PROJET DE RÉFÉRENTIEL

Relatif à la certification RGPD des sous-traitants

Projet de référentiel soumis à consultation publique jusqu'au 28 février 2025.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

À qui s'adresse ce référentiel ?

Ce référentiel constitue la liste des critères auxquels un organisme qui effectue des traitements de données à caractère personnel en qualité de sous-traitant devra démontrer sa conformité en vue d'obtenir la certification de sous-traitant selon le référentiel de la CNIL.

1. Terminologie

RGPD
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 (règlement général sur la protection des données)

CEPD
Comité européen de la protection des données

Certification
Attestation délivrée par un tiers indépendant (organisme de certification) selon laquelle le respect de critères du présent référentiel a été prouvé.

Sous-traitant
L'entité juridique (organisme privé ou public) qui candidate à la certification pour des traitements de données à caractère personnel qu'il effectue pour le compte d'un responsable traitement (et qui obtient ensuite la certification, en cas de succès).

Client
Le responsable de traitement (ou le sous-traitant) qui fait appel au Sous-traitant (qui a obtenu la certification) pour réaliser un traitement de données.

Offre de service
Ensemble de services ou de prestations « sur étagère » que le Sous-traitant propose à plusieurs de ses clients.

Organisme de certification
Organisme chargé de l'évaluation du respect des critères du présent référentiel par le Sous-traitant dans le cadre du processus de certification.

Le système d'information de sous-traitance
L'ensemble des moyens informatiques utilisés par le Sous-traitant pour mettre en œuvre les traitements de données effectués pour le compte de ses clients.

Vulnérabilité critique
Vulnérabilité susceptible d'engendrer un risque élevé pour les personnes concernées en reprenant l'hypothèse d'un impact élevé, sauf à être en mesure de justifier d'un impact moindre.

Entropie
Quantité de hasard contenue dans un mot de passe ou une clé cryptographique, qui correspond à son degré d'imprédictibilité, et donc à sa capacité de résistance à une attaque par force brute.

2. Plan du référentiel

Partie 0. La demande de certification du sous-traitant – l'éligibilité
C0.01 – Identification du demandeur C0.02 – Cas du demandeur multisites C0.03 – Identification des traitements effectués en sous-traitance C0.04 – Applicabilité du RGPD C0.05 – Identification des traitements mis en œuvre en qualité de responsable de traitement C0.06 – Identification des facteurs de risque des traitements C0.07 – Description du système d'information de sous-traitance C0.08 – Cartographie des flux de données C0.09 – Réglementation applicable au sous-traitant
Partie 1. Les conditions de la sous-traitance – les engagements contractuels
C1.01 – Contrat de sous-traitance C1.02 – Description de l'objet de la sous-traitance C1.03 – Durée du traitement C1.04 – Clauses du contrat de sous-traitance C1.05 – Transparence sur l'existence de transferts de données hors Union européenne C1.06 – Transparence sur l'existence de sous-traitances ultérieures C1.07 – Transparence sur les mesures de sécurité C1.08 – Report des obligations aux sous-traitants ultérieurs C1.09 – Engagement d'assistance à l'exercice des droits C1.10 – Engagement d'assistance à la sécurité des données C1.11 – Engagement d'assistance à la notification des violations de données C1.12 – Engagement d'assistance à l'analyse d'impact C1.13 – Engagement de permettre la réalisation d'audits C1.14 – Documentation de la conformité C1.15 – Procédure de recueil des instructions du responsable de traitement C1.16 – Traitements mis en œuvre en qualité de responsable de traitement C1.17 – Cas de la suspension des traitements
Partie 2. L'environnement de la sous-traitance – la préparation du traitement
C2.01 – Informations relatives aux traitements réalisés en sous-traitance C2.02 – Registre des traitements C2.03 – Désignation du délégué à la protection des données C2.04 – Fonction et missions du délégué à la protection des données C2.05 – Désignation d'un référent certification C2.06 – Encadrement des transferts de données hors de l'Union européenne C2.07 – Outils de transfert de données hors de l'Union européenne C2.08 – Cas des transferts de données hors Union européenne par dérogation C2.09 – Procédure de recours à des sous-traitants ultérieurs C2.10 – Encadrement de la sous-traitance ultérieure C2.11 – Description des mesures de sécurité C2.12 – Déclaration d'applicabilité des mesures de sécurité C2.13 – Caractère approprié du niveau de sécurité C2.14 – Analyse des risques de sécurité pour le traitement des données C2.15 – Analyse d'impact relative à la protection des données C2.16 – Procédure de détection, analyse et résolution des incidents de sécurité C2.17 – Procédure relative à l'exercice des droits

Partie 3. La réalisation de la sous-traitance – la mise en œuvre du traitement
C3.01 – Instructions du responsable de traitement C3.02 – Mise en œuvre des mesures de protection des données C3.03 – Evolutions en cours de traitement C3.04 – Exercice des droits des personnes concernées par le traitement C3.05 – Association du délégué à la protection des données C3.06 – Sensibilisation de l'ensemble du personnel à la protection des données C3.07 – Formation du personnel impliqué dans le traitement C3.08 – Engagement de confidentialité du personnel impliqué dans le traitement C3.09 – Ressources pédagogiques en matière de protection des données C3.10 – Registre des incidents de sécurité C3.11 – Notification d'une violation de données constatée par le sous-traitant C3.12 – Réalisation d'audit technique
Partie 4. La fin de la sous-traitance – l'arrêt du traitement
C4.01 – Choix du sort des données C4.02 – Renvoi des données en fin de prestation C4.03 – Suppression des données en base active et archivage C4.04 – Suppression définitive des données C4.05 – Gestion de la sous-traitance ultérieure en fin de prestation C4.06 – Confirmation de la suppression des données
Partie 5. L'amélioration du niveau de protection des données – les plans d'action
C5.01 – Plan d'action pour la sécurité du traitement C5.02 – Plan d'évaluation de la sous-traitance ultérieure C5.03 – Plan d'amélioration C5.04 – Veille et actualisation
Annexe C32. Les mesures techniques et organisationnelles de sécurité – le socle de sécurité
C32.01 – Gestion des clés cryptographiques C32.02 – Chiffrement des données en transit C32.03 – Chiffrement des données au repos C32.04 – Filtrage des flux C32.05 – Gestion des habilitations C32.06 – Gestion des permissions d'accès logique et physique C32.07 – Contrôle des accès physiques C32.08 – Authentification des utilisateurs C32.09 – Complexité des facteurs d'authentification C32.10 – Protection des facteurs d'authentification C32.11 – Gestion des mots de passe C32.12 – Authentification multifacteur C32.13 – Accès au système d'information à distance C32.14 – Contrôle d'accès des serveurs, postes de travail et équipements mobiles C32.15 – Authentification de machine à machine C32.16 – Système de journalisation C32.17 – Sauvegarde des données C32.18 – Archivage des données C32.19 – Reprise d'activité C32.20 – Anonymisation des données C32.21 – Exportation de données C32.22 – Gestion des postes de travail, des équipements mobiles et des supports amovibles C32.23 – Mise au rebut et réaffectation C32.24 – Mises à jour de sécurité C32.25 – Charte informatique

3. Critères du référentiel

Partie 0. La demande de certification du sous-traitant – l'éligibilité

C0.01 – Identification du demandeur

Le Sous-traitant qui candidate à la certification est une entité juridique (organisme privé ou public) qui contractualise avec des clients, responsables de traitement ou sous-traitants, pour le compte desquels il effectue des traitements de données à caractère personnel.

Le Sous-traitant doit être établi sur le territoire de l'Union européenne ou dans un Etat membre de l'espace économique européen (EEE).

C0.02 – Cas du demandeur multisites

Dans le cas où le Sous-traitant réalise les traitements à partir de plusieurs de ses établissements, ceux-ci doivent être situés sur le territoire de l'Union européenne ou de l'EEE. Il doit être en capacité d'imposer le respect des critères du présent référentiel dans l'ensemble de ces établissements.

En matière de protection des données, il doit être en capacité d'imposer :

a) l'application des politiques, mesures et procédures qu'il définit ;

b) la mise en œuvre des mesures correctives et préventives qu'il décide.

Par ailleurs, le Sous-traitant doit être en capacité de démontrer, à partir de son établissement principal, que tous ses établissements respectent les critères du présent référentiel.

C0.03 – Identification des traitements effectués en sous-traitance

Le Sous-traitant doit recenser les traitements qu'il effectue pour le compte d'un ou plusieurs responsables de traitement et qu'il souhaite soumettre à la certification.

En particulier, le Sous-traitant doit identifier pour chacun de ces traitements :

a) les établissements où il effectue les traitements pour le compte de ses clients, c'est-à-dire les locaux où s'exerce son activité (hors activités qu'il sous-traite lui-même à des sous-traitants ultérieurs) ;

b) les sous-traitants auxquels il fait appel dans le cadre des traitements effectués pour le compte de ses clients (ses sous-traitants ultérieurs) ;

c) les établissements et les sous-traitants listés au a) et au b), au sein desquels des personnes disposent d'accès à privilèges au système d'information utilisé pour la mise en œuvre des traitements ou aux locaux d'hébergement des équipements informatiques ;

d) les transferts de données hors de l'Union européenne qu'il met en œuvre ou qu'un de ses sous-traitants met en œuvre ;

e) le ou les processus d'anonymisation qu'il met en œuvre dans le cadre des traitements qu'il effectue ;

f) les dispositions législatives ou réglementaires en matière de protection des données (issues du droit européen ou national – autres que le RGPD) auxquelles il est soumis lorsqu'il effectue les traitements pour le compte de ses clients (critère C0.09).

C0.03bis – Cas des offres de service

Lorsque le Sous-traitant propose à ses clients une *offre de service* qui implique qu'il effectue des traitements de données à caractère personnel pour leur compte, il recense les services pour lesquels il souhaite soumettre à la certification les traitements effectués.

Pour chacun de ces services, le Sous-traitant doit :

a) inclure, aux traitements recensés au critère C0.03, l'ensemble des traitements nécessaires à l'utilisation du service que le Sous-traitant propose, dès lorsqu'ils sont effectués pour le compte de son client, et non pour son propre compte en qualité de responsable de traitement (critère C0.05) ;

b) identifier les dispositions législatives ou réglementaires en matière de protection des données (issues du droit européen ou national – autres que le RGPD) auxquelles son client est susceptible d'être soumis lors de l'utilisation de son service (critère C0.09bis).

C0.04 – Applicabilité du RGPD

Les traitements pour lesquels le Sous-traitant souhaite obtenir une certification (critère C0.03) doivent être soumis aux obligations du RGPD et doivent être effectués pour le compte de clients soumis aux obligations du RGPD.

En particulier, les traitements ne sont pas éligibles à la certification lorsqu'ils sont effectués :

- par ou pour le compte d'une personne physique dans le cadre d'une activité strictement personnelle ou domestique ;

- par ou pour le compte d'une autorité compétente à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

C0.05 – Identification des traitements mis en œuvre en qualité de responsable de traitement

Le Sous-traitant doit recenser les traitements qu'il met en œuvre pour son propre compte, en qualité de responsable de traitement, dans le cadre de la prestation qu'il réalise pour son client.

En particulier, le sous-traitant doit identifier :

a) les traitements qui sont nécessaires à sa prestation, qui ne constituent pas un élément essentiel de son service ou ne vise pas spécifiquement le traitement de données à caractère personnel, et pour lesquels il détermine les finalités et les moyens de manière indépendante de ses clients (par exemple, un traitement de données à caractère personnel qui est nécessaire à la facturation de son service) ;

b) les traitements qu'il est tenu de mettre en œuvre en raison d'une obligation légale lui incombant en application du droit de l'Union ou du droit de l'État membre auquel il est soumis (par exemple, un traitement de données à caractère personnel répondant à des obligations comptables, sociales ou fiscales)

c) les traitements qui consistent à conserver des données à caractère personnel en raison d'un intérêt administratif, par exemple un intérêt en cas de contentieux justifiant de les conserver le temps des règles de prescription/forclusion applicable ;

d) les traitements qui consistent à réutiliser des données qui lui ont été confiées par ses clients dans le cadre de la sous-traitance pour une finalité distincte de celle pour laquelle elles ont été collectées (traitement dit « ultérieur ») ;

Pour chacun de ces traitements, le candidat doit renseigner la base légale retenue, comme par exemple, le fondement d'une mission d'intérêt public ou d'une obligation légale définie par une disposition législative ou réglementaire identifiée au critère C0.09.

C0.06 – Identification des facteurs de risque des traitements

Pour chaque traitement que le Sous-traitant souhaite soumettre à la certification (critère C0.03), il doit renseigner :

a) si ces traitements impliquent des traitements de données à des fins de profilage ou de prédiction en vue d'une évaluation ou notation de personnes ;

b) s'il effectue une prise de décision automatisée ayant un effet juridique ou un effet similaire significatif pour des personnes ;

c) s'il effectue un traitement de surveillance systématique consistant à observer, surveiller ou contrôler des personnes ;

d) s'il effectue un traitement de données sensibles ou hautement personnelles, telles que des catégories particulières de données à caractère personnel visées à l'article 9 du RGPD, des données à caractère personnel relatives aux condamnations pénales ou aux infractions visées à l'article 10 du RGPD ou encore des catégories de données augmentant le risque pour les droits et libertés des personnes, par exemple lorsqu'elles sont liées à des activités domestiques et privées ;

e) s'il effectue un traitement de données à grande échelle ;

f) s'il effectue un croisement ou une combinaison d'ensembles de données ;

g) s'il effectue un traitement de données de personnes vulnérables ;

h) s'il fait un usage innovant ou applique de nouvelles solutions technologiques ou organisationnelles.

Lorsque le Sous-traitant ne dispose pas des éléments permettant de renseigner certains des facteurs de risques a) à h) pour les traitements qu'il effectue pour le compte de ses clients, il justifie les raisons pour lesquelles il ne dispose pas de ces informations.

Co.07 – Description du système d'information de sous-traitance

Le Sous-traitant doit disposer d'une description générale du système d'information qu'il utilise pour les traitements effectués pour le compte de ses clients (le système d'information de sous-traitance)

En particulier, la description du système d'information de sous-traitance doit indiquer :

a) si celui-ci est cloisonné du système d'information que le Sous-traitant utilise pour d'autres traitements réalisés en tant que responsable de traitement (système d'information interne du Sous-traitant) ou pour d'autres traitements effectués en sous-traitance (en dehors de ceux recensés au critère Co.03) ;

b) les postes de travail ou équipements mobiles utilisés pour l'administration du système d'information de sous-traitance ;

c) les postes de travail ou équipements mobiles faisant partie du système d'information de sous-traitance, dans la mesure où ils constituent les moyens de mise en œuvre du traitement.

Co.08 – Cartographie des flux de données

Le Sous-traitant doit disposer d'une cartographie des flux de données qui recense les transmissions de données à caractère personnel, depuis et vers le système d'information de sous-traitance (critère Co.07).

