Volume 1

GUIDE PRATIQUE

de mise en œuvre de la conformité au RGPD par le Sous-Traitant

Grilles de sélection et Registre des traitements du Sous-Traitant

fntc

Sommaire

QUI SOMMES-NOUS ?

La Fédération des Tiers de Confiance du numérique (FnTC) rassemble éditeurs de logiciels, prestataires de services, experts, professionnels réglementés, utilisateurs et structures institutionnelles.

Créée en 2001, la Fédération des Tiers de Confiance du Numérique (FnTC) est aujourd'hui l'une des organisations les plus visibles de l'écosystème numérique.

La Fédération regroupe plus de 160 adhérents qui prennent une part active dans la définition, la mise en œuvre et la promotion de la confiance dans l'économie numérique : des éditeurs de logiciels, des prestataires de services numériques, des experts, des professionnels réglementés, des start-up, des institutions et des utilisateurs des services de confiance. Cette hétérogénéité des acteurs offre à la Fédération un inestimable gisement de compétences pour favoriser une digitalisation fiable et sécurisée.

Avec un souci constant d'éthique, la FnTC œuvre depuis plus de vingt ans dans les domaines historiques de la dématérialisation (signature électronique, archivage électronique, facture électronique, vote électronique, e-finance).

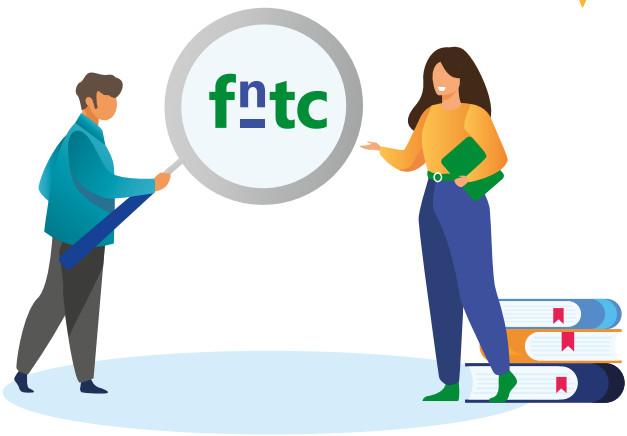
La Fédération agit aujourd'hui également dans les secteurs montants de la digitalisation : Blockchain, KYC, Cachet électronique visible (CEV), e-santé, identité numérique,...

1 PRODUIRE DES EXPERTISES ET DES OUTILS

2 ELABORER DE LA DOCTRINE
Production de différents supports

3 PARTICIPER À LA NORMALISATION ET À LA STANDARDISATION

4 ASSURER DES FORMATIONS UNIVERSITAIRES



GROUPE DE TRAVAIL (GT) RGPD

Lancé en juillet 2018, lors de l'entrée en vigueur du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), le Groupe de travail (GT RGPD) s'est saisi de problématiques spécifiques au Sous-Traitant, un rôle assumé par de nombreux membres de la FnTC.

À la demande des adhérents, un accompagnement s'avérait indispensable, tant sur des questions de fond (périmètres des responsabilités entre le Responsable du Traitement et le Sous-Traitant) que d'un point de vue opérationnel (absence de documentation liée à la conformité).

Le GT RGPD s'est tout d'abord attelé à la réalisation d'**un registre des traitements propre au Sous-Traitant**, ce document incontournable de la conformité RGPD ne faisant l'objet d'aucun modèle opérationnel. Le registre a fait l'objet d'un premier livrable diffusé pour validation auprès des adhérents.

Dans un second temps, le GT RGPD s'est saisi de deux sujets, sources de difficultés pour les Sous-Traitants : **les questionnaires relatifs à la protection des données personnelles imposés par les responsables du traitement** permettant de sélectionner leur prestataire, ainsi que l'épineuse question de **la notification des violations de données personnelles** eu égard aux rôles des parties prenantes (Responsable du Traitement/Sous-Traitant).

Sur le premier sujet, le GT a finalisé un livrable (format tableau) permettant de recenser les questions auxquelles le Sous-Traitant est tenu de répondre et celles relevant de « *bonnes pratiques* » de façon à guider le Sous-Traitant dans ses réponses. S'agissant des Violations de données, les travaux sont toujours en cours. L'objectif en est de proposer aux adhérents un **livrable** qui exposera les éléments essentiels de la notification (partie générale) et des fiches pratiques (partie opérationnelle).

PRÉAMBULE

La Fédération souhaiterait à terme porter un code de conduite lié à ces travaux, et spécifique aux activités de ses adhérents.

Le RGPD est entré en vigueur le 25 mai 2008, des obligations spécifiques sont définies pour le Sous-traitant, dont la tenue du registre des traitements, auxquelles s'ajoutent les obligations d'assistance liées à la sous-traitance vis-à-vis du Responsable du Traitement.

En raison d'un manque de précisions opérationnelles dans le Règlement, et au regard des documents produits par les institutions (CNIL, Comité européen de protection des données), **le GT RGPD de la FnTC a sélectionné des thèmes à traiter afin de permettre au ST d'appréhender au mieux son périmètre d'engagement et de responsabilités** (Partie 1).

Dans un second temps, le GT s'est saisi des problématiques liées aux mesures organisationnelles et de sécurité à mettre en œuvre par le ST pour **accompagner ce dernier dans les réponses à apporter aux demandes (plus ou moins légitimes) de son client, le Responsable du Traitement** (Partie 2).

Enfin, le GT a priorisé la rédaction de **deux modèles de registre** des traitements (approche par client/ Responsable du Traitement, approche par finalité du traitement) à destination des adhérents de la Fédération (Partie 3).

ABRÉVIATIONS

AC

Autorité de contrôle (en France, il s'agit de la Commission Nationale de l'Informatique et des Libertés/ CNIL).

AIPD

Analyse d'impact relative à la protection des données.

BCR

Binding Corporate Rules.

CCT

Clauses contractuelles types.

DCP

Données à caractère personnel.

DPO

Délégué à la protection des données.

PAS

Plan Assurance Sécurité.

PSSI

Politique de Sécurité des Systèmes d'Information.

RGPD

Règlement Général sur la Protection des données.

RT

Responsable du Traitement.

ST

Sous-Traitant.

GLOSSAIRE

Définitions
(dont sources CNIL)

Analyse d'impact relative à la protection des données (AIPD)

AIPD est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée.

Elle concerne les traitements de données personnelles qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Anonymisation

« *L'**anonymisation** est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière irréversible.* »

Binding Corporate Rules (BCR) ou règles d'entreprise contraignantes

Il s'agit de règles internes applicables à l'ensemble des entités d'un groupe qui contiennent les principes clés permettant d'encadrer les transferts de données personnelles vers des pays tiers (qui ne présentent pas un niveau de protection adéquat) ou vers une Organisation internationale.

Clauses contractuelles types du 04/06/2021

Il s'agit de **modèles de clauses contractuelles** adoptés par la Commission européenne permettant d'encadrer :

- la relation RT/ST
- les transferts de DCP vers des pays tiers (qui ne présentent pas un niveau de protection adéquat) ou vers une organisation internationale.

Délégué à la protection des données

Le **délégué à la protection des données** (DPO) est chargé du pilotage de la conformité à la réglementation sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Principe de responsabilité (*Accountability*)

L'***accountability*** désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Protection des données dès la conception (*Privacy by design*)

« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le Responsable du Traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. »

Art. 25-1 RGPD

Protection des données par défaut (*Privacy by default*)

*« Le Responsable du Traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, **par défaut**, seules les **DCP** qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.*

Cela s'applique à la quantité de DCP collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité.

En particulier, ces mesures garantissent que, par défaut, les DCP ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée. »

Art. 25-2 RGPD

Pseudonymisation

La **Pseudonymisation** est : *« Le traitement de DCP de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les DCP ne sont pas attribuées à une personne physique identifiée ou identifiable. »*

Art. 4-5 RGPD

Registre des activités de traitement

Le **Registre des activités de traitement** permet de recenser les traitements de données.

GLOSSAIRE

Responsable du Traitement

Le **Responsable du Traitement** est : « *La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.* »

Art. 4-7 RGPD

Sous-Traitant

Le **Sous-traitant** est : « *La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du Responsable du Traitement.* »

Art. 4-8 RGPD

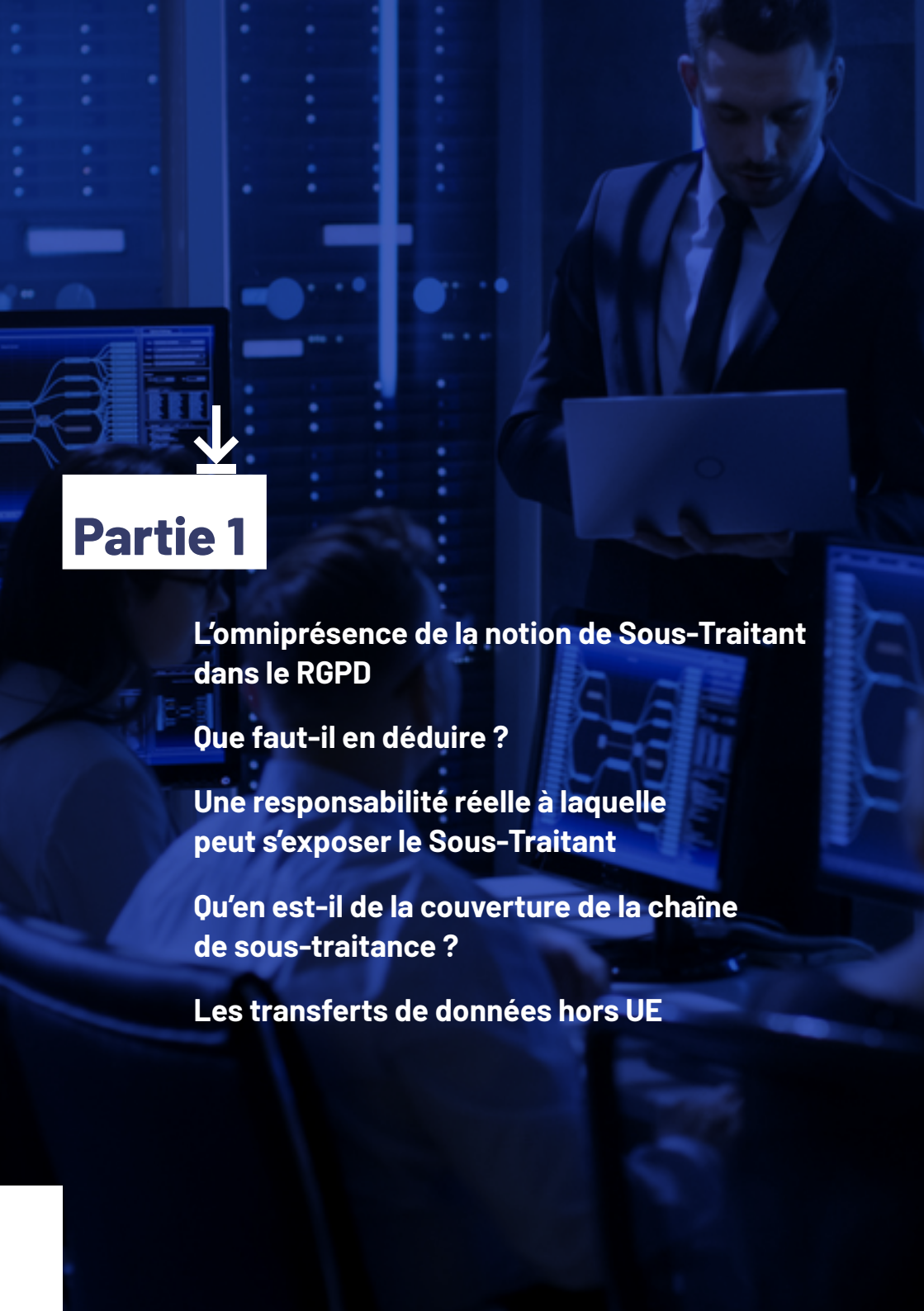
Violation de données à caractère personnel

La **Violation de données à caractères personne**l est : « *Une Violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.* »

Art. 4-12 RGPD.

NOTES

Cet espace vous est dédié pour prendre des notes.



Partie 1

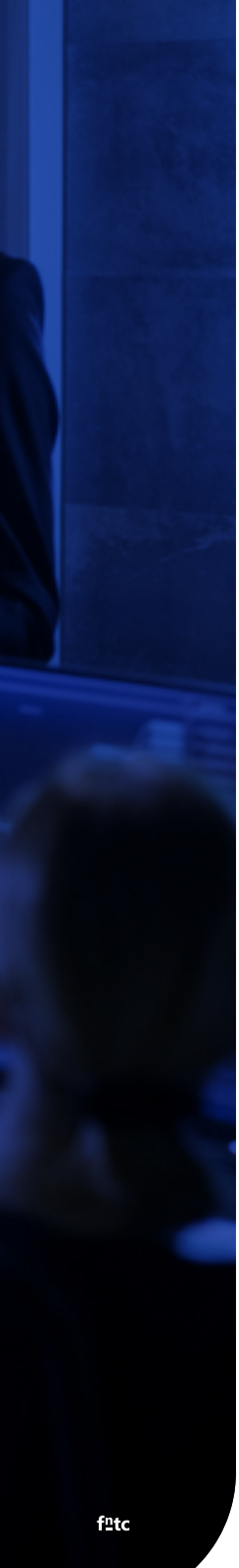
L'omniprésence de la notion de Sous-Traitant dans le RGPD

Que faut-il en déduire ?

Une responsabilité réelle à laquelle peut s'exposer le Sous-Traitant

Qu'en est-il de la couverture de la chaîne de sous-traitance ?

Les transferts de données hors UE



1

LE PÉRIMÈTRE DE L'ENGAGEMENT ET DES RESPONSABILITÉS DU SOUS-TRAITANT

La notion de ST est omniprésente dans le RGPD (plus de 150 occurrences), il n'y a donc aucun doute :

→| le ST est un acteur essentiel de la conformité !

Le RGPD définit des obligations spécifiques pour le ST, telles que la tenue du Registre des traitements de données réalisés pour le compte du RT ou la notification de la Violation de DCP au RT, mais il ne s'y limite pas, bien au contraire !

À y regarder de plus près, l'obligation d'assistance du RT à laquelle est soumis le ST revient à définir un périmètre large de l'engagement et des responsabilités du ST.

LE PÉRIMÈTRE DE L'ENGAGEMENT ET DES RESPONSABILITÉS DU SOUS-TRAITANT

1

L'omniprésence de la notion de Sous-Traitant dans le RGPD

Le tableau ci-dessous présente les différentes références du RGPD en ce qui concerne l'implication du ST dans la conformité légale du RT... Petit panorama donc, sur les obligations directes ou indirectes à prendre en considération en tant que ST.

Dispositions applicables au RT	Implications ST
Principe de responsabilité / *Accountability* Art. 24 Considérant 77	Implication indirecte
Protection dès la conception/ par défaut Art. 25 Considérant 78	Implication indirecte
Responsables conjoints du traitement Art. 26 Considérant 79	Implication indirecte
Analyse d'impact Art. 35-8 Considérant 95	**Implication directe** > « *Le ST doit respecter le code de conduite auquel il a adhéré* »
Consultation préalable de l'AC Art. 36	**Implication directe** Communication de tout document sur les responsabilités respectives RT, ST et RT conjoints

Responsabilité spécifique du ST		
Désignation d'un représentant pour le ST qui n'est pas établi dans L'UE Art. 27	Rôle et dérogations	Considérant 80
Registre des activités de traitement Art. 30-2	Rôle et dérogations	Considérant 82

Dispositions applicables au RT et ST	Implications ST
Transfert de données vers des pays tiers ou Organisation Internationale (OI) **Articles** 44, 46, 47 **et** 49 Considérant 109	**Implication directe** Art. 46 *> Clauses types de protection des données* *> Code de conduite / certification* *> Clauses contractuelles entre le RT et le ST (autorisation de la CNIL requise si les CCT sont modifiées)* Art. 47 *> Règles d'entreprise contraignantes*
Contrat de sous-traitance Art. 28 Considérant 81	**Implication directe – DOCUMENTATION** Art. 28-3 Descriptif du traitement réalisé pour le compte du RT (objet et durée du traitement, nature et finalité du traitement, type de Données, catégories de personnes concernées). *> Fiche du registre correspondante* Art. 28-d) *> Information sur les ST en chaîne (exemple liste des ST) et contrats avec les ST [art. 28-4]* Art. 28-e) *> Procédure de traitement des demandes d'exercice des droits* Art. 28-5 *> Code de conduite applicable* *> Certification*
Sécurité du traitement Article 32 Considérant 83	**Implication directe – DOCUMENTATION** Documentation des mesures techniques et organisationnelles Art. 32 a) à c) *> PSSI ou guide sécurité* Art. 32-d) *> Documentation sur les audits sécurité internes* Art. 32-2 *> Analyse de risque* Art. 32-3 *> Code de conduite applicable* *> Certification*
Notification des Violations de DCP à l'autorité de contrôle Art. 33-2	**Implication directe – DOCUMENTATION** *> Notification dans les meilleurs délais au RT* *> Liste des Violations*

Que faut-il en déduire ?

- Les obligations qui semblent viser exclusivement les RT renvoient pour la majeure partie à une implication du ST dans le processus de conformité (exemple : notification de la Violation de DCP).
- De fait (dispositions et considérants), le ST doit assister le RT pour l'ensemble des obligations qui s'appliquent à ce dernier. Concrètement le ST va devoir communiquer un ensemble de documents lors de son recrutement et, le cas échéant, à la demande du RT, lors de la réalisation des traitements de DCP pour le compte du RT.
- Selon les prestations fournies, le tableau ci-après recense la documentation utile susceptible d'être réclamée au ST par le RT.

Obligation du RT	ST : exemple de document à transmettre
Principe de responsabilité du RT (Art. 24)	Descriptifs des services ou procédures mises en œuvre par le ST, politique de protection des données du ST
Protection dès la conception du traitement/protection par défaut (Art. 25)	Notices techniques des produits/outils
Analyse d'impact relative à la protection des données (Art. 35) – « AIPD »	Toute documentation utile pour la partie « Sécurité » de l'AIPD (exemple : PSSI, PAS)
Consultation préalable de l'AC [risque résiduel élevé sur la vie privée à l'issue de l'analyse d'impact] (Art. 36)	AIPD réalisée par le ST. Toute documentation utile pour la partie « Sécurité » de l'AIPD (exemple : PSSI, PAS)
Sécurité des traitements (Art. 32)	– PSSI, PAS, guide sécurité, toute documentation déterminant les règles de sécurité applicables – Documentation sur les audits internes (rapport d'audit) – Code de conduite / certification

LE PÉRIMÈTRE DE L'ENGAGEMENT ET DES RESPONSABILITÉS DU SOUS-TRAITANT

Obligation du RT	ST : exemple de document à transmettre
Notification des Violations de données (Art. 33)	– Notification formalisée – Liste des Violations
Contrat de sous-traitance (Art. 28)	– Descriptif des traitements réalisés pour le compte du RT ou fiche du Registre ST correspondante – Procédure/politique de restitution/destruction des données
ST en chaîne (Art. 28)	– Liste des ST – Contrats avec les ST – Garanties appropriées (si transfert de données vers Etat tiers)
Exercice des droits des personnes concernées (Art. 12 et Art. 15 et suiv.)	– Procédure de traitement des demandes d'exercice des droits (si prévu au contrat de ST)
Certification/code de conduite (Art. 40 à 42)	– Toute documentation utile pour prouver la certification ou l'adhésion au code de conduite
Transfert de données vers un Etat tiers (Art. 44 et suiv.)	– Garanties appropriées (CCT, BCR) – Clauses contractuelles avec les ST ultérieurs

En fonction de leurs contraintes, de leur activité et de leurs propres obligations légales et contractuelles, il appartient aux ST de vérifier la documentation qu'ils communiquent au RT (voir Partie 2 sur les documents obligatoires et ceux dont la communication relève d'une bonne pratique).

En ce sens, la Fédération recommande de faire référence, dans le Registre, à la documentation attestant de la conformité du ST, non seulement pour maîtriser pleinement son référentiel documentaire (pour la sécurité des traitements, la gestion des Violations de DCP, l'encadrement de la sous-traitance secondaire, etc.), mais aussi pour transmettre et exposer au RT uniquement la documentation strictement nécessaire au périmètre concerné.

Une responsabilité réelle à laquelle peut s'exposer le Sous-Traitant

→| Art. 28-4 RGPD :

« Lorsqu'un ST recrute un autre ST pour mener des activités de traitement spécifiques pour le compte du Responsable du Traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le Responsable du Traitement et le ST conformément au paragraphe 3, sont imposées à cet autre ST par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement.

Lorsque cet autre ST ne remplit pas ses obligations en matière de protection des données, le ST initial demeure pleinement responsable devant le Responsable du Traitement de l'exécution par l'autre ST de ses obligations. »

Qu'en est-il de la couverture de la chaîne de sous-traitance ?

→I ST1 recrute ST2

ST1 est responsable des manquements du ST2.

→I La chaîne de ST est une chaîne de responsabilité mal définie

A priori, avec une lecture littérale de l'article 28 paragraphe 4 du RGPD, le ST1 est responsable de ST2. Le RGPD impose d'encadrer la sous-traitance en chaîne.

Contractuellement, le ST1 doit imposer au ST2 les mêmes obligations relatives à la protection des DCP que celles qui lui sont imposées par le RT.

Un exemple : le RT interdit tout transfert de DCP hors de l'UE. Cette obligation s'applique au ST1 qui doit répercuter cette obligation sur ses propres Sous-Traitants.

En conséquence :

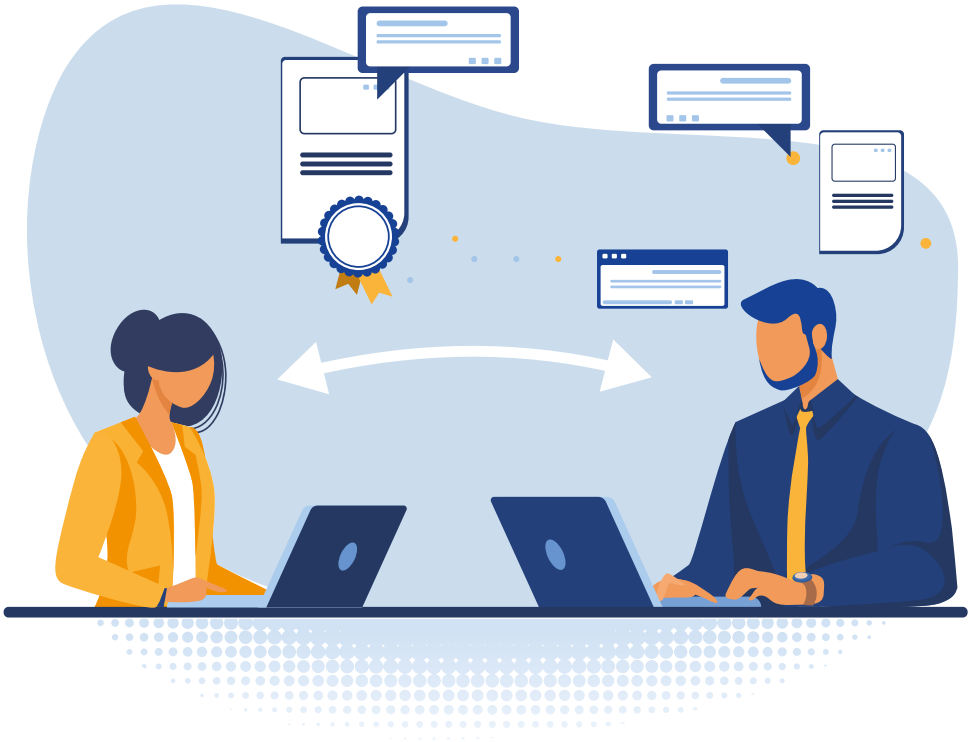
- La couverture contractuelle de la chaîne de ST doit être envisagée.
- Les clauses contractuelles avec les Sous-Traitants secondaires (ST2, ST3, ...) doivent être vérifiées.
- Le ST doit consigner dans le Registre les informations relatives à ses ST secondaires (voir point 2).
- Le ST est tenu à une obligation de transparence vis-à-vis du RT en ce qui concerne ses ST secondaires (voir point 3).

Les travaux réalisés par la Fédération concernant le Registre des Traitements du ST (3) et les mesures organisationnelles & de sécurité à mettre en œuvre par le ST (2) tiennent compte des obligations spécifiques qui s'imposent au ST et s'inscrivent dans le périmètre de l'engagement et des responsabilités de ce dernier (Partie 1).

Les transferts de données hors UE

En ce qui concerne l'encadrement des transferts de données vers des Etats tiers, ce sont les flux sortants de données qui sont visés quelle que soit la qualité de la partie prenante (RT/ST).

- Le ST a les mêmes obligations d'encadrement des transferts de données qu'il opère (CCT, BCR) et est responsable vis-à-vis du RT.
- Pour les CCT, le ST doit se référer au jeu de Clauses de la Commission européenne du 4 juin 2021.



NOTE SUR L'INVALIDATION DU *PRIVACY SHIELD*

1

Dans son arrêt du 16/07/2020, la CJUE a adopté une double position.

Premièrement, la Cour a validé les clauses contractuelles types pour le transfert de données personnelles vers des ST établis dans des pays tiers (Décision 2010/87/UE de la Commission 05/02/2010 modifiée en 2016).

Elle a toutefois précisé que, dans le cas où la réglementation du pays de l'importateur des données impose des mesures contraires aux clauses types, il appartiendra au Responsable du Traitement ou au ST établi dans l'UE de prendre des mesures supplémentaires permettant de pallier l'insuffisance de garanties du pays destinataire.

À défaut de mesures idoines, le RT ou le ST, et, à titre subsidiaire, l'autorité de contrôle compétente « *sont tenus de suspendre ou de mettre fin au transfert de données vers le pays tiers concerné* ».

Deuxièmement, la Cour a invalidé la décision d'adéquation portant sur le Privacy Shield (Décision d'exécution (UE) 2016/1250 de la Commission du 12/07/2016 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis).

Se fondant sur le RGPD (art. 45-2-a) et sur la Charte des droits fondamentaux de l'Union Européenne (art. 7, 8, 47 et 52), la Cour de Justice de l'Union Européenne **a invalidé la décision d'adéquation de la Commission européenne à l'égard des États-Unis** (Privacy Shield).

Suite à l'invalidation du *Privacy Shield*, le ST est également tenu de recourir à des garanties appropriées telles que, notamment les CCT du 4 juin 2021 ou des BCR **pour ses transferts vers les entreprises américaines.** CCT du 4 juin 2021.

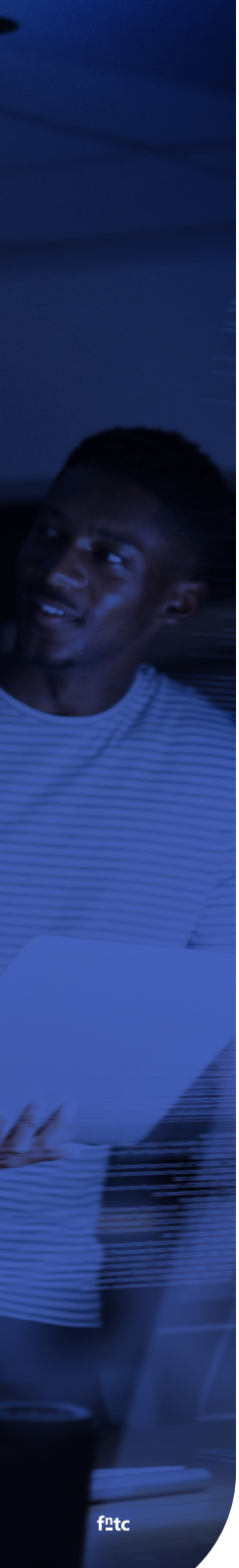
+ Le ST doit consigner dans le registre les informations relatives au transfert des données hors de l'UE (voir Partie 3).

+ Le ST est tenu à une obligation de transparence vis-à-vis du RT en ce qui concerne le transfert des données hors de l'UE (voir Partie 2).

Partie 2

Tableau de mesures organisationnelles

Tableau de mesures de sécurité



2

LES MESURES ORGANISATIONNELLES & DE SÉCURITÉ À METTRE EN ŒUVRE PAR LE SOUS-TRAITANT

Les demandes des responsables du traitement peuvent s'avérer très intrusives et plus exigeantes que les obligations prescrites par le RGPD vis-à-vis des Sous-Traitants. En attestent certains questionnaires transmis par le RT pour sélectionner le ST ou superviser ses activités de traitements.

C'est à partir de ce constat que la Fédération a élaboré les tableaux ci-dessous afin :

→| de distinguer les demandes du RT qui relèvent effectivement d'une obligation légale de celles qui s'inscrivent dans le cadre de bonnes pratiques.

→| de présenter les mesures de sécurité sur lesquelles le ST peut être interrogé par le RT ainsi que les bonnes pratiques en la matière.

LES MESURES ORGANISATIONNELLES & DE SÉCURITÉ À METTRE EN ŒUVRE PAR LE SOUS-TRAITANT

2

Obligatoire ST | Facultatif (bonne pratique)

N°	Questions ?			Commentaires (Dont Références RGPD)
1	Description générale des prestations de l'entreprise			Note explicative à fournir sur l'activité
2	Périmètre couvert par le Prestataire			Note explicative à fournir sur l'activité. Prop indiqué en annexe les éléments du (des) trai → finalité / nature du traitement / catégorie de personnes / durée du (des) traitements(s
	Mesures organisationnelles			
3	Appliquez-vous un Code de conduite au sens du RGPD ?			(Art. 28-5 + Art. 40) Doit permettre de produire une attestation
4	Avez-vous une Certification au sens du RGPD ?			(Art. 28-5 + Art. 42) Doit permettre de produire une attestation
5	Avez-vous désigné un DPO ?			Obligatoire si conditions Art. 37 remplies – Si désignation : Coordonnées DPO à cor
6	Avez-vous un référent interne ?			– Si désignation : Coordonnées référent à
7	Avez-vous sensibilisé votre personnel à la protection des données personnelles ?			– Art. 39-1, qu'il y ait eu, ou non, la désigna – Précisions relatives aux modalités de fo (exemple : fréquence des formations, fo spécifiques ou générales)
8*	Soumettez-vous à une obligation de confidentialité le personnel autorisé à traiter les données ?			(Art. 28-3 (b)) – Obligation de Mention contractuelle (NB : cette obligation peut être légale => te – Communication sur demande RT Recommandation : Liste des personnes hab

TABLEAU DE MESURES ORGANISATIONNELLES

		Motivations (Juridiques, techniques, pratiques...)
		Peut permettre de vérifier les activités de traitement réalisées par le Sous-traitant
osition : il pourrait être tement(s) : es de données / catégories)		Peut permettre de vérifier les activités de traitement réalisées par le Sous-traitant.
de conformité	Oui / Non	**Si le prestataire possède un code de conduite ou une certification liée à la protection des données personnelles (exemple ISO 27701)** : → Produire l'attestation de la certification et/ou le code qui lui permettra de répondre à un certain nombre de question par la mention « *Couvert par la certification X ou le code de conduite* ».
de conformité	Oui / Non	
mmuniquer	Oui / Non	Les précisions relatives aux modalités (exemple : interne/externe, ETP, ...) autres que la désignation et les coordonnées apparaissent inutiles.
a communiquer	Oui / Non	Dans le cas où l'entité ne possède pas officiellement un DPO (exemple entité de quelques personnes), la désignation d'un interlocuteur sous la dénomination « référent interne » a un effet rassurant.
ation d'un DPO ormation ormations	Oui / Non	**Demande optionnelle de fournir la documentation de la formation** qui ne doit pas être intrusive ! → *L'objectif est d'aider le ST à couvrir ses obligations légales et ses bonnes pratiques. La sensibilisation doit rester une bonne pratique.*
xte de référence)	Oui / Non	Possibilité de transmettre la clause de confidentialité à titre de preuve.
ilitées + MAJ		

LES MESURES ORGANISATIONNELLES & DE SÉCURITÉ À METTRE EN ŒUVRE PAR LE SOUS-TRAITANT

2

Obligatoire ST | Facultatif (bonne pratique)

N°	Questions ?	Obligatoire ST	Facultatif (bonne pratique)	Commentaires (Dont Références RGPD)
	Mesures organisationnelles			
9	Pouvez-vous nous fournir l'extrait du registre des traitements objets de la prestation ?			(Art. 30) La communication du registre au RT n'est pa l'article 30 mais un extrait du registre peut ê par le RT
10*	Avez-vous recours à des Sous-Traitants secondaires ?			(Art. 28-2) – Liste des Sous-Traitants secondaires (identification/ coordonnées)
11*	Avez-vous une procédure de demande d'autorisation pour la sous-traitance ultérieure ?			
12*	Comment encadrez-vous les activités sous-traitées ?			☐ Contrat de sous-traitance ☐ DPA (data processing agreement' ou acc traitement de données)
13	Réalisez-vous des traitements hors de l'UE ?			(Art. 44) – Partie relative à la protection des donné sous-traitance (clauses impératives pou & confidentialité, audit) – Obligation de garanties relatives au tran d'adéquation/ CCT / BCR) *NB : peut renvoyer aux Sous-Traitants ultérie*
14*	Si oui, quelles sont les garanties relatives au transfert ?			(Art. 45, 46 et 47) Indiquer les mesures supp adoptées en fonction de la situation de trans (Recommandation du CEPD) ☐ Décision d'adéquation ☐ CCT ☐ BCR
15	Dans le cadre de vos activités, appliquez-vous la Protection des données dès la conception et par défaut (Art. 25) ?			– Procédure documentaire à prévoir : doc notices techniques des produits/outils – A communiquer sur demande du RT

TABLEAU DE MESURES ORGANISATIONNELLES

		Motivations (Juridiques, techniques, pratiques…)
as prévue par, être demandée	Oui / Non	Recommandation FnTC : établir une fiche Registre communicable au RT.
	Oui / Non	Recommandation FnTC : fournir une liste avec leur identification et coordonnées (dans le contrat par exemple).
	Oui / Non	A apprécier au cas par cas.
cord de	Oui / Non	En cas de communication : extrait des clauses RGPD uniquement.
ées du contrat de ur le RT/ sécurité nsfert (Décision urs	Oui / Non	Demander l'entier contrat conclu avec le Sous-Traitant ultérieur est intrusif et donne accès à trop d'informations dont le RT n'a pas à connaître (exemple : données financières) → *L'idée est aussi d'être plus souple dans le cadre général de l'UE et plus strict hors UE.* Fournir la garantie appropriée à la demande du RT (CCT/BCR) et communiquer les mesures supplémentaires recommandées en fonction de la situation de transfert (Recommandation du CEPD).
lémentaires sfert		Indiquer les mesures supplémentaires adoptées en fonction de la situation de transfert (Recommandation du CEPD).
cumentation/	Oui / Non	Ce n'est pas une obligation pour le ST mais c'est très demandé par le RT en pratique dans les contrats.

LES MESURES ORGANISATIONNELLES & DE SÉCURITÉ À METTRE EN ŒUVRE PAR LE SOUS-TRAITANT

2

Obligatoire ST | Facultatif (bonne pratique)

N°	Questions ?	Obligatoire ST	Facultatif (bonne pratique)	Commentaires (Dont Références RGPD)
	Mesures organisationnelles			
16	Avez-vous une politique générale de protection des données ?	■		Art. 28-1 du RGPD
17	Avez-vous une procédure interne de gestion des Violations de données ?		■	Obligation d'assistance
18*	Avez-vous une procédure pour la gestion de l'AIPD ?		■	Obligation d'assistance
19*	Avez-vous une procédure de gestion des demandes d'exercice des droits des personnes au sens du RGPD ?		■	Obligation d'assistance
20	Avez-vous une procédure d'effacement/restitution des données ?	■		Art. 28-3 du RGPD
21	Procédez-vous à des tests réguliers des mesures organisationnelles mises en place ?	■		Art. 32 du RGPD

MODALITÉS

*Cas particulier de la Certification (Art. 42 RGPD) ou de l'Adhésion à un code de conduite (Art. 40 RGPD) : insertion d'une indication de dispense de réponse si certification ou adhésion à un code

Certifications - Liste (non exhaustive) :
- ISO 27001
- ISO 27701
- ...

Code de conduite : *à venir*

TABLEAU DE MESURES ORGANISATIONNELLES

		Motivations (Juridiques, techniques, pratiques...)
	Oui / Non	
	Oui / Non	Recommandation FnTC
	Oui / Non	Recommandation FnTC
	Oui / Non	Recommandation FnTC
	Oui / Non	
	Oui / Non	

LES MESURES ORGANISATIONNELLES & DE SÉCURITÉ À METTRE EN ŒUVRE PAR LE SOUS-TRAITANT

2

Obligatoire ST | Analyse au cas par cas en fonction du tr

N°	Questions ?			Commentaires (Dont Références RGPD)
	Mesures de sécurité techniques			
1	Chiffrement des données			Art. 32
2	Pseudonymisation			Art. 32
3	Anonymisation			Art. 32
4	Cloisonnement physique des données			Art. 32
5	Cloisonnement logique des données			Art. 32
6	Contrôle des accès logiques des utilisateurs internes habilités (salariés, prestataires ou visiteurs)			Art. 32
7	Contrôle des accès logiques des utilisateurs externes habilités (prestataires, visiteurs)			Art. 32
8	Authentification			Art. 32
9	Gestion des mots de passe			Art. 32
10	Traçabilité			Art. 32

TABLEAU DE MESURES DE SÉCURITÉ

raitement et de la sensibilité des données

		Motivations (Juridiques, techniques, pratiques...)
	Oui / Non	En base Canal de transmission Chiffrement systématique ou non Indiquer l'algorithme utilisé
	Oui / Non	Indiquer la méthode utilisée
	Oui / Non	Indiquer la méthode utilisée
	Oui / Non	Serveur dédié Serveur virtuel ou non
	Oui / Non	Sur serveur virtuel dédié Base de données cloisonnées
	Oui / Non	Gestion des profils utilisateurs Outil & procédure Documentation communicable : ☐ Politique de gestion des habilitations ☐ PAS en tout ou partie
	Oui / