exigences opérationnelles.

- Proposer une formation axée sur les fonctions de sécurité sur la base des responsabilités confiées au personnel du CISP et du client avant d'autoriser l'accès aux systèmes du CISP ou d'exécuter les tâches assignées.

- Assurer un suivi des activités de formation à la sécurité exécutées par le personnel du CISP pour vérifier la conformité aux exigences de formation telles que définies par le Code et le RGPD.

- S'assurer que le personnel du CISP et du client ait lu et compris la politique et les procédures du CISP en matière de sécurité de l'information.

- Veiller à ce que tous les utilisateurs ayant accès à un compte administratif utilisent un compte dédié ou secondaire pour les activités complexes, avec des mesures de sécurité spécifiques (ex. : complexité du mot de passe, authentification multi-facteurs, traçabilité des événements pertinents, etc.). Ce compte doit servir uniquement pour les activités administratives et non pas pour naviguer sur Internet, envoyer des e-mails ou pour des activités similaires.

- Limiter l'accès du personnel du CISP, afin qu'il puisse accéder uniquement aux informations relatives aux éléments structurels de l'infrastructure cloud, à leur configuration et à la configuration des environnements logiques attribués aux clients. Mettre en place des dispositifs de contrôle afin de bloquer l'accès du personnel du CISP aux données des clients et aux données applicatives, à moins qu'un client ne soumette explicitement une demande d'assistance, de maintenance ou de mise à jour.

- Mettre en œuvre des mécanismes de contrôle afin d'empêcher les membres du personnel du CISP de garder les sessions de l'infrastructure ouvertes pendant leur absence.

- Établir des politiques visant à interdire au personnel du CISP de conserver par écrit les données d'identification nécessaires pour accéder à l'infrastructure physique du CISP, à l'exception d'un mot de passe superutilisateur, connu de l'administrateur système et conservé par le

gestionnaire opérationnel.

(d) Exigences ISO correspondantes

Les CISPs qui adhèrent aux dispositions du Code sont invités à prendre en compte les contrôles ISO énumérés ci-dessous lors de la mise en œuvre de leurs mesures de sécurité. Un CISP qui a vérifié le respect de ces normes peut s'appuyer sur cette vérification pour démontrer le respect de l'exigence prévue par le présent paragraphe (2) de l'Annexe A.

Contrôles ISO pertinents :

- ISO/IEC 27001 : A.6.1, A.7.2
- ISO/IEC 27017 : 6.1, 7.2
- ISO/IEC 27018 : 6.1, 7.2

(3) Gestion de l'Accès des Utilisateurs

(a) Responsabilités du CISP

Le CISP doit fournir au client un système de gestion des contrôles d'accès pour que le client puisse accéder en tant qu'utilisateur au service d'infrastructure cloud dans le cadre du service. Ce système de gestion des contrôles d'accès doit comprendre, par exemple, des comptes nominatifs (qui peuvent être un compte utilisateur ou un compte de service), un contrôle d'accès à base de rôles et des mots de passe ou d'autres moyens ou politiques d'authentification. Le CISP doit expliquer au client comment fonctionne le système de gestion des contrôles d'accès afin que le client puisse l'utiliser et le configurer conformément aux instructions fournies ci-après.

Le CISP n'est pas responsable des solutions d'accès aux systèmes et aux applications déployés par le client qui utilise le service d'infrastructure cloud.

(b) Responsabilités du client

Le client est seul responsable de l'utilisation et la configuration des systèmes de gestion des contrôles d'accès proposés par le CISP. Le client est responsable de l'attribution des droits d'accès au personnel approprié.

Le client est responsable des solutions d'accès aux systèmes et aux applications qu'il déploie dans le cadre de son utilisation du service d'infrastructure cloud.

(c) Exemples de mesures que le CISP peut adopter

Le tableau ci-dessous dresse une liste des exemples de mesures qu'un CISP peut adopter pour s'acquitter de ses responsabilités en matière de sécurité ce qui concerne la gestion des contrôles d'accès :

Exemples :
• Assurer la gestion active de la durée de vie des comptes, y compris la création, l'utilisation et la suppression des comptes, afin de minimiser les possibilités pour les attaquants de les exploiter. • Désactiver les comptes utilisateurs CISP inactifs après une période d'inactivité définie. • S'assurer que les sessions utilisateurs CISP soient automatiquement bloquées après une certaine période d'inactivité. • Gérer activement des systèmes de gestion des accès axés sur les rôles et les profils • Fournir un accès administratif aux clients pour la configuration d'un environnement logique avec des connexions sécurisés et cryptées à la demande spécifique du client.

(d) Exigences ISO correspondantes

Les CISPs qui adhèrent aux dispositions du Code sont invités à prendre en compte les contrôles ISO énumérés ci-dessous lors de la mise en œuvre de leurs mesures de sécurité. Un CISP qui a vérifié le respect de ces normes peut s'appuyer sur cette vérification pour démontrer le respect de l'exigence prévue par le présent paragraphe (3) de l'Annexe A.

Contrôles ISO pertinents :

- ISO/IEC 27001 : A.9
- ISO/IEC 27017 : 9
- ISO/IEC 27018 : 9

(4) Sécurité physique et environnementale

(a) Responsabilités du CISP

Le CISP doit mettre en place et maintenir des mesures de sécurité physique et environnementale de pointe pour le service d'infrastructure cloud, destinées (i) à aider les clients à protéger leurs données à caractère personnel contre le traitement non autorisé et contre la perte, l'accès ou la divulgation, de manière accidentelle ou illicite et (ii) à empêcher les menaces raisonnables pour l'environnement comme les incendies et les inondations.

(b) Responsabilités du client

Le client ne joue pas un rôle actif dans le maintien de la sécurité physique et environnementale pour le service d'infrastructure cloud. Les clients doivent cependant examiner (a) les informations mises à leur disposition par le CISP concernant la sécurité physique et environnementale du service, (b) la configuration du service d'infrastructure cloud choisie par le client et l'utilisation des fonctionnalités et contrôles mis à disposition pour ce service, et (c) les mesures de sécurité que le client mettra en place en ce qui concerne les aspects de la sécurité relevant de sa responsabilité, et obtenir l'assurance que ces mesures, prises dans leur ensemble, garantissent un niveau approprié de sécurité

pour le traitement que le client effectuera en utilisant ce service.

(c) Exemples de mesures que le CISP peut adopter

Le tableau ci-dessous dresse une liste des exemples de mesures qu'un CISP peut adopter pour s'acquitter de ses responsabilités en ce qui concerne la sécurité physique et environnementale :

Exemples :
• Le zonage des espaces d'hébergement en fonction de leur criticité. La mise en œuvre et le contrôle de ce zonage au moyen de cloisons, clôtures, portes et portillons de sécurité dont l'accès est contrôlé, placé sous vidéosurveillance et surveillé. • L'utilisation de systèmes physiquement et logiquement dispersés pour isoler et exécuter les logiciels qui engendrent des risques plus importants pour le client. • La gestion de l'accès aux centres de données et aux cages au moyen d'un système d'authentification visuelle ou d'un badge, qui limite l'accès permanent aux installations et zones sécurisées du CISP uniquement au personnel autorisé et approuvé. • La mise en place d'un système par lequel un visiteur (c'est-à-dire une personne dont l'accès n'est pas indispensable) doit soumettre une demande pour accéder aux installations et zones sécurisées du CISP, et documenter cette demande, au moyen d'un mécanisme approuvé par le CISP, laquelle demande sera uniquement approuvée par le personnel autorisé du CISP. • La vérification de l'identité des visiteurs qui accèdent aux installations et zones sécurisées du CISP au moyen d'une pièce d'identité officielle avec photo (ex. : permis de conduire, passeport, etc.) ou d'une pièce d'identité avec photo délivrée par un CISP.

(d) Exigences ISO correspondantes

Les CISPs qui adhèrent aux dispositions du Code sont invités à prendre en compte les contrôles ISO énumérés ci-dessous lors de la mise en œuvre de leurs mesures de sécurité. Un CISP qui a vérifié le respect de ces normes peut s'appuyer sur cette vérification pour démontrer le respect de l'exigence prévue par le présent paragraphe (4) de l'Annexe A.

Contrôles ISO pertinents :

- ISO/IEC 27001 : A.11.1, A.11.4.1, A.13.1
- ISO/IEC 27017 : 11.1, 13.1
- ISO/IEC 27018 : 11.1, 13.1

(5) Serveurs et équipements physiques, y compris les pare-feux

(a) Responsabilités du CISP

Le CISP est seul responsable du déploiement, du fonctionnement et de la sécurité du

matériel physique, du système d'exploitation *hôte*, et de la couche de virtualisation, utilisés pour fournir le service d'infrastructure cloud, y compris la configuration nécessaire à la prestation de ce service.

Le CISP doit installer un mécanisme permettant de filtrer les flux de données, comme un pare-feu, autour du périmètre de l'infrastructure cloud dans son ensemble et/ou un pare-feu pour isoler l'instance de service qui est déployée. S'il existe un mécanisme de filtre (tel qu'un pare-feu) pour protéger l'infrastructure du CISP, dans sa globalité, il appartient au CISP de le configurer.

(b) Responsabilités du client

Le client assume seul la gestion de la bonne configuration de tout système et toute application qu'il a déployé(e) sur le service d'infrastructure cloud, y compris le système d'exploitation *invité*, et il est seul responsable de la sécurité des données en transit. La mise à disposition ou non d'un pare-feu pour chaque instance de service dépendra du service. Certains services ne peuvent pas disposer de pare-feux pour une instance spécifique. Dans ce cas, le client devra appliquer son propre pare-feu pour l'instance spécifique.

(c) Exemples de mesures que le CISP peut adopter

Le tableau ci-dessous dresse une liste des exemples de mesures de sécurité qu'un CISP peut adopter pour s'acquitter de ses responsabilités en ce qui concerne la sécurité des serveurs et équipements physiques :

Exemples :
• Établir une base de données pour la gestion de la configuration qui couvre tous les serveurs et équipements physiques et gérer la durée de vie de ces actifs. • Mettre en œuvre des contrôles de sécurité pour garantir la sécurité de la chaîne logistique et assurer la traçabilité des opérations. • Installer et configurer un système de filtrage « data plane » sur les environnements câblés et sans fil pour protéger le réseau du CISP des réseaux externes comme internet. Par exemple, utiliser un pare-feu déployé par un réseau. • S'assurer que les politiques de cloisonnement du réseau (« data plane »), par exemple les règles d'utilisation des pare-feux, respectent les configurations approuvées. Par exemple, (a) les ports, protocoles et services inutiles doivent être restreints sur les périphériques réseau ; (b) les appareils doivent être configurés en mode HD (Haute Disponibilité) ; et (c) les politiques « data plane » (ex : configurations des dispositifs de pare-feu) doivent prévoir un « blocage d'IP étendu » pour la liste d'accès border-net, qui interdit tout ce qui n'est pas spécifiquement approuvé dans les listes de contrôle d'accès. • S'assurer que les politiques « data plane » sont approuvées par un membre dirigeant du CISP et testées avant leur mise en œuvre. • S'assurer que les configurations des pare-feux et les listes de contrôle d'accès (« ACL ») sont gérées par un ingénieur réseau conformément à des ensembles de règles approuvés. Par exemple : (a) l'outil de gestion des ACL doit servir à déployer des ACL approuvées sur les pare-feux du réseau de production ; et (b)

si l'accès à un pare-feu ou un périphérique réseau est impossible au moyen de l'outil de gestion des ACL, le problème doit être examiné et corrigé.

- S'assurer que les règles applicables aux pare-feux sont examinées et approuvées par l'équipe en charge de la sécurité de l'information.
- Étendre les politiques « data plane » aux périphériques réseau en fonction de la plateforme, de l'emplacement et du réseau.

(d) Exigences ISO correspondantes

Les CISPs qui adhèrent aux dispositions du Code sont invités à prendre en compte les contrôles ISO énumérés ci-dessous lors de la mise en œuvre de leurs mesures de sécurité. Un CISP qui a vérifié le respect de ces normes peut s'appuyer sur cette vérification pour démontrer le respect de l'exigence prévue par le présent paragraphe (5) de l'Annexe A.

Contrôles ISO pertinents :

- ISO/IEC 27001 : A.8.1, A.13.1, A.15.1
- ISO/IEC 27017 : 8.1, 13.1, 15.1
- ISO/IEC 27018 : 8.1, 13.1, 15.1

(6) Gestion de la protection des logiciels malveillants

(a) Responsabilités du CISP

Le CISP doit mettre en place un dispositif de protection contre les logiciels malveillants sur les systèmes sensibles (à savoir les systèmes fréquemment affectés ou ciblés) qui font partie du service d'infrastructure cloud.

(b) Responsabilités du client

Le client assure la gestion de la protection contre les logiciels malveillants sur les systèmes et les applications qu'il déploie dans le cadre de son utilisation du service d'infrastructure cloud.

(c) Exemples de mesures que le CISP peut adopter

Le tableau ci-dessous dresse une liste des exemples de mesures de sécurité qu'un CISP peut adopter en rapport avec la gestion de la protection contre les logiciels malveillants sur les systèmes sensibles qui font partie du service d'infrastructure cloud :

Exemples :
• Installer une protection anti-virus sur les serveurs du réseau et sur les postes de travail. • Configurer cet anti-virus dans le but de : (a) vérifier les e-mails, les pièces jointes aux e-mails, les accès internet, et les supports amovibles ; (b) vérifier les fichiers système critiques pendant le démarrage du système ; et (c) bloquer et mettre en quarantaine les codes malveillants et envoyer des alertes à l'administrateur de la sécurité du CISP. • Configurer des systèmes permettant la mise à jour automatique des logiciels anti-virus. • S'assurer que tous les logiciels installés sur une plateforme sont des logiciels systèmes téléchargés à partir de sources authentifiées.

(d) Exigences ISO correspondantes

Les CISPs qui adhèrent aux dispositions du Code sont invités à prendre en compte les contrôles ISO énumérés ci-dessous lors de la mise en œuvre de leurs mesures de sécurité. Un CISP qui a vérifié le respect de ces normes peut s'appuyer sur cette vérification pour démontrer le respect de l'exigence prévue par le présent paragraphe (6) de l'Annexe A.

Contrôles ISO pertinents :

- ISO/IEC 27001 : A.12.2, A.12.5, A.12.6
- ISO/IEC 27017 : 12.2, 12.5, 12.6
- ISO/IEC 27018 : 12.2, 12.5, 12.6

(7) Gestion des vulnérabilités

(a) Responsabilités du CISP

Le CISP doit définir un niveau d'engagement (répartition des tâches entre le CISP et le client, délai entre la définition des correctifs et la mise en œuvre de ces correctifs, etc.) pour le service d'infrastructure cloud. Le CISP est responsable, sauf indication contraire expresse du client dans le Contrat de Services, de la correction des bugs du matériel informatique, de la mise en réseau du matériel informatique, de la couche de virtualisation et des systèmes d'exploitation *hôtes*.

(b) Responsabilités du client

Le client assure la gestion des vulnérabilités sur les systèmes et applications qu'il a déployés et hébergés sur le service d'infrastructure cloud, y compris les systèmes d'exploitation *invités*.