Pour chaque flux de données entrant ou sortant du système d'information de sous-traitance, cette cartographie doit inclure :

a) l'identification et la description du flux, notamment lorsqu'il s'agit de flux d'exportation des données ;

b) l'émetteur du flux (ex : un module applicatif, une personne, une base de données, etc.) ;

c) le récepteur du flux ;

d) si des mesures de chiffrement du flux sont mises en œuvre par le Sous-traitant ;

e) si des mesures de filtrage des flux entrants ont mises en œuvre par le Sous-traitant ;

f) si d'autres mesures de sécurité sont à mettre en œuvre par le récepteur du flux.

Si le système d'information de sous-traitance n'est pas cloisonné de son système d'information interne, le Sous-traitant identifie les flux de données à caractère personnel entre ces deux systèmes d'information.

Note : Les flux de données permettant le maintien en condition opérationnelle de sécurité du système d'information de sous-traitance doivent être inclus dans cette cartographie.

C0.09 – Réglementation applicable au sous-traitant

Le Sous-traitant doit identifier les obligations qui lui incombent en vertu de dispositions législatives ou réglementaires en matière de protection des données (issues du droit européen ou national - autres que le RGPD) lorsqu'il effectue les traitements pour le compte de ses clients (voir critère C0.03).

Pour les traitements soumis à la certification, le Sous-traitant doit :

a) identifier les obligations applicables qui découlent des autres dispositions législatives ou réglementaires que le RGPD et qui nécessitent la mise en œuvre de mesures spécifiques de protection des données ;

b) identifier les autorisations préalables à obtenir auprès de la CNIL, d'une autre autorité de protection des données ou d'une autre autorité compétente, lorsqu'une disposition nationale conditionne la mise en œuvre du traitement à une telle autorisation.

Lors de l'identification des dispositions législatives ou réglementaires applicables, il est notamment vérifié si les traitements sont concernés par :

- des dispositions issues du droit national relatives à des situations particulières de traitement prévues par le RGPD, notamment au Chapitre IX du RGPD ;

- des dispositions issues du droit national ou européen spécifique au secteur d'activité du Sous-traitant ou aux finalités du traitement qu'il met en œuvre pour le compte d'un responsable de traitement.

C0.09bis – Cas d'une offre de service

Lorsque le Sous-traitant propose à ses clients une *offre de service* telle qu'identifiée au critère C0.03bis, il doit identifier les obligations susceptibles d'incomber à ses clients en vertu de dispositions législatives ou réglementaires en matière de protection des données (issues du droit européen ou national - autres que le RGPD) lorsque ceux-ci font usage de son service.

En particulier, pour les dispositions recensées au critère C0.03bis, le Sous-traitant doit identifier les obligations qui nécessitent la mise en œuvre de mesures spécifiques de protection des données pour les traitements soumis à la certification.

Partie 1. Les conditions de la sous-traitance – les engagements contractuels

C1.01 – Contrat de sous-traitance

Le Sous-traitant doit établir un contrat avec chacun de ses clients, responsable de traitement ou sous-traitant, pour lesquels il effectue un traitement de données à caractère personnel.

Ce contrat de sous-traitance doit prendre la forme d'un acte juridique pris au titre du droit d'un État membre de l'Union européenne ou d'un Etat membre de l'espace économique européen (EEE). Il doit définir la juridiction compétente en cas de litige.

C1.02 – Description de l'objet de la sous-traitance

Le contrat qui lie le Sous-traitant à son client doit définir l'objet de la sous-traitance : une description de la prestation demandée qui implique le traitement de données à caractère personnel (ou une description de *l'offre de service* proposée).

La description de l'objet de la sous-traitance doit inclure le détail des traitements réalisés pour le compte du client, notamment :

a) les catégories de personnes concernées : quels sont les types de personnes dont les données sont traitées ou susceptibles de l'être ?

b) les catégories de données à caractère personnel : quel type d'information est traité ?

En particulier, une ou plusieurs des catégories suivantes est-il l'objet du traitement :

- des données sensibles traitées en vertu de l'article 9 du RGPD ;

- des données relatives à des condamnations pénales et à des infractions en vertu de l'article 10 du RGPD ;

- des données relatives à des données de localisation telles que définies par la Directive 2002/58/CE ePrivacy ;

- d'autres données hautement personnelles, telles que le numéro d'identification national ou des données financières susceptibles d'être utilisées pour des paiements frauduleux ;

c) la nature du traitement : quel type de traitement est à réaliser par le Sous-traitant ?

d) la (ou les) finalité(s) pour laquelle (lesquelles) les données sont traitées : à quoi va servir le traitement réalisé pour le compte du client ou à quoi est-il prévu que ce traitement puisse servir ?

La description de l'objet de la sous-traitance peut également inclure explicitement des exclusions de traitement concernant des catégories de personnes concernées, des catégories de données à caractère personnel ou certaines finalités.

C1.03 – Durée du traitement

Le contrat qui lie le Sous-traitant à son client doit définir la durée du traitement des données à caractère personnel réalisé pour le compte de son client.

La durée du traitement doit être définie par :

a) une période qui prédétermine la date à laquelle le traitement prend fin ; ou

b) des conditions contractuelles qui permettront de déterminer la date à laquelle le traitement prendra fin, telle que la durée de validité du contrat, les conditions de tacite reconduction du contrat ou les conditions de rupture du contrat.

C1.04 – Clauses du contrat de sous-traitance

Le contrat qui lie le Sous-traitant à son client doit prévoir l'ensemble des clauses requises à l'article 28.3 du RGPD, à savoir des clauses portant sur :

a) les instructions de traitement, notamment concernant les transferts de données hors de l'Union européenne (critère C1.05);

b) l'engagement de confidentialité des personnes autorisées à traiter les données ou l'obligation légale de confidentialité (critère C3.08);

c) la sécurité du traitement (critère C1.07);

d) l'autorisation de recourir à des sous-traitants ultérieurs (critère C1.06);

e) l'assistance de son client afin d'aider le responsable de traitement dans le cadre de l'exercice des droits des personnes (chapitre III du RGPD –critère C1.09);

f) l'assistance de son client afin d'aider le responsable de traitement dans le cadre de la sécurité des données (article 32-34 du RGPD – critères C1.10 et C1.11), l'analyse d'impact relative à la protection des données et la consultation préalable de l'autorité de contrôle (article 35- 36 du RGPD –critère C1.12);

g) le sort des données au terme du contrat, à savoir leur suppression ou renvoi (critère C4.01);

h) l'audit (critère C1.13) et à la mise à disposition de son client de la documentation nécessaire pour démontrer le respect de ses obligations vis-à-vis du RGPD (critère C1.14).

Le Sous-traitant doit mettre à la disposition de son client toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les clauses a) à h) (critère C1.14).

C1.05 – Transparence sur l'existence de transferts de données hors Union européenne

Le contrat qui lie le Sous-traitant à son client doit prévoir une clause portant sur les instructions de traitement concernant les transferts de données à caractère personnel hors de l'Union européenne (critère C1.04a).

Lors de la phase précontractuelle, le Sous-traitant doit informer son prospect si les traitements à effectuer pour son compte impliquent ou sont susceptibles d'impliquer la mise en place d'un transfert de données à caractère personnel hors de l'Union européenne, y compris lorsque ce transfert est requis pour satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'Etat à laquelle le Sous-traitant est soumis (critère C0.09).

Lorsqu'il communique sur une *offre de service*, le Sous-traitant doit informer ses prospects de l'existence d'un ou plusieurs transferts de données lorsque le choix de son offre implique qu'un transfert de données soit mis en place par lui-même ou par l'un des sous-traitants ultérieurs recrutés dans le cadre de la constitution de cette *offre de service*.

En particulier, l'information fournie aux prospects du Sous-traitant doit préciser si les traitements à effectuer pour leur compte impliquent la mise en œuvre d'un transfert hors de l'Union européenne par dérogation (critère C2.08).

Les critères C2.06 à C2.08 précisent les exigences qui sont à démontrer par le Sous-traitant dans le cadre de la certification pour la mise en place d'un transfert de données.

C1.06 – Transparence sur l'existence de sous-traitances ultérieures

Le contrat qui lie le Sous-traitant à son client doit prévoir une clause portant sur les instructions de traitement concernant l'autorisation de recourir à des sous-traitants ultérieurs (critère C1.04d).

Lors de la phase précontractuelle, le Sous-traitant doit informer son prospect si les traitements à effectuer pour son compte impliquent ou sont susceptibles d'impliquer la mise en place d'une sous-traitance ultérieure.

Pour cela, le Sous-traitant doit fournir à ses prospects la liste des prestataires (ou le type de ces prestataires) auxquels il confiera, ou est susceptible de confier, des traitements à caractère personnel à effectuer pour son compte.

Cette liste indique pour chaque sous-traitant ultérieur :

a) l'objet de la sous-traitance ultérieure : une description de la prestation confiée qui implique le traitement de données à caractère personnel ou de *l'offre de service* utilisée pour faire réaliser le traitement ;

b) la nature du traitement : le type de traitement à réaliser par le sous-traitant ultérieur ;

c) si cette sous-traitance ultérieure implique des transferts de données hors de l'Union européenne.

Lorsqu'il communique sur une *offre de service*, le Sous-traitant doit informer ses prospects de l'existence d'une sous-traitance ultérieure lorsque le choix de son offre implique qu'une sous-traitance soit mise en place par lui-même ou par l'un des sous-traitants ultérieurs recrutés dans le cadre de la constitution de cette *offre de service*.

Le critère C2.09 précise les exigences qui sont à démontrer par le Sous-traitant dans le cadre de la certification pour la mise en place d'une sous-traitance ultérieure.

C1.07 – Transparence sur les mesures de sécurité

Dans le contrat qui le lie avec son client (critère C1.04c), le Sous-traitant s'engage à mettre en œuvre des mesures techniques et organisationnelles permettant d'assurer la sécurité des données à caractère personnel.

Lors de la phase précontractuelle, le Sous-traitant doit informer son prospect des mesures générales de sécurité envisagées pour les traitements à effectuer pour son compte. Si des mesures de substitution aux mesures de sécurité exigées par le critère C2.11 sont prévues, il lui transmet également la déclaration d'applicabilité dont il dispose (critère C2.12).

Les mesures de sécurité doivent faire l'objet d'une description qui couvre les traitements de bout en bout, y compris :

a) la collecte des données auprès du client, des personnes concernées ou auprès d'autres entités indiquées par le client ;

b) l'enregistrement, l'organisation, l'adaptation, la modification, l'utilisation, l'extraction, le rapprochement ou tout autre procédé appliqué aux données ;

c) les opérations de conservation des données, y compris l'archivage intermédiaire ou les sauvegardes à des fins de restauration ;

d) la consultation ou la communication des données, par transmission ou diffusion ou toute autre forme de mise à disposition ;

e) la restitution des données au client ou la destruction de celles-ci.

Le Sous-traitant met également à la disposition de ses prospects la description synthétique du système d'information de sous-traitance (critère C0.07) et la cartographie des flux de données (critère C0.08).

Concernant les informations qui pourraient être exploitées dans le but de provoquer une violation de données à caractère personnel ou qui sont protégées au titre du secret des affaires, du secret de la défense nationale ou d'autres obligations de confidentialité, le Sous-traitant doit communiquer à ses prospects les conditions à remplir pour accéder aux informations nécessitant une protection spécifique.

C1.08 – Report des obligations aux sous-traitants ultérieurs

Dans le contrat qui le lie avec son client, le Sous-traitant doit s'engager à imposer aux sous-traitants ultérieurs des mesures techniques et organisationnelles garantissant les engagements contractuels pris avec son client en matière de protection des données à caractère personnel.

Le critère C2.10 précise les exigences qui sont à démontrer par le Sous-traitant dans le cadre de la certification pour l'encadrement de la sous-traitance ultérieure.

C1.09 – Engagement d'assistance à l'exercice des droits

Dans le contrat qui le lie avec son client (critère C1.04e), le Sous-traitant doit s'engager sur la disponibilité des moyens dont dispose son client pour le solliciter dans le cadre du traitement d'une demande d'exercice des droits des personnes concernées.

En particulier, il doit être convenu :

a) de la répartition des rôles entre les parties pour le traitement des demandes d'exercice des droits. Il doit notamment être défini si le client confie au Sous-traitant le soin de donner suite aux demandes que celui-ci reçoit de la part des personnes concernées ou bien si ces demandes sont à lui transmettre ;

b) des moyens techniques mis à la disposition du client pour que celui-ci puisse donner suite aux demandes qu'il reçoit de la part des personnes concernées ;

c) des conditions spécifiques à prendre en compte par le Sous-traitant lorsque son client lui confie le soin de donner suite aux demandes d'exercice des droits, par exemple les limitations qui peuvent s'appliquer à l'exercice des droits selon la base légale du traitement ;

d) les délais dans lesquels le Sous-traitant doit agir, par exemple pour répondre à une sollicitation de son client dans le cadre du traitement d'une demande d'exercice des droits ou pour transmettre à son client une demande qu'il reçoit.

Le critère C2.17 précise les exigences qui sont à démontrer par le Sous-traitant dans le cadre de la certification concernant les moyens relatifs à l'exercice des droits.

C1.10 – Engagement d'assistance à la sécurité des données

Dans le contrat qui le lie avec son client (critère C1.04f), le Sous-traitant doit s'engager à aider son client à respecter les mesures techniques et organisationnelles de sécurité qu'il met en œuvre, notamment lorsque celui-ci doit agir selon les conditions d'utilisation de son service pour garantir leur efficacité (ex : collecte des données auprès du client).

C1.11 – Engagement d'assistance à la notification des violations de données

Dans le contrat qui le lie avec son client (critère C1.04f), le Sous-traitant doit s'engager à aider son client en cas de violation de données à caractère personnel en rapport avec les données qu'il traite pour le compte d'un responsable de traitement.

En particulier, le Sous-traitant informe son client qu'il dispose d'une procédure de détection, d'analyse et de résolution des incidents de sécurité (critère C2.16) et qu'il peut mobiliser cette procédure pour rechercher un incident de sécurité en lien avec la violation de données rapportée.

C1.12 – Engagement d'assistance à l'analyse d'impact

Dans le contrat qui le lie avec son client (critère C1.04f), le Sous-traitant doit s'engager à aider son client, selon des modalités prévues par contrat, lorsque celui-ci réalise une analyse d'impact relative à la protection des données (AIPD) en tant que responsable de traitement ou y contribue en tant que sous-traitant.

En particulier, le Sous-traitant informe son client qu'il tient à sa disposition la documentation relative au caractère approprié du niveau de sécurité du traitement qu'il effectue pour son compte (critère C2.13).

