CAHIER DES CLAUSES TECHNIQUES PARTICULIERES (CCTP)

IMPRESSION, EDITION, LOGISTIQUE ET LIVRAISON DE DOCUMENTS DOUANIERS POUR LA CCI PARIS ILE-DE-FRANCE

Marché n° 2026-GIE-037

GIE Groupe CCIR PARIS IDF
11 rue Léon Jouhaux
75010 PARIS

Ce document comporte 24 pages y compris celle de garde

GIE
CCI PARIS ILE-DE-FRANCE

SOMMAIRE

1 OBJET DE LA CONSULTATION 4
2 PRESENTATION DU DEPARTEMENT DES FACILITATIONS DU COMMERCE EXTERIEUR DE LA DGA INTERNATIONAL 4
3 SPECIFICATION DES BESOINS 4
3.1 Rôle et responsabilité du titulaire 4
3.2 DESCRIPTION TECHNIQUE DES PRESTATIONS ATTENDUES 5
3.2.1 Type d'imprimés 5
3.3 Prestation logistique des documents douaniers 6
3.4 Système de commande en ligne 6
3.4.1 Sécurisation et identification des utilisateurs 6
3.4.2 Prise en compte de demande de personnalisation et d'extraction sur l'outil de commande en ligne 7
3.5 Gestion du stock et quantités minimales de commande en ligne 8
3.5.1 Détail des stocks minimums et quantités commandées 8
3.5.2 Reprise du stock 8
3.6 Revente de document au réseau des CCI 9
3.7 Clause environnementale 9
4 DELAIS DE FABRICATION ET DELAI DE LIVRAISON DES IMPRIMES POUR LA CCI PARIS ILE-DE-FRANCE. 9
4.1 Délai de fabrication et bon de commande correspondant ..... **Erreur ! Signet non défini.**
4.2 Délai de livraison pour la CCI Paris Ile-de-France et bon de commande correspondant ..... **Erreur ! Signet non défini.**
5 DELAIS ET MODALITES DE LIVRAISON DES IMPRIMES ENTRE LES CCI (HORS CCI PARIS IDF) ET LE TITULAIRE 10
5.1 Délai de livraison 10
5.2 Modalités de livraison 10
5.2.1 Lieux de livraison 10
5.2.2 Horaires de livraison 10
5.2.3 Bon de livraison et contenu 10
6 REUNION 10
7 FICHIER DE REPORTING 10
8 CLAUSES GENERALES DE SECURITE DES SYSTEMES D'INFORMATION 11
8.1 Acronymes et définitions 11
8.1.1 Acronymes 11
8.1.2 Définitions 11
8.2 Gestion des biens 12
8.3 Critères de sécurité 12
8.4 Définitions des clauses de sécurité du système d'information 13
8.5 Plan d'Assurance Sécurité 13
8.6 Appréciation des risques 14
8.7 Organisation de la sécurité avec le titulaire 14
8.8 Obligations du titulaire 14
8.9 Transfert du système 15
8.10 Confidentialité 15
8.11 Localisation des données 15
8.12 Sécurité des développements applicatifs 16
8.13 Suivi et supervision du service hébergé 17
8.14 Gestion des incidents 17
8.15 Gestion des évolutions 18
8.16 Gestion de la continuité 19

8.16.1 Textes de référence 19
8.16.2 Événements couverts 19
8.16.3 Contenu minimal attendu 19
8.16.4 Exigences minimales attendues 20
8.16.5 Tests et mise à jour 20
8.16.6 Transmission 20
8.17 Conformité aux référentiels et réglementations 21
8.18 Relations avec les tiers 21
8.19 Tests de vulnérabilité 22
8.20 Audit sécurité 22
8.21 Manquement et résiliation 23
8.22 Réversibilité 23
8.23 Fin du marché 24
8.24 Protection des traitements de données à caractère personnel du titulaire 24

GIE
CCI PARIS ILE-DE-FRANCE

1 OBJET DE LA CONSULTATION

Le présent marché a pour objet les prestations d'impression, d'édition, de stockage et la logistique de documents douaniers de la CCI Paris Ile-de-France.

2 PRESENTATION DU DEPARTEMENT DES FACILITATIONS DU COMMERCE EXTERIEUR DE LA DGA INTERNATIONAL

L'activité du DFCE (Département des Facilitations du Commerce Extérieur) se répartie entre 3 niveaux :

- Un niveau local par lequel le Département certifie les documents export des exportateurs de son périmètre (Paris Île-de-France). Par certification, on entend la vérification de la conformité des documents par rapport à ce qu'exigent les douanes des pays vers lesquels les marchandises sont envoyées. Les documents certifiés sont répartis en 3 grandes familles : les carnets de passage en douanes ATA pour les exportations temporaires ; les certificats d'origine pour les ventes à l'international et les certificats de libre vente pour les exportions de médicaments et/ou dispositifs médicaux.

- Un niveau national par lequel le DFCE joue un rôle de tête de réseau pour toutes les CCI françaises en matière de certification de documents export en renseignant et conseillant les CCI sur les procédures à appliquer et en dispensant des actions de formation dans ce domaine. Également, le DFCE vend aux CCI françaises les imprimés douaniers objet du marché (voir ci-dessous).

- Un niveau international par lequel le Département représente le réseau français des CCI dans des commissions internationales sur les carnets ATA, les certificats d'origine ; ces commissions étant toutes orientées "facilitation des échanges internationaux".

Le marché des imprimés douaniers porte sur le niveau local et national.

Au niveau local, le DFCE donne les instructions nécessaires au titulaire pour fabriquer les documents, puis les vend à ses clients/exportateurs. Les clients/exportateurs remplissent ces documents puis les font certifier à la CCI Paris Ile-de-France.

Au niveau national, les documents sont revendus aux CCI après fabrication, pour qu'à leur tour, les CCI puissent les vendre à leurs propres clients. Le titulaire sélectionné devra stocker pour le compte de la CCI Paris Ile-de France les documents fabriqués et les livrer pour notre compte aux clients CCI de la CCI Paris Ile-de-France.

Ces documents servent en grande partie au passage en douanes des marchandises mais sont également demandés par les importateurs eux-mêmes mais aussi par les banques dans le cadre des crédits documentaires par exemple.

3 SPECIFICATION DES BESOINS

3.1 Rôle et responsabilité du titulaire

Pour les besoins du Département des Facilitations du Commerce Extérieur de la CCI Paris Ile-de-France et du réseau CCI, le titulaire devra :

- Fabriquer les imprimés douaniers selon demandes du DFCE ;
- Fournir les imprimés dans les délais fixés par le marché ;
- Réserver un espace sécurisé dédié à la CCI Paris Ile-de-France pour le stockage des imprimés ;
- Effectuer les tâches de manutention nécessaires au stockage, à l'emballage et à l'expédition ;
- Assurer la gestion administrative de toutes les commandes (bons de livraison) vers le client CCI Paris Ile-de-France et l'utilisateur final (CCI métropolitaines et DROM-COM, notamment pour ces dernières les formalités de dédouanement) ;
- Assurer le suivi des stocks, veiller régulièrement au stock d'alerte pour éviter toute rupture et en informer la CCI Paris Ile-de-France.