(c) Exemples de mesures que le CISP peut adopter

Le tableau ci-dessous dresse une liste des exemples de mesures qu'un CISP peut adopter pour s'acquitter de ses responsabilités en matière de sécurité ce qui concerne la gestion des vulnérabilités :

Exemples :
• Souscrire à un service de veille des vulnérabilités et enregistrer toutes les vulnérabilités dans la base de données de gestion de configuration du CISP. Analyser toutes les vulnérabilités applicables à un actif afin de définir un ordre de priorité dans la mise en œuvre des correctifs. • S'assurer que les systèmes d'exploitation hôtes exécutent les dernières mises à jour de sécurité fournies par le fournisseur de logiciel. • Effectuer des tests de pénétration pour identifier les vulnérabilités et attaquer les vecteurs qui pourraient être utilisés pour exploiter des progiciels.

(d) Exigences ISO correspondantes

Les CISPs qui adhèrent aux dispositions du Code sont invités à prendre en compte les contrôles ISO énumérés ci-dessous lors de la mise en œuvre de leurs mesures de sécurité. Un CISP qui a vérifié le respect de ces normes peut s'appuyer sur cette vérification pour démontrer le respect de l'exigence prévue par le présent paragraphe (7) de l'Annexe A.

Contrôles ISO pertinents :

- ISO/IEC 27001 : A.6.1.4, A.12.6, A.14.2
- ISO/IEC 27017 : 6.4, 14.2
- ISO/IEC 27018 : 6.4, 14.2

(8) Journalisation et Monitoring

(a) Responsabilités du CISP

Le CISP fournit au client des outils de monitoring (ex : niveau, portée, compte-rendu, interfaces, API) et de journalisation et/ou rapports de suivi (ex : accès, enregistrements, durée d'enregistrement) pour le service d'infrastructure cloud.

(b) Responsabilités du client

Le client est seul responsable pour la journalisation et les systèmes et outils de monitoring qu'il déploie sur le service d'infrastructure cloud, y compris l'utilisation et la configuration des outils de suivi et de journalisation fournis par le CISP.

(c) Exemples de mesures que le CISP peut adopter

Le tableau ci-dessous dresse une liste des exemples de mesures qu'un CISP peut adopter pour s'acquitter de ses responsabilités en matière de sécurité ce qui concerne la journalisation et le monitoring :

Exemples :

- Dresser une liste des événements système qui doivent être enregistrés, notamment les événements suivants : (a) les réussites et échecs d'authentifications et de tentative d'authentification ; (b) les événements liés à la gestion des comptes ;
(c) les préférences en termes de fonctionnalités ; (d) le démarrage et l'arrêt du système ; (e) les suppressions de données, l'accès aux données et les modifications de données ; et (f) les événements infructueux (par exemple, les appels non autorisés).

- Mettre en place des journaux sur les systèmes pour enregistrer au moins les informations suivantes, pour chaque événement système (y compris les événements utilisateur, les événements système et les événements de sécurité) : (a) identification de l'utilisateur (y compris le service, le correspondant et l'utilisateur) ; (b) type d'événement ou API contactée ; (c) date et fuseau horaire ; (d) source de l'événement système ; (e) résultat de l'événement système ; et (f) identité du composant ou de la ressource affecté(e) du système.

- Collecter des journaux à partir de tous les systèmes, dispositifs et composants de réseau vers un service d'enregistrement centralisé qui répartit la capacité de stockage des audits et configure ces audits afin de minimiser le risque que cette capacité soit dépassée et à conserver les audits enregistrés pour une période définie.

- Agréger, corréler, examiner et analyser les journaux pour identifier des anomalies et autres événements malveillants potentiels.

- Contrôler les systèmes et les installations pour détecter les événements de sécurité potentiels, et configurer ces systèmes et installations afin qu'ils génèrent automatiquement des alertes pour signaler ces événements au personnel approprié.

- Protéger les journaux contre l'accès non autorisé. Par exemple, en limitant l'accès aux journaux au personnel autorisé du CISP et en mettant en place un logiciel infalsifiable/visible ou de détection des changements pour détecter la falsification des informations contenues dans ces journaux.

(d) Exigences ISO correspondantes

Les CISPs qui adhèrent aux dispositions du Code sont invités à prendre en compte les contrôles ISO énumérés ci-dessous lors de la mise en œuvre de leurs mesures de sécurité. Un CISP qui a vérifié le respect de ces normes peut s'appuyer sur cette vérification pour démontrer le respect de l'exigence prévue par le présent paragraphe (8) de l'Annexe A.

Contrôles ISO pertinents :

- ISO/IEC 27001 : A.12.4
- ISO/IEC 27017 : 12.4
- ISO/IEC 27018 : 12.4

(9) Équipements en fin de vie

(a) Responsabilités du CISP

Le CISP doit établir un procédé de désinstallation des supports de stockage avant la mise à disposition finale du support de stockage utilisé pour stocker les Données Client lorsque ce support est en fin de vie, afin d'empêcher que les Données Client ne soient exposées à des personnes non autorisées. Le processus de désinstallation sera mené conformément aux usages du secteur (selon la description fournie dans la norme ISO/IEC 27002 ; ou dans les NIST 800-88) pour s'assurer que les Données Client ne peuvent pas être extraites du type de support de stockage utilisé au moyen d'un outil d'extraction de données ou d'informations ou d'autres moyens similaires.

(b) Responsabilités du client

Le client ne joue pas un rôle actif dans la désinstallation des supports de stockage en fin de vie utilisés par le CISP. Les clients doivent cependant examiner (a) les informations mises à leur disposition par le CISP concernant la désinstallation des supports de stockage, (b) la configuration du service d'infrastructure cloud choisie par le client et l'utilisation des fonctionnalités et contrôles mis à disposition pour ce service, et (c) les mesures de sécurité que le client mettra en place en ce qui concerne les aspects de la sécurité relevant de sa responsabilité, et obtenir l'assurance que ces mesures, prises dans leur ensemble, garantissent un niveau approprié de sécurité pour le traitement que le client effectuera en utilisant ce service.

(c) Exemples de mesures que le CISP peut adopter

Le tableau ci-dessous dresse une liste des exemples de mesures qu'un CISP peut adopter pour s'acquitter de ses responsabilités en matière de sécurité ce qui concerne les équipements en fin de vie :

Exemples :
• Utiliser, par exemple, les techniques décrites dans le DoD 5220.22-M (« Manuel Opérationnel du Programme National sur la Sécurité Industrielle ») ou les NIST -88 (« Lignes Directrices sur l'Effacement des Données ») pour détruire les données dans le cadre du processus de désinstallation. • Démagnétiser et détruire physiquement tous les appareils de stockage magnétiques désinstallés conformément aux usages du secteur. • Protéger les supports contra la divulgation non autorisée ou les abus jusqu'à ce qu'ils soient détruits. • Surveiller la manipulation et la conservation des supports. • S'assurer que les supports de stockage utilisés sur un hôte ou un système ne sont jamais réutilisés sur un autre hôte ou système. • Stocker tous les supports dans une poubelle sécurisée, verrouillée/inviolable, dès qu'ils sont été retirés des appareils source. La poubelle doit se situer dans la cage ou le module où les disques durs ont été retirés.

- S'assurer que le support n'est pas transporté en dehors du site sans autorisation préalable et que tout support transporté à l'extérieur des locaux du CISP n'est pas laissé sans surveillance dans un espace public.

- Protéger le support pendant son transport en dehors des frontières physiques du CISP et s'assurer que les activités associées au transport du support sont strictement réservées au personnel autorisé, qui est surveillé et documenté.

(d) Exigences ISO correspondantes

Les CISPs qui adhèrent aux dispositions du Code sont invités à prendre en compte les contrôles ISO énumérés ci-dessous lors de la mise en œuvre de leurs mesures de sécurité. Un CISP qui a vérifié le respect de ces normes peut s'appuyer sur cette vérification pour démontrer le respect de l'exigence prévue par le présent paragraphe (9) de l'Annexe A.

Contrôles ISO pertinents :

- ISO/IEC 27001 : A.8, A.11.2.5, A.11.2.6, A.11.2.7
- ISO/IEC 27017 : 8, 11.2.5, 11.2.6, 11.2.7
- ISO/IEC 27018 : 8, 11.2.5, 11.2.6, 11.2.7

Annexe B – Check-list de Conformité

Cette Check-list de Conformité expose les exigences qu'un CISP doit respecter pour se conformer aux dispositions du Code. Elle fournit également aux CISPs des lignes directrices sur la manière de se conformer aux Exigences du Code et de mettre en œuvre les pratiques techniques et organisationnelles en matière de sécurité décrites en Annexe A. Par souci de clarté, le CISP a l'obligation de respecter les Exigences du Code : les colonnes ci-dessous qui décrivent les contrôles prévus qu'il convient d'appliquer, et les questions pour le CISP, visent à fournir des exemples sur les mesures qu'un CISP doit adopter pour se conformer aux dispositions du Code et sur la façon dont le respect de ces dispositions pourrait être évalué, mais elles ne remplacent pas, ni ne modifient, l'Exigence du Code correspondante.

La Check-list de Conformité vise également à garantir que tous les Organismes de Contrôle utilisent une méthode de vérification cohérente en leur fournissant (i) les exigences sur lesquelles ils doivent s'appuyer pour vérifier le respect des dispositions du Code et (ii) les questions/documents ou supports équivalents qui devraient être utilisés pour effectuer une évaluation de la conformité au Code. La Check-list de Conformité n'a pas vocation à remplacer ou à modifier le Contrat de Services entre un CISP et un client.

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
1	Section 3 Champ d'application	- En ce qui concerne les données à caractère personnel qui sont traitées au nom d'un client qui utilise un service d'infrastructure cloud **(Données Client),** le CISP ne doit pas (a) accéder ou utiliser ces données sauf dans la mesure nécessaire pour fournir les services au client et assurer le maintien de ces services, ou (b) traiter ces données pour ses propres finalités, incluant par exemple à des fins de fouille de données, de profilage ou de prospection commerciale.	En ce qui concerne les données à caractère personnel qui sont traitées pour le compte d'un client qui utilise un service d'infrastructure cloud (**Données Client**), le CISP ne doit pas à (a) accéder ou utiliser ces données sauf dans la mesure nécessaire pour fournir les services au client, ou (b) traiter ces données pour ses propres finalités incluant par exemple, à des fins de fouille de données, de profilage ou de prospection commerciale.		Documentation relative au service, Politiques de protection des données à caractère personnel et/ou Contrat de Services décrivant le champ et l'utilisation des Données Client.			

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
2	Section 4.1. Licéité du traitement des données à caractère personnel	- Le CISP traite uniquement les données à caractère personnel sur instruction du client. - Le CISP doit : (a) se conformer aux instructions du client telles qu'elles sont décrites dans le Contrat de Services et (b) fournir des informations sur le service conformément à la Section 5 (Exigences en matière de Transparence) du Code.	4.1.1 Le CISP respecte les instructions du client lors du traitement de données à caractère personnel : Le CISP doit respecter strictement : (i) les instructions écrites spécifiques du client qui sont contenues ou mentionnées dans le Contrat de Services signé ou ; (ii) les instructions générales qui sont documentées par le CISP dans une liste de services préétablie (intitulée « Catalogue des Services ») que le client peut utiliser.	(i) Tous les traitements spécifiques de Données à caractère personnel sont-ils documentés sous forme d'« instructions » dans les Contrats de Services en cours avec chaque client ou dans des annexes? Comment le CISP s'assure-t-il que les données à caractère personnel sont traitées pour le client conformément aux instructions documentées spécifiques ? (ii) Tous les traitements non spécifiques de données à caractère personnel du client sont-ils effectués en conformité avec le catalogue des services documenté ? Le catalogue des services est-il mis à jour afin de couvrir tous les traitements non spécifiques de données à caractère personnel ?	Documentation des Instructions relatives au Traitement spécifique dans les Contrats de Services ou dans les annexes aux Contrats de Services Documentation du catalogue des Services et preuve de sa mise à jour régulière.	28(3)(a)	Contrats de sous-traitance	

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
3	Section 4.2 Conditions générales contractuelles des services du CISP	- Le CISP traite uniquement les données à caractère personnel sur instruction du client. Un contrat entre le CISP et le Client doit définir les caractéristiques du service et comment il doit être fourni ainsi que les droits et obligations respectifs du CISP et du client (le Contrat de Services) - Le Contrat de Services doit se présenter sous une forme écrite (y compris la forme électronique). - Le Contrat de Services doit avoir force exécutoire entre le CISP et le client. - Le Contrat de Services doit stipuler les obligations du sous-traitant telles que prévues à l'Article 28(3) du RGPD et doit contenir, au minimum, des clauses qui satisfont les exigences qui sont mentionnées comme s'appliquant au CISP en vertu des Obligations du CISP, notamment les Sections 4.1. 4,3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.10, 4.11 et 5. - Le CISP n'est pas autorisé à traiter les Données Client sans qu'un Contrat de Services en place soit en place.	4.2.1 Le traitement des données est couvert par un contrat de services. Tout traitement de données à caractère personnel effectué par le CISP doit faire l'objet d'un contrat de services écrit et signé avec le client. Les Contrats de Services doivent contenir des clauses qui satisfont les obligations du CISP (Licéité du traitement de données à caractère personnel, Sécurité, Transfert de données à caractère personnel vers des pays tiers, sous-traitance, Demandes des personnes concernées, Personnel du CISP, Violation des données, Suppression ou renvoi de données à caractère personnel). 4.2.2. Le traitement est décrit dans un Contrat de Service Les contrats de services doivent être rédigés afin que le client puisse modifier ses cas d'utilisation et les services qu'il utilise. Dans tous les cas, des traces doivent être générées et archivées, détaillant quels services sont utilisés par le client, et quand.	Les Contrats de Services contiennent-ils la description générale du traitement des données à caractère personnel effectué au moyen des Services d'infrastructure cloud ? Le client est-il en mesure de modifier lorsqu'il le souhaite la manière et pour quelle finalité il utilise cette infrastructure pour traiter des données à caractère personnel ? Lorsque des achats de services spécifiques portant sur le traitement de données à caractère personnel sont réalisés, des traces sont-elles générées et archivées ? Ces traces décrivent-elles de manière suffisamment détaillée les services achetés par le client ?	Contrat de Services signé avec les conditions générales annexées au Contrat Le Contrat de Services peut être structuré de n'importe quelle façon, y compris : 1. Un contrat unique ; 2. Un ensemble de documents comme un contrat de services classique et les annexes s'y rattachant (contrats relatifs au traitement de données, contrats de niveaux de service..) ; OU 3. Conditions générales standard en ligne. Traces des achats spécifiques de services réalisés par le client.	28 (3)	Sous-traitant	