C1.13 – Engagement de permettre la réalisation d'audits

Dans le contrat qui le lie avec son client (critère C1.04h), le Sous-traitant doit s'engager à :

a) autoriser son client à demander la réalisation d'audits, de manière régulière et à intervalles raisonnables ;

b) autoriser son client à demander la réalisation d'audits de manière inopinée en présence d'indices de non-conformité ;

c) collaborer à ces audits.

Le Sous-traitant informe son client qu'il peut tenir compte de la certification obtenue selon les critères du présent référentiel lorsque celui-ci décide d'un examen ou d'un audit.

Le Sous-traitant ne doit pas imposer contractuellement à son client que l'audit soit effectué par un auditeur qu'il choisit ou mandate de manière unilatérale.

C1.14 – Documentation de la conformité

Dans le contrat qui le lie avec son client (critère C1.04h), le Sous-traitant doit s'engager à mettre à la disposition de son client toutes les informations nécessaires pour qu'il démontre le respect de ses engagements et obligations en matière de protection des données à caractère personnel. Ces informations incluent la documentation requise par le présent référentiel.

Note : lorsque le Sous-traitant transmet à son client la documentation de certification officielle (certificat) ou d'autres documents relatifs à la certification obtenue selon les critères du présent référentiel (par exemple, une synthèse du rapport d'audit), il transmet ces documents en totalité conformément à ses engagements pris avec l'organisme de certification.

Note : Concernant les informations nécessitant une protection spécifique, le Sous-traitant communique à ses clients (et ses prospects) les conditions à remplir pour qu'ils puissent y avoir accès. Cette protection concerne notamment la documentation de la description de mesures organisationnelles ou techniques qui pourrait être exploitée dans le but de provoquer une violation de la sécurité des données ou qui est protégée au titre du secret des affaires, du secret de la défense nationale ou d'autres obligations de confidentialité.

C1.15 – Procédure de recueil des instructions du responsable de traitement

Le Sous-traitant doit mettre en œuvre une procédure relative au recueil des instructions du responsable de traitement qui prévoit, avant de démarrer les traitements recensés au critère C0.03 puis au cours du traitement, qu'il :

a) dispose d'instructions pour le traitement de données à caractère personnel et les conserve sous une forme écrite et datée ;

b) informe son client s'il est tenu de procéder à un traitement de données à caractère personnel dans le cadre de sa prestation ou de son *offre de service* en raison d'une obligation légale lui incombant en application du droit de l'Union ou du droit de l'État membre auquel il est soumis;

c) renseigne son client sur la manière dont il traitera ses demandes portant sur de nouvelles instructions données pendant la durée du traitement ;

d) informe son client que pour chaque nouvelle instruction :

- il évaluera si son instruction est susceptible de constituer une violation du RGPD ou d'autres dispositions législatives ou réglementaires en matière de protection des données (issues du droit européen ou national au critère C0.09) ;

- il l'informera lorsqu'il aboutit à la conclusion que les instructions de son client ne sont pas conformes au RGPD au regard des éléments dont il dispose ;

- il lui demandera de compléter ses instructions ou de les modifier afin de résoudre les non-conformités identifiées par son évaluation ;

e) indique à son client par quel moyen et dans quels délais il l'informera de toute évolution envisagée ou constatée en cours de traitement (critère C3.03) et si ces changements ont des conséquences sur la mise en œuvre des instructions ou impliqueraient une adaptation des instructions.

C.1.15bis – Cas d'une offre de service

Dans le cas où le Sous-traitant propose une *offre de service* à ses clients, la procédure relative aux instructions du responsable de traitement (critère C1.15) doit également préciser qu'il :

a) répond aux questions de son client concernant la description de son *offre de service* (critère C1.02).

En particulier, le Sous-traitant doit renseigner son client sur les conditions d'utilisation de son *offre de service* concernant :

- les catégories de personnes prises en compte ;

- les catégories de données prises en charge ;

- la nature des traitements pris en charge ;

- la (les) finalité(s) de traitement envisagé(es) ;

- les transferts de données hors de l'Union européenne (critère C1.05) ;

- des traitements confiés à des sous-traitants ultérieurs (critère C1.06) ;

- des mesures de sécurité (critère C1.07) ;

b) permet à son client d'exprimer son besoin en matière de protection de données à caractère personnel, notamment ses demandes portant sur la configuration ou le paramétrage de *l'offre de service* ;

c) aide son client à documenter ses instructions pour que celles-ci incluent la configuration ou le paramétrage de *l'offre de service* retenue ;

d) le cas échant, identifie les demandes qui ne correspondent pas aux conditions de *l'offre de service* proposée.

Dans ce cas, le Sous-traitant doit :

- aider son client à documenter ses instructions pour que celles-ci incluent les instructions complémentaires qui sont nécessaires pour répondre à son besoin, lorsqu'elles peuvent être prises en charge dans le cadre d'une *offre de service* adaptée ; ou

- faire preuve de transparence envers son client sur les besoins qui ne pourront pas être pris en charge dans le cadre de son *offre de service*.

C1.16 – Traitements mis en œuvre en qualité de responsable de traitement

Dans le cas où le Sous-traitant prévoit de traiter des données, pour son propre compte en qualité de responsable de traitement, dans le cadre de la prestation de service qu'il réalise pour son client (traitements identifiés au critère C0.05), il doit s'assurer que :

a) dans le cas d'un traitement dit « ultérieur », il dispose d'une autorisation écrite et spécifique du responsable de traitement dans laquelle celui-ci précise qu'un test de compatibilité a été réalisé et qu'il conclut à la compatibilité du traitement ultérieur conformément à l'article 6.4 du RGPD ;

b) dans le cas d'une obligation légale incombant au Sous-traitant en application du droit de l'Union ou du droit de l'État membre auquel il est soumis et/ou d'une conservation de données en raison d'un intérêt administratif, le Sous-traitant informe son client de ce traitement conformément au critère C1.15b et des données à caractère personnel qui sont concernées.

Par exception au critère C1.16 b), le sous-traitant ne doit pas informer son client du traitement qu'il est tenu de mettre œuvre en application du droit de l'Union ou du droit de l'État membre auquel il est soumis, si la loi le lui interdit pour des motifs importants d'intérêt public.

C1.17 – Cas de la suspension des traitements

Le Sous-traitant doit informer son client que celui-ci peut donner instruction de suspendre le traitement des données à caractère personnel dans les circonstances suivantes :

a) le Sous-traitant a fait l'objet d'une décision de suspension ou de retrait d'une certification délivrée en application de l'article 42 et 43 du RGPD selon les critères du présent référentiel ; et

b) l'objet de cette certification retirée ou suspendue inclut des traitements effectués pour le compte de son client.

Le Sous-traitant informe sans délai son client lorsqu'une telle décision de suspension ou de retrait de certification lui est notifiée.

Le Sous-traitant informe également son client lorsqu'il décide de résilier une certification délivrée en application de l'article 42 et 43 du RGPD selon les critères du présent référentiel (en cours de validité) ou s'il décide de ne pas la renouveler, lorsque l'objet de cette certification inclut les traitements effectués pour le compte de son client.

Partie 2. L'environnement de la sous-traitance – la préparation du traitement

C2.01 – Informations relatives aux traitements réalisés en sous-traitance

Pour chaque traitement que le Sous-traitant effectue pour le compte d'un ou plusieurs clients (traitements identifiés au critère C0.03), il doit disposer les informations suivantes :

a) nom et description des traitements mis en œuvre (nature du traitement) ;

b) date de démarrage du traitement ;

c) date de dernière mise à jour des informations relatives au traitement ;

d) date de fin du traitement ;

e) nom/coordonnées de chaque client et coordonnées d'un point de contact (ex : courriel du délégué à la protection des données) ;

f) identification des données sensibles ou hautement personnelles ;

g) identification des sous-traitants ultérieurs : nom/coordonnées des sous-traitants ultérieurs et description des traitements (nature du traitement) ;

h) identification des transferts de données hors de l'Union européenne : nom du pays tiers de destination des données, nom/coordonnées de l'entité juridique importatrice des données, type de garantie pour la mise en place du transfert (critère C2.07) ou dérogation qui s'applique (critère C2.08).

Le Sous-traitant doit disposer de ces informations au démarrage du traitement (critère C3.01). Il doit les actualiser à l'occasion des évolutions appliquées aux traitements (critère C3.03) et à la fin du traitement (critère C4.06).

Lorsque des traitements similaires sont réalisés pour le compte d'un nombre important de clients dans le cadre d'une *offre de service*, le Sous-traitant dispose de moyens permettant d'accéder aux noms et coordonnées de chaque client.

Lorsque *l'offre de service* proposée par le Sous-traitant présente plusieurs configurations (ex : options ou variantes d'une offre commune), le Sous-traitant dispose de moyens permettant d'accéder aux noms et coordonnées des clients pour chacune de ces configurations.

C2.02 – Registre des traitements

Le Sous-traitant doit être en capacité d'extraire les informations requises par le critère C2.01 et de les inclure dans un document (registre) comprenant également les informations suivantes :

a) nom/coordonnées de son entité juridique ;

b) nom/coordonnées du représentant de son entité juridique ;

c) nom/coordonnées de son délégué à la protection de données.

Les informations requises au e) du critère C2.01 (nom/coordonnées de chaque client) n'ont pas à être extraites en totalité pour les inclure dans ce document (registre). A la place, une catégorie de clients ou *l'offre de service* commune à plusieurs clients peut y être indiquée, dès lors que cette indication permet d'accéder, par d'autres moyens, aux noms et coordonnées de tous les clients concernés.

C2.03 – Désignation du délégué à la protection des données

Le Sous-traitant doit désigner un délégué à la protection des données auprès de la CNIL ou d'une autre autorité de protection des données.

Dans le cadre de ses fonctions et missions (critère C2.04), le délégué à la protection des données accompagne et conseille le Sous-traitant sur la conformité des traitements recensés au critère C0.03.

Le Sous-traitant doit publier les coordonnées permettant de prendre directement contact avec le délégué à la protection des données.

Le Sous-traitant doit informer l'ensemble de son personnel de la désignation de son délégué à la protection des données et de son rôle au sein de l'organisme (ses missions). Il en informe également les organes décisionnaires de l'organisme et les instances représentatives du personnel (lorsqu'elles existent).

C2.04 – Fonction et missions du délégué à la protection des données

Le Sous-traitant doit s'assurer du respect de ses obligations relatives à la fonction du délégué à la protection des données et à ses missions, telles que définies aux articles 38 et 39 du RGPD, notamment :

a) en définissant l'ensemble des missions dont le délégué est chargé, y compris en matière d'information, de conseil et de contrôle ;

b) en sollicitant ses conseils en amont de la mise en œuvre des traitements, pour leur modification ou pour l'actualisation des informations qui y sont associées (critère C3.05);

c) en lui fournissant les moyens nécessaires à la réalisation de ses missions (ex : ressources et moyens d'accès) et en prenant en considération les actions correctives et évolutives que le délégué propose ;

d) en s'assurant que le délégué dispose de compétences (connaissance et/ou expérience) en matière de protection des données et en lui permettant d'entretenir ses connaissances spécialisées.

Lorsque le Sous-traitant définit les missions de son délégué à la protection des données, il ne doit :

- ni fournir d'instruction pour l'exercice de ses missions ;

- ni lui confier d'autres missions susceptibles de constituer un lien d'intérêt pouvant mettre en cause son impartialité ou son indépendance dans l'exercice de ses missions de délégué à la protection des données.

C2.05 – Désignation d'un référent certification

Le Sous-traitant désigne une personne chargée de veiller au respect des critères du présent référentiel (« référent certification » à la protection des données à caractère personnel). En particulier, celui-ci est chargé de veiller à ce que le Sous-traitant mène les actions requises par le présent référentiel.

Le délégué à la protection des données à caractère personnel peut se voir attribuer le rôle de « référent certification » pour les actions qui n'entraînent pas de conflit d'intérêts avec ses missions.

C2.06 – Encadrement des transferts de données hors de l'Union européenne

Conformément à ses engagements contractuels en matière de transferts de données à caractère personnel hors de l'Union européenne (critère C1.05), le Sous-traitant doit justifier pour chaque transfert qu'il met en œuvre en qualité d'exportateur des données que :

a) le pays tiers d'établissement de l'importateur des données (ex : un sous-traitant ultérieur établi hors de l'Union européenne) bénéficie d'une décision d'adéquation de la Commission européenne, telle prévue à l'article 45 du RGPD ; ou

b) il met en œuvre l'un des outils de transfert parmi ceux prévus à l'article 46 du RGPD (critère C2.07).

Pour certains pays, la décision d'adéquation de la Commission européenne peut prévoir certaines limitations du champ de son application. Si c'est le cas, le sous-traitant doit s'assurer que :

- l'importateur a réalisé les formalités nécessaires dans le pays où il est établi (ex : aux États-Unis, l'importateur figure dans la liste du Département du Commerce étatsunien - EU-US Data Privacy Framework) ;

- les traitements recensés au critère C0.03 sont couverts par les secteurs déterminés par la décision d'adéquation du pays tiers où l'importateur est établi (ex : au Canada, l'importateur est une organisation du secteur privé qui effectue le traitement dans le cadre d'une activité commerciale).

A défaut, il répond aux conditions spécifiques des dérogations prévues à l'article 49 du RGPD (critère C2.08).

C2.07 – Outils de transfert de données hors de l'Union européenne

Afin de justifier de garanties appropriées pour l'encadrement de chaque transfert hors de l'Union européenne (critère C2.06b), le Sous-traitant doit mettre en œuvre l'un des outils suivants :

a) la signature par le Sous-traitant (exportateur) de clauses types de protection des données adoptées par la Commission européenne avec l'importateur établi hors de l'Union européenne ;

b) l'adhésion à des règles d'entreprise contraignantes (BCR), approuvées au titre de l'article 47 du RGPD, et auxquelles le Sous-traitant (exportateur) et l'importateur établi hors de l'Union européenne sont adhérents, pour un périmètre d'application qui concerne les traitements recensés au critère C0.03 ;

c) la signature par le Sous-traitant (exportateur) de clauses types de protection des données, adoptées par la CNIL ou une autre autorité de contrôle, avec l'importateur établi hors de l'Union européenne ;

d) l'adhésion à un code de conduite, approuvé au titre de l'article 40.3 du RGPD, par l'importateur établi hors de l'Union européenne pour un périmètre d'application qui concerne les traitements recensés au critère C0.03 ;

e) l'adhésion à un mécanisme de certification, approuvé au titre de l'article 42.2 du RGPD, par l'importateur établi dans un pays tiers et pour lequel l'importateur dispose d'un certificat en cours de validité pour un périmètre d'application qui concerne les traitements recensés au critère C0.03 ;

f) un arrangement administratif ou un texte juridiquement contraignant et exécutoire est pris pour permettre la coopération entre le Sous-traitant (exportateur) et une autorité publique (Mémorandum of Understanding dit MOU ou MMOU, convention internationale, etc.).