3.2 DESCRIPTION TECHNIQUE DES PRESTATIONS ATTENDUES

3.2.1 Type d'imprimés

Afin de permettre aux entreprises françaises d'exporter leurs produits de manière définitive ou temporaire (notamment dans le cadre de toute action commerciale de prestation de marchés étrangers), les chambres de Commerce et d'Industrie mettent à leur disposition les documents officiels d'accompagnement qu'elles authentifient, qui ont pour objet de faciliter leur passage en douane et d'effectuer leurs formalités « ad-hoc ».

Les imprimés « certificats d'origine » seront réalisés sur papier laser uniquement et sécurisés sur trame anti-photocopie. Les « feuillets vierges pour les carnets ATA » de couleur (bleus, blancs, jaunes, verts, orange) devront comportés un logo ATA sur tous les feuillets et être sécurisés sur trame anti-photocopies.

Les éléments concernant la charte graphique et autres informations spécifiques pour l'impression en quadricolor (qui ne sont pas mentionnés dans le CCTP) seront fournis au Titulaire lors de la première réunion de cadrage pour la bonne exécution des prestations.

Par ailleurs, le titulaire devra répondre à une vigilance dans la qualité de finition des imprimés, notamment pour éviter tout décalage des champs d'écritures à l'impression.

Lorsque les documents livrés présentent un défaut, ils sont remplacés par le titulaire à ses frais dans un délai inférieur ou égal à celui de la commande initiale.

Il s'agit des documents suivants :

3.2.1.1 Certificats d'origine communautaire laser, sécurisés (trame anti-photocopie)

- IMC005 - Certificat d'origine original laser 80g (saumon) sécurisé
- IMC006 - Certificat d'origine copie laser 80g (jaune) sécurisé
- IMC004 - Certificat d'origine demande laser 80g (rose) sécurisé
- IMC012 - Certificat d'origine laser 80g- assemblé 1 original + 2 copies sécurisé

3.2.1.2 Feuilles vierges sécurisés (trame anti-photocopie)

- Feuille vierge couleur jaune (sécurisée) 120g
- Feuille vierge couleur jaune (sécurisée) 80g
- Feuille vierge couleur blanche (sécurisée) 120g
- Feuille vierge couleur blanche (sécurisée) 80g

- Feuille vierge couleur verte (sécurisée) 120g
- Feuille vierge couleur bleue (sécurisée) 120g
- Feuille vierge couleur bleue (sécurisée) 80g
- Feuille vierge couleur orange (sécurisée) 120g

3.2.1.3 Certificat de circulation des marchandises sécurisés (trame anti-photocopie)

✓ Documents pour impression laser (= les certificats d'origine)

- EUR1
- ATR

IMPORTANT : Un spécimen des imprimés évoqués ci-dessus est disponible sur simple demande.

3.3 Prestation logistique des documents douaniers

Le titulaire a en charge la logistique des documents douaniers qu'il a édités pour la CCI Paris Ile-de-France.

Au titre de l'exécution des prestations de logistique, le titulaire assurera le stockage, la manutention, l'emballage, la gestion des commandes passées par la CCI Paris Ile-de-France, les expéditions de documents douaniers de certificats d'origine, de Carnets ATA et ATR/EUR1 à destination de l'ensemble des CCI métropolitaines et des DROM COM ainsi que la gestion électronique des commandes passées par les CCI.

Le titulaire assure le suivi informatique des mouvements de stockage et d'expédition.

3.4 Système de commande en ligne

Le titulaire devra disposer d'un système de commande en ligne dédié pour l'ensemble du réseau des CCI.
Toute commande est obligatoirement passée par le biais du système de commande en ligne, sécurisé par un identifiant et un mot de passe propre à chacun des utilisateurs.

Ce système permettra aux CCI de pouvoir optimiser et simplifier le processus de commande auprès du titulaire. Le titulaire reçoit les commandes des CCI via le système de commande en ligne. Il livre les documents objet de la commande dans les délais de livraison indiqués dans l'offre du titulaire.

Toute commande reçue en dehors de ce circuit n'est pas traitée.
La CCI Paris Ile-de-France se chargera de la facturation des commandes reçues et effectuées par le titulaire, auprès de chacune des CCI.

La CCI Paris Ile-de-France réalise des commandes d'imprimés auprès du titulaire qui se chargera de les stocker dans ses locaux.
Chaque CCI commande, auprès du titulaire du marché, les imprimés qu'il livre à partir du stock existant.

Remarque : Ce système n'est pas un outil de paiement en ligne.

3.4.1 Sécurisation et identification des utilisateurs

Pour se connecter au portail de commande en ligne, chaque CCI, disposera d'un identifiant et d'un mot de passe personnalisé.

Les mots de passe doivent être transmis de manière sécurisée à l'utilisateur. L'utilisateur doit pouvoir modifier son mot de passe lors de sa première connexion.

Chaque utilisateur n'est autorisé à accéder qu'à son compte pour la prise en compte de ces commandes.
En cas de départ d'un administrateur disposant des privilèges sur des composants des Systèmes d'Informations :

- Les comptes individuels dont il disposait doivent être inactivés ;
- Les éventuels mots de passe d'administration dont il avait connaissance doivent être changés (exemples : mot de passe des comptes CCI ou comptes de services utilisés dans le cadre des fonctions de l'administrateur)

La création des profils d'utilisateurs attendus est décrite ci-dessous :

- ✓ Profil des différentes CCI : l'accès leur permet de passer des commandes ;

- ✓ Profil du titulaire : il lui permet de recevoir les commandes à réaliser, gérer la logistique à mettre en place, préparer les commandes, les livrer, éditer les bons de livraison ;

- ✓ Profil CCI Paris Ile-de-France : il permet à la CCI Paris Ile-de-France d'avoir un état des commandes déjà effectuées ou en cours de traitement ou en attente de traitement. Il permet également la réalisation d'extraction de données telles que les bons de commandes par commande, demande d'établissement de factures en format PDF par commande et par zone de facturation, édition statistique par mois. Notamment, les statistiques doivent permettre à la CCI Paris Ile-de-France d'établir précisément le CA mensuel de vente des imprimés global et par CCI.

  De plus, la CCI Paris Ile-de-France pourra :
  - Superviser les comptes client : valider ou bloquer les commandes ;
  - Mettre à jour les tarifs ;
  - Administration des messages : confirmation de commande, alerte de commandes ;

Le portail fera l'objet d'une maintenance et de mises à jour régulières.

3.4.2 Frais d'expédition

Les frais d'expédition, tels que complétés par le titulaire dans son offre seront implémentés directement lors de la commande en ligne, au regard des quantités commandées par chacune des CCI.

3.4.3 Prise en compte de demande de personnalisation et d'extraction sur l'outil de commande en ligne

3.4.3.1 Demande de Personnalisation

Une personnalisation sur l'outil de commande en ligne peut faire l'objet de demandes de la CCI Paris Ile-de-France, auprès du titulaire (exemple message à destination des CCI indiquant la période de fermeture pour congés du titulaire, ajout d'une zone de facturation identifiant le récepteur de la demande d'établissement de facture).
A ce titre, il appartient au titulaire de proposer une zone « commentaires » ou « libre » permettant d'indiquer les informations afin qu'aucun coût supplémentaire ne soit généré.

