MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

Guide « Sous-traitance »

Document d'accompagnement du kit sécurité des systèmes d'information pour les espaces numériques de travail

ENT
Espace numérique de travail

Document d'accompagnement
version 1.0
Juin 2022

Direction du numérique pour l'éducation – bureau SN1

Table des matières

1. Introduction

1.1. Avant-propos

Dans le cadre du déploiement et de la mise en œuvre des espaces numériques de travail dans le 1er et 2ème degré de l'enseignement scolaire, le ministère de l'Éducation nationale a élaboré un schéma directeur des espaces numériques de travail (SDET) dont l'objectif est de fournir un cadre de cohérence national pour les projets ENT et d'orienter l'offre de solutions ENT.

Le SDET pose « les principes directeurs de l'élaboration et de la mise en œuvre d'une solution ENT en partenariat avec les collectivités territoriales qui les financent et les académies qui assurent l'accompagnement des utilisateurs ».

Dans cette volonté d'accompagner les partenaires et acteurs, l'Éducation nationale propose un ensemble de guides thématiques portant sur la sécurité des espaces numériques de travail à destination des différents acteurs conçu comme un cadre de référence commun.

Ce kit SSI est proposé dans un contexte de sécurisation nécessaire et pour répondre tout à la fois aux exigences sociales des usagers et à la réglementation en termes de protection des données ou de continuité pédagogique.

1.2. Présentation du KIT SSI pour les ENT

Le Kit SSI pour les ENT est un ensemble de guides pratiques qui recouvrent les domaines suivants :

- La gouvernance de la sécurité des systèmes d'information
- La sous-traitance
- La mise en œuvre des téléservices
- La gestion des incidents

Il a pour objectifs :

- D'outiller les porteurs de projets ENT dans la mise en œuvre de la politique de sécurité tout au long du cycle de vie des ENT. En particulier, les guides prescrivent un ensemble de recommandations pour répondre à la réglementation et aux principes de la gestion de risque, aussi bien en phase de déploiement, d'utilisation ou d'évolution de l'ENT ;
- De fournir un cadre commun de références aux acteurs, partenaires et sous-traitants en rappelant en particulier les règles auxquelles se conforme l'Éducation nationale ;
- De répondre de façon simple et non ambiguë aux différentes situations et problèmes qui peuvent se poser aux responsables et acteurs des ENT.

Dans la continuité des guides proposés par l'ANSSI, en particulier le guide à destination de collectivités territoriales, ce kit SSI vise de façon plus générale à :

- *Donner confiance aux usagers dans l'utilisation des services numériques;*
- *Garantir la sécurité des données à caractère personnel conformément à la réglementation;*
- *Appuyer la transformation numérique des administrations de l'État ;*
- *Renforcer la sécurité des acteurs critiques pour l'État.*

1.3. Présentation du guide sous-traitance

Le présent guide couvre le domaine de la sous-traitance et en particulier des relations entre :

- Sous-traitant et porteur de projet ;
- Sous-traitant et chef d'établissement ;
- Sous-traitant et parents d'élèves.

Il propose un ensemble de recommandations sous l'axe du cycle de vie de l'ENT et sous l'axe des types de prestations externes qui peuvent être envisagées.

A l'instar des autres guides, il aborde les trois étapes du cycle de vie de l'ENT : l'élaboration de l'appel d'offre, l'exploitation de l'ENT, et la fin de l'ENT. Il est conçu comme un ensemble de recommandations ou règles qui rappellent les exigences réglementaires en particulier dans le champ de la protection des données à caractère personnel, ainsi que l'organisation, le rôle et missions des différents acteurs et leur articulation.

Il couvre les différents types de prestation qui peuvent être :

- La fourniture d'une solution clé en main au travers d'un hébergement ;

- La mise à disposition d'une solution logicielle hébergée sur les infrastructures du porteur de projet voir de l'établissement ;
- Un hébergement d'infrastructure ou d'équipements qui supporteraient une solution ENT opérée par le porteur de projet.

2. Objectifs détaillés

2.1. Objectifs détaillés du guide

Les objectifs sont détaillés ci-après avec un n° d'occurrence qui ne présume ni de l'importance ni de l'ordonnancement de l'objectif.

Objectif n°1 : expliciter les clauses obligatoires dans les appels d'offres et préciser l'articulation des CCT et CCAG PI.

