

PARTENARIAT - ECHANGE DE DONNÉES

RÈGLES DE SÉCURITÉ

Référence	SSI-REG-TST_Parteneriat - Echange de données_V1.2
Clef GED	185487
Version	V1.3
Classification	Interne
Date	15/01/2021
État	Validé
Auteur(s)	Filière Sécurité des SI
Approbateur(s)	Sylvain Lambert
Validation	Direction de la maîtrise des risques

Identification du document

Référence	Titre du document	
SSI-REG-TST_Partenerariat - Echange de données_V1.2	Partenariat – Echange de données	
Version	État du document	Auteurs
1.3	Final	Filière Sécurité des SI

Classification	
Niveau	Diffusion
Interne	Le personnel de France Travail et à ses tiers formellement autorisés (ayant signé une convention, charte de sécurité, clause de confidentialité,...)

Mises à jour		
Version	Date	Nature de la modification
1.0	24 Janvier 2014	Création du document
1.1	30 mai 2014	Relecture thématique SSI – groupe de travail filière SSI
1.2	04 mai 2017	Mises à jour dans le cadre de la refonte du référentiel initiée en 2016
1.2	15 janvier 2021	Ajout de la nécessité de répondre aux exigences de sécurité au travers un PAS (plan assurance Sécurité)
1.3	22 janvier 2024	Mise à jour suite changement de marque

Relectures et validations				
Version	Relu par	Direction	Date	Statut
1.0	RSSI Sylvain Lambert	DSI	06/02/2014	validé
1.1	RSSI Sylvain Lambert	DSI	30/05/2014	validé
1.2	RSSI Sylvain Lambert	DSI	04/05/2017	validé
1.2	Robert Laupy	DGA-DMR	29/06/2017	validé

Documents de référence	
Référence colibri	Titre du document

SOMMAIRE

1. PRÉAMBULE	5
2. RÈGLES DE SÉCURITÉ	6
2.1. Mesures générales de protection du système d'information et des données	6
2.2. Confidentialité des informations	7
2.3. Sécurité des matériels et logiciels	8
2.4. Accès Logique	10
2.5. Surveillance et auditabilité de la nature et de l'origine des accès	11
2.6. Politique d'échange de données avec le Partenaire	11
2.7. Respect des dispositions « Informatique et libertés »	12
2.8. Gouvernance du partenariat	14
3. ANNEXE	15
3.1. Liste des règles	15

A INSERER AU CONTRAT

La société,, ci-après dénommée "le Partenaire", s'engage à respecter les règles de sécurité et de confidentialité du présent document.

1. PRÉAMBULE

Le présent document a pour objectif de réduire les risques de sécurité pouvant peser sur le SI de France Travail dans le cadre d'un partenariat d'échange de données. À titre d'exemple, il s'agit entre autres des risques liés à la divulgation, le vol ou l'altération des informations confidentielles, ainsi qu'à l'usurpation d'identité.

Les exigences de ce document ont vocation à être intégrées dans l'accord contractualisé avec le co-contractant (partenaire de France Travail ou un sous-traitant de France Travail) mais également dans le cadre du choix du co-contractant, par exemple dans la rédaction du cahier des charges.

Les dispositions prises par le prestataire pour répondre aux exigences de sécurité du présent document devront être formalisées au sein d'un PAS (Plan d'Assurance Sécurité).

2. RÈGLES DE SÉCURITÉ

2.1. MESURES GÉNÉRALES DE PROTECTION DU SYSTÈME D'INFORMATION ET DES DONNÉES

CL- 1. Général - Engagements de sécurité générale

Le Partenaire s'engage à prendre toutes les précautions utiles afin de préserver la sécurité des informations communiquées par France Travail.

Il veille notamment à assurer :

- La confidentialité des informations en empêchant leur divulgation à des tiers non autorisés.
- L'intégrité des informations en empêchant leur modification ou destruction en dehors du cadre du partenariat, et ce de façon intentionnelle ou accidentelle.
- La disponibilité des informations, leur conservation et la disponibilité des systèmes d'information utilisés dans le cadre du partenariat.
- La traçabilité des opérations et de l'origine des données.

Dans ce cadre, les mesures de sécurité mises en œuvre doivent répondre aux exigences de sécurité de France Travail et faire l'objet d'un commun accord entre le Partenaire et France Travail.

France Travail doit au préalable avoir évalué le niveau de sensibilité des informations concernées lui appartenant et en avoir informé le Partenaire.

Le Partenaire s'engage à mettre à disposition de France Travail les politiques et procédures de sécurité mises en œuvre pour assurer le respect de l'exécution de ces dispositions.

➔ Le niveau de sécurité démontré par le partenaire sera déterminant dans le positionnement du RSSI.

CL- 2. Général - Propriété des informations et détournement de finalité

Sauf mention écrite contraire, les informations fournies par France Travail ne doivent pas être considérées comme une cession ou un échange. Elles ne doivent pas être cédées à un tiers sans accord préalable et formalisé de France Travail.

Les informations fournies par France Travail et/ou créées pour son compte restent la propriété de France Travail; leur utilisation par le Partenaire est soumise à l'accord préalable de France Travail.

Aucun autre traitement que ceux prévus ne doit être exécuté sur les informations fournies par France Travail ou leurs résultats. Tout traitement doit être adapté au but pour lequel il a été mis en place et ne doit pas servir d'autres fins.

CL- 3. Général – Engagement de confidentialité du Partenaire

Le Partenaire s'engage pendant toute la période du partenariat à respecter les règles suivantes pour toute information relatives au présent accord :

- N'utiliser les documents ou informations de France Travail qu'aux fins exclusives de réalisation de la prestation ;
- Ne pas divulguer les informations de France Travail sauf accord préalable et écrit de France Travail ;
- Ne pas faire, ni laisser faire de communication publique ou privée, écrite ou orale, mentionnant tout ou partie desdites informations sauf accord préalable et écrit de France Travail ;

Le Partenaire se porte garant du respect de cette obligation par ses préposés/intervenants. Il s'engage à porter à la connaissance de ses préposés les obligations de confidentialité auxquelles ils sont tenus et prend toutes les mesures nécessaires à leur respect.

2.2. CONFIDENTIALITÉ DES INFORMATIONS

CL- 4. Confidentialité - Définition

Toute information de France Travail échangée dans le cadre du partenariat doit être considérée comme « confidentielle » par le Partenaire sauf cas contraire dûment précisé par Pole emploi.

Les informations confidentielles portées à la connaissance du Partenaire, peuvent regrouper les informations visuelles ou orales, documents et données de quelque nature que ce soit et quel qu'en soit le support (physique ou électronique).

CL- 5. Confidentialité - Clause de confidentialité

Le Partenaire s'engage à appliquer les mesures suivantes sur les informations « confidentielles » de France Travail :

- N'exécuter aucun autre traitement que ceux prévus sur ces informations ou leurs résultats.
- Ne divulguer les informations confidentielles qu'aux seuls membres de son personnel ayant à les connaître sous réserve que ces derniers s'engagent à respecter les obligations de confidentialité contenues dans le présent accord.

Le Partenaire se porte garant du respect de cette obligation de confidentialité par ses préposés/intervenants. Il s'engage à porter à leur connaissance les obligations de confidentialité auxquelles ils sont tenus et prend toutes les mesures nécessaires à leur respect.

CL- 6. Confidentialité - Durée de la clause

Le Partenaire s'engage à faire respecter par son personnel intervenant les clauses de confidentialité formalisées dans le présent accord. Ces clauses prennent effet à compter de la signature de l'accord par les Parties. L'obligation de confidentialité s'applique sans limitation de durée.

2.3. SÉCURITÉ DES MATÉRIELS ET LOGICIELS

CL- 7. Sécurité matériels/logiciels – Sécurité physique

Le Partenaire doit s'assurer que des mesures suffisantes ont été mises en œuvre en matière de sécurité et sûreté physique sur le site d'hébergement des données de France Travail (protection du site et sécurité des accès, sécurité électrique et système de climatisation, etc.) afin de garantir la protection des données notamment contre le vol.

CL- 8. Sécurité matériels/logiciels – Hébergement d'informations confidentielles

Les données confidentielles de France Travail hébergées chez le Partenaire doivent être isolées des données lui appartenant ou appartenant à d'autres tiers et non accessibles par d'autres tiers. Leur stockage doit être sécurisé (chiffrement desdites données).

CL- 9. Sécurité matériels/logiciels – Gestion de la capacité

De manière proactive, le Partenaire doit superviser l'utilisation des ressources informatiques utilisées dans le cadre du Partenariat dont il a la charge, et informer immédiatement France Travail d'éventuels problèmes de capacité qui pourraient apparaître dans le futur.