3.4.3.2 Extractions

Le titulaire devra mettre à disposition du DFCE de la CCI Paris Ile-de-France, une macro permettant d'effectuer les extractions sur l'outil de commande en ligne.

Ces extractions seront impérativement au format « EXCEL » et devront répondre à minima aux demandes ci-dessous :

- Extraction d'un fichier client avec coordonnées et mot de passe des CCI (en la qualité « d'administrateur » de la CCI Paris Ile-de-France)
- Extraction d'un fichier de données comptables
- Extraction d'un fichier de gestion des stocks

La CCI Paris Ile-de-France détaillera précisément au titulaire le contenu des données pour chacun des fichiers. La macro mise à disposition sera aux frais du titulaire.

3.4.3.3 Assistance en ligne

Une assistance en ligne pour toute question relative à l'utilisation du portail ou à la résolution de dysfonctionnement constaté devra être mise en place pendant toute la durée du marché, du lundi au vendredi, aux heures ouvrables telles que précisées par les candidats. L'assistance ne généra aucun coût supplémentaire.

3.5 Gestion du stock et quantités minimales de commande en ligne

3.5.1 Détail des stocks minimums et quantités commandées

Le titulaire prévoit un espace dédié à la CCI Paris Ile-de-France avec une surface pour le stockage des documents, dans de bonnes conditions de sécurité, de conservation et souscrit les assurances couvrant la reconstitution du stock à sa valeur en cas de sinistre éventuel. Le niveau souhaité des stocks d'alerte sera communiqué au titulaire lors de la réunion de cadrage.

Le système de commande en ligne doit, par ailleurs permettre d'améliorer le suivi des stocks en temps réel et devra être capable d'extraire des données électroniques permettant à la CCI Paris Ile-de-France d'automatiser le circuit comptable (demande d'établissement de facture) et ainsi optimiser les temps de saisie.

Le titulaire transmet mensuellement un tableau de suivi des stocks indiquant les quantités expédiées par mois, le stock réel, les stocks minimum et d'alerte. Un inventaire des stocks est réalisé à la fin de l'année par le titulaire et pourra se faire en présence de la CCI Paris Ile-de-France.

Les stocks minimum et d'alerte sont précisés dans l'Annexe 3 du CCTP.

3.5.2 Reprise du stock

La CCI Paris Ile-de-France, propriétaire du stock des imprimés informe l'ancien prestataire et le nouveau titulaire des conditions de reprise du stock dans le présent article.

<u>En début de marché</u> :

Le titulaire récupèrera les stocks restants au 31/12/2026 auprès de l'ancien prestataire du marché. Les informations nécessaires à la récupération des stocks lui seront fournies lors de la première réunion de cadrage. Il a à sa charge et à ses frais l'acheminement des stocks vers sa zone de stockage. Il adresse un état du stock récupéré à la CCI Paris Ile-de-France.

En fin de marché :

Le titulaire dresse un état des stocks en 2 exemplaires, le premier est adressé à la CCI Paris Ile-de-France et le second accompagne le stock en fin de marché, transmis au nouveau titulaire.

Pour information, un état des stocks au 30/09/2026 est joint en Annexe 2 du CCTP.

3.6 Revente de document au réseau des CCI

Revente des documents douaniers CCI Paris Ile-de-France

Le titulaire s'interdit expressément de vendre directement au réseau des CCI, l'ensemble des documents douaniers objet du présent marché ; sauf après consultation et accord écrit de la CCI Paris Ile-de-France.

3.7 Clause environnementale

Le titulaire devra prendre en compte les objectifs de développement durable conformément à l'article L2111-1 de code de la commande publique.
Les candidats devront attester de l'obtention du label « Imprim'Vert » ou équivalent, et justifier l'emploi de papier « FSC », « PEFC » ou équivalent ou recyclé.

Il doit fournir dans son offre un justificatif attestant l'obtention de cette marque ou d'un équivalent délivré par un organisme extérieur à l'entreprise attestant :

- Une bonne gestion des déchets dangereux et la détention d'une autorisation de déversement si l'entreprise est raccordée au réseau ;
- Un stockage sécurisé des liquides neufs dangereux et des déchets liquides en cours d'utilisation ou non afin d'éviter toute pollution accidentelle ;
- Une exclusion des produits étiquetés toxiques ;
- Une sensibilisation environnementale du personnel de l'entreprise ;
- Un suivi trimestriel des consommations énergétiques (électricité, gaz, fuel, GPL et autre combustible utilisé au sein de l'entreprise) et la transmission de ces données à chaque renouvellement de la marque « Imprim'Vert », « FSC » ou équivalent.

Toute autre démarche environnementale devra être mentionnée et fera l'objet d'une attention particulière.

4 DELAIS DE FABRICATION DES IMPRIMES POUR LA CCI PARIS ILE-DE-FRANCE.

Le délai de fabrication des imprimés, commandés par la CCI Paris Ile-de-France, quel que soit le nombre d'exemplaires, devra être conforme au délai indiqué dans l'offre du titulaire.
Les délais maximaux de fabrication ne pourront cependant excéder 21 jours ouvrés.

Les délais courent à compter du jour et de l'heure de réception du bon de commande par le titulaire (avis de réception faisant foi).

La durée de validité du dernier bon de commande ne pourra excéder 6 mois à compter de la date d'échéance du marché.

5 DELAIS ET MODALITES DE LIVRAISON DES IMPRIMES

5.1 Délai de livraison

Le délai de livraison des imprimés démarre à compter du jour et de l'heure de réception du bon de commande par le titulaire via l'outil de commande (avis de réception faisant foi) soit :

a) 2 jours ouvrés maximum pour les CCI situées en France métropolitaine ;
b) 3 jours ouvrés maximum pour les CCI situées dans les DROM-COM.

5.2 Modalités de livraison

5.2.1 Lieux de livraison

Les lieux de livraison correspondent à l'ensemble des CCI métropolitaines et des DROM COM faisant la demande de documents douaniers de certificats d'origine, de certificats de circulation et de Carnets ATA.

L'Annexe 1 du CCTP précise la répartition géographique des expéditions de l'année 2025.

5.2.2 Horaires de livraison

Les horaires de livraison seront à déterminer avec chaque correspondant des CCI métropolitaines et des DROM COM faisant une demande de documents douaniers de certificats d'origine, de certificats de circulation et de Carnets ATA.

5.2.3 Bon de livraison et contenu

Le titulaire doit établir un bon de livraison dans les conditions décrites au CCAG FCS. Néanmoins, le bon de livraison devra impérativement préciser, outre les données obligatoires précisées dans l'Acte d'Engagement valant CCAP, la référence du bon de commande, le nom du service émetteur, le code du client CCI et l'adresse de facturation à prendre en compte par la CCI Paris Ile-de-France lors de la refacturation à la CCI.

6 REUNION

L'organisation de réunion téléphonique ou physique pourra être fixée sur simple demande de la CCI Paris Ile-de-France pour faire un point sur l'exécution du marché. En cas de dysfonctionnement, la CCI Paris Ile-de-France pourra également convoquer le titulaire, en respectant un délai de prévenance de 2 jours ouvrés. A cette fin le titulaire devra se rendre disponible sous 8 jours ouvrés, sauf impossibilité dûment justifiée.