	Section 4.3. Sécurité	- Le CISP doit mettre en œuvre et maintenir des mesures techniques et organisationnelles appropriées à l'installation de centre de données, ses serveurs, son équipement réseau et héberger les systèmes logiciels qui sont sous le contrôle du CISP et qui sont utilisés pour fournir son service. L'Annexe A du Code (Responsabilités en matière de Sécurité) définit les standards minimums de sécurité et décrit les exigences de sécurité qui doivent être adoptées par CISP pour qu'un service adhère au Code. - Les mesures techniques et organisationnelles mises en place par le CISP doivent : (a) être conçues pour aider les clients à protéger leurs données à caractère personnel contre le traitement non autorisé et la perte, l'accès ou la divulgation, accidentelle ou illicite, et (b) prendre en compte chacune des obligations du CISP en matière de sécurité décrites en Annexe A (Responsabilités en matière de Sécurité). - Les CISPs doivent s'employer activement à s'assurer ce que les mesure de sécurité qu'ils mettent en œuvre n'empêchent pas les clients de déployer leurs meilleures pratiques en matière de sécurité. Par exemple, les clients doivent pouvoir librement effectuer le chiffrement de leurs données à caractère personnel en toute sécurité. - Le CISP doit mettre à disposition un mécanisme permettant de filtrer les flux de données, comme un pare-feu, autour du périmètre de l'infrastructure cloud dans son ensemble et/ou un pare-feu pour isoler l'instance de service qui est déployée. - Les CISPs doivent également désigner un point de contact au sein du CISP chargé de répondre aux questions des clients concernant les aspects relatifs à la protection des données ou à la sécurité du service.	4.3.1. Des mesures organisationnelles et techniques sont mises en place. Les mesures techniques et organisationnelles adoptées pour les installations de centre de données, serveurs, équipements réseau et systèmes logiciels hôtes du CISP doivent : (a) être conçues pour aider les clients à protéger leurs données à caractère personnel contre le traitement non autorisé et la perte, l'accès ou la divulgation accidentelle ou illicite, et (b) tenir compte des responsabilités en matière de sécurité du CISP telles qu'elles sont décrites en Annexe A (Responsabilités en matière de Sécurité). L'Annexe A définit les responsabilités en matière de sécurité d'un CISP et du client dans le cadre de services d'infrastructure cloud. L'Annexe A définit une norme minimale pour les responsabilités en matière de sécurité. 4.3.2. Des mesures techniques et organisationnelles pour garantir la sécurité sont maintenues Des mesures techniques et organisationnelles doivent être mises en place pour garantir la sécurité (ex : gestion des accès, gestion des menaces et vulnérabilités, etc.). Un programme de sécurité doit être	Quelles sont les mesures de sécurité (techniques et organisationnelles) que le CISP a mises en place pour empêcher le traitement non autorisé et la perte, l'accès ou la divulgation accidentelle ou illicite ? Le CISP a-t-il mis en place les types de mesures de sécurité prévus par l'Annexe A ? Le CISP a-t-il établi un programme documenté pour la sécurité de l'information ? Qui en est responsable ? La sécurité du CISP et les programmes pour la sécurité de l'information mis en place par le CISP sont-ils régulièrement évalués et examinés ?	Documentation sur les mesures de sécurité qui relèvent de la responsabilité du CISP, y compris la documentation sur les mesures de sécurité adoptées pour se conformer à l'Annexe A. Documentation sur le programme pour la sécurité de l'information mis en place par le CISP (avec une description des risques identifiés et des mesures prises pour atténuer ces risques), et sur les responsabilités qui en découlent. Concrétisation de l'examen et de l'évaluation de la sécurité du CISP ainsi que du programme pour la sécurité de l'information du CISP.	32 (1)	Sécurité du traitement	

			documenté et appliqué par le personnel du CISP. 4.3.3. Des audits et tests réguliers du programme de sécurité du CISP sont réalisés					

Cadre de Contrôle du CC du CISP						**Articles du RGPD**		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**

		- Le CISP doit maintenir un programme sur la sécurité de l'information dans le but de : (a) identifier les risques raisonnablement prévisibles pour la sécurité du Réseau du CISP, et (b) minimiser les risques de sécurité, notamment en procédant à des analyses de risque et à des tests réguliers. - Le CISP doit désigner un ou plusieurs membres de son personnel pour coordonner et assumer la responsabilité du programme sur la sécurité de l'information. - Le CISP doit procéder à des examens réguliers de la sécurité du Réseau du CISP et de l'adéquation de son programme sur la sécurité de l'information. - Le CISP doit évaluer en permanence la sécurité du Réseau du CISP afin de déterminer si des mesures de sécurité supplémentaires ou différentes sont nécessaires pour faire face aux nouveaux risques de sécurité ou aux résultats obtenus à l'issue de ses propres examens périodiques. - Le CISP peut être amené à modifier les normes de sécurité sur la base desquelles son programme sur la sécurité de l'information peut être évalué, mais il doit au moins continuer, pendant toute la durée du Contrat de Services, à assurer le même niveau de sécurité que celui qui est décrit dans ses normes de sécurité à la date de prise d'effet du Contrat de Services.	Le programme pour la sécurité de l'information du CISP doit être régulièrement évalué et examiné. Le CISP doit notifier au client tout changement qu'il considère comme étant un abaissement des normes de sécurité du CISP à la date de prise d'effet du Contrat de Services, en lui communiquant des informations sur (i) la nature du changement, (ii) la finalité du changement et sa date de prise d'effet.					

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
		- Le CISP doit notifier au client tout changement qu'il considère objectivement comme ayant une incidence sur le champ de son programme sur la sécurité de l'information ou sur les mesures de sécurité techniques et organisationnelles relevant de sa responsabilité à la date de prise d'effet du Contrat de Services. Cette notification doit avoir lieu avant la modification des normes de sécurité du CISP, sauf si le CISP peut démontrer que cette modification doit être effectuée de toute urgence pour corriger une vulnérabilité de sécurité.						

	Section 4.4. Transfert des données à caractère personnel vers des pays tiers	- Le service du CISP offre au client la possibilité de choisir d'utiliser le service pour stocker et traiter ses données exclusivement sur les territoires de l'EEE, évitant ainsi l'application des règles du RGPD régissant le transfert de données à caractère personnel en dehors de l'EEE. - Le CISP doit fournir au client des informations sur la région et le pays dans lequel ses données sont stockées et traitées par ou au nom du CISP (que ces données soient ou non stockées et traitées exclusivement sur les territoires de l'EEE, ou dans un pays tiers). Si le CISP sous-traite une partie du traitement auprès d'autres sous-traitants, il doit également communiquer les informations mentionnées à la Section 4.5. Pour des raisons de sécurité, seule une localisation générale (une ville ou partie d'une ville ou d'une région	4.4.1. Les politiques et procédures relatives aux dispositifs de transfert des données (à caractère personnel) sont documentées Le CISP doit définir un cadre de réglementation du mécanisme de transfert des données, y compris les mécanismes couvrants : - Les transferts sur la base d'une décision d'adéquation - Les règles d'entreprise contraignantes - Les clauses contractuelles types 4.4.2. Traitement des données à caractère personnel. Le client doit avoir la possibilité de choisir	Le CISP a-t-il documenté un cadre de politiques et procédures relatif aux mécanismes de transfert de données à caractère personnel, que le client peut utiliser pour garantir la licéité du transfert des données à caractère personnel ou sur lequel le CISP peut s'appuyer pour s'assurer de la licéité de ses propres opérations sur les données données à caractère personnel ? Le CISP a-t-il communiqué au client des informations sur la région où les données à caractère personnel sont stockées ? Le CISP a-t-il donné	Politiques et procédures documentées décrivant les mécanismes de transfert de données à caractère personnel. Interface/site internet de communication/documentation/gestion sur laquelle/lequel : (a) le CISP indique au client dans quelle région les données à caractère personnel sont stockées. (b) Le CISP donne au client la possibilité de choisir le lieu où les données à caractère personnel seront stockées.	44	Principes de transfert	ISO/IEC 27001 : A.13.2.1 A.13.2.2 ISO/IEC 27018 : 12.1

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Pièces justificatives (ou documents équivalents) pour vérifier le respect des exigences du Code (à remettre par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
		) doit être communiquée. Cette description générale doit au moins permettre au client qui utilise le service d'identifier l'État membre de l'UE dont il relève pour effectuer ses activités de traitement. - Le CISP doit communiquer à l'Autorité de Contrôle compétente l'adresse exacte des installations concernées, si cette information est requise par l'Autorité de Contrôle compétente pour satisfaire ses obligations au regard de la législation européenne en matière de protection des données. - Pour les services qui peuvent être exécutés indifféremment en plusieurs endroits différents du Réseau du CISP, les CISPs doivent rendre ces informations facilement accessibles au client (par exemple sur le site internet du CISP) et lui permettre de choisir le(s) lieu(x) au sein du Réseau du CISP dans lequel/lesquels leurs données seront traitées. - Les CISPs doivent fournir à leurs clients la possibilité de choisir d'utiliser le service exclusivement sur les territoires de l'EEE. Tout transfert de données à caractère personnel vers un pays situé en dehors de l'EEE pour la fourniture des services du CISP, y compris l'accès à partir d'un pays tiers situé en dehors de l'EEE, ne peut se faire que sur instruction du	et de faire appliquer une limite à l'utilisation des données à caractère personnel exclusivement dans l'Union européenne. 4.4.3. La localisation des données est communiquée par le CISP. La localisation générale (Ville ou pays) des données à caractère personnel traitées par le CISP, ou en son nom (y compris ses autres sous-traitants) doit être communiquée au client. 4.4.4. Le client est en mesure de choisir la localisation des données. Le client aura la possibilité de choisir le lieu où les données à caractère personnel sont stockées.	au client la possibilité de choisir le lieu où les données à caractère personnel sont stockées ? Preuves concernant les mécanismes de transfert des données tels que le Contrat de Services et les avenants/annexes s'y rapportant, les SCCS (clauses contractuelles types), les BCRs (règles d'entreprise contraignantes), les déclarations le cas échéant.			

		client au CISP. - Le CISP doit aider les clients, en tant qu'exportateurs, à se conformer à leurs obligations du chapitre V du RGPD pour le transfert licite de données à caractère personnel vers le pays concerné, y compris les transferts en vertu d'une décision d'adéquation alors en vigueur (par exemple, actuellement, vers la Suisse, Israël et autres) (Art 45 du RGPD) ou soumis à des garanties appropriées (telles que, actuellement, les règles d'entreprise contraignantes ou les clauses contractuelles types de protection des données adoptées par la Commission (Art 46 du RGPD)), si : (i) le client transfère des données depuis l'EEE pour les stocker en utilisant le service du CISP, y compris lorsque les données sont transférées afin de fournir des services de « sauvegarde » aux centres de données de l'EEE en cas d'évènement de force majeure ou de continuité du CISP, dans tout pays situé en dehors de l'EEE qui n'est pas reconnu par la Commission européenne comme offrant un niveau de protection adéquat des données à caractère personnel ; ou (ii) le client a choisi d'autoriser le CISP, sur ses instructions, à accéder aux données stockées en utilisant le service du CISP au sein de l'EEE à partir du pays mentionné au point (i) ci-dessus. Le Contrat de Service entre le CISP et le client doit préciser les circonstances dans lesquelles il peut y avoir un transfert de données en dehors de l'EEE sur instruction du client (y compris la fourniture d'instructions via les outils de configuration du CISP et les API pour les services du CISP) ainsi que la délimitation des responsabilités entre le client (en tant qu'exportateur) et le CISP (en tant qu'importateur) concernant ce transfert. En outre, le CISP doit fournir au client les informations appropriées, notamment sur le lieu du traitement concerné, afin de permettre au client de vérifier au cas par cas, avant tout transfert, si la législation ou la pratique du pays						

		tiers concerné assure le niveau de protection des données requis dans l'EEE, de manière à déterminer si les garanties fournies par les garanties appropriées choisies peuvent être en pratique respectées. Si tel n'est pas le cas, la responsabilité d'identifier et de mettre en œuvre les mesures supplémentaires en plus des garanties appropriées concernées pour assurer aux données transférées un niveau de protection essentiellement équivalent à celui prévu dans l'EEE repose sur le client, si nécessaire avec l'aide du CISP (en tant qu'importateur de données). Le Comité Européen de la Protection des Données a publié une recommandation [insérer le lien] sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE qui peut aider le CISP dans l'évaluation du pays tiers et dans l'identification des mesures supplémentaires appropriées. Aucun transfert de données à caractère personnel vers un pays hors de l'EEE ne sera initié par le CISP dans le cadre de la fourniture des services, si le CISP n'a pas reçu les instructions du client pour le faire. Le CISP vérifie au cas par cas, avant tout transfert ou toute divulgation de données à caractère personnel en réponse à un jugement d'une juridiction ou à une décision d'une autorité administrative d'un pays tiers, que ce jugement ou cette décision peut être reconnu ou exécuté sur la base d'un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, afin de garantir la légalité de ce transfert ou de cette divulgation. Si tel n'est pas le cas, et sans préjudice d'autres motifs de transfert en vertu du chapitre V du RGPD, le CISP doit définir et mettre en œuvre des mesures visant à garantir que tout transfert ou divulgation non autorisé par le droit de l'Union						

		soit refusé au pays tiers demandeur.						

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
	Section 4.5. Sous-traitance	- Le CISP doit obtenir l'autorisation du client avant d'autoriser un autre sous-traitant à traiter des Données Client. - Cette autorisation peut être soit : Spécifique : dans ce cas, le CISP doit informer le client par écrit, y compris par format électronique, des sous-traitants spécifiques qu'il envisage de recruter. Le CISP pourra recruter l'autre sous-traitant qu'il a sélectionné pour traiter des Données Client uniquement si le responsable du traitement y consent ; ou Générale : dans ce cas, le consentement du client peut être donné de manière générale dans le cadre du Contrat de Services. En particulier, le Contrat de Services doit définir les situations et les conditions dans lesquelles le CISP peut recruter d'autres sous-traitants pour exécuter des activités de traitement spécifiques au nom du client sans qu'il soit nécessaire d'obtenir l'autorisation de ce dernier. - Dans les deux cas, le CISP doit informer le client par écrit (y compris par voie électronique) des changements prévus concernant ses autres sous-traitants, dans un délai raisonnable avant le changement	4.5.1 Le client a obtenu l'autorisation du CISP Le CISP doit obtenir le consentement du client avant d'autoriser un autre sous-traitant à accéder /traiter les données à caractère personnel du client. Ce consentement doit être obtenu au moyen (1) de contrats de services décrivant les autres sous-traitants recrutés par le CISP et au moyen (2) d'une communication écrite spécifique. 4.5.2 Des informations sur l'autre sous-traitant sont disponibles Une liste à jour des autres sous-traitants autorisés à accéder/traiter les données à caractère personnel du client, incluant leur rôle et leur localisation spécifique, doit être mise à la disposition du client. Par ailleurs, le CISP doit notifier au moyen d'une communication écrite tous les changements ou toutes les mises à jour important(e)s concernant la liste	Le CISP a-t-il obtenu le consentement du client avant d'autoriser un autre sous-traitant à accéder et traiter les données à caractère personnel du client ? Ce consentement est-il obtenu dans le cadre du Contrat de Services ? Est-ce que le CISP maintient et publie une liste à jour des autres sous-traitants Autorisés à accéder aux données à caractère personnel du client ? En cas de relation de sous-traitance impliquant l'accès/le traitement des données à caractère personnel, y-a-t-il un contrat de service en place entre le CISP et l'autre sous-traitant ?	Documentation attestant du consentement du client avant d'autoriser un autre sous-traitant à accéder et traiter les données à caractère personnel du client Contrat de services signé par le client et décrivant la liste des autres sous-traitants recrutés par le CISP et accédant/traitant des données à caractère personnel, ainsi que leur localisation. Contrats de Services entre le CISP et les autres sous-traitants.	28 (2) et 28 (4)	Sous-traitant	Lignes directrices à mettre en œuvre ISO/IEC/27018 : 8.1 ISO/IECC 27001: A.13.2.2 A.15

		envisagé pour permettre au client d'examiner ce changement et de s'opposer à l'autre sous-traitant. - Le CISP doit maintenir une liste à jour des autres sous-traitants qui traitent des Données Client. Cette liste doit indiquer la localisation de l'autre sous-traitant et elle doit être facilement accessible pour le client au moment de l'acceptation du Contrat de Services et pendant toute sa durée. Cette liste actualisée doit être mise à la disposition du client au moyen d'un lien URL, ou autrement par écrit à la demande du client. Avant d'autoriser le nouveau sous-traitant à accéder aux Données Client : (i) si le CISP obtient l'autorisation générale du client pour recruter d'autres sous-traitants, il doit communiquer au client : l'identité et la localisation générale (tel qu'un pays ou une zone régionale spécifique) de ce nouveau sous-traitant ; le droit pour le client de s'opposer à ce nouveau sous-traitant (comme il est indiqué ci-dessus au point (a)) ; et le délai dont le client dispose pour exercer son droit d'opposition. Ce délai doit donner au client un délai raisonnable pour examiner le changement. (ii) si le CISP obtient une autorisation spécifique pour recruter d'autres sous-traitants, il doit mettre à disposition du client l'identité et la localisation générale (tel qu'un pays ou une zone régionale spécifique) de ce nouveau sous-traitant et obtenir l'autorisation spécifique du client avant de recruter ce sous-traitant. - Le CISP doit imposer à son sous-traitant les mêmes obligations contractuelles en matière	des sous-traitants. 4.5.3 Des Contrats de Services sont conclus avec des sous-traitants Lorsque le CISP recrute un autre sous-traitant pour accéder et traiter les données à caractère personnel de l'organisation cliente, cette relation doit être régie par un contrat qui lie le CISP et cet autre sous-traitant 4.5.4. Mesures de sécurité Les mesures de sécurité applicables mentionnées à la Section 4.3 et en Annexe A (Responsabilités en matière de Sécurité) sont mises en place par le CISP pour s'assurer que ces sous-traitants, fournisseurs ou autres prestataires tiers qui ne traitent pas les Données Client ne puissent pas accéder ou traiter les Données Client.					