Objectif n°2 : proposer des clauses additionnelles dans les appels d'offre pour mieux prendre en compte les responsabilités partagées et relations entre partenaires.

Objectif n° 3 : Fixer des règles sur le fonctionnement en cours d'exploitation.

Objectif n° 4 : préconiser des procédures sur le traitement de certains processus qui tiennent compte des responsabilités respectives des collectivités territoriales et autorités académiques.

Objectif n° 5 : rappeler les prescriptions légales découlant de la protection des données à caractère personnel, des relations entre usagers et administration dans le cadre des échanges électroniques.

2.2. Ce qu'est ce guide

Ce guide fournit dans le contexte particulier de la gestion des sous-traitants un ensemble de recommandations à destination des acteurs et fournit une synthèse du cadre légal. La plupart des recommandations ou principes énumérés dans ce guide fournit un cadre de référence pour les autorités académiques et collectivités territoriales dans le cadre des obligations légales ou contractuelles découlant du RGPD, du code de l'éducation, des marchés publics ou de l'ordonnance du 8 décembre 2005.

Elles fixent également les obligations des sous-traitants et les exigences attendues pour ces derniers dans le cadre de l'exécution du marché qu'elle qu'en soit sa forme.

Ces recommandations précisent sous forme de règles ce que peuvent, doivent ou devraient faire les acteurs pour répondre anticiper les obligations légales ou réglementaires dans le cadre de la relation contractuelle. Il propose également des clauses additionnelles aux clauses RGPD susceptibles d'être incluses dans le cahier des charges.

2.3. Ce que n'est pas ce guide

Ce guide n'est pas un catalogue de mesures techniques ou organisationnelles qui s'imposeraient à chacun des acteurs. Il ne se substitue en rien aux procédures ou processus mis en œuvre par les académies ou par les collectivités territoriales dans le cadre du principe de libre administration des collectivités territoriales.

3. Contexte

3.1. Périmètre

Le présent guide s'intéresse à la gestion de la sous-traitance dans le cadre du déploiement et de l'exploitation des espaces numériques de travail.

Pour la protection des données à caractère personnel, la sous-traitance est encadrée par le RGPD et complétée pour ce périmètre par les clauses contractuelles type.

La PSSIE, dans son objectif 8 relatif à la gestion des prestataires, rappelle la nécessité de « *veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers.* ». Le guide prend en compte les risques liés à la perte de maitrise sur les ENT qu'engendre l'externalisation et propose des recommandations qui peuvent être utilisées comme base de la rédaction de clauses SSI à inclure dans les marchés. Pour cela il s'appuie sur le guide ANSSI d'externalisation des systèmes d'information.

3.2. Le cahier des charges

En sus des clauses contractuelles type ou reprenant l'article 28.3 du RGPD, des clauses de sécurité doivent être ajoutés dans le cahier des charges pour :

- Préciser certaines dispositions des CCT comme la restitution des données par exemple ;
- Ajouter des clauses pour définir des exigences opposables au prestataire sur la gestion des incidents ou la participation à des instances de pilotage par exemple.

Ces clauses servent de base à la production d'un plan d'assurance sécurité qui devra être exigé du candidat dans le cadre d'un appel d'offre ENT comme en dispose le guide ANSSI d'externalisation :

> *Les candidats doivent fournir, en réponse à la consultation, un document contractuel appelé plan d'Assurance Sécurité. Ce document précise les dispositions prises par le futur prestataire pour répondre aux exigences de sécurité du donneur d'ordres pendant toute la durée du contrat*

Le cahier des charges intégrera :

- Les clauses sécurité relatives au RGPD ;
- Les CGAG-PI ;
- Des clauses additionnelles conformément au guide ANSSI d'externalisation

4. Rôle de chaque acteur et actions attendues

4.1. Porteur de projet

Action(s) à mener	Responsabilité(s)
Établir un contrat clair en utilisant le kit de conventionnement RGPD	Article 28.3 du RGPD. Organiser les rapports et obligations respectives du sous-traitant et du responsable de traitement (le porteur de projet)

Tableau 1 : Actions attendues du porteur de projet

4.2. Autorité académique

Action(s) à mener	Responsabilité(s)
Établir un contrat clair	Article 28.3 du RGPD. Organiser les rapports et obligations respectives du sous-traitant et du responsable de traitement

Tableau 2 : Actions attendues de l'autorité académique

4.3. DPD/RSSI/DSI de l'académie

Action(s) à mener	Responsabilité(s)
Apporter un rôle de conseil et d'expertise dans la rédaction du cahier des charges	Rôle de conseil

Action(s) à mener	Responsabilité(s)
Participer à la gestion des incidents	Obligation d'information du DPD en cas d'incident Chaine opérationnelle de sécurité

Tableau 3 : Actions attendues du DPD

4.4. Sous-traitant

Action(s) à mener	Responsabilité(s)
Établir un contrat clair	Article 28.3 du RGPD. Organiser les rapports et obligations respectives du sous-traitant et du responsable de traitement (académie ou collectivité territoriale)
Documenter l'activité de sous-traitance	Veiller au respect des instructions du responsable de traitement et les documenter ; Tenir un registre des activités de traitement (art. 30.2 du RGPD)
Participer aux instances de pilotage de la sécurité	Clauses contractuelles

Tableau 4 : Actions attendues du sous-traitant

Si un chef d'établissement du second degré ne souhaite pas bénéficier de l'ENT proposé par l'académie/la collectivité territoriale, il sera de se responsabilité d'établir un contrat clair avec le sous-traitant.

5. Recommandations aux acteurs

5.1. Principes

5.1.1. Principes relatifs au RGPD

Contenu des clauses

Les relations contractuelles entre le sous-traitant et le responsable de traitement sont régis par des clauses qui intègrent les dispositions obligatoires de l'article 28 du RGPD.

Le marché dans ses clauses relatives à la protection des données à caractère personnel reprendra donc l'ensemble de dispositions de l'article 28 ou intégrera les clauses contractuelles types (CCT) entre les responsables du traitement et les sous-traitants au titre de l'article 28.

Il est possible d'ajouter aux CCT ou dispositions obligatoires de l'article 28 des clauses ou des garanties supplémentaires « *condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées* ».[1]

Les clauses qui peuvent être ajoutées visent à mieux prendre en compte de la répartition des compétences entre les collectivités territoriales et l'administration déconcentrée de l'Éducation nationale.

Ces clauses additionnelles et non contradictoires[2] avec l'article 28 du RGPD ou les CCT peuvent porter par exemple sur :

- La réalisation d'audit technique ou organisationnel ;
- La mise à disposition des logs ;

[1] Source : https://www.cnil.fr/fr/clauses-contractuelles-types-entre-responsable-de-traitement-et-sous-traitant

[2] Clause 2 alinéa a des CCT

- La participation à des instances de pilotage de la sécurité ;

L'article 5 des CCAG PI invitent les acheteurs « pour rédiger les documents particuliers du marché, à consulter le guide du sous-traitant élaboré par la CNIL et disponible sur son site Internet »

5.1.2. Principes relatifs à la sécurité de l'information

Les espaces numériques de travail sont susceptibles d'héberger des données qui ne sont pas des données à caractère personnel mais dont la confidentialité doit cependant être garantie.

De plus, ces espaces peuvent voir leur sensibilité modifiée en fonction de situation du contexte national ou international, en situation de pandémie par exemple, ou parce qu'ils sont susceptibles d'être le support d'épreuves. Il peut donc s'avérer nécessaire d'assurer certain un niveau de disponibilité qui impliquent des mesures de sécurité.

Enfin, en cas d'externalisation de l'exploitation, que celle-ci soit hébergé de façon externe ou pas, le cahier de charges doit prévoir des mesures pour diminuer les risques relatifs à :

- La perte de maîtrise du système d'information ;
- La perte ou la divulgation des données ;
- L'hébergement mutualisé ;

Conformément aux préconisations du guide ANSSI relatif à l'infogérance.