7 FICHIER DE REPORTING

Le titulaire est tenu de communiquer sur simple demande de la CCI Paris Ile-de-France ou de mettre à disposition via l'outil et dans un délai de 3 jours ouvrés (si demande d'envoi), les statistiques de commandes effectuées sur la période demandée.

Ces statistiques seront communiquées au format Excel et comprendront à minima :

- La date du bon de commande
- Le numéro de bon de commande
- L'année d'exercice facturée

- Le numéro de marché,
- L'entité commanditaire
- La référence de la fourniture commandée,
- La désignation de la fourniture commandée,
- Les quantités correspondantes par type d'imprimés
- Le montant des fournitures HT et TTC

8 CLAUSES GENERALES DE SECURITE DES SYSTEMES D'INFORMATION

8.1 Acronymes et définitions

8.1.1 Acronymes

Les acronymes utilisés dans les présentes clauses sont :

- **ANSSI** Agence nationale de la sécurité des systèmes d'information
- **CNIL** Commission nationale de l'informatique et des libertés
- **RGS** Règlement général de sécurité
- **RGPD** Règlement Général sur la Protection des Données
- **IaaS** Infrastructure as a Service
- **RSSI** Responsable de la Sécurité du Système d'Information
-

8.1.2 Définitions

- **Actions d'administration** – ensemble des actions d'installation, de suppression, de modification et de consultation de la configuration d'un système participant au système d'information du service et susceptibles de modifier le fonctionnement ou la sécurité de celui-ci.
- **Audit** – processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure les exigences d'un référentiel sont satisfaites.
- **Bien** – tout élément représentant de la valeur pour le service à qualifier.
- **Cloud computing (informatique en nuage)** – modèle permettant un accès aisé, généralement à la demande, et au travers d'un réseau, à un ensemble de ressources informatiques partagées et configurables.
- **État de l'art** – ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine réglementaire.
- **Incident lié à la sécurité de l'information** – un ou plusieurs événement(s) liés à la sécurité de l'information, indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme ou de menacer la sécurité de l'information.
- **Infrastructure technique** – ensemble des composants matériels et logiciels nécessaires à la mise à disposition de ressources affectées à la demande (virtualisées ou non). Ce socle permet l'accomplissement de la prestation dans le cadre d'un service IaaS, ou sert de base à la construction du service dans les autres cas.
- **Interface d'administration** – interface logicielle permettant à une entité disposant des privilèges requis (un administrateur, un compte de service, un développeur « DevOps », etc.) de réaliser des actions d'administration d'un système d'information.
- **Menace** – cause potentielle d'un incident indésirable pouvant nuire à un système ou à un organisme.

- **Mesure de sécurité** – mesure qui modifie la vraisemblance ou la gravité d'un risque. Elle comprend la politique, les procédures, les lignes directrices, et les pratiques ou structures organisationnelles, et peut être de nature administrative, technique, managériale ou juridique.
- **Politique** – intentions et orientations d'un organisme telles que formalisées par sa direction.
- **Prestataire d'audit de la sécurité des systèmes d'information** – organisme réalisant des prestations d'audit de la sécurité des systèmes d'information. Il est dit qualifié si un organisme de qualification a attesté de sa conformité au Référentiel d'exigences des prestataires d'audit de la sécurité des systèmes d'information.
- **Risque** – effet de l'incertitude sur l'atteinte des objectifs. Il est exprimé en termes de combinaison des conséquences d'un événement et de sa vraisemblance.
- **Sécurité d'un système d'information** – ensemble des moyens techniques et non-techniques de protection permettant à un système d'information d'assurer la disponibilité, l'intégrité et la confidentialité des données, traitées ou transmises, et des services connexes que ces systèmes offrent ou rendent accessibles.
- **Supervision** – surveillance du bon fonctionnement d'un système d'information ou d'un service. Elle concerne la collecte de données (mesures, alarmes, etc.) mais elle ne permet pas d'agir sur l'élément surveillé (ce qui relève des tâches d'administration).
- **Système d'information –** ensemble organisé de ressources (matériels, logiciels, personnels, données et procédures) permettant de traiter et de diffuser de l'information.
- **Vulnérabilité** – faiblesse d'un bien ou d'une mesure pouvant être exploitée par une menace ou un groupe de menaces.

8.2 Gestion des biens

Les biens essentiels de la CCI Région Paris Île-de-France sont les informations et fonctions importantes que la CCI Région Paris Île-de-France utilise pour exercer ses missions.
Ces biens sont caractérisés par des critères de disponibilité, de confidentialité et d'intégrité qui, s'ils venaient à être altérés, pourraient remettre en cause tout ou partie du système d'information de la CCI Région Paris Île-de-France.

Il est donc impératif que des exigences de sécurité portent sur tous les biens externalisés.

La démarche utilisée pour inventorier les biens essentiels au fonctionnement du système d'information externalisé doit être formalisée entre la CCI Région Paris Île-de-France et le titulaire et être compatible avec les méthodes d'analyse de risques reconnues dans la profession.

L'objectif final est de maîtriser précisément les informations et fonctions importantes du système d'information de la CCI Région Paris Île-de-France qui seront confiées au titulaire.
Les exigences de sécurité des SI définis par la CCI Région Paris Île-de-France est disponible en annexe.

8.3 Critères de sécurité

La CCI Région Paris Île-de-France retient 4 critères sur lesquels elle a défini sa politique de sécurité des systèmes d'information que sont :

- La **disponibilité :** reflète le besoin que des biens essentiels soient accessibles et fonctionnels à tous les utilisateurs de la CCI Région Paris Île-de-France à un moment donné.
    - La solution doit avoir des temps de disponibilité tels que définis dans la clause relative au niveau de service exigé.

- L'**intégrité** : reflète le besoin que des biens essentiels ne soient pas altérés. Elle correspond autant à leur niveau de conformité qu'à leur stabilité, leur exactitude, leur complétude.
  - Des mécanismes doivent être prévus pour détecter et corriger une perte d'intégrité. Tous les biens essentiels concernés doivent demeurer parfaitement intègres.
- La **confidentialité** : reflète le besoin que des biens essentiels ne soient ni compromis ni divulgués. Elle correspond au nombre ou catégories de personnes autorisées à y accéder.
  - Des fonctionnalités doivent être proposées pour assurer la confidentialité des échanges, aussi bien pour les transferts de messages que pour leur stockage. Tous les biens essentiels concernés ne doivent être accessibles qu'aux collaborateurs ou membres directement concernés et identifiés.
- La **traçabilité** : reflète le besoin que les opérations sur les biens essentiels soient enregistrées, de façon que l'altération de l'un des critères de disponibilité, d'Intégrité ou de confidentialité puisse être détectée.
  - La traçabilité mise en œuvre doit être compatible avec les standards techniques ou réglementaires de la profession. Tous les biens essentiels concernés doivent faire l'objet d'une traçabilité de toutes les opérations de création, modification et de suppression.

8.4 Définitions des clauses de sécurité du système d'information

Les exigences concernent le périmètre de sécurité commun à la CCI Région Paris Île-de-France et au titulaire dans le cadre de la prestation d'externalisation.
Les exigences de sécurité doivent être couvertes par le titulaire par la mise en place de dispositifs de sécurité décrits ci-dessous.