		de protection des données que celles énoncées dans le Contrat de Services entre le CISP et le client. - Le CISP doit mettre en place des dispositions opérationnelles concernant son autre sous-traitant afin de fournir un niveau identique ou supérieur au niveau de protection des données défini dans le Contrat de Services. Le CISP doit être en mesure de démontrer au client au moyen de preuves documentaires appropriées qu'il a pris de telles mesures. - Le CISP doit limiter le traitement des Données Client par son autre sous-traitant dans la mesure strictement nécessaire pour fournir ou maintenir les services. - Le CISP demeure pleinement responsable devant le client du respect de ses obligations de protection des données à caractère personnel et de l'exécution des obligations de protection des données à caractère personnel de l'autre sous-traitant en vertu du Contrat de Services.						

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
	Section 4.6. Démontrer la conformité	- Pour permettre au client d'exercer ses droits en vertu de l'Article 28(3)(h) du RGPD, le CISP doit : (i) communiquer au client les informations et la documentation appropriées telles qu'elles sont décrites à la Section 4.6(a) et (ii) soumettre ses installations de traitement des données à des audits réalisés par un tiers indépendant comme indiqué à la Section 4.6(b). - Les CISPs doivent respecter les Exigences en matière de Transparence énoncées à la Section 5 et doivent communiquer les informations nécessaires concernant les contrôles de sécurité mis en place pour les services proposés aux clients afin que les clients comprennent ces contrôles de sécurité et qu'ils puissent raisonnablement vérifier que le CISP respecte les obligations de sécurité définies dans le Contrat de Services. - Si ces informations ne sont pas confidentielles ou sensibles, elles doivent être mise à la disposition du client par un processus simple (ex : via site i du CISP). - Lorsque ces informations sont considérées comme trop sensibles pour être communiquées, le CISP doit exposer la	4.6.1. La description des contrôles de sécurité du CISP est documentée. Le CISP doit fournir suffisamment d'informations concernant les contrôles de sécurité mis en place pour les services proposés au client afin que celui-ci puisse garantir que ces contrôles de sécurité sont appropriés, du moins au niveau de leur conception. 4.6.2. Les contrôles de sécurité du CISP sont audités par des tiers de confiance. L'adéquation et l'efficacité opérationnelle des contrôles de sécurité du CISP peuvent être vérifiées au moyen d'audits externes. Si ces audits sont réalisés, ils doivent suivre un cadre tel que le cadre de Sécurité reconnu, réalisés en conformité avec la norme applicable, effectués par des professionnels de la sécurité qualifiés et générer un rapport. 4.6.3. Le CISP doit fournir au client les documents source nécessaires pour lui permettre de vérifier l'adéquation des contrôles	Le client a-t-il reçu les informations et la documentation nécessaires à propos des contrôles de sécurité mis en place pour être en mesure de vérifier, de manière raisonnable, que le CISP respecte ses obligations en matière de sécurité définies dans le Contrat de Services ? Un audit externe a-t-il été réalisé pour s'assurer de la bonne efficacité opérationnelle des contrôles de Sécurité du CISP ? Si ces audits sont réalisés, sont-ils conformes aux conditions énumérées : cadre de Sécurité reconnu, réalisés en vertu des normes applicables, effectués par des experts de la sécurité et générer un rapport.	Documentation détaillant les contrôles de sécurité du CISP et la conformité du CISP aux obligations en matière de sécurité définies dans le Contrat de Services. Rapports d'audit externe couvrant l'efficacité opérationnelle des contrôles de Sécurité du CISP.	28 (3) (h)	Sous-traitant	L'audit des contrôles de sécurité du prestataire de services réalisé par un tiers ne relève pas de la norme ISO27001.

		situation au client, si cela est nécessaire pour que le client comprenne les mesures de sécurité adoptées par le CISP. - Les CISPs peuvent demander aux clients de payer des frais supplémentaires pour ces informations ou peuvent choisir de fournir ces informations sans frais supplémentaires. Les frais supplémentaires doivent être raisonnables, basés sur les coûts, proportionnés aux efforts fournis pour communiquer ces informations, et ils ne doivent pas servir à empêcher les clients d'accéder aux informations sur les contrôles de sécurité du service. Les CISPs doivent indiquer clairement aux clients quelles informations qui peuvent être communiquées sans frais supplémentaires et celles qui sont uniquement disponibles moyennant des frais supplémentaires. - Le CISP doit fournir un dispositif (gratuit ou moyennant une contrepartie raisonnable) pour les clients qui ont des questions concernant la protection des données ou la sécurité en rapport avec le service, leur permettant de se mettre en contact avec le personnel du CISP correspondant ou le représentant désigné par le CISP pour traiter ces questions. Ces dispositifs doivent aider le client à exécuter ses obligations en qualité de responsable du traitement et doivent être appropriés et proportionnés au service d'infrastructure cloud en question. Le CISP doit également s'engager sur les délais de réponse, conformément aux accords définis dans le Contrat de Services. - Le client peut également demander à recevoir le rapport annuel produit par l'Organisme de Contrôle du CISP conformément à la Section 7.2 (a) du Code. - Si les informations communiquées par le CISP (y compris les informations fournies à la Section 4.6(a) et dans le rapport annuel préparé par l'Organisme de Contrôle dans le	de sécurité. 4.6.4. Si le client peut démontrer que l'audit externe et/ou les documents source mentionnés ci-dessus ne permettent pas de vérifier l'adéquation des contrôles de sécurité applicables au service, alors une approche proportionnée doit être adoptée, dans des conditions contrôlées, y compris par l'intermédiaire de l'Organisme de Contrôle compétent pour vérifier que le CISP respecte les dispositions du Code.					

		cadre de sa mission décrite à la Section 7.2(a)) ne sont pas suffisantes pour vérifier la conformité du CISP avec ses obligations au titre du RGPD telles que décrites dans les Exigences du Code, alors le client peut choisir de faire valoir ses droits en vertu de l'Article 28(3)(h) du RGPD comme suit : • le client peut demander par écrit au CISP que l'Organisme de Contrôle procède à une vérification, dans la mesure strictement nécessaire pour démontrer la conformité du CISP aux Exigences du Code, dès lors que celle-ci n'a pas déjà été démontrée (incluant par tout rapport déjà préparé par l'Organisme de Contrôle dans le cadre de sa mission décrite à la Section 7.2(a)) ; • le CISP doit autoriser l'Organisme de Contrôle à effectuer cette vérification ; • au vu des risques de sécurité potentiels pour les autres clients et pour le service en général, l'accès direct aux sites ou aux systèmes du CISP par l'Organisme de Contrôle doit être autorisé uniquement s'il n'existe aucun autre moyen raisonnable de démontrer la conformité du CISP, et s'il est exécuté dans des conditions contrôlées (convenues d'un commun accord entre le CISP et l'Organisme de Contrôle) qui perturbent le moins possible le CISP, n'entrainent pas de risque pour la sécurité et la continuité du service aux autres clients, et ne font pas en sorte que le CISP enfreigne une obligation ou un devoir légal qu'il pourrait avoir. • Lorsque les informations communiquées par le CISP en vertu de la Section 4.6 ne suffisent pas à démontrer la conformité du CISP tel qu'exigé par l'Art 28(3)(h), le client peut demander au CISP de prendre des						

		mesures complémentaires pour démontrer cette conformité, qui peuvent inclure des demandes auprès de l'Organisme de Contrôle. Si la réponse du CISP ou de l'Organisme de Contrôle à cette demande ne suffit pas à démontrer que le CISP respecte les obligations qui lui incombent en vertu de l'Article 28 du RGPD, le client peut demander des informations complémentaires au CISP au travers d'un nouvel audit, notamment des inspections, par un auditeur sélectionné par le client à partir d'une liste d'auditeurs agréés fournie par le CISP à l'avance. Cet audit sera mené de la façon la moins intrusive possible pour le CISP afin de vérifier s'il a respecté ses obligations en vertu de l'Article 28 du RGPD, et il sera soumis à (i) des contrôles raisonnables déterminés par le CISP afin d'éviter les risques pour les autres clients ou le CISP, notamment un contrôle de la sécurité des installations du CISP et le maintien de la continuité des opérations ; (ii) l'acceptation par le client des conditions visant à protéger les informations confidentielles du CISP ; et (iii) l'obligation du client de payer les frais raisonnables de l'audit. Le client et le CISP discuteront de bonne foi et s'accorderont sur le champ des activités de l'audit avant de réaliser cet audit.						

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre (incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
	Section 4.7. Droits des personnes concernées	- Le CISP doit offrir au client la possibilité de rectifier, d'effacer, de limiter, d'accéder ou de porter (dans un format structuré, couramment utilisé et lisible par machine) les Données Client dans le cadre du service ou de concevoir et déployer leurs propres solutions en utilisant le service. - Le CISP doit fournir une explication sur la manière dont ces capacités seront fournies au client dans le cadre des informations requises conformément à la Section 5 (Transparence).	4.7.1 Des procédures/outils sont mis en place pour pouvoir prendre les mesures nécessaires au regard des données à caractère personnel. Ces procédures et outils doivent être mis en place par le CISP pour permettre au client de répondre, en temps voulu et de manière adéquate, aux demandes concernant les droits des personnes concernées (information, rectification, limitation, effacement...). D'autre part, le CISP doit permettre au client de déployer une solution propre pour répondre à ces demandes. 4.7.2. Transparences des informations fournies par le CISP Les informations concernant la manière dont ces procédures et outils permettent de répondre, en temps voulu et de manière adéquate, aux demandes concernant les droits des personnes concernées doivent être fournies en toute transparence par le CISP	Y-a-t-il des procédures/outils en place pour répondre aux demandes du client concernant les droits des personnes concernées ? Le CISP offre-t-il au client la possibilité de déployer une solution propre lui permettant de prendre les mesures nécessaires pour répondre aux demandes des personnes concernées concernant leurs données ?	Documentation sur les procédures/outils mis en place pour traiter les demandes concernant les droits des personnes concernées.	28 (3) (e)	Contrats de sous-traitance	

			au client.					
	Section 4.8 Personnel du CISP	- Le CISP doit imposer des obligations contractuelles appropriées stipulant que les membres du personnel du CISP qui sont autorisés à accéder aux Données Client doivent préserver la confidentialité de ces données. - Le CISP doit mettre en œuvre et maintenir des contrôles d'accès et des politiques afin de limiter son personnel traitant les Données Client au personnel de CISP qui a besoin de traiter les Données Client pour fournir les services au client. - Le CISP soit sélectionner les contrôles d'accès appropriés, à savoir : (i) limiter l'accès physique aux installations de centre de données au personnel autorisé uniquement ; (ii) limiter l'accès technique pour héberger des logiciels et réseaux au personnel autorisé	4.8.1. Des accords de confidentialité sont signés par les employés du CISP qui traitent des données à caractère personnel Tous les employés du CISP qui ont accès à ces données doivent signer un accord de confidentialité, sauf si cette question n'est pas adressée dans leur contrat de travail. 4.8.2. Une procédure de gestion des accès est mise en place Les politiques et procédures sur les contrôles d'accès doivent être documentées et des mécanismes doivent être mis en place pour empêcher le personnel du CISP d'accéder à des données non nécessaires/légitimes pour eux, et	La confidentialité des données à caractère personnel traitées par les employés du CISP est-elle couverte par le document signé par chaque employé du CISP qui est amené à manipuler des données à caractère personnel (contrat de travail, accord de confidentialité) ? Le CISP a-t-il mis en place des politiques et procédures documentées sur les contrôles d'accès pour limiter l'accès du personnel du CISP traitant les données du client au seul personnel	Contrat de travail/accord de confidentialité signé par chaque employé du CISP qui manipule des données à caractère personnel. Politiques et procédures mises en place par le CISP concernant les contrôles d'accès aux données à caractère personnel	28 (3) (b)	Sous-traitant	La documentation et la Signature d'accords de confidentialité par les utilisateurs des données à caractère personnel ne sont pas couvertes par la norme des ISO27001. La limitation des données (à caractère personnel) sensibles n'est pas

		uniquement (iii) journaliser les accès du personnel du CISP aux Données Client. Dès que le personnel du CISP n'a plus besoin de traiter les Données Client, le CISP doit supprimer ces privilèges d'accès dans les meilleurs délais. - Le personnel du CISP peut avoir besoin d'accéder aux Données Client pour exécuter les services. Dans ce cas, l'accès sera uniquement autorisé dans la mesure nécessaire pour gérer le service. Le personnel qui n'a pas besoin d'accéder aux Données Client pour gérer le service sera soumis à des contrôles d'accès appropriés destinés à leur interdire tout accès.	lorsque cela n'est plus nécessaire.	qui a besoin de traiter les données du client afin de lui fournir des services ?				couverte par la norme ISO27001.