Pour la mise en œuvre de l'outil de transfert, le Sous-traitant doit :

- identifier si la législation et les pratiques en vigueur dans le pays de destination des données sont susceptibles de porter atteinte à l'efficacité des garanties apportées via l'outil de transfert utilisé ;

- si c'est le cas, identifier et documenter les mesures supplémentaires (techniques, contractuelles et organisationnelles) qui permettent d'assurer un niveau de protection des données essentiellement équivalent à celui conféré au sein de l'EEE[1].

C2.08 – Cas des transferts de données hors Union européenne par dérogation

En l'absence de décision d'adéquation (critère C2.06) et lorsque le Sous-traitant n'est pas en mesure d'utiliser un outil de transfert de données hors de l'Union européenne (critère C2.07), il doit :

a) s'abstenir de procéder à la mise en œuvre d'un transfert de données hors de l'Union européenne ; ou

b) justifier de la mise en œuvre d'un transfert de données par dérogation à condition :

- de respecter de l'ensemble des conditions du recours aux dérogations prévues à l'article 49.1 du RGPD[2] ;

- de documenter les raisons ne lui permettant pas d'utiliser un outil de transfert de données pour la mise en œuvre du transfert.

[1] Selon les recommandations 01/2020 du CEPD
[2] Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679

C2.09 – Procédure de recours à des sous-traitants ultérieurs

Conformément à ses engagements contractuels pour la mise en place d'une sous-traitance ultérieure (critère C1.06), le Sous-traitant doit fournir à son client la liste des sous-traitants ultérieurs afin d'obtenir son autorisation.

Le Sous-traitant doit mettre en œuvre une procédure relative à la sous-traitance ultérieure pour :

a) avant la signature du contrat :

- informer ses prospects de la liste des prestataires ou du type de ces prestataires auxquels le Sous-traitant confiera des traitements et leur transmettre les informations visées au critère C1.06 ;

- répondre aux demandes d'information de ses prospects portant sur les mesures techniques et organisationnelles visant à la protection des données à caractère personnel dans le cadre de chaque sous-traitance ultérieure ;

b) après la signature du contrat :

- soumettre à ses clients une demande d'autorisation spécifique avant le recrutement d'un sous-traitant ultérieur lorsque celui-ci ne figure pas déjà dans la liste des prestataires fournie lors de la signature du contrat (option d'une autorisation spécifique préalable) ; ou

- lorsque le Sous-traitant dispose de l'autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs, informer spécifiquement ses clients avant le recrutement d'un sous-traitant ultérieur qui s'ajouterait à liste des prestataires fournie lors de la signature du contrat ou qui viendrait se substituer partiellement ou totalement à un prestataire de cette liste (option d'une autorisation écrite générale).

Lorsque le Sous-traitant recrute un sous-traitant ultérieur après la signature du contrat, il transmet à son client les informations visées au critère C1.06 et l'informe de la date à laquelle le recrutement est envisagé. Le Sous-traitant doit soumettre sa demande d'autorisation (option d'une autorisation spécifique préalable) ou informer son client (option d'une autorisation écrite générale) au moins 1 mois avant cette date.

La procédure relative à la sous-traitance ultérieure doit permettre au client du Sous-traitant de prendre une décision au sujet de l'autorisation demandée (option d'une autorisation spécifique préalable) ou lui permettre d'exercer son droit d'opposition (option d'une autorisation écrite générale). Si toutes les informations nécessaires à sa prise de décision n'ont pas été transmises initialement et sont dûment réclamées par le client, le délai d'information de 1 mois démarre à compter de la date du dernier envoi d'information dans le cadre du respect du présent référentiel.

Le Sous-traitant doit informer son client des conséquences en cas d'objection au recrutement d'un sous-traitant ultérieur en cours de sous-traitance.

C2.10 – Encadrement de la sous-traitance ultérieure

Lorsque le Sous-traitant recrute un sous-traitant ultérieur, il doit :

a) s'assurer que le recrutement du sous-traitant ultérieur est conforme aux instructions du responsable de traitement et aux engagements contractuels pris avec son client, notamment concernant la transparence sur l'existence de sous-traitances ultérieures (critère C1.06), les transferts de données hors de l'Union européenne (critères C1.05 et C2.06) et la description des mesures de sécurité (critère C2.11) ;

b) appliquer la procédure relative aux nouvelles instructions du responsable de traitement (critère C1.15), lorsque le recrutement implique une évolution des moyens essentiels du traitement ;

c) établir un contrat avec le sous-traitant ultérieur qui inclut les clauses listées au critère C1.04 ;

d) mettre à jour les informations relatives aux traitements (critère C2.01) et la liste des sous-traitants ultérieurs (critère C2.09).

C2.11 – Description des mesures de sécurité

Le Sous-traitant doit documenter une description des mesures techniques et organisationnelles de sécurité qu'il met en œuvre pour effectuer les traitements pour le compte de ses clients.

A minima, la description des mesures de sécurité doit inclure :

a) les mesures de gestion des clés cryptographiques (critère C32.01) ;

b) les mesures de chiffrement au repos et en transit des flux de données (critères C32.02 et C32.03) ;

c) les mesures de filtrage des flux de données (critère C32.04) ;

d) les mesures de gestion des habilitations des utilisateurs et des permissions d'accès (critères C32.05 et C32.06) ;

e) les mesures de contrôle des accès physiques (critère C32.07)

f) les mesures d'authentification des utilisateurs, de complexité et de protection des facteurs d'authentification et de gestion des mots de passe (critères C32.08 à C32.11) ;

g) les mesures relatives à l'authentification multifacteur et à l'accès à distance au système d'information (critères C32.12 et C32.13) ;

h) les mesures relatives à l'authentification machine à machine, et au contrôle d'accès des serveurs, postes de travail et équipements mobiles (critères C32.14 et C32.15) ;

i) les mesures de journalisation (critère C32.16)

j) les mesures de sauvegarde et d'archivage des données (critères C32.17 et C32.18) ;

k) les mesures de reprise d'activité (critère C32.19) ;

l) les mesures relatives à l'anonymisation de données (critère C32.20) ;

m) les mesures relatives à l'exportation des données (critère C32.21) ;

n) les mesures de gestion des postes de travail, des équipements mobiles et des supports amovibles (critère C32.22)

o) les mesures de mise au rebut et réaffectation du matériel (critère C32.23) ;

p) les mesures relatives aux mises à jour de sécurité des serveurs, postes de travail et équipements mobiles (critère C32.24) ;

q) les mesures relatives à la charte de confidentialité (critère C32.25).

En complément des mesures de sécurité exigées aux critères C2.11 a) jusqu'à q), la description des mesures techniques et organisationnelles de sécurité doit également inclure :

- les mesures de sécurité nécessaires du fait d'obligations qui s'imposent au Sous-traitant pour les traitements recensés au critère C0.03 quand elles découlent d'autres dispositions législatives et réglementaires que le RGPD (critère C0.09) ;

- les mesures de sécurité correspondant aux moyens essentiels du traitement que le responsable de traitement indique par ses instructions (critère C1.15) ou par le choix d'une configuration ou d'un paramétrage de *l'offre de service* (critère C1.15bis) ;

- les mesures de sécurité qui ont été déterminées en tant que mesures supplémentaires nécessaires pour la mise en œuvre d'un transfert de données hors de l'Union européenne (critère C2.07).

- les mesures de sécurité qui ont été déterminées en tenant compte des risques spécifiques que présente le traitement (critère C2.13) ;

- les mesures de sécurité relatives à la suppression définitive des données (critère C4.04).

C2.12 – Déclaration d'applicabilité des mesures de sécurité

Pour les mesures de sécurité exigées aux critères C2.11 a) jusqu'à q), le Sous-traitant peut justifier ne pas appliquer une ou plusieurs de ces mesures. Dans ce cas, le Sous-traitant dispose d'une déclaration d'applicabilité qui, pour chaque mesure non-appliquée (ou appliquée partiellement) :

a) identifie les mesures prévues aux critères C2.11 a) jusqu'à q) qui ne sont appliquées dans le contexte des traitements recensés au critère C0.03 ;

b) fournit les raisons conduisant le Sous-traitant à ne pas appliquer totalement ces mesures, comme par exemple pour le critère C2.11 f), lorsque le maintien de la mise en œuvre du traitement requiert l'utilisation d'un équipement spécifique qui ne permet pas de conditionner l'accès à son interface de gestion à une authentification des utilisateurs ;

c) décrit les mesures de substitution que le Sous-traitant met en œuvre en remplacement partiel ou total d'une mesure prévue aux critères C2.11 a) jusqu'à q), comme par exemple pour le critère C2.11 f), l'installation dans une salle dont l'accès physique requiert une authentification par badge d'un équipement dont l'interface de gestion ne permet pas l'authentification des utilisateurs ;

d) fournit l'échéance à laquelle le Sous-traitant envisage de mettre en œuvre la mesure de sécurité exigée par les critères C2.11 a) jusqu'à q) ou bien indique que les mesures de substitution sont permanentes.

Conformément au critère C2.13, le Sous-traitant justifie, par les risques, le caractère approprié des mesures de substitution qu'il définit en remplacement partiel ou total de chaque mesure de sécurité exigée aux critères C2.11 a) jusqu'à q).

Dans cette déclaration d'applicabilité, le Sous-traitant peut également préciser certaines mesures d'amélioration de la sécurité qu'il prévoit de mettre en œuvre en fournissant l'échéance à laquelle ces mesures seront effectives (critère C5.03)

C2.13 – Caractère approprié du niveau de sécurité

Dans le cas où le Sous-traitant propose une *offre de service* à ses clients, il est susceptible de tenir à leur disposition :

a) des éléments d'analyse de risques justifiant de la mise en œuvre de mesures techniques et organisationnelles d'un niveau de sécurité approprié pour les traitements qu'il propose d'effectuer pour le compte de ses clients (ex : analyse de risque EBIOS Risk Manager ou ISO/IEC 27005:2022) ;

b) des éléments d'analyse d'impact relative à la protection des données (ex : modèle d'AIPD prérempli).

Si le Sous-traitant met à la disposition de ses clients de tels éléments d'analyse, il doit s'assurer du respect des conditions requises par les critères suivants :

- le critère C2.14, s'agissant d'éléments d'analyse des risques de sécurité pour les traitements des données ;

- le critère C2.15, s'agissant d'éléments d'analyse d'impact relative à la protection des données.

Sinon, le Sous-traitant doit :

- définir une liste d'événements redoutés, qui portent atteinte à la confidentialité, l'intégrité ou la disponibilité des données à caractère personnel qui font l'objet d'un traitement recensé au critère C0.03, en lien avec les facteurs de risque identifiés au critère C0.06 ;

- identifier les mesures spécifiques de limitation (ex : mesures interdisant l'impression de certains documents) et les mesures de sécurité supplémentaires à celles exigées aux critères C2.11 a) jusqu'à q) (ex : impressions sécurisées par code PIN ou badge) qui permettent atténuer la vraisemblance des risques identifiés, notamment lorsque le traitement porte sur des données sensibles ;

- en cas de mise en œuvre de mesures de substitution (critère C2.12), justifier par une analyse de risque partielle, limitée à des événements redoutés portant uniquement sur les moyens de traitement concernés, que ces mesures de substitution présentent un risque résiduel comparable dans le contexte de la mise en œuvre des traitements recensés au critère C0.03.

C2.14 – Analyse des risques de sécurité pour le traitement des données

Lorsque le Sous-traitant met à la disposition de ses clients des éléments analyse des risques de sécurité pour le traitement des données (critère C2.13a), il doit :

a) définir une liste d'événements redoutés, qui portent atteinte à la confidentialité, d'intégrité ou de disponibilité des données à caractère personnel qui font l'objet d'un traitement recensé au critère C0.03, en lien avec les facteurs de risque identifiés au critère C0.06 ;

b) pour chaque événement redouté, déterminer *a minima* :

- une source de risque (humaine ou non-humaine) qui pourrait en être à l'origine ; et

- les menaces qui rendent l'événement redouté possible ;

c) justifier de l'application d'une méthode pour apprécier :

- la probabilité qu'un événement redouté survienne (vraisemblance d'une atteinte à la confidentialité, à l'intégrité ou à la disponibilité de données à caractère personnel) ;

- la gravité des conséquences si l'événement redouté survenait, notamment pour les personnes concernées (impact potentiel sur les droits et libertés des personnes) ;

d) identifier les mesures de sécurité (techniques et organisationnelles) permettant d'atténuer la vraisemblance des risques identifiés (et leur gravité lorsque cela est possible et dans la mesure où le Sous-traitant dispose d'informations suffisantes sur la nature, la portée, le contexte et les finalités du traitement mis en œuvre par le responsable de traitement) ;

e) conclure à un risque résiduel qui résulte de la mise en œuvre de tout ou partie des mesures de sécurité identifiées, en indiquant :

- les mesures de sécurité mises en œuvre par le Sous-traitant dès le démarrage des traitements, y compris lorsqu'elles impliquent des sous-traitants ultérieurs (voir critère C2.11) ;

- les mesures de sécurité planifiées par le Sous-traitant et qu'il s'engage à mettre en œuvre à une échéance prévisionnelle (voir critère C5.01) ;

- les mesures de sécurité qui nécessitent une mise en œuvre par son client.

Le sous-traitant doit s'assurer que les éléments d'analyse des risques de sécurité mis à la disposition de ses clients mentionnent la date de réalisation de cette analyse (ou de sa dernière actualisation). Lorsqu'ils sont transmis à un client, ces éléments d'analyse ne doivent pas dater de plus de 2 ans.

C2.15 – Analyse d'impact relative à la protection des données

Lorsque le Sous-traitant met à la disposition de ses clients des éléments d'analyse d'impact relative à la protection des données (critère C2.13b), il doit :

a) identifier les hypothèses à faire confirmer par le client, compte-tenu de la nature, de la portée, du contexte et des finalités du traitement que le Sous-traitant peut méconnaître ;

b) identifier les informations qui sont à compléter par le client (ou à retenir si plusieurs options prédéterminées sont envisagées par le Sous-traitant) ;

c) justifier de mesures garantissant la proportionnalité et la nécessité du traitement en documentant les choix proposés par le Sous-traitant pour respecter les obligations suivantes :

- le(s) finalité(s) (cf. art. 5.1 (b) du RGPD)

- le fondement (cf. art. 6 du RGPD)

- la minimisation des données (cf. art. 5.1 (c) du RGPD)

- la qualité des données (cf. art. 5.1 (d) du RGPD)

- la durée de conservation (cf. art. 5.1 (e) du RGPD)

d) justifier de mesures protectrices des droits et libertés des personnes proposées par le Sous-traitant pour respecter les obligations suivantes :

- l'information des personnes concernées (cf. art. 12, 13 et 14 du RGPD) ;

- le recueil du consentement (cf. art. 7 et 8 du RGPD) ;

- le droit d'accès et à la portabilité (cf. art. 15 et 20 du RGPD) ;

- les droits de rectification et d'effacement (cf. art. 16 et 17 du RGPD) ;

- les droits de limitation du traitement et d'opposition (cf. art. 18 et 21 du RGPD) ;

- la sous-traitance (cf. art. 28 du RGPD) ;

- les transferts de données (cf. art. 44 à 49 du RGPD) ;

e) justifier de mesures de sécurité appropriées aux risques pour les personnes, à partir d'une analyse qui respecte les conditions requises par le critère C2.14 ;

f) conclure à un risque résiduel pour les personnes concernées par le traitement des données, uniquement si le Sous-traitant :

- dispose de la totalité des informations relatives à la nature, à la portée, au contexte et aux finalités du traitement ; ou

- est en capacité de déterminer les hypothèses qui conditionnent cette conclusion et qu'il informe son client qu'il lui appartient de confirmer ces hypothèses.