Ainsi, le guide actuel reprend la classification opérée dans le guide ANSSI en considérant que les tâches externalisées peuvent être réalisées dans les locaux du prestataire, du porteur de projet voir dans l'établissement lui-même. Sont pris en compte :

- L'hébergement de service : le prestataire fournit au porteur de projet ou à l'établissement un ENT conçu comme un service global, accessible via un navigateur internet et la fédération. Cet hébergement peut être dédié ou mutualisé.
- La gestion de l'ENT hébergé chez le porteur de projet voir dans l'établissement. Cette gestion regroupe selon le guide ANSSI les activités de support fonctionnel, de maintenance préventive ou corrective, et de gestion des évolutions.
- La gestion d'infrastructures qui englobe la tierce maintenance applicative, les hébergements secs ou les hébergements d'infrastructures ou équipements en dehors de la fourniture de solutions ENT. Ce cas moins fréquent que les deux premiers sont toutefois pris en compte dans la mesure où il est nécessaire de fournir aux prestataires des prescriptions en termes de supervision de la sécurité, de stockage ou de sauvegardes.

5.1.3. Principes relatifs à la résiliation ou à la fin du marché

Le marché doit préciser les dispositions relatives à la fin du marché qui peut résulter

- De l'arrivée à échéance du marché parce qu'il n'est pas reconduit (décision explicite, absence de clauses de reconduction) ;
- D'un manquement du titulaire ou d'un de ses sous-traitants à ses obligations légales ou contractuelles

Résiliation du marché

En cas de manquement par le titulaire du marché ou un de ses sous-traitants à ses obligations légales et contractuelles relatives à la protection des données personnelles et sans préjudice des sanctions prévues par le RGPD, le marché peut être résilié pour faute en application de l'article 39 des CCAG PI.

Des dispositions identiques peuvent être indiquées dans le cahier des charges pour des manquements non liés aux obligations légales ou contractuelles découlant du RGPD.

Conséquence de la fin du marché

En cas de non-renouvellement ou de résiliation du marché, le porteur de projet ENT doit s'assurer de la destruction effective des données par le titulaire du marché.

Conformément aux CCAG PI[3] « *l'acheteur, ou l'organisme mandaté à cette fin, peut, pendant une période de six mois à compter de la fin ou de la résiliation du marché, exercer un contrôle dans les locaux du titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées* »

Des précisions complémentaires peuvent être apportées en termes de :

- Fourniture des sauvegardes au titulaire et délais de rétention des sauvegardes d'exploitation par le prestataire ;
- D'engagement sur l'honneur ou production de certificats attestant de la destruction effective des données ;

[3] Se référer au chapitre 6 - Référentiels applicables

- Contrôle documentaire portant sur les instructions fournies aux collaborateurs ou sous-traitants du titulaire, historique des scripts ou programmes de destructions des données sur les baies de stockages, destruction des sauvegardes incrémentales ou totales d'exploitation ;
- Réalisation d'un audit de contrôle par un prestataire non concurrent du titulaire.

5.2. Recommandations

R1

Rédiger les clauses générales relatives à la sécurité de l'information

Les clauses du marché doivent prévoir des clauses relatives à la sécurité de l'information et à la protection des données à caractère personnel.

Les clauses relatives à la protection des données étant rendus obligatoires par l'article 28, les CCT peuvent être utilisées de façon privilégiée.

Les clauses relatives à la sécurité de l'information et à la protection des données peuvent s'appuyer sur les CCAG PI.

Il est conseillé dans le cadre de la consultation, de demander aux candidats de fournir, un plan d'assurance sécurité. Pour mémoire ce document précise « *les dispositions prises par le futur prestataire pour répondre aux exigences de sécurité du donneur d'ordres pendant toute la durée du contrat* »

R2

Mettre à disposition les journaux d'événements et conservation des traces

Clause particulière du marché

Le chef d'établissement ou l'autorité académique est fondé à demander communication des journaux en cas de réquisition par l'autorité judiciaire. Indépendamment d'une réquisition, le chef d'établissement est fondé à obtenir la communication de logs dans le cas d'une enquête administrative.

Le prestataire doit dans sa réponse à appel d'offre préciser :

- Les mécanismes qu'il met en œuvre pour gérer les journaux en particulier dans des environnements mutualisés ;
- La politique de sauvegarde en regard des obligations réglementaires ;
- Le service offert au client afin que celui puisse disposer des journaux le concernant ;

Le porteur de service fournit ses éléments à la demande du chef d'établissement sur enquête ou au chef d'établissement ou à l'autorité académique qui ferait l'objet d'une réquisition.