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**

	Section 4.9 Violation des données	- Le CISP doit établir une politique de gestion des incidents qui décrit les procédures à suivre pour identifier les violations de données à caractère personnel dont il a connaissance, et y répondre. Cette politique doit contenir : • des lignes directrices sur la façon de traiter les incidents, incluant qui responsable de la gestion des incidents au sein du CISP ; • des lignes directrices concernant les aspects constitutifs d'une violation de données à caractère personnel au regard du RGPD, et des directives permettant de déterminer les types d'incidents qui doivent être notifiés au client en fonction de leur impact potentiel sur les Données Client ; • une obligation de mener des enquêtes rapides dès lors qu'un CISP prend connaissance d'une violation de données présumée afin de déterminer s'il y a eu violation, et quelles Données Client ont pu être affectées ; • une procédure de mise en œuvre d'activités de correction visant à atténuer l'impact d'une violation de données et à remédier aux vulnérabilités exposées par les incidents de sécurité ; • une procédure pour notifier le client sans délai dès lors qu'un CISP a obtenu l'assurance qu'une violation de données a eu lieu en rapport avec les Données Client de ce client ; • un classement des types d'incidents	4.10.1. Une politique de gestion des incidents de sécurité est documentée Le CISP doit mettre en place une politique de gestion des incidents de sécurité comprenant : a/ des directives pour décider des types d'incidents qui doivent être notifiés au client en fonction de leur impact potentiel sur les données ; b/ des lignes directrices sur la façon de traiter les incidents ; et c/ une spécification des informations qu'il convient de mettre à la disposition du client à la suite de l'incident. 4.10.2 Un plan d'intervention en cas de Violation de Données est défini et documenté Le CISP doit définir un plan de détection/réponse en cas de violation des données et d'incident, qui couvre : - l'identification d'une violation de données à caractère personnel - la détermination des contrôles d'atténuation pertinents - l'évaluation de l'impact de cette violation de données à caractère personnel 4.10.3 Le Client est notifié en cas de violation des données En cas de violation de données, le CISP doit notifier cette violation au client dans un délai raisonnable après en avoir pris connaissance et sans retard	Le CISP a-t-il mis en place une politique de gestion des incidents de sécurité ? Le CISP a-t-il défini et documenté un plan d'intervention en cas de Violation de Données et un mécanisme de détection des incidents ? Comment une violation de Sécurité est-elle notifiée au client ? Que contient cette notification ?	Documentation concernant la politique de gestion des incidents de sécurité mise en place par le CISP. Documentation relative au plan d'intervention en cas de Violation de données Exemple de notification d'une Violation de Sécurité	33 et 28 (3)(f)	Notification d'une violation à l'autorité	

		par gravité, et des calendriers indicatifs pour les principales étapes d'enquête, ainsi que la notification prévue du/des client(s) (le cas échéant), en fonction de la gravité de l'incident ; • l'escalade appropriée, au sein même de la gouvernance du CISP, des questions de réponse aux incidents ; • une spécification des informations qu'il convient de mettre à la disposition du client à la suite d'une violation de données ; et • une procédure visant à coopérer avec les clients dans les cas où le client informe le CISP d'une violation de données, tel que fournir toutes les informations préliminaires disponibles pour aider le client à respecter ses obligations prévues par l'Article 33(1) du RGPD. - Si le CISP prend connaissance de la destruction, la perte ou l'altération, ou de la divulgation non autorisée de Données Client, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite, sur l'équipement ou les installations du CISP, le CISP en informera le client dans les meilleurs délais. - La notification doit, dans la mesure où le CISP a connaissance de ces informations en sa qualité de sous-traitant : (i) décrire la nature de la violation de sécurité, (ii) décrire les conséquences de la violation, (iii) décrire les mesures prises ou que le CISP propose de prendre pour remédier à l'incident et (iv) communiquer le nom et les coordonnées d'un point de contact au sein du CISP.	injustifié. La notification doit : (i) décrire la nature de la violation de sécurité, (ii) décrire les conséquences de la violation, (iii) décrire les mesures prises ou que le CISP propose de prendre pour remédier à l'incident et (iv) fournir le nom et les coordonnées d'un point de contact au sein du CISP.					

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
	Section 4.10 Suppression ou renvoi de données à caractère personnel.	- Le CISP doit donner au client la possibilité d'extraire et de supprimer les Données Client dans leur ensemble. - Le CISP doit fournir dans les informations requises en vertu de la Section 5 (Transparence), une explication sur la manière dont ces capacités seront f mises à la disposition du client. - Le CISP doit toujours suivre les instructions fournies par le client en ce qui concerne le renvoi ou la suppression des Données Client. - En l'absence d'instructions du client, le CISP doit, par défaut, supprimer les Données Client dans un délai raisonnable après l'expiration ou la résiliation du service.	4.11.1. Des mesures techniques et organisationnelles pour le retrait des données à caractère personnel sont documentées et mises en place Le CISP doit donner au client la possibilité au client de récupérer et de supprimer les données à caractère personnel pour lesquelles le client est responsable du traitement, (a) dans le cadre du service, ou (b) en permettant au client de concevoir et déployer leurs propres solutions de suppression et de renvoi en utilisant le service. 4.11.2. Transparences des informations fournies par le CISP Les informations concernant la manière dont ces procédures et outils permettent de répondre, en temps voulu et de manière adéquate, aux demandes concernant les droits des personnes concernées doivent être fournies en toute	Le client a-t-il la possibilité de récupérer et de supprimer les données à caractère personnel pour lesquelles il agit en qualité de responsable du traitement ? Cette possibilité est-elle accordée dans le cadre du service ou en autorisant le client à déployer son propre outil de renvoi /de suppression ?	Documentation sur les procédures/outils mis en place pour autoriser le client à récupérer/supprimer des données à caractère personnel.	28(3)(g)	Sous-traitant	

			transparence par le CISP au client.					

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
	Section 4.11. Registres des activités de traitement.	- Le CISP doit tenir un registre écrit (y compris sous forme électronique) des activités de traitement qu'il effectue pour le compte de ses clients qui sont des responsables du traitement, comprenant : • le nom et les coordonnées du client ; • les catégories de traitement effectué par le client (ces catégories peuvent être décrites dans des termes généraux, par exemple en référence aux services fournis par le CISP) ; • si le CISP a mis en œuvre ou met à disposition du client un mécanisme de transfert reconnu en vertu du Chapitre V du RGPD ; et • une description générale des mesures de sécurité mises en place (par exemple, les mesures adoptées pour se conformer à l'Annexe A). - Le CISP doit mettre ce registre à la disposition d'une Autorité de Contrôle sur demande.	Tenue des registres appropriés concernant les activités de traitement que le CISP exécute pour le compte de ses clients. Ces registres doivent contenir : -le nom et les coordonnées du client ; -les catégories de traitement effectué par le client (ces catégories peuvent être décrites dans des termes généraux, par exemple en référence aux services fournis par le CISP) ; - si le CISP a mis en œuvre ou met à disposition du client un mécanisme de transfert reconnu en vertu le cas échéant, les mécanismes que le CISP a mis en œuvre ou mis à la disposition du du Chapitre V du RGPD ; et - une description générale des mesures de sécurité mises en place (par exemple, les mesures adoptées pour se conformer à l'Annexe A).	Le CISP tient-t-il à jour des registres des activités de traitement qu'il met en oeuvre pour le compte de ses clients ?	Documentation relative aux registres des activités de traitement.	30(2)	Registres des activités de traitement.	

		- Le CISP maintiendra des registres des services utilisés par ses clients tel que requis par le RGPD ; toutefois, le client est la seule partie avec de la visibilité sur les détails spécifiques des données à caractère personnel qu'il choisit de traiter en utilisant ces services (et il a par ailleurs l'obligation de tenir des registres en application de l'Article 30(1) du RGPD).						

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
	Section 5.1 Un Contrat de Services qui prévoit une répartition des responsabilités entre le CISP et le Client pour la sécurité du service	- Le Contrat de Services doit définir les responsabilités en matière de sécurité du CISP et du client pour la durée dudit contrat.	5,1. Le partage des responsabilités est défini et documenté Le partage des responsabilités entre le CISP et le client doit être défini et documenté dans le Contrat de Services. Il doit être documenté au moyen d'une matrice basée sur un cadre reconnu (ISO27001 ou NIST) dans laquelle les responsabilités partagées du CISP ainsi que du client sont mises en évidence, de même que les responsabilités non attribuées (le cas échéant).	Le contrat de services prévoit-il une répartition claire des responsabilités entre le CISP et le client en ce qui concerne la sécurité du Service ? La description de la répartition des responsabilités entre le CISP et le client est-elle mise à disposition du client par le CISP?	Documentation relative au service ou au contrat de services, qui décrit le partage des responsabilités entre le CISP et le client. Autre documentation accessible au client concernant la répartition des responsabilités en matière de sécurité entre le CISP et le client.	28(3)(a)	Contrats de sous-traitance	La répartition des responsabilités entre le client et le prestataire de services n'est pas pleinement couvert par la norme ISO27001. La documentation relative à la répartition des responsabilités n'est pas requise par la norme ISO27001
	Section 5.2 Une déclaration de haut niveau sur les objectifs de sécurité et les normes applicables au service	- Le CISP doit déclarer (a) les objectifs que les mesures de sécurité mises en place par le CISP pour le service sont censées atteindre, et le cas échéant (b) les standards que le CISP s'engage à suivre pour la mise en œuvre de ces mesures de sécurité. Reportez-vous à l'Annexe A (Responsabilités en matière de Sécurité) pour plus d'informations. - Le CISP doit informer les clients lorsqu'un	5.2. Les objectifs en matière de sécurité et les normes de sécurité sont documentés Le CISP doit documenter les objectifs des mesures de sécurité mises en œuvre pour chaque service fourni ainsi que les normes appliquées pendant la mise en œuvre. Les procédures documentées doivent être	Les objectifs des mesures de sécurité mises en œuvre sont-ils documentés par le CISP ? Les normes appliquées par le CISP pendant la mise en œuvre des mesures de sécurité sont-elles définies et documentées par le CISP ?	Documentation, accessible au client, concernant les mesures de sécurité mises en œuvre par le CISP, Documentation, accessible au client, concernant les normes appliquées par le CISP pendant			Les mesures de sécurité sont couvertes par le cadre de contrôle de la norme ISAE3000 mais la documentation des objectifs, si les mesures mises en

		service d'infrastructure cloud a vocation à aider les clients à respecter une norme reconnue ou une disposition légale applicable à un type de traitement spécifique (ex : le traitement des données concernant la santé).	mises à jour régulièrement par le CISP. Le CISP doit informer le client lorsqu'un service spécifique a vocation à aider les clients à respecter une norme reconnue ou une disposition légale applicable à un type de traitement spécifique (ex : le traitement des données concernant la santé).	La documentation relative aux normes de sécurité applicables est-elle mise à jour régulièrement par le CISP ? Les services spécifiques visant à aider les clients à respecter une norme reconnue ou une disposition légale applicable à un type de traitement spécifique, sont-ils documentés et communiqués aux clients ?	la mise en œuvre des mesures de sécurité. Documentation, accessible au client, concernant la norme ou la disposition légale spécifique sur laquelle s'appuie l'infrastructure cloud.			œuvre sont requises, par la norme ISO27001.
	Section 5.3. Informations concernant la conception et la gestion du service	- Le CISP doit transmettre aux clients des informations sur l'infrastructure dont il dispose et sur la façon dont elle est utilisée pour fournir le service (c'est-à-dire les installations, le réseau, le matériel informatique et le logiciel opérationnel qui soutiennent la fourniture et l'utilisation des services).	5.3. Le service fourni par le CISP est documenté Le CISP doit communiquer au client des informations concernant le service fourni (architecture, localisation de l'hébergement, autres sous-traitants, dispositifs de sécurité, options de sécurité)	Le CISP a-t-il communiqué au client des informations concernant le service fourni ? (architecture, localisation de l'hébergement, autres sous-traitants, dispositifs de sécurité, options de sécurité)	Documentation, accessible au client, décrivant l'infrastructure fournie au client. Documentation, accessible au client, décrivant l'utilisation de cette infrastructure par le CISP. Ces informations peuvent inclure, par exemple : - L'architecture de haut niveau de l'infrastructure - La localisation générale des installations d'hébergement du CISP - L'autre sous-traitant autorisé par le CISP à accéder aux données client - Les dispositifs de sécurité du service			La norme ISO27001 n'impose pas la communication des services fournis par le prestataire de services (CISP).

					- Les options qui sont proposées au client pour renforcer la sécurité du service			

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
	Section 5.4 Informations à l'appui des processus de gestion du risque et des critères du CISP	- Le CISP doit fournir au client des informations démontrant l'existence et la pertinence du programme de gestion des risques du CISP afin que le client puisse utiliser et intégrer les contrôles du CISP dans son propre cadre de gestion des risques.	5.4. Le programme de gestion du risque du CISP est documenté Le CISP doit fournir au client des informations démontrant l'existence et la pertinence du programme de gestion des risques du CISP afin que le client puisse utiliser et intégrer les contrôles du CISP dans son propre cadre de gestion des risques.	Le CISP a-t-il fourni au client des informations démontrant l'existence et le caractère adéquat du programme de gestion du risque qu'il a mis en place ?	Documentation, accessible au client, concernant le cadre de gestion du risque établi par le CISP (méthodologie, outils, mesures, univers de risque, etc.) Rapports sur les évaluations du risque internes et/ou externes réalisées ou commanditées par le CISP, mis à la disposition du client			
	Section 5.5 Informations concernant les mesures de sécurité mises en place par le CISP pour le service	- Le CISP doit fournir toutes les informations nécessaires concernant les mesures de sécurité adoptées pour les services proposés aux clients, afin d'aider les clients à comprendre les dispositifs contrôles mis en place pour le service qu'ils utilisent et comment ces dispositifs de contrôle ont été approuvés. - Le CISP doit, en particulier, décrire : • les procédures de sécurité physique et opérationnelle pour l'infrastructure du réseau et du serveur sous la	5.5. Les mesures de sécurité du CISP sont documentées Les mesures de sécurité mises en place pour le service proposé aux clients doivent être documentées et communiquées par le CISP. Cette information doit inclure les mesures de sécurité sous la gestion du CISP (appliquées pour chaque client) et les mesures de sécurité qui peuvent être choisies par le client en option	Les informations concernant les mesures de sécurité mises en place pour le service proposé aux clients sont-elles suffisamment documentées et communiquées par le CISP ? Ces informations couvrent-elles les mesures de sécurité sous la gestion du CISP (appliquées pour chaque	Documentation, accessible au client, concernant les mesures de sécurité mises en place (procédures, guide, carte technique, etc.), couvrant par exemple : la sécurité physique et environnementale ; la sécurité du réseau ; la gestion de la continuité de l'exploitation ; la gestion des modifications			La norme ISO 27001 n'impose pas la communication des mesures de sécurité à des tiers par le prestataire de services.

		supervision du CISP ; et • les dispositifs et contrôle de sécurité disponibles pour l'utilisation et la configuration par les clients sur le service (sur chacun desquels le CISP doit maintenir une posture sécurisée par défaut). - Ces informations doivent inclure, par exemple, des informations concernant : • la sécurité physique et environnementale ; • la sécurité du réseau ; • des contrôles logiques ou physiques pour garantir l'isolement des données du client, comme la segmentation réseau des principes de stockage des données ; • la gestion de la continuité de l'exploitation ; • la gestion des modifications ; et les dispositifs de sécurité des comptes.		client) ainsi que les mesures de sécurité qui peuvent être choisies par le client en option ?	; et les dispositifs de sécurité des comptes.			