Le Sous-traitant doit s'assurer que les éléments d'analyse d'impact mis à la disposition de ses clients mentionnent la date de réalisation de cette analyse (ou de sa dernière actualisation). Lorsqu'ils sont transmis à un client, ces éléments d'analyse ne doivent pas dater de plus de 2 ans.

C2.16 – Procédure de détection, analyse et résolution des incidents de sécurité

Le Sous-traitant doit définir une procédure relative à la détection, l'analyse et la résolution des incidents de sécurité dans le but de prévenir ou amoindrir l'impact de toute violation de données à caractère personnel pour les traitements qu'il effectue pour le compte de ses clients.

Cette procédure doit permettre au Sous-traitant de :

a) détecter les incidents de sécurité au moyen de :

- signalements de la part de son personnel, de ses sous-traitants, de ses clients (demande d'assistance) et de ceux relayés par son délégué à la protection des données ;

- mécanismes automatisés de signalement d'événements suspects ou susceptibles de constituer un incident de sécurité (par exemple, au moyen de notifications applicatives générées à partir du contrôle des traces du système de journalisation - critère C32.16) ;

- la vérification du bon fonctionnement du système d'information de sous-traitance (par exemple, une revue périodique des traces du système de journalisation - critère C32.16) ;

b) analyser un incident de sécurité et qualifier sa nature, notamment en déterminant :

- s'il peut être confirmé ;

- sa source ;

- le périmètre du système d'information de sous-traitance concerné par l'incident (ou susceptible de l'être) ;

c) déterminer si un incident de sécurité est susceptible de porter atteinte à la confidentialité, l'intégrité ou la disponibilité de données à caractère personnel qui sont traitées pour le compte de ses clients et ainsi d'être qualifié comme une violation de données (critère C3.11) ;

d) prendre des mesures nécessaires de contingence afin d'endiguer la violation de données dès lors que l'analyse menée par le Sous-traitant au b) conclut que celle-ci est confirmée ;

En particulier, la procédure doit prévoir des mesures organisationnelles de gestion de crise. Cela inclut la mise en place du processus de décision permettant au Sous-traitant de mettre temporairement à l'arrêt les traitements effectués pour le compte de ses clients et de mettre en sécurité les données à caractère personnel (critère C32.19) ;

e) déterminer les mesures correctrices à mettre en œuvre compte-tenu des circonstances de l'incident de sécurité, de l'estimation de son impact et de sa récurrence.

C2.17 – Procédure relative à l'exercice des droits

Le Sous-traitant doit définir une procédure relative aux traitements des demandes d'exercice des droits qui lui permet de réaliser les opérations suivantes dans le cadre du traitement qu'il met en œuvre pour le compte de son client :

a) extraire les données à caractère personnel relatives à un individu (ex : demande d'accès) ;

b) modifier les données à caractère personnel relatives à un individu (ex : demande de rectification) ;

c) supprimer les données à caractère personnel relatives à un individu (ex : demande effacement) ;

d) arrêter le traitement pour un individu (ex : demande d'opposition) ;

e) modifier le traitement pour un individu (ex : demande de limitation).

À défaut de disposer d'une procédure lui permettant de réaliser ces opérations, le Sous-traitant doit :

- fournir une interface de gestion des demandes d'exercice des droits permettant à son client de réaliser lui-même ces opérations (critère C1.09b) ;

- informer son client dans le cadre des échanges sur les moyens techniques prévus au critère C1.09 quand il n'est pas en mesure de réaliser certaines de ces opérations compte tenu du contexte du traitement.

Partie 3. La réalisation de la sous-traitance – la mise en œuvre du traitement

C3.01 – Instructions du responsable de traitement

Au démarrage du traitement, le Sous-traitant doit disposer des instructions du responsable de traitement pour les traitements effectués pour le compte de son client. Pour cela, il doit mettre en œuvre la procédure relative aux instructions du responsable de traitement (critère C1.15).

Ces instructions doivent inclure :

a) la description des données nécessaires à la réalisation du traitement, que celles-ci soient collectées par le Sous-traitant pour le compte du responsable de traitement ou transmises par son client (critère C1.02) ;

b) la durée de conservation des données nécessaires à la réalisation du traitement, à l'issue de laquelle le Sous-traitant peut appliquer une purge sélective des données en base active ou un archivage en base intermédiaire (critères C32.18) ;

c) les catégories de destinataires qui pourront avoir accès aux données traitées par le Sous-traitant, notamment les différentes catégories de personnes qui seront habilités à accéder aux données au cours du traitement (critère C32.05) ;

d) les mesures de sécurité correspondant aux moyens essentiels du traitement, à l'exception des moyens non-essentiels comme par exemple des aspects organisationnels pour leur mise en œuvre, le choix d'un type particulier de matériel ou d'un logiciel pour la mise d'une mesure technique ou encore des mesures de sécurité opérationnelle dès lors qu'elles satisfont au niveau de sécurité déterminé par le responsable traitement (critère C2.11) ;

e) les conditions spécifiques aux demandes d'exercice des droits qui sont à prendre en compte par le Sous-traitant, lorsque le responsable de traitement lui confie le soin d'y donner suite, par exemple les limitations qui peuvent s'appliquer à l'exercice des droits selon la base légale du traitement (critère C1.09) ;

f) les instructions relatives au caractère concis, transparent, compréhensible et aisément accessible de l'information des personnes, lorsque le responsable de traitement lui confie le soin d'informer les personnes concernées par le traitement des données ;

g) les instructions relatives au caractère libre, spécifique, éclairé et univoque du consentement des personnes, lorsque le responsable de traitement lui confie de recueillir le consentement des personnes concernées par le traitement des données ;

h) les instructions relatives aux transferts de données en dehors de l'Union européenne (critère C1.05).

Le Sous-traitant doit informer son client des conditions que celui-ci doit respecter lors de sa prestation (ou les conditions d'usage de son service) et qui sont nécessaires afin de garantir l'effectivité des mesures de protection des données que le Sous-traitant met en œuvre conformément aux instructions du responsable de traitement.

En particulier, le Sous-traitant doit informer son client lorsque la mise en œuvre opérationnelle de certaines mesures de sécurité est sous sa responsabilité, par exemple, dans le cas où la gestion d'une partie des habilitations d'accès au système d'information de sous-traitance est réalisée par son client. Dans ce cas, le Sous-traitant doit lui fournir des ressources explicatives à son client afin de l'aider à la mise en œuvre de ces mesures de sécurité (critère C3.09bis).

C3.01bis – Cas d'une offre de service

Dans le cas où le Sous-traitant propose une *offre de service* à ses clients, les instructions du responsable de traitement (critère C3.01) doivent également inclure :

- la configuration ou le paramétrage de *l'offre de service* retenue par le client (critère C1.15bis c) ;

- les adaptations de *l'offre de service* qui ont été convenues entre le Sous-traitant et son client (critère C1.15bis d).

C3.02 – Mise en œuvre des mesures de protection des données

Dès le démarrage du traitement, le Sous-traitant doit mettre en œuvre les mesures de protection des données à caractère personnel conformément aux instructions du responsable de traitement (critère C3.01).

Il doit s'assurer du maintien de ces mesures *a minima* tous les ans.

Le Sous-traitant doit s'assurer que son personnel est informé des instructions du responsable de traitement en rapport avec les tâches qu'il exécute pour la mise en œuvre du traitement (critère C3.07).

En particulier, le personnel du Sous-traitant doit être informé que :

- les données ne peuvent être traitées sans instruction du responsable du traitement, à moins que ce traitement figure dans la liste des traitements mis en œuvre en qualité de responsable de traitement (critère C1.16) ;

- toute évolution envisagée pour le traitement nécessite une analyse des conséquences sur la mise en œuvre des instructions, et au besoin, ou de nouvelles instructions de la part du responsable de traitement (critère C3.03).

C3.03 – Evolutions en cours de traitement

Au cours du traitement, le Sous-traitant doit actualiser les mesures de protection des données à caractère personnel lorsqu'il est informé par son client d'une évolution des instructions du responsable de traitement (critère C1.15d).

Lorsque le Sous-traitant envisage une évolution des moyens du traitement ou lorsqu'il est informé par un sous-traitant ultérieur que celui-ci envisage une évolution des moyens du traitement, le Sous-traitant doit :

a) évaluer si cette évolution constituerait un changement des moyens essentiels du traitement qu'il effectue pour le compte du responsable de traitement (critère C3.01) ;

b) réévaluer les risques en prenant l'hypothèse de cette évolution (critère C2.13), si cette évolution constitue ou impliquerait une évolution des mesures de sécurité ;

c) appliquer le processus relatif à l'encadrement de la sous-traitance ultérieure (critères C2.10), si l'évolution envisagée impliquerait le recrutement d'un nouveau sous-traitant ultérieur ou le choix d'une *offre de service* différente ;

d) appliquer le processus relatif à l'encadrement des transferts de données hors de l'Union européenne (critère C2.07), si l'évolution envisagée impliquerait la mise en place d'un nouveau transfert hors l'Union européenne ou un transfert vers un autre pays ;

e) informer son client de l'évolution qu'il envisage dès lors que son évaluation conclut à une modification des moyens essentiels du traitement, de la sous-traitance ultérieure ou d'un transfert de données, conformément à la procédure relative aux instructions du responsable de traitement (critère C1.15) ;

f) fournir à son client les informations utiles à sa décision, en particulier la documentation actualisée dans l'hypothèse de cette évolution (critère C1.14).

Le Sous-traitant informe également son client de la date à laquelle il envisage d'appliquer ces évolutions (critère C1.15e).

Avant d'appliquer une modification des moyens essentiels du traitement, le Sous-traitant doit disposer des instructions mises à jour par le responsable de traitement dûment informé du projet.

C3.04 – Exercice des droits des personnes concernées par le traitement

Le Sous-traitant doit mettre en œuvre les moyens convenus avec son client afin d'aider le responsable de traitement à donner suite aux demandes d'exercice des droits (critère C1.09).

Selon les engagements pris par le Sous-traitant et les instructions du responsable de traitement relatives à l'exercice des droits (critères C1.09 et C3.01), le Sous-traitant doit :

a) s'assurer du fonctionnement de l'interface de gestion mise à la disposition de son client ou, à chaque demande de son client, mettre en œuvre la procédure relative aux opérations à réaliser sur les données à caractère personnel dans les délais convenus avec son client (critère C2.17) ;

b) à réception d'une demande d'exercice de droits de la part d'une personne concernée, transmettre cette demande à son client ou y donner suite lorsque le responsable de traitement lui confie le soin de donner suite aux demandes d'exercice de droits.

C3.05 – Association du délégué à la protection des données

Le Sous-traitant doit associer le délégué à la protection des données aux actions qu'il mène en matière de protection des données pour répondre aux critères du présent référentiel.

En particulier, le Sous-traitant doit solliciter les conseils de son délégué à la protection des données pour :

a) l'identification et l'évolution des informations relatives aux traitements, concernant le contrat de sous-traitance et le registre des traitements (critères C1.02 et C2.02) ;

b) l'identification et l'actualisation des risques applicables aux traitements (critère C2.13) ;

c) l'identification et l'actualisation de la réglementation applicable (critère C0.09) ;

d) la détermination et l'évolution des mesures de sécurité (critère C2.11) ;

e) l'encadrement des transferts de données hors de l'Union européenne (critère C2.06) ;

f) la définition et l'évolution des procédures relatives aux instructions (critère C1.15), à la sous-traitance ultérieure (C2.10), à la détection, l'analyse et la résolution des incidents de sécurité (critère C2.16), à l'exercice des droits (critère C2.17) ;

g) la sensibilisation et la formation du personnel (critères C3.06 et C3.07) ;

h) l'élaboration de ses plans d'action en matière de protection des données (critères C5.01 à C5.03).

C3.06 – Sensibilisation de l'ensemble du personnel à la protection des données

Le Sous-traitant doit disposer d'un programme de sensibilisation à la protection des données à caractère personnel pour son personnel qu'il identifie comme une source de risque humaine potentielle pour les traitements des données recensé au critère C0.03 (critère C2.13).

En particulier, ce programme de sensibilisation doit prévoir :

a) lors du recrutement du personnel, des sessions de sensibilisation, organisées au plus tard dans les 3 mois qui suivent le recrutement d'une personne ;

b) des sessions régulières de sensibilisation, organisées au moins une fois par an ;

c) un test destiné à évaluer la compréhension du contenu du programme de sensibilisation, organisé au moins une fois par an.

Le contenu du programme de sensibilisation doit couvrir *a minima* ;

- la notion d'instruction du responsable de traitement et les règles internes de gestion des données à caractère personnel auxquels le Sous-traitant est soumis lorsqu'il effectue un traitement pour le compte d'un responsable de traitement (critère C1.15). Par exemple, que faire si j'ai besoin d'accéder temporairement aux données à caractère personnel du traitement ?

- les règles de sécurité imposées par la charte informatique (critère C32.25). Par exemple, est-ce que la charte informatique m'autorise à brancher une clef USB sur mon poste de travail et, si oui, à quelles conditions ?

- la conduite à tenir et les personnes à contacter en cas de survenance d'un évènement inhabituel en lien avec le traitement des données ou en cas d'incident de sécurité (critère C2.16). Par exemple, que faire si je reçois un courriel sur ma boîte professionnelle m'invitant à renseigner en urgence des informations sur une plateforme en ligne en l'absence de mon collègue ?

- les droits des personnes et le rôle du Sous-traitant dans l'assistance du responsable de traitement pour donner suite aux demandes d'exercice de droits des personnes concernées (critère C2.17). Par exemple, que faire si une personne me sollicite pour exercer un droit d'accès concernant des données à caractère personnel ?

Les exigences relatives aux ressources pédagogiques utilisées dans le cadre du programme de sensibilisation du personnel sont définies au critère C3.09.

C3.07 – Formation du personnel impliqué dans le traitement

Le Sous-traitant doit disposer d'un programme de formation adapté au personnel qui intervient dans la mise en œuvre des traitements recensés au critère C0.03.