CL- 10. Sécurité matériels/logiciels – Gestion des vulnérabilités

Le Partenaire doit mettre en œuvre une politique pour protéger les ressources informatiques utilisées dans le cadre du Partenariat contre les programmes malveillants et garantir le maintien en conditions de sécurité de ces ressources, en particulier concernant les mises à jour de sécurité (correctifs).

Pour ce faire, le Partenaire doit mettre en œuvre :

- Des procédures de distribution des signatures antivirales.
- Des procédures d'analyse et de déploiement des correctifs de sécurité.
- Des procédures de remontée et d'analyse des virus et malware détectés.

En outre, un système de filtrage des codes malveillants (virus, vers, etc.) doit être mis en place entre le Partenaire et France Travail. Toute alerte, provenant de ces systèmes, doit être remontée à France Travail.

Dans le cas de données du Partenaire transmises à France Travail :

- Le Partenaire prend toutes les précautions nécessaires pour éviter l'introduction de tout programme malveillant dans le système d'information de France Travail et adopte les mesures adéquates s'il constate l'existence d'un tel programme malveillant. À cet effet, le Partenaire réalise tous les tests adéquats et s'engage à contrôler les éléments informatiques préalablement à leur livraison à France Travail.
- En cas d'introduction d'un tel programme malveillant, le Partenaire et France Travail conviennent de collaborer afin d'en déterminer l'origine d'un commun accord et d'en éradiquer les conséquences.

CL- 11. Sécurité matériels/logiciels – Gestion des incidents

Le Partenaire doit prendre les dispositions pour limiter le nombre et les impacts des incidents de sécurité SI et mettre en place les circuits d'alerte, de traitement et de reporting associés. Ces dispositions doivent :

- Être formalisées dans un processus de gestion des incidents.
- Être partagées entre le Partenaire et France Travail pour permettre un retour à un service nominal dans les meilleurs délais.

Ces procédures doivent notamment prévoir les mesures de lutte contre la fuite d'information en cas d'incident impactant des données confidentielles.

Si l'incident engendre un risque de sécurité important pour France Travail, il doit faire l'objet d'une notification sans délai au RSSI de France Travail.

CL- 12. Sécurité matériels/logiciels – Gestion des changements

Le Partenaire doit respecter les conditions suivantes pour la planification des interventions et changements (mise à jour logicielle ou matérielle, etc.) effectués sur les ressources informatiques utilisées dans le cadre du partenariat :

- Être réalisés dans les plages d'intervention préalablement convenues avec France Travail.
- Être communiqués à France Travail pour information.
- Être documentés et programmés.
- Comporter un plan de retour arrière.

En complément, tout changement modifiant le contexte de sécurité de France Travail doit faire l'objet d'un accord préalable du RSSI de France Travail.

CL- 13. Sécurité matériels/logiciels – Existence de sauvegarde

Le Partenaire est tenu d'assurer la sauvegarde des informations de France Travail qu'il traite dans son système d'information, de telle manière à permettre la restauration du service et des données, notamment en cas d'incident de sécurité sur ces données.

CL- 14. Sécurité matériels/logiciels – Sécurité des sauvegardes de données confidentielles

Dans le cas de sauvegardes de données confidentielles de France Travail effectuées par le Partenaire :

- Le Partenaire doit réaliser des sauvegardes sous réserve que le mode de duplication ait été agréé par France Travail.
- Il doit protéger les sauvegardes comme les éléments originaux, afin d'éviter toute possibilité d'accès, fortuit ou intentionnel, par des tiers ou des employés non autorisés.
- Les conditions de restitution de ces sauvegardes à France Travail ou de destruction par un mode agréé par France Travail, sont prévues dans la convention, en accord avec France Travail.

- Les supports magnétiques amovibles contenant des données de France Travail doivent être identifiés, protégés contre tout accès non autorisé et périodiquement inventoriés.

2.4. ACCÈS LOGIQUE

CL- 15. Accès Logique - Données confidentielles

L'accès aux données confidentielles de France Travail est soumis à l'autorisation préalable de France Travail.

Tout accès logique à des données confidentielles de France Travail doit être soumis à une authentification préalable.