Cadre de Contrôle du CC du CISP						Articles du RGPD		
	Section du Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus pour respecter les Exigences du Code** **(Intitulé du contrôle et description du contrôle en accord avec les Exigences du Code)**	**Exemples de questions auxquelles le CISP doit répondre** **(incluses dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuves (ou documents équivalents) pour vérifier le respect des exigences du Code (à documenter par le CISP - à vérifier par l'Organisme de Contrôle sur site ou hors site selon la pertinence du contrôle en jeu)**	**Article n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
	Section 5.6 La documentation relative au système de gestion de la sécurité de l'information du CISP	Le CISP doit mettre à la disposition des clients suffisamment d'informations sur le système de gestion de la sécurité de l'information en place pour les services proposés aux clients afin que les clients puissent raisonnablement vérifier la conformité du CISP avec les obligations de sécurité du Contrat de Services telles que décrites à la Section 4.6 (Protection des Données ; Démontrer la conformité) du présent Code.	Le système de gestion de la sécurité de l'information du CISP est documenté Les informations concernant le système de gestion de la sécurité de l'information du CISP doivent être mise à la disposition du client afin que celui-ci puisse vérifier la conformité du CISP avec les obligations de sécurité telles qu'elles sont décrites dans le contrat de services.	Les informations concernant la documentation du système de gestion de la sécurité de l'information du CISP qui sont fournies au client sont-elles suffisamment détaillées pour permettre à celui-ci de vérifier la conformité du CISP avec les obligations de sécurité telles qu'elles sont décrites dans le contrat de services ?	Documentation, accessible au client, décrivant le programme de gestion de la sécurité de l'information du CISP.			
	Section 5.7 Informations concernant le fonctionnement du service qui permettent au client de i) rectifier, effacer, limiter, accéder ou transférer des Données Client ; et ii) récupérer et supprimer des Données Client.	- Le CISP doit communiquer au client des informations sur les capacités dont il dispose pour lui permettre de : - rectifier, effacer, limiter, accéder ou porter des Données Client conformément à la Section4.7 du présent Code (Droits des personnes concernées) ; et - récupérer et supprimer des Données Client conformément à la Section 4.10 du présent Code (Suppression ou renvoi de données à caractère personnel).	**Communication des capacités du CISP** Le CISP doit communiquer au client des informations sur les capacités dont il dispose pour lui permettre de : • rectifier, effacer, limiter, récupérer ou porter des Données Client ; et récupérer et supprimer des Données Client.	La documentation fournissant au client les informations concernant les capacités dont il dispose par le CISP est-elle suffisamment détaillée pour permettre au client de vérifier que le service du CISP lui permet de rectifier, d'effacer, de limiter, de récupérer ou de transférer des Données Client ?	Documentation fournissant au client les informations concernant les capacités dont il dispose pour lui permettre de : - Rectifier, effacer, - limiter, récupérer ou transférer des Données Client ; et - récupérer et supprimer des Données Client.			ISO/IEC 27018 : 2.1

Check-list de Conformité spécifique à l'Annexe A

Cadre de Contrôle du CC du CISP – Spécifique à l'Annexe – Responsabilités en matière de sécurité					Articles du RGPD		
Référence dans le Code CISPE	**Exigences du Code** **(À mettre en œuvre par le CISP et vérifiées par l'Organisme de Contrôle)**	**Contrôles prévus** **(Intitulé du contrôle et description du contrôle)**	**Questions à** **(inclure dans la vérification de l'état de préparation à la protection de la Vie privée de CISPE)**	**Preuve (ou documents équivalents) pour vérifier la conformité aux exigences du code (à documenter par l'entité)**	**Article** **n°**	**Nom**	**Commentaires sur la cartographie (lorsque partiellement couverte par ISO27001)**
(1) Gestion de la Sécurité des Informations	- Le CISP doit avoir une direction et un soutien clairs au niveau de la direction pour la sécurité du service. - Le CISP doit mettre en place un ensemble de politiques sur la sécurité de l'information approuvées par la direction qui régissent la sécurité du service. - Le CISP doit mettre en œuvre un système de gestion de la sécurité de l'information ou un dispositif équivalent. Le champ d'application du système de gestion de la sécurité de l'information doit couvrir le service. - Le CISP doit désigner un ou plusieurs membres de son personnel pour coordonner et assumer la responsabilité du système de gestion de la sécurité de l'information.	• S'assurer que les politiques et procédures sur la sécurité de l'information couvrent, au minimum : (a) la portée et les limites du programme sur la sécurité de l'information, y compris l'activité, l'organisation, les emplacements, les actifs et la technologie ; (b) les politiques d'utilisation qui définissent un usage approprié des technologies importantes comme les appareils mobiles, la technologie sans fil, les e-mails et internet ; et (c) les tâches et missions de gestion et de mise en œuvre des politiques sur la sécurité de l'information. • S'assurer que le cadre de la politique sur la sécurité de l'information du CISP couvre, au minimum, les aspects suivants : (a) gestion d'actifs ; (b) ressources humaines ; (c) contrôles d'accès ; (d) sécurité physique et environnementale ; (e) cycle de vie du développement d'un système ; (f) gestion des incidents ; (g) continuité de l'exploitation ; (h) conformité ; et (i) utilisation d'un appareil mobile.		Documentation, accessible au client, concernant les normes appliquées par le CISP pendant la mise en œuvre des mesures de sécurité. Documentation, accessible au client, concernant la norme ou la disposition légale spécifique sur laquelle s'appuie l'infrastructure cloud			ISO/IEC 27001 : A.5

		• Communiquer les politiques sur la sécurité de l'information à tous les membres du personnel du CISP (y compris les fournisseurs et partenaires commerciaux), ainsi que les mises à jour régulières. • Développer des procédures opérationnelles visant à orienter l'exploitation des systèmes et des services dans l'environnement du CISP, le cas échéant.					

(2) Sécurité des Ressources Humaines	- Le CISP doit mettre en place une structure organisationnelle pour gérer la mise en œuvre de la sécurité de l'information dans les services qu'il propose, avec une définition claire des rôles et responsabilités. - Le CISP doit créer une organisation pour la sécurité de l'information gérée par son personnel de sécurité et dirigée par le Responsable de la Sécurité de l'Information (CISO) ou toute personne occupant un poste équivalent. L'organisation de la sécurité du CISP doit établir et maintenir des politiques et procédures officielles visant à définir des normes d'accès logique au système et à l'infrastructure hébergés par le CISP. Ces politiques identifient également des responsabilités fonctionnelles pour l'administration de l'accès logique et de la sécurité. Le CISP assure la formation de ses employés et prestataires à ces politiques et procédures. Des procédures doivent être mises en place pour ajouter, modifier ou désactiver les comptes utilisateurs des employés et prestataires du CISP, le cas échéant, et pour examiner ces comptes de façon périodique. Par ailleurs, la configuration de mots de passe complexes pour l'authentification des utilisateurs sur les systèmes du CISP est gérée conformément à la politique de mot de passe du CISP qui doit s'aligner sur la norme en vigueur en matière de mot de passe, notamment en ce qui concerne la complexité	• S'assurer que le conseil d'administration du CISP soit tenu informé des incidents, des menaces et du statut des dispositifs d'amélioration de la sécurité. • Mettre en place un programme de sensibilisation aux questions de sécurité pour les membres du personnel du CISP afin de s'assurer qu'ils adoptent les bons comportements et possèdent les compétences nécessaires pour garantir la sécurité du CISP. • Mettre à jour le programme de sensibilisation aux questions de sécurité du CISP pour faire face aux nouvelles technologies, aux menaces, aux normes, au respect de la vie privée et à la protection des données et aux exigences opérationnelles. • Proposer une formation axée sur les fonctions de sécurité sur la base des responsabilités confiées au personnel du CISP et du client avant d'autoriser l'accès aux systèmes du CISP ou d'exécuter les tâches assignées. • Assurer un suivi des activités de formation à la sécurité exécutées par le personnel du CISP pour vérifier la conformité aux exigences de formation telles que définies par le Code et le RGPD. • S'assurer que le personnel du CISP et du client ait lu et compris la politique et les procédures du CISP		Politiques sur la sécurité, politiques sur la sécurité des Ressources Humaines, formations sur la sécurité (sur site/en ligne), politiques sur les technologies de l'information, politiques de mots de passe.			ISO/IEC 27001 : A.6.1 A.7.2

	minimale, la longueur, l'historique du mot de passe, le blocage en cas d'échecs d'authentification répétés ou l'authentification multi-facteurs. Les demandes de modification d'accès doivent être enregistrées au moyen d'un outil de gestion des autorisations, sur un journal d'audit, ou tout dispositif équivalent. Le CISP doit appliquer le principe de moindre privilège, en accordant aux utilisateurs un accès strictement nécessaire pour mener à bien leurs missions. Les comptes utilisateurs sont conçus pour fournir un accès minimum. Tout accès au-delà de ces moindres privilèges requiert une autorisation préalable.	en matière de sécurité de l'information. Veiller à ce que tous les utilisateurs ayant accès à un compte administratif utilisent un compte dédié ou secondaire pour les activités complexes, avec des mesures de sécurité spécifiques (ex : complexité du mot de passe authentification multi-facteurs, traçabilité des événements pertinents, etc.). Ce compte doit servir uniquement pour les activités administratives et non pas pour naviguer sur internet, envoyer des e-mails ou pour des activités similaires. • Limiter l'accès du personnel du CISP, afin qu'il puisse accéder uniquement aux informations relatives aux éléments structurels de l'infrastructure cloud, à leur configuration et à la configuration des environnements logiques attribués aux clients. Mettre en place des dispositifs de contrôle afin de bloquer l'accès du personnel du CISP aux données des clients et aux données applicatives, à moins qu'un client ne soumette explicitement une demande d'assistance, de maintenance ou de mise à jour. • Mettre en œuvre des mécanismes de contrôle de façon à empêcher les membres du personnel du CISP de garder les sessions de l'infrastructure ouvertes pendant leur absence. • Établir des politiques visant à interdire au					

		personnel du CISP de conserver par écrit les données d'identification nécessaires pour accéder à l'infrastructure physique du CISP, à l'exception d'un mot de passe superutilisateur, connu de l'administrateur système et conservé par le gestionnaire					

(3) Gestion de l'Accès des Utilisateurs	- Le CISP doit fournir au client un système de gestion des contrôles d'accès pour que le client puisse accéder en tant qu'utilisateur au service d'infrastructure cloud dans le cadre du service. Ce système de gestion des contrôles d'accès doit comprendre, par exemple, des comptes nominatifs (qui peuvent être un compte utilisateur ou un compte de service), un contrôle d'accès à base de rôles et des mots de passe ou d'autres moyens ou politiques d'authentification. Le CISP doit expliquer au client comment fonctionne le système de gestion des contrôles d'accès afin que le client puisse l'utiliser et le configurer conformément aux instructions fournies ci-après.	• Assurer la gestion active de la durée de vie des comptes, y compris la création, l'utilisation et la suppression des comptes, afin de minimiser les possibilités pour les attaquants de les exploiter. • Désactiver les comptes utilisateurs CISP inactifs après une période d'inactivité définie. • S'assurer que les sessions utilisateurs CISP soient automatiquement bloquées après une certaine période d'inactivité. • Gérer activement des systèmes de gestion des accès axés sur les rôles et les profils • Fournir un accès administratif aux clients pour la configuration d'un environnement logique avec des connexions sécurisées et chiffrées à la demande spécifique du client.		Politiques sur la gestion de l'accès des utilisateurs			ISO/IEC 27001 : A.9

(4) Sécurité physique et environnementale	- Le CISP doit mettre en place et maintenir des mesures de sécurité physique et environnementale de pointe pour le service d'infrastructure cloud, destinées (i) à aider les clients à protéger leurs données à caractère personnel contre le traitement non autorisé et contre la perte, l'accès ou la divulgation, de manière accidentelle ou illicite et (ii) à empêcher les menaces raisonnables pour l'environnement comme les incendies et les inondations.	• Le zonage des espaces d'hébergement en fonction de leur criticité. La mise en œuvre et le contrôle de ce zonage au moyen de cloisons, clôtures, portes et portillons de sécurité dont l'accès est contrôlé, placé sous vidéosurveillance et surveillé. • L'utilisation de systèmes physiquement et logiquement dispersés pour isoler et exécuter les logiciels qui engendrent des risques plus importants pour le client. • La gestion de l'accès aux centres de données et aux cages au moyen d'un système d'authentification visuelle ou d'un badge, qui limite l'accès permanent aux installations et zones sécurisées du CISP uniquement au personnel autorisé et approuvé. La mise en place d'un système par lequel un visiteur (c'est-à-dire une personne dont l'accès n'est pas indispensable) doit soumettre une demande pour accéder aux installations et zones sécurisées du CISP, et documenter cette demande, au moyen d'un mécanisme approuvé par le CISP, laquelle demande sera uniquement approuvée par le personnel autorisé du CISP. • La vérification de l'identité des visiteurs qui accèdent aux installations et zones sécurisées du CISP au moyen d'une pièce d'identité officielle avec photo (ex : permis de conduire, passeport, etc.) ou d'une pièce d'identité avec photo délivrée par un CISP.		Politiques relatives à la sécurité physique et environnementale.			ISO/IEC 27001: A.11.1 A.11.1.4 A.13.1

(5) Serveurs et équipements physiques, y compris les pare-feux	- Le CISP est seul responsable du déploiement, du fonctionnement et de la sécurité du matériel physique, du système d'exploitation *hôte*, et de la couche de virtualisation, utilisés pour fournir le service d'infrastructure cloud, y compris la configuration nécessaire à la prestation de ce service. - Le CISP doit installer un mécanisme permettant de filtrer les flux de données, comme un pare-feu, autour du périmètre de l'infrastructure cloud dans son ensemble et/ou un pare-feu pour isoler l'instance de service qui est déployée. S'il existe un mécanisme de filtre (tel qu'un pare-feu) pour protéger l'infrastructure du CISP, dans sa globalité, il appartient au CISP de le configurer.	• Établir une base de données pour la gestion de la configuration qui couvre tous les serveurs et équipements physiques et gérer la durée de vie de ces actifs. • Mettre en œuvre des contrôles de sécurité pour garantir la sécurité de la chaîne logistique et assurer la traçabilité des opérations. • Installer et configurer un système de filtrage « data plane » sur les environnements câblés et sans fil pour protéger le réseau du CISP des réseaux externes comme internet. Par exemple, utiliser un pare-feu déployé par un réseau. • S'assurer que les politiques de cloisonnement du réseau (« data plane »), par exemple les règles d'utilisation des pare-feux, respectent les configurations approuvées. Par exemple, (a) les ports, protocoles et services inutiles doivent être restreints sur les périphériques réseau ; (b) les appareils doivent être configurés en mode HD (Haute Disponibilité) ; et (c) les politiques « data plane » (ex : configurations des dispositifs de pare-feu) doivent prévoir un « blocage d'IP étendu » pour la liste d'accès border-net, qui interdit tout ce qui n'est pas spécifiquement approuvé dans les listes de contrôle d'accès. • S'assurer que les politiques « data plane » sont approuvées par un membre dirigeant du CISP et testées avant leur mise en œuvre. • S'assurer que les configurations des pare-feux et les listes de contrôle		Politiques relatives aux serveurs et équipements physiques.			ISO/IEC 27001 : A.8.1 A.15.1 A.13.1

		d'accès (« ACL ») sont gérées par un ingénieur réseau conformément à des ensembles de règles approuvés. Par exemple : (a) l'outil de gestion des ACL doit servir à déployer des ACL approuvées sur les pare-feux du réseau de production ; et (b) si l'accès à un pare-feu ou un périphérique réseau est impossible au moyen de l'outil de gestion des ACL, le problème doit être examiné et corrigé. • S'assurer que les règles applicables aux pare-feux sont examinées et approuvées par l'équipe en charge de la sécurité de l'information. • Étendre les politiques « data plane » aux périphériques réseau en fonction de la plateforme, de l'emplacement et du réseau.					