En particulier, ce programme de formation doit prévoir :

a) des sessions de formation aux mesures et aux procédures relatives aux traitements effectués pour le compte d'un responsable de traitement, organisées au plus tard dans le mois qui suit l'affectation d'une personne à une tâche en lien avec les traitements recensés au critère C0.03 ;

b) des sessions de formation sur l'actualisation et l'évolution des mesures et des procédures relatives aux traitements, organisées au moins une fois par an ;

c) un test destiné à évaluer l'application des mesures et procédures, organisé au moins une fois par an.

Le contenu du programme de formation doit couvrir *a minima* :

- les objectifs du référentiel général d'aptitudes et de compétences en Annexe 1 du référentiel de certification des prestataires de formation à la protection des données à caractère personnel, lorsque ces objectifs s'appliquent aux tâches à effectuer par le personnel[3] ;

- les procédures définies par le Sous-traitant relatives aux instructions (critère C1.15), à la sous-traitance ultérieure (C2.10), à la détection, l'analyse et la résolution des incidents de sécurité (critère C2.16), à l'exercice des droits (critère C2.17) ;

- les engagements pris en matière de protection des données au travers de l'engagement de confidentialité (critère C3.08) ;

- les risques identifiés et les mesures de sécurité déterminées par le Sous-traitant pour la mise en œuvre du traitement (critère C2.11 et C2.13).

Les exigences relatives aux ressources pédagogiques utilisées dans le cadre du programme de formation du personnel sont définies au critère C3.09.

[3] https://www.cnil.fr/fr/certification-des-prestataires-de-formation-la-protection-des-donnees-la-cnil-publie-un-referentiel

C3.08 – Engagement de confidentialité du personnel impliqué dans le traitement

Le Sous-traitant doit faire signer un engagement de confidentialité au personnel qui intervient dans la mise en œuvre des traitements recensés au critère C0.03 ou prévoir une clause de confidentialité spécifique concernant les données à caractère personnel dans les contrats de travail du personnel concerné (critère C1.04b).

En particulier, le personnel concerné doit s'engager à :

a) ne pas utiliser les données à caractère personnel à des fins autres que celles prévues par ses missions ;

b) ne divulguer ces données qu'à des personnes habilitées à les recevoir ;

c) ne faire aucune copie de ces données, sauf à ce que cela soit nécessaire à l'exécution de ses tâches ;

d) appliquer les mesures définies par le Sous-traitant afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;

e) appliquer les mesures définies par le Sous-traitant pour préserver la sécurité de ces données ;

f) en cas de cessation de ses fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

C3.09 – Ressources pédagogiques en matière de protection des données

Le Sous-traitant doit disposer de ressources pédagogiques, à destination de son personnel, relatives à la protection des données dans le contexte des traitements effectués pour le compte d'un responsable de traitement.

Ces ressources pédagogiques doivent :

a) être accessible à tout moment par l'ensemble du personnel ;

b) faire l'objet d'une diffusion régulière auprès du personnel, au travers d'actions de sensibilisation (critère C3.06), de l'organisation de sessions de formation (critère C3.07) et d'actions de communication au moins une fois par an ;

c) être actualisées régulièrement, pour prendre en compte les évolutions du traitement (critère C3.03) et la veille réalisée en matière de protection des données (critère C5.04), au moins une fois par an.

C3.09bis – Cas d'une offre de service

Dans le cas où le Sous-traitant propose une *offre de service* à ses clients, il doit :

a) disposer d'une documentation explicative des conditions relatives à la protection des données à respecter lors de l'utilisation de son service ;

b) fournir cette documentation explicative à ses clients, au plus tard au démarrage du traitement.

C3.10 – Registre des incidents de sécurité

Le Sous-traitant doit mettre en œuvre la procédure relative à la détection et la résolution des incidents de sécurité pour le système d'informations de sous-traitance (critère C2.16).

En particulier, il enregistre dans un registre les faits relatifs à chaque incident de sécurité ayant fait l'objet d'une qualification (critère C2.16c), y compris lorsque le Sous-traitant conclut que l'incident de sécurité n'a pas porté atteinte à la confidentialité, l'intégrité ou la disponibilité de données à caractère personnel, à savoir *a minima* :

a) la date à laquelle l'incident est intervenu ;

b) la date à laquelle le Sous-traitant en a eu connaissance ;

c) la date à laquelle l'incident a été endigué (si des mesures d'endiguement ont été prises) ;

d) la source de l'incident, y compris quand l'origine de l'incident est en dehors du périmètre du système d'information de sous-traitance ;

e) le périmètre du système d'information de sous-traitance concerné par l'incident ;

f) les éventuelles mesures correctrices qui ont été déterminées dans le cadre de la résolution de l'incident de sécurité (critère C2.16d et C2.16e).

C3.11 – Notification d'une violation de données constatée par le sous-traitant

Le Sous-traitant alerte ses clients de toute violation de données établie dans le cadre de la mise en œuvre de la procédure relative à la détection et la résolution des incidents de sécurité (critère C3.10).

Lors de la notification d'une violation de données à son client, le Sous-traitant lui fournit *a minima* les informations suivantes :

a) une description de la nature de la violation constatée, notamment :

- les catégories et le nombre approximatif de personnes concernées (lorsque les traitements qu'il effectue pour le compte de son client lui permettent d'avoir accès à ce type d'informations) ou le périmètre du système d'information concerné par l'incident (dans le mesure où cela permet à son client d'en déduire cette information) ;

- les catégories et le nombre approximatif d'enregistrements concernés ou le périmètre du système d'information concerné par l'incident;

b) les coordonnées d'un point de contact auprès duquel son client peut obtenir des informations supplémentaires au sujet de la violation de données ;

c) les conséquences probables de la violation de données, les mesures prises pour endiguer immédiatement la violation de données et les mesures déterminées pour remédier à la violation, y compris celles proposées pour atténuer les éventuelles conséquences négatives pour les personnes concernées par le traitement des données.

Si le Sous-traitant n'est pas en mesure de fournir toutes ces informations en même temps, il doit notifier à son client la violation de données dès qu'elle est établie en lui fournissant les informations disponibles à ce moment-là.

C3.12 – Réalisation d'audit technique

Le Sous-traitant doit faire réaliser un audit technique du système d'information de sous-traitance par un prestataire de service indépendant *a minima* tous les ans.

Lorsque le Sous-traitant détermine le périmètre de cet audit technique, il sélectionne les cibles prioritaires du système d'information de sous-traitance à évaluer, en fonction des risques supposés du traitement pour les personnes concernées, parmi :

- les moyens de traitement exposés sur internet, en particulier les moyens informatiques qui peuvent permettre l'accès aux données à caractère personnel ;

- les moyens informatiques que les utilisateurs habilités par le Sous-traitant sont autorisés à utiliser en dehors des locaux pour accéder aux données à caractère personnel ;

- les moyens de traitement internes, en particulier les moyens informatiques qui peuvent permettre l'accès aux données à caractère personnel.

Cet audit technique doit comporter un test d'intrusion afin de mettre à l'épreuve le système d'information de sous-traitance aux attaques à distance suivantes :

a) l'identification de service ou de flux réseau ouverts sur internet, notamment ceux qui ne correspondraient pas à des flux de données entrants/sortants recensés par la cartographie des flux (critère C0.08) ou qui devraient faire l'objet d'un filtrage (critère C32.04) ;

b) l'état d'application des mises à jour de sécurité (critère C32.24) ;

c) l'exploitation de vulnérabilités réseau, applicatives et système, dans la partie du système d'information de sous-traitance qui est exposée à internet ;

Lorsque le Sous-traitant a réalisé un test d'intrusion à distance dans l'année précédente et que ses conclusions n'ont révélé aucune vulnérabilité critique pour les moyens informatiques à risques du système d'information de sous-traitance, il ne renouvelle pas le même test et doit réaliser un autre type d'audit technique, tel que :

- un test d'intrusion à distance, en boîte grise ou blanche, avec tentative d'élévation de privilèges, de maintien d'accès ou de propagation latérale ;
- un test d'intrusion ciblant la partie interne du système d'information de la sous-traitance ;
- un test d'intrusion physique, impliquant l'intrusion d'une personne dans ses locaux ;
- un audit d'architecture ;
- un audit de code ;
- un audit de configuration.

Le Sous-traitant doit disposer d'un plan d'action pour la remédiation des vulnérabilités identifiées dans les conclusions du dernier rapport de l'audit technique (critère C5.01). Les dates de chaque action correctrice qui a été réalisée par le Sous-traitant pour résoudre les vulnérabilités critiques identifiées doivent y être documentées.

Note : Un audit technique reposant uniquement sur des logiciels entièrement automatisés de détection de vulnérabilités n'est pas considéré comme un audit technique répondant à ce critère.

Partie 4. La fin de la sous-traitance – l'arrêt du traitement

C4.01 – Choix du sort des données

Lorsque le contrat prend fin, le Sous-traitant doit disposer des instructions du responsable de traitement quant au sort des données. Pour cela, il doit mettre en œuvre la procédure relative au recueil des instructions du responsable de traitement (critère C1.15).

Ces instructions doivent déterminer si le Sous-traitant doit :

a) supprimer toutes les données à caractère personnel traitées pour le compte de son client ; ou

b) renvoyer toutes les données à caractère personnel à son client et détruire les copies existantes en sa possession.

C4.02 – Renvoi des données en fin de prestation

Pour le renvoi des données à caractère personnel à son client (critère C4.01b), le Sous-traitant met en œuvre des mesures garantissant la confidentialité des données, à savoir :

a) il s'assure de l'authenticité de l'instruction dont il dispose afin de prévenir le risque d'usurpation d'identité ;

b) il habilite les personnes désignées par son client comme destinataires de ces données ou fournit à son client les moyens techniques pour habiliter lui-même ces personnes (critère C32.05) ;

c) il applique un chiffrement aux données à renvoyer ou s'assure d'un chiffrement de bout en bout du flux des données transmises (critères C32.02) ;

d) lorsque le chiffrement appliqué nécessite le partage d'un secret avec son client pour que celui-ci puisse accéder aux données renvoyées (clef secrète ou certificat), il s'assure de la sécurité des moyens utilisés pour le partage de ce secret selon les conditions de sécurité prévues au critère C32.01 (Gestion des clés cryptographiques).

Si le Sous-traitant restitue les données à caractère personnel à son client en lui fournissant les moyens techniques de les obtenir de manière autonome, il informe son client des modalités d'accès aux données et du délai dont il dispose pour en faire une copie.

Les données doivent être restituées dans un format structuré accompagné de la documentation explicative du format de ces données. Lors de la restitution des données, le Sous-traitant applique les mesures de sécurité relatives à l'exportation des données à caractère personnel (critère C32.21).

C4.03 – Suppression des données en base active et archivage

Lorsque sa prestation prend fin et que le renvoi des données a été effectué selon les instructions de son client (critère C4.02), le Sous-traitant supprime toutes les données à caractère personnel relatives à sa prestation dans le système d'information de sous-traitance (base active).

Pour les données que le sous-traitant est tenu de conserver en raison d'une obligation légale lui incombant en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis (critère C0.05b), il applique les mesures sécurité prévues au critère C32.18.

C4.04 – Suppression définitive des données

Pour supprimer les données à caractère personnel lorsque sa prestation est terminée, le Sous-traitant met en œuvre des mesures de suppression définitive qui s'appliquent :

a) aux données en base active ;

b) aux sauvegardes réalisées pour la sécurité des traitements ;

c) aux archives intermédiaires ;

d) aux traces de journalisation.

Ces mesures de suppression définitive doivent inclure :

- un écrasement logique des données, par exemple au moyen d'une réécriture multiples par des données nulles ou aléatoires ; ou

- un mécanisme de chiffrement permettant de rendre les données inaccessibles, à condition que les clefs de chiffrement soient détruites.

Note : La suppression des liens vers les données visant à les rendre inaccessibles aux applications utilisées pour les traitements ne constitue pas un effacement définitif (effacement logique).

C4.05 – Gestion de la sous-traitance ultérieure en fin de prestation

Dans le cas où le Sous-traitant a mis en place une sous-traitance ultérieure pour réaliser les traitements effectués pour le compte du responsable de traitement (critère C2.10), il doit :

a) transmettre au sous-traitant ultérieur l'instruction du responsable de traitement de supprimer les données ;

b) conserver une information datée attestant de la suppression effective des données.

C4.06 – Confirmation de la suppression des données

Lorsque le Sous-traitant supprime des données à caractère personnel en base active (critère C4.03), il informe son client :

a) de la date de suppression effective des données dans le système d'information de sous-traitance ;

En cas de sous-traitance ultérieure, cette date est postérieure à la date de suppression effective des données à caractère personnel chez tous les sous-traitants ultérieurs (critère C4.05) ;

b) du délai de suppression automatique qui s'applique aux sauvegardes de données réalisées pour garantir la sécurité du traitement au cours de sa mise en œuvre (critère C32.17) ;

En cas de sous-traitance ultérieure, ce délai est supérieur à la durée de conservation des sauvegardes la plus longue parmi les sous-traitants ultérieurs ;

c) de la durée de conservation qui s'applique aux données qu'il est tenu de conserver en raison d'une obligation légale en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis (critère C0.05b) ;

En cas de sous-traitance ultérieure, le Sous-traitant tient à la disposition de son client :

- la liste des sous-traitants ultérieurs qui ont déclaré être tenu de réaliser un traitement en vertu du droit de l'Union ou du droit national auxquels ils sont soumis ;

- la durée de conservation nécessaire à ces traitements, lorsqu'elle est définie par ces obligations légales.

Le Sous-traitant doit mettre à jour les informations relatives aux traitements qui sont nécessairement à l'actualisation du registre des traitements (critère C2.01).

Partie 5. L'amélioration du niveau de protection des données – les plans d'action

C5.01 – Plan d'action pour la sécurité du traitement

Le Sous-traitant doit établir un plan d'action sur 3 ans afin de maintenir et améliorer le niveau de sécurité du traitement des données.

Ce plan d'action pour la sécurité du traitement doit recenser :

- les mesures organisationnelles et techniques de sécurité de sécurité que le Sous-traitant a prévu de mettre en œuvre à une échéance définie ;
- celles que le Sous-traitant envisage de mettre en œuvre mais qui ne sont pas encore planifiées.

Les mesures du plan d'action doivent inclure :

a) les mesures d'amélioration de la sécurité dont la planification est annoncée dans la déclaration d'applicabilité (critère C2.12)

b) les mesures de sécurité prévues en annexe 1, uniquement lorsque la mise en œuvre de mesures de substitution est justifiée par une analyse de risque (critère C2.13).

c) les mesures de sécurité planifiées dans le cadre de l'analyse de risques de sécurité réalisée par le Sous-traitant (critère C2.14);

d) les mesures correctrices déterminées dans le cadre de la résolution des incidents de sécurité (critère C3.10) ;

e) les mesures de remédiation pour les vulnérabilités identifiées en conclusion des audits techniques (critère C3.12) ;

Le Sous-traitant doit établir une priorité pour planifier la mise en œuvre des mesures de sécurité, en prenant en considération l'état des connaissances, les coûts de mise en œuvre et la nature, la portée, le contexte et les finalités du traitement ainsi que les risques pour les droits et libertés des personnes dans la mesure où le Sous-traitant en a connaissance.