R3

Réaliser des contrôles

Clause particulière du marché

Les clauses contractuelles doivent garantir que le responsable ou co-responsable de traitement puissent accéder à l'ensemble de la documentation du sous-traitant qui démontre le respect de ces obligations vis-à-vis du RGPD.

Cette documentation comprend à minima :

- Les éléments contractuels de la prestation ;
- Le registre de traitement ;
- Le suivi des incidents ;
- Le suivi des instructions du responsable de traitement ;
- Le suivi des mesures correctives ou préventives ;
- Les mesures de sécurité.

Cette clause doit préciser que les contrôles pourront être réalisées par un tiers qui ne pourra déontologiquement pas être un concurrent du titulaire du marché.

R4

Réaliser des audits

Clause particulière du marché

Il est recommandé dans le cadre du marché de prévoir la réalisation d'audit de sécurité pour contrôler la prise en compte des exigences sécurité du porteur de projet ENT.

Cette faculté est prévue à l'article 19.3 des CGAP-PI qui stipule que :

> *L'acheteur peut effectuer ou de faire effectuer un audit de sécurité auprès du titulaire ou le cas échéant de ses sous-traitants afin de s'assurer de la prise en compte effective du niveau de sécurité requis par l'acheteur.*
> *Le titulaire est informé quinze jours à l'avance (date de l'audit, modalités financières pour l'acheteur et le titulaire, etc.).*

Ces audits doivent pouvoir être réalisés par le porteur de projet ou un tiers mandaté par celui-ci. Les clauses du marché doivent également préciser le périmètre, la périodicité des audits, les modalités de réalisation.

On se référera également pour élaborer ces clauses au guide de l'externalisation de l'ANSSI et plus particulièrement à son §5.8.

R5

Informer le chef d'établissement

Clause particulière du marché – exploitation

Le chef d'établissement doit être informé de tout incident de sécurité ou vulnérabilité affectant un autre établissement dans le cas d'un hébergement mutualisé ou d'une évolution affectant un hébergement mutualisé et des mesures conservatoires ou palliatives prises pour traiter l'incident.

De façon plus générale, Le chef d'établissement doit être informé de tout événement affectant l'hébergement de son ENT y compris dans le cas d'un hébergement mutualisé.

Dans le cas d'une solution progicielle implantée sur le réseau de l'établissement une clause doit prévoir également une information obligatoire du prestataire

Ce devoir d'information s'applique également pour tout incident ou menace potentielle affectant un ENT opéré par le porteur de projet.

L'objet de cette information est double. Sur un plan opérationnel, il s'agit de fournir dans l'attente des correctifs des mesures conservatoires ou les éléments d'appréciation pour décider d'une éventuelle suspension de l'ENT. Sur le plan de la relation avec les usagers, il s'agit de fournir les éléments indispensables pour que le chef d'établissement puisse éventuellement communiquer auprès des parents d'élèves.

R6

Prévenir les attaques

Le contrat passé avec le prestataire lorsqu'il est hébergeur d'une solution ENT doit prévoir une clause spécifiques relatives aux cyber attaques informatiques.

Cette clause pourra décrire :

- La sécurité de l'exploitation et la prévention des attaques ;
- La gestion des évolutions ;
- La gestion des événements et la conservation des journaux ;
- Le traitement général des incidents ou des vulnérabilités de jour zéro.

Lors d'un incident, le porteur de projet doit être en mesure d'exiger la communication des journaux, la participation du prestataire à la gestion de l'incident, voir le déclenchement d'un audit.

Afin de rédiger la clause relative à la prévention des attaques, on se référera particulièrement à l'annexe 3 du guide pour l'externalisation de l'ANSSI.

R7

Gérer la réversibilité

En cas de changement de prestataire, une clause doit être prévue pour la reprise des données et leur transfert sécurisé. Il s'agit de toutes les DCP, ainsi que les données résultant de l'exploitation, du fonctionnement ou de la configuration de l'ENT.

Cette clause précise la clause 8 du CCT au terme de la prestation du service de traitement et la clause 16 en cas de non-respect du marché et de résiliation. Outre les violations de la réglementation RGPD ou des clauses du CCT, le non-respect du plan d'assurance sécurité ou un changement d'actionnariat du prestataire constituent des motifs potentiels d'activation de la clause de réversibilité.

Il doit être possible au porteur de projet de fixer les modalités de transfert des données, de vérification de la qualité des données transférées, et de contrôle de l'effectivité de leur destruction par le sous-traitant.

Dans ce cadre, le prestataire doit :

- Garantir le service et sa qualité jusqu'au terme du marché ;
- Fournir le conseil et l'assistance nécessaire au porteur de projet pour faciliter le transfert des données ;
- Assurer un transfert sécurisé des données au futur prestataire ou au porteur de projet ;

- Conserver les données jusqu'à un terme fixé afin de garantir un contrôle de la qualité des données transférées ;
- Accepter la réalisation d'un contrôle effectif de la destruction des données.

(Voir également recommandations R9 et R10).

Afin de rédiger la clause relative à la réversibilité, on s'appuiera sur le §5.12 du guide pour l'externalisation de l'ANSSI.

R8

Mettre en place une procédure pour le droit d'accès ou de rectification

Le droit d'accès aux données par les usagers est garanti par le responsable de traitement.

Dans le cas d'une co-traitance, les partenaires préciseront le DPD de l'entité chargé.

En complément de la liste tenue par la CNIL et disponible sur la plateforme ouverte des données publiques françaises (site data.gouv.fr), une procédure doit être établie pour préciser les modalités d'exercice ou de rectification.

Cette procédure précise également les modalités de communication entre le prestataire dans le cas où le droit d'accès ou de rectification est exercé auprès de ses services. Elle prévoira si le prestataire peut faire suite à ce droit pour le compte du responsable de traitement et dans le cas contraire comment et dans quel délai il doit prévenir le responsable de traitement.

R9

Organiser la restitution des données

Il est nécessaire de garantir la qualité et l'exploitabilité des données restituées en vue de leur exploitation future.

Afin de réaliser les tests des sauvegardes restituées, une clause peut être ajoutée pour prévoir un délai de rétention pendant une période de six mois à compter de la fin ou de la résiliation du marché.

Ce délai peut être utile pour s'assurer de l'intégrité des données restituée. En tout état de cause, le contrôle des données restituées doit intervenir avant un éventuel contrôle de la destruction des données (voir recommandation R10).

R10

Contrôler la destruction effective des données

La suppression effective des données doit pouvoir être contrôlé par le porteur de projet.

Cette faculté est prévue par l'article 19-3 des CCAG-PI stipule que « *l'acheteur, ou l'organisme mandaté à cette fin, peut, pendant une période de six mois à*

compter de la fin ou de la résiliation du marché, exercer un contrôle dans les locaux du titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées. »

Cet article peut être complété par une clause qui précise :

- La destruction en présence du porteur de projet ou d'un tiers mandaté ;
- La production d'un certificat de destruction des données ;
- La documentation du processus de destruction (identification des systèmes de stockage, dates, heures)

R11

Associer le sous-traitant aux instances de pilotage.

Les collectivités territoriales et les autorités académiques disposent de leur propre instance de gouvernance de la sécurité. Il est impératif d'associer aux instances opérationnelles le sous-traitant, éventuellement ses sous-traitants, pour coordonner les actions prévues au marché en termes de sécurité.

Ces instances de pilotage traite des questions relatives à « la gestion des droits et la gestion des incidents, détection des anomalies et préconisation d'améliorations, exploitation des résultats des audits de contrôle des prestations sécurité » ainsi que des questions relatives au RGPD, à l'homologation et à son suivi.

i

Le guide de l'externalisation de l'ANSSI propose dans son §5.4 une clause comité de suivi qui peut être utilisée pour rédiger une clause du marché afin d'associer le sous-traitant à l'instance ou aux instances de pilotage.

6. Référentiels applicables

Nom	Objet	Ressources/Liens
CCAG -PI	Mesures de sécurité, protection des données	https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043310613
Guide de l'externalisation ANSSI	Règles de sécurité applicables dans le cadre de la sous-traitance	https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf
Clause contractuelle type	Décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux clauses contractuelles types entre les responsables du traitement et les sous-traitants au titre de l'article 28	https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32021D0915
Guide CNIL du sous-traitant	Obligations du sous-traitant dans le cadre du RGPD	https://www.ssi.gouv.fr/uploads/2020/01/anssi-guide-securite_numerique_collectivites_territoriales-reglementation1.pdf (Fiche 2)