(6) Gestion de la protection des logiciels malveillants	- Le CISP doit mettre en place un dispositif de protection contre les logiciels malveillants sur les systèmes sensibles (à savoir les systèmes fréquemment affectés ou ciblés) qui font partie du service d'infrastructure cloud.	• Installer une protection par anti-virus sur les serveurs du réseau et sur les postes de travail. • Configurer cet anti-virus dans le but de : (a) vérifier les e-mails, les pièces jointes aux e-mails, les accès internet, et les supports amovibles ; (b) vérifier les fichiers système critiques pendant le démarrage du système ; et (c) bloquer et mettre en quarantaine les codes malveillants et envoyer des alertes à l'administrateur de la sécurité du CISP. • Configurer des systèmes permettant la mise à jour automatique des logiciels anti-virus. • S'assurer que tous les logiciels installés sur une plateforme sont des logiciels systèmes téléchargés à partir de sources authentifiées.		Politiques de gestion de la protection des logiciels malveillants.			ISO/IEC 27001 : A.12.2 A.12.5 A.12.6
(7) Gestion des vulnérabilités	- Le CISP doit définir un niveau d'engagement (répartition des tâches entre le CISP et le client, délai entre la définition des correctifs et la mise en œuvre de ces correctifs, etc.) pour le	• Souscrire à un service de veille des vulnérabilités et enregistrer toutes les vulnérabilités dans la base de données de gestion de configuration du CISP. Analyser toutes les vulnérabilités applicables à un actif afin de définir un ordre de priorité dans la mise en œuvre des correctifs.		Politiques de gestion des vulnérabilités.			ISO/IEC 27001 : A.6.1.4 A.12.6 A.14.2

	service d'infrastructure cloud. - Le CISP est responsable, sauf indication contraire expresse du client dans le Contrat de Services, de la correction des bugs du matériel informatique, de la mise en réseau du matériel informatique, de la couche de virtualisation et des systèmes d'exploitation *hôtes*.	• S'assurer que les systèmes d'exploitation hôtes exécutent les dernières mises à jour de sécurité fournies par le fournisseur de logiciel. • Effectuer des tests de pénétration pour identifier les vulnérabilités et attaquer les vecteurs qui pourraient être utilisés pour exploiter des progiciels.					
(8) Journalisation et Monitoring	- Le CISP fournit au client des outils de contrôle (ex : niveau, portée, compte-rendu, interfaces, API) et de journalisation et/ou rapports de suivi (ex : accès, enregistrements, durée d'enregistrement) pour le service d'infrastructure cloud.	• Dresser une liste des événements système qui doivent être enregistrés, notamment les événements suivants : (a) les réussites et échecs d'authentifications et de tentative d'authentification ; (b) les événements liés à la gestion des comptes ; (c) les préférences en termes de fonctionnalités ; (d) le démarrage et l'arrêt du système ; (e) les suppressions de données, l'accès aux données et les modifications de données ; et (f) les événements infructueux (par exemple, les appels non autorisés). • Mettre en place des journaux sur les systèmes pour enregistrer au moins les informations suivantes, pour chaque événement système (y compris les événements utilisateur, les événements système et les événements de sécurité) : (a) identification de l'utilisateur (y compris le service, le correspondant et l'utilisateur) ; (b) type d'événement ou API contactée ; (c) date et fuseau horaire ; (d) source de l'événement système ; (e) résultat de l'événement système ; et (f) identité du composant ou de la ressource affecté(e) du système. • Collecter des journaux à partir de tous les		Politiques de journalisation et de monitoring.			ISO/IEC 27001 : A.12.4

		systèmes, dispositifs et composants de réseau vers un service d'enregistrement centralisé qui répartit la capacité de stockage des audits et configure ces audits de façon à minimiser le risque que cette capacité soit dépassée et à conserver les audits enregistrés pour une période définie.					

		• Agréger, corréler, examiner et analyser les journaux pour identifier des anomalies et autres événements malveillants potentiels. • Contrôler les systèmes et les installations pour détecter les événements de sécurité potentiels, et configurer ces systèmes et installations afin qu'ils génèrent automatiquement des alertes pour signaler ces événements au personnel approprié. • Protéger les journaux contre l'accès non autorisé. Par exemple, en limitant l'accès aux journaux au personnel autorisé du CISP et en mettant en place un logiciel infalsifiable/visible ou de détection des changements pour détecter la falsification des informations contenues dans ces journaux.					

(9) Équipements en fin de vie	Le CISP doit établir un procédé de désinstallation des supports de stockage avant la mise à disposition finale du support de stockage utilisé pour stocker les Données Client lorsque ce support est en fin de vie, afin d'empêcher que les Données Client ne soient exposées à des personnes non autorisées. Le processus de désinstallation sera mené conformément aux usages du secteur (selon la description fournie dans la norme ISO/IEC 27002 ; ou dans les NIST 800-88) pour s'assurer que les Données Client ne peuvent pas être extraites du type de support de stockage utilisé au moyen d'un outil d'extraction de données ou d'informations ou d'autres moyens similaires.	• Utiliser, par exemple, les techniques décrites dans le DoD 5220.22-M (« Manuel Opérationnel du Programme National sur la Sécurité Industrielle ») ou les NIST -88 (« Lignes Directrices sur l'Effacement des Données ») pour détruire les données dans le cadre du processus de désinstallation. • Démagnétiser et détruire physiquement tous les appareils de stockage magnétiques désinstallés conformément aux usages du secteur. • Protéger les supports contre la divulgation non autorisée ou les abus jusqu'à ce qu'ils soient détruits. • Surveiller la manipulation et la conservation des supports. • S'assurer que les supports de stockage utilisés sur un hôte ou un système ne sont jamais réutilisés sur un autre hôte ou système. • Stocker tous les supports dans une poubelle sécurisée, verrouillée/inviolable, dès qu'ils sont été retirés des appareils source. La poubelle doit se situer dans la cage ou le module où les disques durs ont été retirés. • S'assurer que le support n'est pas transporté en dehors du site sans autorisation préalable et que tout support transporté à l'extérieur des locaux du CISP n'est pas laissé sans surveillance dans un espace public. • Protéger le support pendant son transport en dehors des frontières		Politiques relatives aux équipements en fin de vie.			ISO/IEC 27001 : A.8 A.11.2.5 A.11.2.6 A.11.2.7

		physiques du CISP et s'assurer que les activités associées au transport du support sont strictement réservées au personnel autorisé, qui est surveillé et documenté.					

Légende

Couvert par la norme ISO27001
Partiellement couvert par la norme ISO27001
Non couvert par la norme ISO27001

Les exigences couvertes par la norme ISO27001 et les exigences partiellement couvertes par la norme ISO27001 sont collectivement désignées les Exigences Auditables du Code.

Annexe C – Modèle de Déclaration d'Adhésion

Il s'agit d'une Déclaration d'Adhésion **(« Déclaration »)** au Code de Conduite des Fournisseurs de Services d'Infrastructure Cloud relatif à la Protection des Données (le **« Code »).** À moins qu'ils ne soient définis autrement, les termes portant une majuscule qui sont utilisés dans la présente Déclaration auront la signification qui leur est attribuée dans le Code.

(1) Services couverts par cette Déclaration

La présente Déclaration couvre le(s) service(s) d'infrastructure cloud ci-dessous (les **« Services »**). Si cette Déclaration concerne plusieurs services, veuillez fournir des détails pour chaque service mentionné ci-dessous.

	Nom du Service (Apparaîtra sur le Registre Public CISPE)	**Autres informations** (Facultatif et n'apparaîtra pas sur le Registre Public CISPE)
Service 1	[Insérer]	[Insérer]
Service 2	[Insérer]	[Insérer]
etc.		

(2) Déclaration faite par le CISP

Cette Déclaration doit être faite par une entité qui agit en tant vendeur de référence du/des Service(s) (le **« CISP »**). Si cette Déclaration est faite par plusieurs CISPs, veuillez fournir des détails pour chaque CISP mentionné ci-dessous et dans la déclaration visée à la Section 5. Ces informations apparaîtront sur le Registre Public CISPE

	Dénomination sociale	**Adresse**
Vendeur de Référence 1	[Insérer]	[Insérer]
Vendeur de Référence 2	[Insérer]	[Insérer]
etc.		

(3) Procédure de déclaration

Cette Déclaration est faite conformément à :

- la procédure d'Autoévaluation.
- la procédure d'Adhésion Contrôlée.

Votre choix déterminera la Marque que le CISP est en droit d'utiliser en lien avec le(s) Service(s). Dans chaque cas, la Déclaration d'Adhésion doit être accompagnée d'une Check-list de Conformité complète et démontrer la conformité par référence à la Check-list de Conformité.

(4) Check-list de Conformité

Les Exigences du Code mentionnées dans la Check-list de Conformité comme étant auditables sont des Exigences Auditables du Code. Veuillez joindre la Check-list de Conformité et des copies de toutes pièces justificatives référencées en ce qui concerne les Exigences Auditables du Code.

Indiquez si le(s) document(s) à l'appui couvrent uniquement des Services en particulier. Si vous utilisez plusieurs documents à l'appui pour plusieurs services, vous devez compléter la Check-list de Conformité séparément pour chaque Service.

(5) Organisme de Contrôle proposé

Veuillez insérer le nom complet et l'adresse de l'Organisme de Contrôle que vous proposez :

	Dénomination sociale	**Adresse**
Organisme de Contrôle	[Insérer]	[Insérer]

(6) Confirmation par l'Organisme de Contrôle (uniquement pour les Déclarations effectuées selon la procédure d'Adhésion Contrôlée)

Veuillez joindre une confirmation écrite délivrée par l'Organisme de Contrôle indiquant que le service du CISP est conforme aux Exigences Auditables du Code. (Cette confirmation doit être signée par l'Organisme de Contrôle compétent.)

(7) Déclaration

En apposant sa signature ci-dessous, le(s) CISP(s) confirme(nt) que :

(a) à la date de la présente Déclaration les Services respectent les Exigences du Code ;

(b) si le CISP a choisi la Procédure d'Auto-Adhésion, le CISP doit soumettre le Service pour examen à l'Organisme de Contrôle dans les 12 mois suivant la consignation de cette Déclaration dans le Registre Public CISPE ;

(c) le CISP doit se conformer aux procédures d'examen, de réclamation et de mise à exécution définies par l'Organisme de Contrôle dans la Section 7 (Gouvernance) du Code ; et

(d) si un changement au niveau d'un ou plusieurs Services nécessite de mettre à jour le matériel mentionné dans la Déclaration, alors (i) le CISP doit immédiatement en informer le Secrétariat, et
(ii) coopérer avec le Secrétariat pour opérer les mises à jour du matériel en question.

[NOM DU CISP 1]

Par : _____

Nom : _____

Fonction : _____

Date : _____

[NOM DU CISP 2]

Par : _____

Nom : _____

Fonction : _____

Date : _____

Annexe D – Autorités de Contrôle de l'EEE

Autriche	Österreichische Datenschutzbehörde
Belgique	Autorité de protection des données - Gegevensbeschermingsautoriteit
Bulgarie	Commission for Personal Data Protection
Croatie	Croatian Personal Data Protection Agency
Chypre	Commissioner for Personal Data Protection
République Tchèque	The Office for Personal Data Protection
Danemark	Datatilsynet
Estonie	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)
Finlande	Médiateur à la protection des données
France	Commission Nationale de l'Informatique et des Libertés – CNIL
Allemagne	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Grèce	Hellenic Data Protection Authority
Hongrie	National Authority for Data Protection and Freedom of Information
Islande	The Icelandic Data Protection Authority
Irlande	Data Protection Commissioner
Italie	Garante per la protezione dei dati personali
Lettonie	Data State Inspectorate
Liechtenstein	Data Protection Office
Lituanie	State Data Protection
Luxembourg	Commission Nationale pour la Protection des Données
Malte	Office of the Data Protection Commissioner
Pays-Bas	Autoriteit Persoonsgegevens
Norvège	Datatilsynet
Pologne	The Bureau of the Inspector General for the Protection of Personal Data – GIODO
Portugal	Comissão Nacional de Protecção de Dados – CNPD
Roumanie	The National Supervisory Authority for Personal Data Processing
Slovaquie	Office for Personal Data Protection of the Slovak Republic
Slovénie	Information Commissioner
Espagne	Agencia de Proteccion de Datos

Suède	Datainspektionen
Royaume-Uni	The Information Commissioner's Office

Annexe E – Synthèse des Consultations des Acteurs

Les consultations du CISPE sont divisées en plusieurs catégories : (i) consultation interne entre les membres du CISPE (ii) consultation avec la task force CCTF créée par CISPE pour un examen du Code par des pairs, avec la participation d'experts indépendants du secteur (iii) échanges réguliers avec les organismes publics et réglementaires (iv) organisation de réunions publiques et participation à ces réunions (v) consultations avec des experts indépendants de la sécurité des données et des prestataires d'assurance/d'audit, y compris les candidats potentiels à l'Organisme de Contrôle. Ces consultations se sont tenues dans un esprit de transparence et d'ouverture pour améliorer le Code au bénéfice des utilisateurs d'infrastructures cloud.

1. Consultation interne entre les membres du CISPE

CISPE compte 27 membres représentant des entreprises de plusieurs tailles dont les établissements principaux se situent dans plus de 14 États Membres de l'Union européenne. À chaque étape de l'élaboration du Code, les membres ont été consultés sur la dernière version et invités à approuver cette version.

Par ailleurs, plusieurs organisations non-membres de CISPE ont tout de même déclaré que les services qu'elles proposent respectent les dispositions du Code. À l'heure actuelle, plus de 107 services d'infrastructure cloud ont été déclarés comme respectant les dispositions du Code sous son ancienne forme (non approuvée). Des discussions se sont tenues avec plusieurs de ces CISPs adhérents concernant les exigences du Code. Les organisations adhérentes ont publié leur adhésion au Code, par exemple sur le site internet de leur société, et les réactions de leurs clients ont été prises en compte.

CISPE a également sollicité les experts du cabinet d'avocats Baker McKenzie pour l'élaboration du Code et pour évaluer son positionnement sur le marché, y compris du point de vue des organisations clientes.

Des cabinets d'audit de renommée internationale ont collaboré avec les membres du CISPE dans l'élaboration de la substance du Code.

Les analystes IDC et Gartner ont interrogé les membres du CISPE à propos de l'élaboration du Code et de sa pertinence pour les utilisateurs d'infrastructures cloud en Europe et au-delà des frontières européennes. Tous deux ont publié un rapport sur l'évaluation du Code CISPE.

2. CCTF (Task Force du Code de Conduite)

La Task Force du Code de Conduite a été créée volontairement par CISPE début 2017 en tant qu'organe statutaire, dans l'objectif de faire évaluer le Code par des pairs et d'obtenir leurs points de vue sur le Code au fur et à mesure de son élaboration. La CCTF se compose à la fois de : 1) représentants des membres du CISPE chargés spécifiquement d'évaluer le Code par des pairs du point de vue des acteurs du marché (y compris Dada, SolidHost, Ikoula, OVH, Outscale et Amazon Web Services) ; 2) experts indépendants non-membres du CISPE qui ont été invités à exprimer leur propre point de vue (y compris d'autres cabinets d'avocats, universitaires, centres de protection des données, ISP, et autres prestataires de services cloud non affiliés à CISPE). EuroCIO, l'association des CIO européens a également accepté de jouer le rôle d'Observateur au sein de la CCTF.

La CCTF a été consultée sur toutes les itérations de l'élaboration du Code au fur et à mesure de son évolution depuis sa formation, au travers des réunions suivantes :

22/5/2017 – Réunion de la CCTF

Première réunion de la CCTF pour examiner le Code CISPE et formuler des observations sur sa dernière version.

23/06/2017 – Réunion CCTF CISPE avec des Invités

Réunion à Florence entre les membres de la CCTF et les clients italiens du CISPE, notamment l'Italian chapter de

l'EuroCIO, dans l'objectif de saisir les points de vue des clients sur le Code CISPE.