Lorsque l'authentification se fait par mot de passe, celui-ci doit rester confidentiel. Tout comme l'identifiant, il est personnel, unique et incessible. La construction de l'authentifiant (le mot de passe) doit garantir un niveau de robustesse suffisant. À titre d'exemple, les critères suivants sont considérés comme sécurisés par France Travail :

- Avoir une longueur minimale de 8 caractères.
- Être composé de caractères appartenant aux trois classes suivantes : lettres (a...z et A...Z), chiffres (0...9) et caractères spéciaux (&@à(|...).
- Être différent des 5 mots de passe précédents.
- Être changé au moins tous les 90 jours.

Le contrôle d'accès logique aux données confidentielles de France Travail doit permettre de distinguer les différents types d'accès (lecture, mise à jour, exécution) et garantir que les données ne sont accessibles qu'aux seules personnes préalablement autorisées.

CL- 16. Accès Logique - Données non confidentielles

L'accès aux données non confidentielles de France Travail ne nécessite pas une authentification préalable. L'accès à ces données doit cependant respecter la condition suivante :

- Accès soumis à l'accord préalable de France Travail.

CL- 17. Accès Logique - Cas d'une communication application à application (accès à des services internes)

En cas de mise en œuvre d'une communication application à application, les services internes France Travail sont exposés au Partenaire au travers de l'infrastructure sécurisée définie au catalogue des solutions d'architecture technique de la DSI pole emploi. Une authentification forte est requise. Les modalités pratiques de déclinaison de ces principes sont adaptées au cas par cas en fonction des contraintes identifiées.

2.5. SURVEILLANCE ET AUDITABILITÉ DE LA NATURE ET DE L'ORIGINE DES ACCÈS

CL- 18. Auditabilité - Traçabilité sur le transfert des données

Le Partenaire est tenu d'assurer la possibilité de garder de manière exploitable, sur une durée de six mois les données lui permettant de contrôler la réception et l'exploitation des données transmises par France Travail. Les traces doivent comporter *a minima* : nature, référence, et horodatage. France Travail pourra lui demander la fourniture de ces traces

CL- 19. Auditabilité - Traçabilité de la nature et de l'origine des accès pour des données confidentielles

Si des données confidentielles sont concernées, le Partenaire est tenu de garder de manière exploitable, sur une durée d'un an la trace des actions réalisées dans son système d'information sur les ressources informatiques utilisées dans le cadre du partenariat à des fins de contrôle et de preuves. Les traces doivent comporter *a minima* : nature, référence, et horodatage. »

Il s'agit notamment de pouvoir fournir à France Travail les données permettant de contrôler la nature et l'origine des accès aux données de France Travail, particulièrement les accès en modification.

CL- 20. Auditabilité - Audit et contrôle du Partenaire

Le Partenaire s'engage à assurer un suivi permanent de son niveau de maîtrise des risques et du respect des politiques et règles de sécurité applicables sur le périmètre du partenariat, y compris auprès de ses propres sous-traitants.

Le Partenaire doit effectuer périodiquement des revues pour vérifier la conformité avec les dispositions du présent accord.

En cas d'incident de sécurité avéré ou bien d'alerte identifiée dans le cadre du suivi global du partenariat, le Partenaire autorise France Travail à réaliser un audit du partenariat. L'audit pourra être mené, y compris dans les locaux du Partenaire, par des visites programmées, afin de vérifier notamment que les procédures de maîtrise des risques liés aux systèmes d'information prévues au présent accord sont respectées.

2.6. POLITIQUE D'ÉCHANGE DE DONNÉES AVEC LE PARTENAIRE

CL- 21. Interconnexion - Clause générale

Le type d'interconnexion entre le Partenaire et France Travail doit être adapté à la sensibilité des données échangées et peut nécessiter des mesures de protection des échanges spécifiques (sécurisation SSL/HTTPS, Certificats/VPN, Liaison dédiées, etc.).

- L'exigence minimale de sécurité de France Travail pour les échanges (authentification et transfert de données) avec le Partenaire est une réalisation des échanges au moyen d'un protocole sécurisé (par exemple SSL/HTTPS, etc.).

- Le descriptif de l'interconnexion technique (incluant les aspects sécurité) et une matrice de flux entre le Partenaire et France Travail doivent être établis et validés par les deux parties.

CL- 22. Interconnexion - Accès aux applications internes de France Travail

L'accès par le Partenaire aux applications internes France Travail ne peut se faire qu'à travers la passerelle de sécurisation définie au catalogue de solutions d'architecture technique de la DSI de France Travail.