8.5 Plan d'Assurance Sécurité

Le titulaire doit démontrer qu'il adopte de manière formelle et non empirique une approche des risques dans la fourniture de sa prestation.

L'objectif est de mettre en œuvre et maintenir un niveau de sécurité de l'information et de service conforme au niveau de sécurité mis en place à la CCI Région Paris Île-de-France.
La CCI Région Paris Île-de-France exige de tout prestataire que la sécurité des systèmes d'information qu'il gère ainsi que son propre système d'information soit piloté. Dans ce contexte, le titulaire doit avoir une politique de sécurité formalisée ainsi que des procédures opérationnelles qui lui permettent d'appliquer ladite politique.

Sa politique de sécurité doit notamment respecter les bonnes pratiques de sécurité relevant de l'hygiène informatique, telles que décrites dans le guide « Hygiène Informatique » de ANSSI (http://ssi.gouv.fr).
Le titulaire peut également faire état des certifications dont il dispose dans ce domaine notamment dans le cadre des normes ISO 27001 et 22301. Dans ce cas il fournira une copie des certificats afin d'apporter la preuve de la certification.

La CCI Région Paris Île-de-France se réserve le droit de vérifier que la sécurité effectivement mise en œuvre correspond bien au niveau annoncé par le titulaire.
Tout prestataire et tout sous-traitant doit garantir que les services qu'il fournit ne remettent pas en cause le niveau global de sécurité.

Dans le cas spécifique du recours à des sous-traitants, le titulaire doit garantir que le niveau de sécurité informatique dont il a fait état est respecté pour tous ses sous-traitants.

Le titulaire doit fournir un plan d'assurance sécurité décrivant l'ensemble des dispositions spécifiques qu'il met en œuvre pour garantir le respect des exigences de sécurité de la CCI Région Paris Île-de-France.

8.6 Appréciation des risques

Le titulaire doit documenter une appréciation des risques couvrant l'ensemble du périmètre du service en utilisant une méthode documentée garantissant la reproductibilité et comparabilité de la démarche.

L'appréciation des risques doit prendre en compte :

- La gestion des informations de la CCIR selon leurs besoins de sécurité
- Les risques ayant des impacts sur les droits et libertés des personnes concernées en cas d'accès non autorisé, de modification non désirée et de disparition de données à caractère personnel ;
- Les risques de défaillance des mécanismes de cloisonnement des ressources de l'infrastructure technique (mémoire, calcul, stockage, réseau) partagées entre les différents clients du titulaire ;
- Les risques liés à l'effacement incomplet ou non sécurisé des données stockées sur les espaces de mémoire ou de stockage partagés entre les différents clients du titulaire, en particulier lors des réallocations des espaces de mémoire et de stockage ;
- Les risques liés à l'exposition des interfaces d'administration sur un réseau public.

Les exigences légales et réglementaires spécifiques liées aux types d'informations confiées par la CCI Région Paris Île-de-France au titulaire doivent être prise en compte dans l'appréciation des risques.
La direction du titulaire doit accepter formellement les risques résiduels identifiés dans l'appréciation des risques.

Le titulaire doit réviser annuellement l'appréciation des risques et à chaque changement majeur pouvant avoir un impact sur le service.

8.7 Organisation de la sécurité avec le titulaire

L'organisation de la sécurité au sein de la CCI Région Paris Île-de-France est pilotée par le Responsable de la Sécurité du Système d'Information (RSSI). Avec l'appui de la Direction Générale, le RSSI a en charge la mise en place et le suivi de la Politique de Sécurité des Systèmes d'Information de la CCI Région Paris Île-de-France.

Le RSSI est responsable de l'intégration des clauses de sécurité dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques de la CCI Région Paris Île-de-France.

En fonction de la taille des projets, le RSSI peut être amené à nommer un correspondant sécurité spécifique au projet pour suivre l'application des mesures de sécurité par le titulaire.

8.8 Obligations du titulaire

Le titulaire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier il s'engage à informer la CCI Région Paris Île-de-France des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.
Les délais et procédures d'application des correctifs seront à valider par le RSSI de la CCI Région Paris Île-de-France.

Outre le respect de ses obligations au titre de la convention de service, le titulaire informera préalablement la CCI Région Paris Île-de-France de toute opération susceptible de provoquer l'indisponibilité ou une dégradation des performances du système.
Le titulaire est responsable du maintien en condition de sécurité du système pendant toute la durée des prestations.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.
Pour y parvenir le titulaire pourra, notamment, se référer aux publications de l'ANSSI.

8.9 Transfert du système

Le titulaire se porte garant de l'intégrité et de la confidentialité des données qui lui sont confiées pendant la phase de transfert du système d'information. Il appartient en particulier au titulaire de faire des sauvegardes des informations de la CCI Région Paris Île-de-France et de gérer ces sauvegardes de manière à permettre une reprise en cas d'incident lors de la bascule du système.

8.10 Confidentialité

Les parties s'engagent à ne pas divulguer le présent marché et toute information, de quelque nature que ce soit, échangée à l'occasion de son exécution et à prendre toutes mesures organisationnelles et techniques propres à empêcher une telle divulgation. Elles se portent garant du respect par leurs salariés de cette obligation de confidentialité, même après que ceux-ci auront cessé leurs fonctions.

Les informations couvertes par l'interdiction de divulgation de confidentialité concernent notamment :

- Le contenu hébergé : les informations ou fonctions traitées par le système ;
- Les informations dont la divulgation est de nature à porter atteinte à la sécurité du système (mots de passe, clés de chiffrement, documentations relatives à l'architecture et la sécurité du système, etc.).
-

Cette obligation se maintient pendant toute la durée d'exécution du présent accord, mais aussi à son terme tant que ces informations n'ont pas été rendues publiques par la volonté de la CCI Paris Ile de France.

Le titulaire pourra toutefois communiquer lesdites informations à ses fournisseurs ou sous-traitants sous réserve de leur imposer la même obligation de confidentialité. Les parties s'engagent au respect de l'obligation de confidentialité par les personnes auprès desquelles la diffusion de l'information est expressément autorisée.

8.11 Localisation des données

Les lieux d'hébergement des données doivent satisfaire aux exigences de sécurité de la CCI Région Paris Île-de-France et aux dispositions de la loi informatique et liberté du 6 janvier 1978, du règlement européen 2016/679 et de la directive 2016/680.

Le titulaire doit communiquer la liste de tous les lieux de stockage de données et de traitement des données (site d'hébergement principal, site(s) de secours, etc.).
Si la faisabilité technique de cette exigence peut s'avérer délicate dans le cadre d'architectures distribuées, il est demandé au titulaire d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier à la suite d'un incident.

Le titulaire peut réaliser des opérations de support aux commanditaires depuis un État hors de l'Union Européenne. Il doit communiquer à la CCI Région Paris Île-de-France la liste des opérations qui peuvent être effectuées par le support depuis un État hors de l'Union Européenne, et les éventuels mécanismes permettant d'en assurer le contrôle d'accès et la supervision depuis l'Union Européenne.

Des exigences complémentaires sont applicables aux données personnelles, se référer au chapitre correspondant.