20/10/2017 – Réunion CCTF CISPE

Réunion de la CCTF en Espagne pour discuter de la dernière version du Code CISPE et formuler des observations à cet égard.

28/11/2017 – Réunion CCTF CISPE

Nouvelle réunion pour discuter de la récente lettre du G29 et des aspects spécifiques du Code CISPE et formuler des observations concernant les éléments à améliorer.

17/12/2017 – Appel du CISPE avec la participation de la CCTF

Point téléphonique avec la CCTF pour discuter des observations qu'elle a formulées à l'égard du Code CISPE.

08/01/2018 – Appel CCTF CISPE

Discussion sur les aspects spécifiques du Code qu'il convient d'améliorer.

05/02/2018 – Appel CCTF CISPE

Nouvelle discussion détaillée sur les aspects à améliorer dans la version préliminaire du Code CISPE.

27/02/2018 – Appel CCTF CISPE

Analyse et discussion à propos des observations du Groupe de Travail « Article 29 » sur la version préliminaire du Code CISPE et instructions concernant les nouvelles améliorations à apporter à l'élaboration du Code.

22/3/2018 – Réunion du Conseil Mixte du CISPE et de la CCTF

Atelier de deux jours pour discuter des nouvelles révisions de la version préliminaire du Code CISPE à la lumière des observations formulées par le Groupe de Travail « Article 29 ».

26/04/2018 – Appel CCTF CISPE

Nouvelle discussion détaillée sur les dernières itérations de l'élaboration du Code CISPE et observations formulées à CISPE concernant certains aspects spécifiques.

03/05/2018 – Appel CCTF CISPE

Nouvel appel de la CCTF pour discuter des améliorations dans l'élaboration de certains aspects spécifiques du Code.

28/06/2018 – Réunion CCTF CISPE

Réunion pour discuter d'une nouvelle version préliminaire du Code qui répond aux observations du G29.

30/10/2018 – Réunion CCTF CISPE

Réunion pour discuter en détail des commentaires de la CNIL sur la version préliminaire du Code CISPE et des améliorations potentielles pour y répondre, ce qui a permis de faire des observations à CISPE sur les améliorations rédactionnelles.

10/04/2019 – Appel CCTF CISPE

Appel pour discuter en détail des commentaires de la CNIL sur la version préliminaire du Code CISPE et des

améliorations potentielles pour y répondre, ce qui a permis de faire des observations à CISPE sur les améliorations rédactionnelles.

3. Consultations avec des organismes publics et réglementaires

Depuis les premières versions du Code CISPE, de nombreux échanges ont eu lieu avec les représentants des Autorités de Protection des Données (DPA), la Commission européenne et les États Membres.

- **Autorités de Protection des Données :** CISPE et ses membres ont échangé avec plusieurs DPA dans les pays où les membres du CISPE ont établi leur siège et sont actifs. Le Code a tout d'abord été soumis spécifiquement à la consultation du Groupe de Travail « Article 29 » en mars 2017, qui a fourni des commentaires sur son élaboration en février 2018. En mai 2018, une audience s'est tenue avec le Groupe de Travail « Article 29 » concernant des éléments spécifiques. Les Autorités de Contrôle d'Italie, de Suède, de France, de République tchèque, de Hongrie, du Luxembourg, d'Allemagne, des Pays-Bas, du Royaume-Uni, d'Espagne, de Lettonie, d'Irlande, de Grèce ont participé à cette audience, de même que le Contrôleur Européen de la Protection des Données. Le Code a ensuite été soumis à la CNIL pour d'autres observations informelles.
- **Commission européenne :** Depuis février 2006, CISPE et ses membres échangent régulièrement avec des fonctionnaires de la Commission européenne à propos du Code CISPE. Les Directions Générales concernées sont les suivantes : la DG JUST, la DG CONNECT, la DG GROW, la DG IT et la DG HOME.
- **États Membres :** Les membres du CISPE ont régulièrement organisé des réunions avec les États Membres, dans les pays où ils opèrent, notamment la France, l'Allemagne, l'Espagne, la Pologne, le Danemark/le Conseil Nordique, le Royaume-Uni, l'Irlande, Malte et l'Italie. CISPE a également été invité à présenter le Code CISPE lors du Sommet franco-allemand du numérique du 13 décembre 2016.

4. Réunions publiques

Les membres du CISPE ont activement participé à plusieurs réunions avec des acteurs du secteur, notamment le groupe EC Digital Single Market (DSM) Cloud, Cloud Select Industry Group (CSIG), et à des ateliers sur la sécurité du cloud, et ont présenté les concepts fondamentaux du Code lors de ces réunions. Ces réunions ont donné la possibilité de discuter du contenu du Code CISPE et de recueillir les observations des utilisateurs du cloud et d'autres acteurs.

Date	Localisation	Réunion	Commentaires
27 juin 2016	Belgique, Bruxelles	EC Cloud Select Industry Group (CSIG)	Première réunion plénière du groupe C-SIG durant laquelle CISPE a présenté sa version préliminaire du Code CISPE.
27 septembre 2016	Belgique, Bruxelles	Parlement européen	Annonce publique du Code CISPE.
20 septembre 2016	Pays-Bas, Amsterdam	HostingCon	Présentation publique du Code CISPE.
24 janvier 2017	France, Lille	Forum international de la cybersécurité (FIC 2017)	Séance plénière/Experts RGPD. Présentation du Code CISPE.
7 février 2017	Belgique, Bruxelles	Xupery workshop « The GDPR : How codes of conduct will meet the challenges »	CISPE a participé au débat et a présenté le Code CISPE.
15 février 2017	Belgique, Bruxelles	EC Cloud Select Industry Group (CSIG)	Présentation du Code CISPE.
28. mars 2017	Allemagne, Rust	World Hosting Days	Présentation du Code CISPE.
27-30 mars 2017	Allemagne, Rust	World Hosting Days	CISPE a diffusé des informations concernant le Code CISPE.

25 avril 2017	France, Paris	Association Française des Hébergeurs Agréés de Données de Santé à Caractère Personnel (AFHADS)	Présentation du Code de Conduite CISPE.
14 juin 2017	Pays-Bas, Amsterdam	Board EuroCIO	Échange de points de vue sur le Code CISPE.
23 juin 2017	Italie, Florence	CISPE	Réunion avec les utilisateurs des clouds italiens
29 juin 2017	Belgique, Bruxelles	Réunion EC DSM Cloud Stakeholder	CISPE a dressé un état des lieux du Code CISPE.
5 juillet 2017	France, Paris	Cloud Week Paris	Séance d'experts RGPD. Présentation du Code CISPE.
22 août 2017	Uruguay, Montevideo	Personal Data Protection Forum	Présentation du Code CISPE.
22 septembre 2017	France, Paris	CYGAL/Systematic	Présentation du Code CISPE.
17 octobre 2017	France, Paris	OVH Summit	Séance de travail des analystes du marché sur le Code CISPE.
6-7 novembre 2017	Belgique, Bruxelles	IAPP Europe Data Protection Congress 2017	Présentation du Code CISPE lors de deux séances : « Accountability Made Easy with the GDPR Tools » et « Deciphering GDPR: DPIA, Data Breach Notification, Portability and Security »
17 novembre 2017	Pologne, Lodz	The Convent of Data Protection Poland	Présentation du Code CISPE.
23 novembre 2017	Danemark, Copenhague	Cloud Forum Denmark	Présentation du Code CISPE.
6 décembre 2017	Royaume-Uni, Londres	FinTech Connect	Présentation du Code CISPE.
7 décembre 2017	Belgique, Bruxelles	EBF Cloud Banking Forum	Présentation du Code CISPE lors d'une réunion d'experts.
10 mars 2018	Allemagne, Rust	Cloud Fest (anciennement World Hosting Days)	Présentation du Code CISPE.
19 avril 2018	France, Sophia Antipolis	ETSI	Sommet – « Releasing the flow – data protection & privacy » Présentation du Code CISPE lors d'une réunion d'experts.
19 avril 2018	Belgique, Bruxelles	AWS Public Sector Summit	Présentation du Code CISPE lors de la réunion « GDPR: Security and data protection at the core of your strategy ».
20 septembre 2018	France, Paris	Cloud study trip	Présentation du Code CISPE des associations cloud néerlandaise et danoise.
6 décembre 2018	Autriche, Vienne	EC DSM Cloud Stakeholder Group	Présentation du panel sur les Codes de Conduite – Présentation du Code CISPE

Annexe F – Modèle de Notification d'une Violation de Sécurité

Ce modèle peut être utilisé par un CISP pour notifier une violation de sécurité à ses clients. Il est fourni à titre d'exemple uniquement, et illustre la forme et les types d'informations que le CISP peut être amené à renseigner pour notifier une violation de sécurité à ses clients. Le CISP n'a pas l'obligation d'utiliser ce modèle.

1. Identification du CISP

Nom de l'organisation (CISP) :

Adresse du siège de l'organisation :

Point de contact disponible pour répondre à toute autre demande concernant la violation :

Nom :

Fonction :

E-mail :

Téléphone :

Délégué à la protection des données (uniquement s'il est nommé et s'il est différent du point de contact)

Nom :

E-mail :

Téléphone :

2. Nature de la Notification

Notification Initiale :

Notification de suivi :

En cas de notification de suivi, veuillez indiquer la date de la notification initiale :

3. Description de la violation de sécurité

[Sur la base des informations dont dispose le CISP, décrivez ce qu'il s'est passé et/ou ce qui a mal tourné]

4. Conséquences de la violation

[Sur la base des informations dont dispose le CISP, indiquez des détails concernant les effets connus/potentiels de la violation]

5. Mesures prises ou envisagées par le CISP en réponse à la violation

[Décrivez les démarches/mesures entreprises par le CISP et les autres mesures envisagées par le CISP et le client]

Annexe G – Glossaire

ACL désigne les listes de contrôle d'accès.

Exigences Auditables du Code désigne les Exigences du Code reconnues dans le secteur comme étant auditables et qui sont spécifiées dans la Check-list de Conformité.

Task Force du Code de Conduite CISPE ou **CCTF** désigne un ensemble de douze personnes maximum, nommées par les membres du CISPE, qui justifient (i) d'une expertise dans le domaine de l'informatique cloud et/ou de la protection des données, et/ou (ii) d'une bonne maîtrise des « business models » de l'informatique cloud, conformément aux indications du paragraphe 7.1 du Code.

CISC, **Comité de Surveillance Indépendant du Code**, ou **Membres du CISC** désigne le Comité de Surveillance Indépendant du Code qui se compose de trois experts indépendants ayant reçu une formation universitaire, technique ou juridique nommés par le Comité Exécutif, comme indiqué au paragraphe 7.1 du Code.

Réseau du CISP désigne les installations de centre de données, serveurs, équipements réseau et systèmes logiciels hôtes du CISP qui sont sous le contrôle du CISP et utilisés pour fournir le service du CISP.

CISPE désigne l'Association des fournisseurs européens d'infrastructures Cloud.

Registre Public CISPE désigne le site internet qui contient la liste des CISPs ayant déclaré leur adhésion au présent Code, accessible à l'adresse suivante https://cispe.cloud.

CISP désigne les fournisseurs de services d'infrastructure Cloud.

Code désigne le présent Code de Conduite.

Exigences du Code désigne les Exigences en matière de Protection des Données et les Exigences en matière de Transparence décrites aux chapitres 4 et 5 du Code.

Autorité Compétente désigne l'autorité de protection des données indépendante désignée par chaque État Membre de l'Union européenne en charge de surveiller l'application du RGPD.

Procédure de Réclamations désigne la procédure décrite au Chapitre 7.2(a) du Code qui permet de traiter les réclamations des clients, des personnes concernées, ou de tout autre CISPE concernant la conformité des services aux Exigences du Code.

Liste de Contrôle de la Conformité désigne la liste de contrôle exposée en Annexe B du Code.

Lignes Directrices sur l'Utilisation des Marques de Conformité désigne les lignes directrices relatives à l'utilisation de la Marque par les CISPs.

Marque de Conformité désigne le symbole collectif démontrant qu'un service respecte les Exigences du Code.

Données Client désigne les données à caractère personnel qui sont traitées au nom d'un client qui utilise un service d'infrastructure cloud.

Déclaration d'Adhésion désigne le modèle de déclaration exposé en Annexe C du Code qu'un CISP doit présenter pour confirmer que son service respecte les Exigences du Code.

Autorité de Contrôle Désignée désigne l'Autorité de Contrôle pour le Code, à savoir la Commission Nationale de l'Informatique et des Libertés (CNIL).

DPA désigne les autorités de protection des données.

DSM désigne le Marché Unique Numérique de la Commission européenne.

EEE désigne l'Espace économique européen.

Matrice d'Exécution désigne le tableau présenté au paragraphe 7.2(b) du Code.

Comité Exécutif désigne les 5 à 10 représentants élus par l'Assemblée Générale, conformément aux indications du paragraphe 7.1 du Code

Premier Avertissement Écrit désigne le premier avertissement écrit adressé à un CISP par l'Organisme de Contrôle s'il constate, à l'issue d'un examen, qu'un CISP n'a pas respecté une exigence du Code, conformément aux indications du paragraphe 7.2(b) du Code.

Exigence du RGPD désigne les exigences applicables aux sous-traitants en vertu du RGPD.

Assemblée Générale désigne le groupe de représentants avec droit de vote de chaque CISP participant au Code, comme indiqué au paragraphe 7.1 du Code.

Règlement Général sur la Protection des Données ou **RGPD** désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

Logiciel d'Exploitation Hôte désigne le logiciel utilisé par le CISP pour fournir des services d'infrastructure cloud aux clients.

IaaS désigne infrastructure-as-a-service.

Marque(s) désigne la Marque de Conformité et/ou la Marque d'Auto-Adhésion.

État Membre désigne un État membre de l'Union européenne.

Organisme de Contrôle désigne l'organisme nommé par un CISP à partir d'une liste conservée par le CISC pour contrôler que le CISP respecte les dispositions du Code.

Atelier d'un Organisme de Contrôle désigne les ateliers annuels que le CISP doit organiser et auxquels participent les Organismes de Contrôle pour discuter des difficultés pratiques auxquelles les Organismes de Contrôle ont été confrontés en examinant l'application des dispositions du Code.

Observateurs désigne les représentants qui ne sont pas affiliés à l'Assemblée Générale mais qui sont nommés par le Comité Exécutif pour y participer en tant qu'observateurs sans droit de vote.

Rapport désigne le rapport produit par un Organisme de Contrôle après chaque examen du respect des dispositions du Code par un CISP, qui synthétise ses conclusions.

Obligation du CISP désigne l'explication de l'Exigence du RGPD concernée dans le cadre des services d'infrastructure cloud.

SaaS désigne software-as-a-service.

Second Avertissement Écrit désigne le second avertissement écrit adressé à un CISP par l'Organisme de Contrôle s'il constate, à l'issue d'un examen, qu'un CISP n'a pas respecté les exigences du Code dans un délai de 60 jours après réception d'un Premier Avertissement Écrit, conformément aux indications du paragraphe 7.2(b) du Code.

Secrétariat désigne l'organisme nommé par le Comité Exécutif responsable de l'administration quotidienne du Code.

Contrat de Services désigne le contrat entre le CISP et le client qui définit les caractéristiques du service et les modalités de sa prestation ainsi que les droits et obligations du client.

Services désigne les services d'infrastructure cloud spécifiés en Annexe C.

PME désigne les petites et moyennes entreprises.