CL- 23. Interconnexion - Organisme de la sphère sociale

L'application de la convention technique d'échange INTEROPS est obligatoire pour un partenariat entre France Travail et un organisme de la sphère sociale.

La documentation de référence INTEROPS est disponible sur le site <http://www.interops.fr/> ou en annexe du présent accord.

CL- 24. Disponibilité - Continuité d'activité

Le Partenaire doit être en mesure d'assurer la continuité des activités concernées par le partenariat en cas de sinistre majeur. Pour ce faire, le Partenaire doit présenter ou décrire à France Travail son plan de secours en cas de sinistre pouvant affecter les travaux réalisés pour France Travail.

Des tests réguliers doivent être menés par le Partenaire pour vérifier la validité du plan de secours informatique et des sauvegardes. Les résultats (partiels) de ces tests pourront être demandés par France Travail dans le cadre du suivi du partenariat.

2.7. RESPECT DES DISPOSITIONS « INFORMATIQUE ET LIBERTÉS »

CL- 25. CNIL – Respect de la législation en vigueur relative à la protection des données personnelles

Les parties s'engagent à traiter les données à caractère personnel conformément à la loi et aux décrets en vigueur applicables, notamment en ce qui concerne la sécurité et la confidentialité desdites données.

Ils ont connaissance de l'existence du règlement européen sur la protection des données à caractère personnel, relatif à l'informatique, aux fichiers et aux libertés, qui pourrait s'appliquer à tout manquement de leur part mettant en jeu des données à caractère personnel.

CL- 26. Remontée des plaintes et des failles de sécurité

Le partenaire s'engage à communiquer à France Travail la survenance de toute faille de sécurité ayant des conséquences directes ou indirectes sur le traitement, ainsi que toute plainte qui lui serait adressée par tout individu concerné par le traitement réalisé au titre du partenariat. Cette communication devra être effectuée dans les plus brefs délais et au maximum trente-six heures après la découverte de la faille de sécurité ou suivant réception d'une plainte.

CL- 27. Localisation des données

a) Dans le cas d'archives publiques :

Le Partenaire s'engage à héberger, traiter, et faire transiter les données de France Travail uniquement sur le territoire Français. Ceci en respect des exigences imposées par la législation sur les archives publiques.

b) Autres cas :

Le partenaire s'engage à héberger, traiter et faire transiter les données à caractère personnel de France Travail sur le territoire des états membres de l'Union Européenne et au sein des pays reconnus comme adéquats par la Commission Européenne (cf. liste des pays autorisés sur le site internet de la CNIL).

2.8. GOUVERNANCE DU PARTENARIAT

CL- 28. Gouvernance - Communication des informations relatives à la sous-traitance

Lorsque le Partenaire a recours à des sous-traitants il doit en informer France Travail et lui fournir la liste des destinataires des données en précisant la localisation de l'hébergement des données, le Partenaire s'engage à reporter dans les engagements qu'il contracte avec des sous-contractants les obligations qui lui incombent au titre de l'accord avec France Travail, notamment l'obligation de localisation de l'hébergement et du transfert des données de France Travail sur le territoire des états membres de l'Union Européenne et au sein des pays reconnus comme adéquats par la Commission Européenne (cf. liste des pays autorisés sur le site internet de la CNIL).

Le Partenaire reste seul responsable vis-à-vis de l'exécution de ses obligations contractuelles résultant du présent accord.

CL- 29. Gouvernance - Interlocuteur sécurité

Pour faciliter le suivi des aspects sécurité et notamment des engagements sécurité établis au titre du partenariat, un contact privilégié doit être identifié chez le Partenaire. A France Travail, le RSSI fait office de point de contact sécurité dans le cadre du partenariat, avec possibilité de délégation.

Des comités de suivi spécifiques aux aspects sécurité pourront être organisés à la demande de France Travail ou du Partenaire ; par exemple si le besoin est identifié dans le cadre du suivi global du partenariat.

De la même manière, à la demande de France Travail ou du Partenaire, des indicateurs de sécurité pourront être définis et mis en œuvre (après validation des deux parties).

CL- 30. Gouvernance - Gestion de fin du partenariat

Au terme du partenariat, ou en cas de rupture anticipée de ce dernier pour quelque cause que ce soit, le Partenaire et ses éventuels sous-contractants s'engagent à restituer sans délai à France Travail l'intégralité des informations, notes, documents, logiciels et plans remis dans le cadre du partenariat et à certifier par écrit à France Travail ne pas avoir conservé d'informations.

De plus, le Partenaire s'engage à ne plus utiliser les données, informations, documentations techniques, référentiels qui lui ont été confiés par France Travail au cours du partenariat.

3. ANNEXE

3.1. LISTE DES RÈGLES

CL- 1.	GÉNÉRAL - ENGAGEMENTS DE SÉCURITÉ GÉNÉRALE	6
CL- 2.	GÉNÉRAL - PROPRIÉTÉ DES INFORMATIONS ET DÉTOURNEMENT DE FINALITÉ	6
CL- 3.	GÉNÉRAL – ENGAGEMENT DE CONFIDENTIALITÉ DU PARTENAIRE	7
CL- 4.	CONFIDENTIALITÉ – DÉFINITION	7
CL- 5.	CONFIDENTIALITÉ – CLAUSE DE CONFIDENTIALITÉ	7
CL- 6.	CONFIDENTIALITÉ – DURÉE DE LA CLAUSE	7
CL- 7.	SÉCURITÉ MATÉRIELS/LOGICIELS – SÉCURITÉ PHYSIQUE	8
CL- 8.	SÉCURITÉ MATÉRIELS/LOGICIELS – HÉBERGEMENT D’INFORMATIONS CONFIDENTIELLES	8
CL- 9.	SÉCURITÉ MATÉRIELS/LOGICIELS – GESTION DE LA CAPACITÉ	8
CL- 10.	SÉCURITÉ MATÉRIELS/LOGICIELS – GESTION DES VULNÉRABILITÉS	8
CL- 11.	SÉCURITÉ MATÉRIELS/LOGICIELS – GESTION DES INCIDENTS	9
CL- 12.	SÉCURITÉ MATÉRIELS/LOGICIELS – GESTION DES CHANGEMENTS	9
CL- 13.	SÉCURITÉ MATÉRIELS/LOGICIELS – EXISTENCE DE SAUVEGARDE	9
CL- 14.	SÉCURITÉ MATÉRIELS/LOGICIELS – SÉCURITÉ DES SAUVEGARDES DE DONNÉES CONFIDENTIELLES	9
CL- 15.	ACCÈS LOGIQUE - DONNÉES CONFIDENTIELLES	10
CL- 16.	ACCÈS LOGIQUE - DONNÉES NON CONFIDENTIELLES	10
CL- 17.	ACCÈS LOGIQUE - CAS D’UNE COMMUNICATION APPLICATION À APPLICATION (ACCÈS À DES SERVICES INTERNES)	10
CL- 18.	AUDITABILITÉ - TRAÇABILITÉ SUR LE TRANSFERT DES DONNÉES	11
CL- 19.	AUDITABILITÉ - TRAÇABILITÉ DE LA NATURE ET DE L’ORIGINE DES ACCÈS POUR DES DONNÉES CONFIDENTIELLES	11
CL- 20.	AUDITABILITÉ - AUDIT ET CONTRÔLE DU PARTENAIRE	11
CL- 21.	INTERCONNEXION - CLAUSE GÉNÉRALE	11
CL- 22.	INTERCONNEXION - ACCÈS AUX APPLICATIONS INTERNES DE FRANCE TRAVAIL	12
CL- 23.	INTERCONNEXION - ORGANISME DE LA SPHÈRE SOCIALE	12
CL- 24.	DISPONIBILITÉ - CONTINUITÉ D’ACTIVITÉ	12
CL- 25.	CNIL – RESPECT DE LA LÉGISLATION EN VIGUEUR RELATIVE À LA PROTECTION DES DONNÉES PERSONNELLES	12
CL- 26.	REMONTÉE DES PLAINTES ET DES FAILLES DE SÉCURITÉ	12
CL- 27.	LOCALISATION DES DONNÉES	13
CL- 28.	GOVERNANCE - COMMUNICATION DES INFORMATIONS RELATIVES À LA SOUS-TRAITANCE	14
CL- 29.	GOVERNANCE - INTERLOCUTEUR SÉCURITÉ	14
CL- 30.	GOVERNANCE - GESTION DE FIN DU PARTENARIAT	14