Le plan d'action pour la sécurité du traitement est actualisé chaque année, au besoin en replanifiant la mise en œuvre des mesures de sécurité selon la priorité des nouvelles mesures à planifier.

Le Sous-traitant conserve l'historique du plan d'action pendant 1 an minimum. Il y indique la date à laquelle chaque mesure planifiée a été mise en œuvre

C5.02 – Plan d'évaluation de la sous-traitance ultérieure

Le Sous-traitant doit établir un plan d'évaluation sur 3 ans qui couvre l'ensemble des sous-traitants ultérieurs.

Ce plan d'évaluation doit évaluer, en priorité et de manière renforcée, les sous-traitants ultérieurs quand le traitement qui leur est confié :

- est concerné par un ou plusieurs des facteurs de risque listés au critère C0.06 ;
- consiste à informer les personnes concernées du traitement des données, recueillir un consentement, collecter des données à caractère personnel auprès des personnes ou donner suite aux demandes d'exercice de droits ;
- a fait l'objet de réclamations ou de plaintes de la part des personnes concernées (critère C5.03);
- est concerné par une évolution de la réglementation (critère C5.04).

Le plan d'évaluation doit prévoir qu'au moins un des sous-traitants ultérieurs sera évalué de manière renforcée chaque année.

Cette évaluation renforcée doit inclure une vérification de :

a) la mise en oeuvre des engagements contractuels pris par le sous-traitant ultérieur, notamment l'autorisation de recourir à des sous-traitants (critère C1.04d) et les transferts de données hors de l'Union européenne (critère C1.05) ;

b) selon la nature du traitement confié au sous-traitant ultérieur, la mise en œuvre des instructions du responsable de traitement concernant, par exemple, l'information les personnes, le recueil d'un consentement, la collecte des données à caractère personnel auprès des personnes ou la suite donnée aux demandes d'exercice de droits ;

c) la mise en œuvre des mesures organisationnelles et techniques de sécurité qui correspondent aux instructions du responsable de traitement et aux engagements contractuels pris avec le Sous-traitant (critère C2.11) ;

d) la notification des violations de données constatées par le sous-traitant ultérieur (critère C3.11) ;

e) la suppression définitive des données à la fin du traitement réalisé pour le compte d'un responsable de traitement (critère C4.05) ;

Le plan d'évaluation de la sous-traitance ultérieure est actualisé tous les ans pour prendre en considération :

- une évolution de la liste des sous-traitants ultérieurs (critère C2.09) ;

- une évolution des traitements qui leur sont confiés, par exemple dans le cadre de modification des traitements (critère C3.03), d'actions menées pour la sécurité du traitement ou l'amélioration du traitement (critères C5.01 et C5.03) ou du fait de l'évolution de la réglementation (critère C5.04).

Le Sous-traitant informe son client de tout manquement d'un sous-traitant ultérieur à ses obligations contractuelles.

C5.03 – Plan d'amélioration

Le Sous-traitant doit établir un plan d'amélioration qui vise à identifier et mettre en œuvre les actions utiles à l'amélioration de sa prestation ou de son *offre de service* en matière de protection des données.

Les actions du plan d'amélioration n'incluent pas :

- les actions pour la sécurité du traitement et pour l'évaluation de la sous-traitance ultérieure, qui sont respectivement l'objet des critères C5.01 et C5.02 ;

- les actions requises par les critères du présent référentiel, qui doivent être achevées pour obtenir la certification et que le Sous-traitant doit ensuite pouvoir démontrer à tout moment pour maintenir la certification obtenue.

Ce plan d'amélioration doit identifier les actions utiles à mettre en œuvre, notamment à partir de :

a) la mise en place d'un processus de recueil et de gestion des demandes d'amélioration et des réclamations de la part des personnes concernées, que le Sous-traitant recueille directement auprès des personnes concernées par le traitement, reçoit via son délégué à la protection des données ou qui lui sont transmises par ses clients ;

b) la mise en place d'un processus de recueil et de gestion des demandes d'amélioration et des réclamations de la part de ses clients, par exemple, en ce qui concerne l'assistance à l'exercice des droits, l'assistance à la sécurité des données, l'assistance à la notification des données, l'assistance à l'analyse d'impact, l'engagement de permettre la réalisation d'audits, etc. ;

c) la mise en œuvre de la procédure de recueil des instructions du responsable de traitement, en ce qui concerne les instructions complémentaires à l'*offre de service* et celles qui ne peuvent pas être prises en charge (critère C1.15d).

Lorsqu'il communique auprès des personnes concernées et auprès de ses clients au sujet du recueil et de la gestion des demandes d'amélioration et des réclamations qu'il met en place, le sous-traitant les informe qu'ils peuvent également soumettre l'objet de leur demande à l'organisme de certification dès lors qu'ils souhaitent signaler ce qui leur apparait être une non-conformité aux obligations du RGPD qui incombent au Sous-traitant.

Le Sous-traitant conserve l'historique du plan d'amélioration pendant 1 an minimum. Il y indique les actions d'amélioration de sa prestation ou de son offre de service qu'il décide de mettre en place.
C5.04 – Veille et actualisation Le Sous-traitant doit mettre en place une veille juridique et technologique qui lui permet notamment de : a. anticiper l'évolution des obligations qui lui incombent en vertu de dispositions législatives et réglementaires en matière de protection des données (critère C0.9) ; b. anticiper l'évolution du contexte de traitement, notamment en matière de cybersécurité pour l'actualisation des sources de risques, des menaces qui rendent un événement redouté possible et de l'appréciation qu'un événement redouté survienne (critères C2.13 et C2.14) ; c. être informé sur l'état de l'art des technologies mises en œuvre dans le système d'information de sous-traitance, par exemple en matière de chiffrement des données en transit et au repos (critères C32.2 et C32.3), de protection des facteurs d'authentification (critère C32.10), d'anonymisation (critère C32.20), etc. ;

Annexe 1 : Mesures de sécurité

Annexe C32. Les mesures techniques et organisationnelles de sécurité
C32.01 – Gestion des clés cryptographiques Les mesures de gestion des clés cryptographiques qui sont documentées au critère C2.11 doivent prévoir la mise en œuvre d'une procédure de gestion des outils cryptographiques et de gestion des clés de chiffrement/déchiffrement. Cette procédure doit notamment définir : a) les règles de création, renouvellement et destruction des clés cryptographiques ; b) les règles de stockage des clés cryptographiques et notamment les mesures de cloisonnement de ces clés par rapport aux données chiffrées. Ces mesures de cloisonnement peuvent consister en du cloisonnement système, applicatif ou cryptographique ; c) les règles à suivre en cas de révocation de clés cryptographiques.
C32.02 – Chiffrement des données en transit Les mesures de chiffrement en transit qui sont documentées au critère C2.11 doivent prévoir le chiffrement des flux entrant et sortant qui sont recensés par la cartographie des flux de données (voir critère C0.08). La description des mesures de chiffrement doit être accompagnée de références à l'état de l'art (par exemple : recommandations contenues dans des normes, guides de bonnes pratiques, recommandations nationales ou européennes) qui démontre leur efficacité pour : a) les protocoles utilisés pour la protection des flux réseau ; b) les algorithmes de chiffrement utilisés ; c) les tailles des clés de chiffrement. Lorsque le Sous-traitant n'est pas en mesure de mettre en place des mesures de chiffrement garantissant que seul le récepteur des données est en capacité de les déchiffrer, il documente cette limitation dans la description des mesures de chiffrement.
C32.03 – Chiffrement des données au repos Les mesures de chiffrement au repos qui sont documentées au critère C2.11 doivent prévoir le chiffrement en base active des données sensibles au sens de l'article 9 du RGPD traitées par le Sous-traitant. La description des mesures de chiffrement au repos doit être accompagnée de références à l'état de l'art (par exemple : recommandations contenues dans des normes, guides de bonnes pratiques, recommandations nationales ou européennes) qui démontre leur efficacité pour : a) les algorithmes de chiffrement utilisés ; b) les tailles des clés de chiffrement ; c) les durées de conservation des données chiffrées au repos.
C32.04 – Filtrage des flux Les mesures de filtrage des flux qui sont documentées au critère C2.11 doivent prévoir que seuls les flux entrant/sortant recensés dans la cartographie des flux (voir critère C0.08) sont autorisés. Tous les autres flux envisageables doivent en conséquence être bloqués ou filtrés par des dispositifs logiciels, matériels ou réseau.

C32.05 – Gestion des habilitations

Les mesures de gestion des habilitations et des permissions d'accès aux données qui sont documentées au critère C2.11 doivent prévoir :

a) différents profils d'habilitation afin de limiter l'accès aux données aux seuls utilisateurs ayant besoin d'y accéder pour l'accomplissement de leur mission, selon un principe de moindre privilège ;

b) la validation par un responsable (par exemple : un supérieur hiérarchique ou un chef de projet) de chaque demande d'habilitation d'un nouvel utilisateur issu de son personnel et de chaque modification apportée aux habilitations de son personnel (par exemple : à l'occasion d'un changement de mission ou de poste).

c) la suppression, dans un délai déterminé par le Sous-traitant, des habilitations d'un utilisateur à la fin de son contrat de travail ou de la prestation au bénéfice du Sous-traitant.

Les mesures de gestion des habilitations et des permissions d'accès aux données doivent définir au moins un profil d'administrateur à haut privilège. Plusieurs profils de ce type peuvent être définis quand les tâches et domaines de responsabilité d'administration peuvent être séparés.

Le Sous-traitant doit réaliser une revue régulière, *a minima* annuelle, des habilitations afin d'identifier et de supprimer les comptes non utilisés et de réaligner les droits accordés sur les fonctions et missions de chaque utilisateur.

Dans le cas où le Sous-traitant propose une *offre de service* qui permet à ses clients de prendre à leur charge la gestion des habilitations et des permissions d'accès d'une partie des utilisateurs, cette *offre de service* doit lui permettre de :

- utiliser différents profils d'habilitation, notamment un profil d'administrateur du service qui diffère des autres profils d'utilisation du service ;

- exercer un contrôle sur les habilitations qui inclut l'enregistrement, la modification, la suppression et l'accès aux habilitations et aux permissions d'accès associées.

C32.06 – Gestion des permissions d'accès logique et physique

Les mesures de gestion des habilitations et des permissions d'accès aux données qui sont documentées au critère C2.11 doivent prévoir que les permissions d'accès sont retirées dès le retrait des habilitations.

Cela concerne à la fois :

a) les permissions d'accès logique (ex : l'accès à une ressource informatique) ;

b) les permissions d'accès physique (ex : l'accès aux locaux hébergeant les infrastructures du système d'information de sous-traitance).

C32.07 – Contrôle des accès physiques

Les mesures de contrôle des accès physiques qui sont documentées au critère C2.11 doivent protéger l'accès aux bâtiments du Sous-traitant et aux salles hébergeant les infrastructures du système d'information de sous-traitance (par exemple : salle de serveurs, armoire informatique, etc.).

Les mesures de contrôle des accès physiques à ces zones sécurisées doivent inclure :

a) des mesures complémentaires à celles prévues pour l'accès aux bâtiments ;

b) l'habilitation des personnes ayant besoin d'accéder physiquement à ces zones (voir critère C32.05) ;

c) la journalisation des traces d'accès physiques à ces zones (voir critère C32.16), par exemple au moyen de la tenue d'un registre des entrées/sorties, en l'absence de moyens d'accès informatisés (ex : badge avec gestion centralisée) ;

d) l'accompagnement permanent de tout visiteur par une personne habilitée dans ces zones sécurisées.

C32.08 – Authentification des utilisateurs

Les mesures d'authentification des utilisateurs qui sont documentées au critère C2.11 doivent prévoir que chaque utilisateur disposant d'une habilitation pour accéder aux données (voir critère C32.05) doit :

a) être doté d'un identifiant qui lui est propre pour toute utilisation de moyens informatiques ;

b) s'authentifier pour vérifier son identité et ses droits d'accès avant d'accéder à des données à caractère personnel ;

c) vérifier l'identité du serveur d'authentification, par exemple au moyen d'un certificat d'authentification de serveur ;

d) chiffrer le canal de communication entre le serveur authentifié et le client conformément au critère C32.03 relatif au chiffrement des flux de données.

Dans le cas où le Sous-traitant propose une *offre de service* qui permet la délégation à son client de l'authentification d'une partie des utilisateurs, le service doit permettre à son client de :

- identifier chaque utilisateur du service via l'identifiant unique fourni par le client ;

- conditionner l'accès du service à une authentification préalable de l'utilisateur ;

- détecter et journaliser de façon accessible au client les tentatives d'authentification qui semblent incompatibles avec l'unicité de l'identifiant qui est fourni par le client.

C32.09 – Complexité des facteurs d'authentification

Les mesures d'authentification des utilisateurs qui sont documentées au critère C2.11 doivent préciser si elles font intervenir l'un des facteurs suivants (ou plusieurs d'entre eux dans le cas d'une authentification multifacteur) :

a) un facteur de connaissance (ce que l'on sait), par exemple un mot de passe ;

b) un facteur de possession (ce que l'on a), par exemple un code à usage unique généré par une application mobile dédiée.

Dans le cas d'une authentification faisant uniquement intervenir un mot de passe, l'entropie du mot de passe doit être de 80 bits minimum, ce qui correspond par exemple à au moins :

- 12 caractères comportant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles ; ou

- 14 caractères comportant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire.

Dans le cas d'une authentification faisant intervenir un mot de passe et des mesures de restriction d'accès, l'entropie du mot de passe doit être de 50 bits minimum, ce qui correspond par exemple à au moins :

- 8 caractères comportant les 4 catégories de caractères (majuscules, minuscules, chiffres et caractères spéciaux à choisir dans une liste d'au moins 11 caractères spéciaux possibles) ; ou bien

- 16 chiffres.

Les mesures de restriction d'accès doivent permettre de limiter le nombre possible de tentatives d'authentification pendant une période donnée et doivent comporter au moins :

- une temporisation de l'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement en fonction du nombre de tentatives dans un laps de temps déterminé ; ou bien

- un mécanisme déterminant un nombre maximal de tentatives autorisées dans un délai donné, avec au maximum 10 tentatives par heure ; ou bien

- un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (par exemple : mise en œuvre de « captcha ») ; ou bien

- un blocage du compte utilisateur après un nombre d'authentifications échouées consécutives au plus égal à 10, assorti d'un mécanisme de déblocage.

Dans le cas d'une authentification par mot de passe faisant également intervenir un matériel détenu par l'utilisateur (facteur de possession) et avec des mesures de blocage de l'accès après 3 échecs, l'entropie du mot de passe doit être de 13 bits minimum, ce qui correspond par exemple à au moins 4 chiffres.

C32.10 – Protection des facteurs d'authentification

Les mesures relatives à la protection des facteurs d'authentification qui sont documentées au critère C2.11 doivent :

a) interdire l'envoi de mots de passe en clair à travers un canal de communication ;

b) interdire la conservation de mots de passe en clair sur un support de stockage ;

c) appliquer aux mots de passe une fonction de hachage cryptographique à l'état de l'art, comprenant l'utilisation d'un sel ou d'une clé pseudo-aléatoire avant stockage ainsi que des paramètres relatifs aux coûts en temps et/ou en mémoire nécessaires à une attaque par force brute.

C32.11 – Gestion des mots de passe

Les mesures d'authentification des utilisateurs qui sont documentées au critère C2.11 doivent :

a) définir la périodicité de renouvellement des mots de passe des comptes administrateur ;

b) attribuer un mot de passe temporaire et modifiable par l'utilisateur lui-même lors de la première authentification lorsque ce mot de passe est attribué par un administrateur ou automatiquement par le système lors de la création du compte ou d'une réinitialisation ;

c) ne pas renvoyer d'information permettant de déduire l'existence d'un compte utilisateur lors de l'échec d'une authentification.

C32.12 – Authentification multifacteur

Les mesures d'authentification des utilisateurs qui sont documentées au critère C2.11 doivent définir les catégories d'utilisateurs soumis à une authentification multifacteur pour l'accès au système d'information.

Les utilisateurs suivants doivent être soumis à une authentification multifacteur, faisant intervenir *a minima* deux catégories de facteurs d'authentification distinctes pour les personnes habilitées :

a) les utilisateurs disposant d'un compte administrateur (voir critère C32.05) ;

b) les utilisateurs habilités à accéder à des données sensibles au sens de l'article 9 du RGPD qui sont traitées par le Sous-traitant ;

c) les utilisateurs habilités à accéder au système d'information à distance via l'usage d'un réseau virtuel privé (voir critère C32.13).

C32.13 – Accès au système d'information à distance

Les mesures d'accès au système d'information à distance qui sont documentées au critère C2.11 doivent :

a) conditionner cet accès à distance à l'usage d'un réseau virtuel privé (VPN) dont les flux de communication sont chiffrés conformément aux mesures de chiffrement des flux (critère C32.03) et selon une authentification multifacteur (critère C32.12).

b) établir la liste des catégories d'utilisateur disposant d'un accès à distance.

C32.14 – Contrôle d'accès des serveurs, postes de travail et équipements mobiles

Les mesures de contrôle d'accès des serveurs, postes de travail et équipements mobiles, qui sont documentées au critère C2.11 doivent autoriser à se connecter aux réseaux du système d'information de sous-traitance uniquement les équipements utilisés par les personnes habilitées.

C32.15 – Authentification de machine à machine

Les mesures d'authentification machine à machine, c'est-à-dire sans action d'un utilisateur, qui sont documentées au critère C2.11 doivent exiger de :

a) faire contrôler l'identité du serveur d'authentification par le client, par exemple au moyen d'un certificat d'authentification de serveur ;

b) chiffrer le canal de communication entre le serveur authentifié et le client conformément au critère C32.02 relatif au chiffrement des flux de données ;

c) assurer l'authentification du client conformément au critère C32.01 relatif à la gestion des clés cryptographiques et C32.10 relatif à la protection des facteurs d'authentification.

C32.16 – Système de journalisation

Les mesures de journalisation qui sont documentées au critère C2.11 doivent prévoir l'enregistrement des actions des utilisateurs du système d'information de sous-traitance dans des « fichiers journaux » (ou « traces »).

Pour chaque action enregistrée, les traces doivent inclure *a minima* :

a) l'identifiant de l'utilisateur prévu par les mesures d'authentification (voir critère C32.08) ;

b) l'horodatage de l'action réalisée ;

c) la nature des actions effectuées (par exemple : opération d'accès en lecture ou en écriture, création, modification, suppression, etc.).

Lorsque des opérations de maintenance par des tiers sont envisagées dans le système d'information de sous-traitance, elles doivent être journalisées explicitement comme étant réalisées par ces tiers.

Dans le cas où le Sous-traitant propose une *offre de service* qui permet à ses clients de prendre à leur charge la gestion des habilitations et des permissions d'accès d'une partie des utilisateurs (critères C32.05 et C32.06), le service doit inclure une fonction de consultation des traces de ces utilisateurs.

Les mesures de journalisation doivent définir la durée de conservation des traces. Cette durée doit être comprise entre six mois et un an à compter de la collecte des données, sauf à justifier de la nécessité de limiter ou d'étendre la durée de conservation des traces pour :

- respecter une obligation légale portant sur cette durée de conservation (critère C0.09) ;

- répondre à un besoin de gestion des contentieux ou de contrôle interne (critère C1.16) ;

- réaliser une analyse post-incident de sécurité afin d'atténuer un risque pour les personnes concernées par le traitement des données (critère C2.16).

Le Sous-traitant doit réaliser un contrôle des traces. Ce contrôle doit lui permettre de détecter d'éventuelles anomalies (par exemple : volume de trafic réseau anormal, nombreuses tentatives d'authentification, élévations de privilèges anormales, etc.).

Les mesures de journalisation doivent définir la périodicité du contrôle des traces. Les analyses résultant de ce contrôle doivent être conservées pendant la même durée que les traces.

Le Sous-traitant doit informer les utilisateurs, par exemple lors de l'authentification ou de l'accès au système d'information de sous-traitance, de la mise en place du système de journalisation, après information et consultation des instances représentatives du personnel.

C32.17 – Sauvegarde des données

Les mesures de sauvegarde des données qui sont documentées au critère C2.11 doivent prévoir la sauvegarde des données à caractère personnel traitées par le Sous-traitant pour le compte de son client.

Les mesures de sauvegarde doivent définir :

a) les catégories de données à caractère personnel auxquels la sauvegarde est appliquée (ou bien les espaces de stockage) ;

b) la fréquence des intervalles des sauvegardes ;

c) les supports de conservation des sauvegardes ;

d) le type de chiffrement appliqué aux données sauvegardées, conformément aux mesures de chiffrement au repos (voir critère C32.03).

Au moins un des supports de conservation des sauvegardes doit être :

- isolé hors ligne du système d'information de sous-traitance utilisé pour le stockage en base active des données pendant la durée du traitement ;

- stocké sur un site géographiquement distinct du site principal hébergeant le système d'information de sous-traitance utilisé pour le stockage en base active des données pendant la durée du traitement.

Dans le cas d'une *offre de service*, le Sous-traitant doit définir les mesures de sauvegarde de manière à permettre le redémarrage du traitement dans le cadre d'une reprise d'activité suite à une perte totale des données à caractère personnel en base active (critère C32.19).

C32.18 – Archivage des données

Les mesures d'archivage qui sont documentées au critère C2.11 doivent prévoir l'archivage intermédiaire des données à caractère personnel sur instruction de son client (critère C3.01).

Les mesures d'archivage doivent définir :

a) les supports de stockage des archives intermédiaires ;

b) le type de chiffrement appliqué aux archives intermédiaires, conformément aux mesures de chiffrement au repos (critère C32.03).

Les supports de stockage des archives intermédiaires doivent être isolés du système d'information de sous-traitance utilisé pour le stockage des données, en base active, pendant la durée du traitement.

C32.19 – Reprise d'activité

Les mesures de reprise d'activité qui sont documentées au critère C2.11 doivent prévoir un plan d'arrêt et de reprise des traitements. Ce plan peut s'inscrire dans un plan de reprise d'activité (PRA), au périmètre plus large.

Le plan d'arrêt et de reprise des traitements doit documenter :

a) le processus de décision pour l'arrêt temporaire du traitement dans le but de limiter l'impact pour les personnes, qui précise notamment le ou les responsables ayant autorité pour une prise d'une décision et les conditions qui sont anticipées pour envisager l'arrêt temporaire du traitement ;

b) le processus à suivre pour mettre fin à la perturbation ou l'interruption de l'activité, en application de la procédure de détection, d'analyse et de résolution des incidents de sécurité prévue au critère C2.16 ;

c) le processus de décision pour la reprise du traitement ;

d) la procédure de restauration des sauvegardes (critère C32.17).

Le plan de reprise d'activité doit être testé *a minima* tous les 3 ans en ce qui concerne :

- la mise en œuvre du processus de décision d'arrêt/reprise du traitement, au moyen d'un exercice de gestion de crise ;

- la restauration des sauvegardes, au moyen d'un environnement de pré-production conforme aux mesures de sécurité documentés au critère C2.11.

C32.20 – Anonymisation des données

Les mesures d'anonymisation des données qui sont documentées au critère C2.11 doivent prévoir un processus d'anonymisation contextuel aux données initiales à anonymiser et définir :

a) la nature des données initiales faisant l'objet d'une mesure d'anonymisation ;

b) le volume de données initiales faisant l'objet de la mesure ;

c) la précision des données initiales faisant l'objet de la mesure ;

d) le nombre approximatif de personnes concernées auxquelles les données initiales se rapportent ;

e) les moyens raisonnablement susceptibles d'être utilisés pour tenter de réidentifier une personne par le responsable de traitement ou par toute autre personne ;

f) les moyens raisonnablement susceptibles d'être utilisés pour tenter de réidentifier une personne par le destinataire qui sollicite le jeu de données anonymes, notamment :

- les informations auxiliaires, c'est-à-dire qui permettraient l'identification, dont ce destinataire dispose ou pourrait disposer, y compris d'autres jeux de données présumément anonymes issus des mêmes données initiales ;

- les différents accès qu'il a pu avoir à d'autres jeux de données comprenant aussi les données initiales ;

- les moyens informatiques (puissance de calcul, en particulier) dont il dispose ou pourrait disposer.

Le processus d'anonymisation doit être réalisé selon des techniques à l'état de l'art. La description des mesures d'anonymisation doit être accompagnée des références (par exemple : recommandations contenues dans des normes, guides de bonnes pratiques, recommandations nationales ou européennes, articles de recherche) qui démontre que les personnes auxquelles les données initiales se rapportent ne sont pas ou plus identifiables.

C32.21 – Exportation de données

Les mesures d'exportation des données qui sont documentées au critère C2.11 doivent couvrir les flux sortants recensés au critère C0.08 (cartographie des flux) associés à l'exportation de données à caractère personnel traitées pour le compte d'un client en dehors du système d'information de la sous-traitance.

Pour chaque exportation de données, qu'elle soit ponctuelle ou récurrente, les mesures doivent inclure :

a) la tenue d'une traçabilité des exportations, comprenant une description des données exportées, le destinataire et la date d'exportation ainsi que les références aux données concernées ;

b) la suppression ou l'anonymisation des données exportées lorsqu'elles ne sont plus nécessaires.

Lorsque les mesures de maintenance et de correction de défauts du système d'information de sous-traitance nécessitent l'extraction des données à caractère personnel pour réaliser des tests ou une recette, le Sous-traitant applique les mesures relatives aux exportations des données décrites ci-dessus et accompagne la description des données exportées/extraites d'une justification de leur nécessité pour ces tests ou recette.

C32.22 – Gestion des postes de travail, des équipements mobiles et des supports amovibles

Les mesures de gestion des postes de travail et équipement mobiles qui sont documentées au critère C2.11 doivent prévoir la mise en œuvre d'une procédure de gestion des postes de travail, des équipements mobiles et des supports amovibles utilisés par les personnes habilitées.

Cette procédure doit notamment s'assurer que les postes de travail mis à la disposition du personnel disposent :

a) de comptes nominatifs respectant le critère C32.05 relatif à la gestion des habilitations ;

b) d'une authentification des utilisateurs (critère C32.08) ;

c) d'un chiffrement des supports de stockage respectant le critère relatif au chiffrement au repos (critère C32.03) ;

d) d'un mécanisme de verrouillage automatique des sessions ;

e) de mesures de filtrage ne permettant qu'aux seuls flux explicitement autorisés d'être ouverts sur les équipements individuels ;

f) d'outils de détection de logiciels malveillants régulièrement mis à jour ;

g) d'un mécanisme permettant à un administrateur de déclencher un effacement à distance des données stockées, pour les équipements mobiles ;

h) d'un mécanisme de gestion des mises à jour de sécurité (critère C32.24) ;

i) d'une désactivation de l'exécution automatique depuis les supports amovibles.

Dans le cas où certains postes de travail ne sont pas sous le contrôle du Sous-traitant, les mesures de sécurité à mettre en place sur les postes de travail doivent être encadrées au moyen d'une convention entre les parties concernées et imposer les exigences a) jusqu'à i).

C32.23 – Mise au rebut et réaffectation

Les données personnelles contenues dans tout équipement ou support stockant des données personnelles issues du système d'information de sous-traitance doivent être effacées de façon sécurisée et définitive avant leur mise au rebut ou réaffectation.

Dans le cas où les données personnelles sont chiffrées au repos conformément aux critères (gestion des clés et chiffrement au repos), cet effacement peut être réalisé par l'effacement sécurisé et définitif des clés de chiffrement et/ou déchiffrement.

C32.24 – Mises à jour de sécurité

Les mesures de mise à jour de sécurité qui sont documentées au critère C2.11 doivent prévoir la mise en œuvre d'une procédure de gestion des mises à jour de sécurité relatives aux serveurs, postes de travail et des équipements mobiles utilisés pour accéder au système d'information de sous-traitance.

Cette procédure de gestion des mises à jour doit prévoir :

a) une veille relative aux mises à jour de sécurité pour les logiciels et les équipements matériels utilisés dans le système d'information de sous-traitance ;

b) l'application systématique des mises à jour critiques de sécurité dans un court délai ;

c) l'enregistrement de la date des mises à jour appliquées et de leur criticité.

C32.25 – Charte informatique

Le Sous-traitant doit faire signer une charte informatique à chaque utilisateur du système d'information de sous-traitance issu de son personnel.

Cette charte doit inclure :

a) les sanctions encourues en cas de non-respect de ces obligations ;

b) les règles concernant la bonne gestion des facteurs d'authentification par les utilisateurs, notamment des mots de passe (pratiques interdites, moyens mnémotechniques, gestionnaire de mots de passe, etc.) ;

c) les règles concernant la bonne gestion des supports amovibles (vérification des supports amovibles pouvant être connectés aux postes de travail et plus généralement au système d'information de la sous-traitance avant toute connexion afin de s'assurer qu'ils ne contiennent pas de logiciels malveillants) ;

d) la conduite à tenir et la personne à contacter en cas de perte ou de vol d'un équipement mobile ou d'un support de stockage (critère C32.22) ;

e) la conduite à tenir et la liste des personnes à contacter en cas d'incident de sécurité ou de survenance d'un évènement inhabituel (critère C2.16).

Le Sous-traitant doit donner une force contraignante à cette charte, par exemple en l'annexant à son règlement intérieur ou aux contrats de travail de son personnel.