8.12 Sécurité des développements applicatifs

Le titulaire est tenu d'assurer la sécurité des développements conformément à l'état de l'art dans chacune des technologies mises en œuvre.
Le titulaire doit documenter et mettre en œuvre des règles de développement sécurisé des logiciels et des systèmes, et les appliquer aux développements internes.
Il doit documenter et mettre en œuvre une formation adaptée en développement sécurisé aux employés concernés.

Ci-après une liste, non exhaustive, de règles applicables :

- Environnement applicatif maintenu en tenant compte des recommandations d'application de correctifs par les éditeurs ;
- Contrôle rigoureux des entrées utilisateurs ;
- Sécurisation des accès aux interfaces d'administration et aux fonctions d'administration ;
- Installation du minimum de fonctions nécessaires lors de l'installation ;
- Principe du moindre privilège ;
- Utilisation de mots de passe dans le code interdite ;
- Mise en œuvre d'une gestion efficace des erreurs ;
- Protection des codes sources contre toute divulgation et contre toute altération ;
- Protection des sessions contre l'usurpation ;
- Protection des données saisies en entrée et envoyées en sortie contre les attaques par injection ou par XSS ;
- Chiffrements des flux sensibles ;
- Protection des clés privée de chiffrement.
- etc. …

Pour la mise en œuvre de technologies web, le titulaire prend en compte l'ensemble du spectre des vulnérabilités et des attaques existantes en matière d'applications web sur la base du référentiel de l'OWASP (Open Web Application Security Project).

A ce titre, le titulaire doit procéder aux tests de sécurité relatifs aux 10 risques les plus fréquents des applications web dans le cadre du développement des systèmes d'informations.
La recette de l'application comprend un audit du code permettant de s'assurer d'une implémentation conforme aux exigences de sécurité. La correction d'éventuelles anomalies détectées lors de la revue de code sont à la charge du titulaire.

Le titulaire s'engage à corriger toute vulnérabilité qui aurait été identifiée dans son code.

La CCI Région Paris Île-de-France se réserve le droit de vérifier qu'un audit du code a bien été réalisé et les corrections apportées.

Développement externalisé
Le titulaire doit documenter et mettre en œuvre une procédure permettant de superviser et de contrôler l'activité de développement externalisé des logiciels et des systèmes. Cette procédure doit s'assurer que l'activité de développement externalisé soit conforme à la politique de développement sécurisé du titulaire et permette d'atteindre un niveau de sécurité du développement externe équivalent à celui d'un développement interne.

8.13 Suivi et supervision du service hébergé

Le titulaire doit mettre à disposition de la CCI Région Paris Île-de-France des indicateurs du service hébergé. Les indicateurs attendus sont notamment (liste non exhaustive) :

- Fréquence et suivi des mises à jour effectuées ;
- Durée d'indisponibilité maximum et suivi de ces indisponibilités ;
- Fréquence des sauvegardes et tests de restauration effectués ;

Et dans le cadre de serveurs dédiés à la CCI Région Paris Île-de-France, des indicateurs sur les ressources :

- Charge réseau ;
- Charge processeur utilisée et pourcentage de la charge ;
- Charge mémoire utilisée et pourcentage de la charge ;
- etc. …

8.14 Gestion des incidents

Responsabilités et procédures

Le titulaire doit documenter et mettre en œuvre une procédure permettant d'apporter des réponses rapides et efficaces aux incidents de sécurité. Ces procédures doivent définir les moyens et délais de communication des incidents de sécurité auprès de la CCI Région Paris Île-de-France ainsi que le niveau de confidentialité exigé pour cette communication.
Le titulaire doit informer ses employés et l'ensemble des tiers participant à la mise en œuvre du service de cette procédure.

Le titulaire doit documenter toute violation de données à caractère personnel et en informer la CCI Région Paris Île-de-France. Conformément au RGPD, la violation doit être notifiée à la CNIL si elle présente un risque pour les droits et libertés des personnes concernées. Elle doit faire l'objet d'une information auprès des personnes concernées lorsque le risque pour leur vie privée est élevé.

Signalements liés à la sécurité de l'information

Le titulaire doit documenter et mettre en œuvre une procédure exigeant de ses employés et des tiers participant à la mise en œuvre du service qu'ils lui rendent compte de tout incident de sécurité, avéré ou suspecté ainsi que de toute faille de sécurité.
Le titulaire doit documenter et mettre en œuvre une procédure permettant à l'ensemble des commanditaires de signaler tout incident de sécurité, avéré ou suspecté et toute faille de sécurité.

Le titulaire doit communiquer sans délai à la CCI Région Paris Île-de-France les incidents de sécurité et les préconisations associées pour en limiter les impacts. Il doit permettre à la CCI Région Paris Île-de-France de choisir les niveaux de gravité des incidents pour lesquels il souhaite être informé.

Le titulaire doit communiquer les incidents de sécurité aux autorités compétentes conformément aux exigences légales et réglementaires en vigueur.

En cas d'éventuelles attaques informatiques, la réactivité étant extrêmement importante, il convient au titulaire d'identifier et de communiquer à la CCI Région Paris Île-de-France :

- Un ou plusieurs contacts techniques joignables 24/24, 7/7, tous les jours de l'année ;
- Un ou plusieurs contacts décisionnels 24/24, 7/7, tous les jours de l'année.

Appréciation des événements liés à la sécurité de l'information et prise de décision
Le titulaire doit apprécier les événements liés à la sécurité de l'information et décider s'il faut les qualifier en incidents de sécurité. Pour l'appréciation, il doit s'appuyer sur une ou plusieurs échelles (estimation, évaluation, etc.) partagées avec la CCI Région Paris Île-de-France.

Note : Les incidents de sécurité incluent les violations de données à caractère personnel.
Le titulaire doit utiliser une classification permettant d'identifier clairement les incidents de sécurité touchant des données relatives à la CCI Région Paris Île-de-France, conformément aux résultats de l'appréciation des risques. Cette classification doit inclure les violations de données à caractère personnel.

Recueil de preuves

Le titulaire doit documenter et mettre en œuvre une procédure permettant d'enregistrer les informations relatives aux incidents de sécurité et pouvant servir d'éléments de preuve.
Réponse aux incidents liés à la sécurité de l'information
Le titulaire doit traiter les incidents de sécurité jusqu'à leur résolution et doit informer la CCI Région Paris Île-de-France conformément aux procédures.

Le titulaire doit archiver les documents détaillant les incidents de sécurité.
Il est recommandé que le prestataire fasse appel à un prestataire de réponse aux incidents de sécurité [PRIS] qualifié pour traiter les incidents de sécurité nécessitant une expertise supplémentaire.
Tirer des enseignements des incidents liés à la sécurité de l'information

Le titulaire doit documenter et mettre en œuvre un processus d'amélioration continue afin de diminuer l'occurrence et l'impact de types d'incidents de sécurité déjà traités.

8.15 Gestion des évolutions

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité.
En cas d'évolution, le titulaire devra vérifier que sa mise en œuvre est conforme aux exigences contractuelles et en apporter la justification auprès de la CCI Région Paris Île-de-France, avant validation par ce dernier.

Le titulaire devra appliquer les correctifs de sécurité des différents composants du système d'information selon les exigences présentées dans l'annexe « Exigence de sécurité des systèmes d'information La CCI Région Paris Île-de-France mesure la gravité des failles selon le « Common Vulnerability Scoring System » (CVSS).

Le titulaire indiquera les mesures techniques, organisationnelles et procédurales qu'il s'engage à prendre pour maintenir en condition de sécurité son système d'information.
Les délais et procédures d'application des correctifs seront à valider auprès du RSSI de la CCI Région Paris Île-de-France.

8.16 Gestion de la continuité

Compte tenu du caractère sensible, confidentiel et impératif des prestations d'impression des documents douaniers, le titulaire doit disposer, à la date de notification du marché et pendant toute sa durée d'exécution, d'un Plan de Continuité d'Activité (PCA) et d'un Plan de Reprise d'Activité (PRA) adaptés aux prestations objet du marché. Ces dispositifs devront permettre d'assurer la continuité ou le rétablissement des prestations dans les meilleurs délais (en cas d'incident susceptible d'affecter la production, le traitement, le stockage, le conditionnement ou l'acheminement des documents.

8.16.1 Textes de référence

Le titulaire réalisera des prestations conformément aux textes de référence en vigueur, notamment la norme ISO 22301 ou équivalent.

Le titulaire devra présenter son SMCA, sa politique de confidentialité et justifiera de références équivalentes au présent marché.

8.16.2 Événements couverts

Le PCA/PRA devra couvrir notamment les situations suivantes :

· indisponibilité du personnel clé ;
· panne des équipements d'impression ou de façonnage ;
· panne informatique ou perte de données ;
· cyberattaque ou compromission du système d'information ;
· coupure électrique prolongée ;
· indisponibilité des locaux de production ;
· sinistre (incendie, dégât des eaux, catastrophe naturelle) ;
· rupture logistique ;
· tout incident susceptible d'impacter la prestation.

8.16.3 Contenu minimal attendu

Le PCA/PRA devra comporter au minimum :

8.16.3.1 Organisation de crise

· désignation des responsables ;
· procédure d'escalade ;
· annuaire de crise actualisé ;
· modalités de communication avec le pouvoir adjudicateur.

8.16.3.2 Moyens de secours

· équipements de production redondants ;

· solutions informatiques de secours ;
· sauvegardes sécurisées ;
· solutions alternatives de transport et de livraison.

8.16.3.3 Reprise d'activité Le titulaire précisera :

· le délai maximal de redémarrage des productions ;
· le délai maximal de reconstitution des données ;
· les moyens mobilisables en situation de crise ;
· les priorités de traitement des commandes.

8.16.3.4 Sites de repli

Le titulaire indiquera :

· l'existence ou non d'un site de secours ;
· sa localisation ;
· sa capacité de production ;
· les délais d'activation.

8.16.4 Exigences minimales attendues

Le titulaire garantit :
· une sauvegarde quotidienne des données de production ;
· la conservation sécurisée des fichiers ;
· la possibilité de relancer une production interrompue ;
· la traçabilité des opérations réalisées en mode dégradé.

8.16.5 Tests et mise à jour

Le PCA/PRA devra être testé au minimum une fois par an. Le titulaire conservera les comptes rendus des exercices et les tiendra à disposition du pouvoir adjudicateur sur simple demande. Toute modification substantielle du PCA/PRA devra être portée à la connaissance du pouvoir adjudicateur.

8.16.6 Transmission

Le pouvoir adjudicateur pourra demander à tout moment :
· la version à jour du PCA ;
· la version à jour du PRA ;
· les résultats des derniers tests réalisés ;
· les mesures correctives mises en œuvre.

Tout incident majeur susceptible d'affecter la continuité des prestations ou la confidentialité est porté sans délai à la connaissance du DFCE. Cette information est accompagnée d'une première analyse d'impact, des mesures correctives mises en œuvre et des dispositions prises pour assurer la poursuite de l'exécution du marché.

8.17 Conformité aux référentiels et réglementations

La CCI Région Paris Île-de-France apporte une attention particulière à la conformité de ses biens essentiels externalisés, aussi bien dans le domaine réglementaire, que dans le domaine technique et normatif.
Elle est assujettie, par son statut, au respect du RGS. Le titulaire devra donc s'assurer de la compatibilité des solutions qu'il propose avec ce référentiel.
La CCI Région Paris Île-de-France utilise les référentiels recommandés par ANSSI ainsi que les guides diffusés par la CNIL.

Dans le domaine normatif, la CCI Région Paris Île-de-France s'appuie sur l'ensemble des normes de la série ISO 27000 (notamment ISO 27001 – 27002 – 27005) pour la mise en place de la gestion de la sécurité et sur les normes de la série ISO 22301 pour la gestion de la continuité d'activité.

Tous les services externalisés chez un titulaire doivent être compatibles avec les exigences réglementaires, normatives et techniques sur lesquelles s'appuie la CCI Région Paris Île-de-France.
Le titulaire fera état des certificats obtenus et audits réalisés couvrant la sécurité des systèmes d'information (ISO 27001 – 27017 – 27018 – 22301, SOC3, SSAE18/ISAE 3402, Privacy Shield, PCI DSS, …).

Si le titulaire propose une solution dans un mode dit « Cloud computing », il doit identifier clairement ses responsabilités et celle de son sous-traitant le cas échéant ainsi que leur conformité à la législation. Le « Cloud computing » étant basé sur l'utilisation de multiples serveurs répartis, il se peut que ces serveurs soient situés en dehors du territoire français, voire européen.

Dans tous les cas, et en l'absence de modification législative, le titulaire devra se conformer au principe de l'article 68 de la loi informatique et libertés du 6 janvier 1978 :
« Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet. Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées. »

L'article 69 de ladite loi prévoit expressément les outils permettant d'encadrer ce type de transferts : clauses contractuelles types, BCR, règles internes d'entreprises.
Le titulaire devra également se conformer au règlement européen 2016/679 et la directive 2016/680 en vigueur.

8.18 Relations avec les tiers

Identification des tiers

Le titulaire doit tenir à jour une liste de l'ensemble des tiers participant à la mise en œuvre du service (hébergeur, développeur, intégrateur, archiveur, sous-traitant opérant sur site ou à distance, fournisseurs de climatisation, etc.). Cette liste doit être exhaustive, préciser la contribution du tiers au service et au traitement de données à caractère personnel, et tenir compte des cas de sous-traitance à plusieurs niveaux.
Le titulaire doit tenir à disposition de la CCI Région Paris Île-de-France la liste de l'ensemble des tiers qui peuvent accéder aux données et l'informer de tout changement de sous-traitants au sens de l'article 28 du RGPD afin que la CCI Région Paris Île-de-France puisse émettre des objections à cet égard.

La sécurité dans les accords conclus avec les tiers

Le titulaire doit exiger des tiers participant à la mise en œuvre du service, dans leur contribution au service, un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Il doit le faire au travers d'exigences, adaptées à chaque tiers et à sa contribution au service, dans les cahiers des charges ou dans les clauses de sécurité des accords de partenariat. Le titulaire doit inclure ces exigences dans les contrats conclus avec les tiers.
Le titulaire doit contractualiser, avec chacun des tiers participant à la mise en œuvre du service, des clauses d'audit permettant à un organisme de qualification de vérifier que ces tiers respectent les exigences du présent référentiel.

Le titulaire doit définir et attribuer les rôles et les responsabilités relatives à la modification ou à la fin du contrat le liant à un tiers participant à la mise en œuvre du service.

Surveillance et revue des services des tiers

Le titulaire doit documenter et mettre en œuvre une procédure permettant de contrôler régulièrement les mesures mises en place par les tiers participant à la mise en œuvre du service pour respecter les exigences de sécurité des systèmes d'information de la CCI Région Paris Île-de-France.

Gestion des changements apportés dans les services des tiers

Le titulaire doit documenter et mettre en œuvre une procédure de suivi des changements apportés par les tiers participant à la mise en œuvre du service susceptibles d'affecter le niveau de sécurité du système d'information du service.
Dans la mesure où un changement de tiers participant à la mise en œuvre du service affecte le niveau de sécurité du service, le prestataire doit en informer l'ensemble la CCI Région Paris Île-de-France sans délais et mettre en œuvre les mesures permettant de rétablir le niveau de sécurité précédent.

Engagements de confidentialité

Le prestataire doit documenter et mettre en œuvre une procédure permettant de réviser au moins annuellement les exigences en matière d'engagements de confidentialité ou de non-divulgation vis-à-vis des tiers participant à la mise en œuvre du service.

8.19 Tests de vulnérabilité

Le titulaire accepte que la CCI Région Paris Île de France réalise des tests de vulnérabilités (non intrusif et non destructif) sans en être préalablement averti avec des scanners de tests de vulnérabilité (Exemple : Nessus).
Le titulaire prendra l'engagement que l'hébergeur, si ce n'est pas le titulaire, autorise la CCI Région Paris Île de France à exécuter les tests de vulnérabilité.

8.20 Audit sécurité

La CCI Région Paris Île-de-France se réserve le droit de diligenter un audit à tout moment pour contrôler que les engagements pris par le titulaire pour garantir la sécurité de la solution sont mis en place.

La CCI Région Paris Île-de-France se réserve le droit de requérir l'expertise d'un prestataire d'audit de sécurité des systèmes d'information.

Dans tous les cas, les audits respecteront les règles suivantes :

- Si l'audit est confié à un tiers indépendant, son intervention s'effectue aux frais de la CCI Paris Ile de France excepté si l'audit fait suite à un incident de sécurité, il sera alors à la charge du titulaire ;
    - L'audit ne doit en aucun cas perturber la bonne délivrance des services ;
    - Le cadre de l'audit devra être défini au préalable ;
    - L'audit sera mené durant les heures de travail du titulaire.

Cet audit peut être réalisé par la CCI Région Paris Île-de-France, ou un prestataire mandaté après avoir notifié le titulaire dans un délai de 10 jours ouvrables par lettre recommandé AR.
Dans le cas d'une intervention d'urgence, suite par exemple à la survenance d'un incident de sécurité, ce délai est réduit à 24 heures à partir de la notification de l'incident de sécurité et s'effectuera aux frais du titulaire.

Si le titulaire propose une solution dans un mode dit « Cloud computing » directement ou indirectement (infrastructures techniques reposant sur du « Cloud computing »), il doit fournir annuellement un rapport SOC 1 type 2 (SSAE18 ou ISEA 3402) et SOC 3.

Un rapport SOC 2 sera fourni au RSSI de la CCI Paris Île-de-France après signature d'un engagement de confidentialité.
Ces audits de sécurité sont aux frais du titulaire.

8.21 Manquement et résiliation

Dans le cas où le GIE Groupe CCI Paris Ile de France aurait connaissance d'un manquement avéré aux règles relatives à la sécurité des systèmes d'information telles que décrites ci-dessus, le marché pourrait être suspendu jusqu'à ce que le titulaire apporte des corrections jugées satisfaisantes par le GIE Groupe CCI Paris Ile de France.

Le GIE Groupe CCI Paris Ile de France se réserve le droit de mener ensuite un audit en respectant un délai de prévenance de 24 heures.
Il pourrait être mis fin au marché si le manquement n'est pas réparé dans les délais convenus entre les deux parties ou en cas de nouveau manquement.

8.22 Réversibilité

En cas d'arrêt des prestations confiées au titulaire par le GIE Groupe CCI Paris Ile de France, l'ensemble des matériels, logiciels et documentations confiés au titulaire doivent être restitués.
Le titulaire s'engage à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par la CCI Région Paris Île-de-France, ou par un autre prestataire de service.

Le titulaire s'engage à garantir, lors du transfert, la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations.
Le déménagement de cet ensemble des locaux du titulaire sera assuré aux frais du titulaire dans un délai maximum d'un mois après l'arrêt des prestations confiées au titulaire.
Une non-restitution de tout ou partie de cet ensemble sera considérée et traitée comme une perte.
Une restitution partielle peut être demandée par la CCI Région Paris Île-de-France, en cas d'arrêt d'une partie des prestations avant la fin du marché. Dans ce cas, le titulaire en sera informé au moins un mois avant la fin des prestations.

8.23 Fin du marché

À la fin du marché liant le titulaire et au GIE Groupe CCI Paris Ile de France, que le marché soit arrivé à son terme ou pour toute autre cause, le titulaire doit assurer un effacement sécurisé de l'intégralité des données au GIE Groupe CCI Paris Ile de France. Cet effacement peut être réalisé suivant l'une des méthodes suivantes, et ce dans un délai précisé dans la convention de service :

- Effacement par réécriture complète de tout support ayant hébergé ces données ;
- Effacement des clés utilisées pour le chiffrement des espaces de stockage de la CCI Région Paris Île-de-France ;
- Recyclage sécurisé.

Le titulaire doit également supprimer les données techniques relatives à la CCI Région Paris Île-de-France (annuaire, certificats, configuration des accès, etc.).

8.24 Protection des traitements de données à caractère personnel du titulaire

Le titulaire doit justifier du respect des principes de protection des données pour les traitements de données à caractère personnel mis en œuvre pour son propre compte. Il doit justifier au minimum les points suivants :

- Les finalités des traitements déterminées, explicites et légitimes ;
- La traçabilité des activités de traitement pour son compte et celui de son commanditaire ;
- Le fondement licite des traitements ;
- L'interdiction du détournement de finalité des traitements ;
- Les données utilisées respectent le principe du minimum nécessaire et suffisant pour les traitements ; ainsi sont adéquates, pertinentes et limitées ;
- La qualité des données utilisées pour les traitements maintenue : données exactes et tenues à jour ;
- Les durées de conservation définies et limitées.

Le titulaire doit justifier, pour les traitements de données à caractère personnel mis en œuvre pour son propre compte, du respect des droits des personnes concernées. Il doit justifier au minimum les points suivants :

- L'information des usagers via un traitement loyal et transparent ;
- Le recueil du consentement des usagers : exprès, démontrable et retirable ;
- La possibilité pour les usagers d'exercer les droits d'accès, de rectification et d'effacement ;
- La possibilité pour les usagers d'exercer les droits de limitation du traitement, de portabilité et d'opposition.

Lorsqu'il agit en qualité de sous-traitant au sens de l'article 28 du RGPD, le titulaire doit apporter assistance et conseil à la CCI Région Paris Île-de-France en l'informant si une instruction de ce dernier constitue une violation des règles de protection des données.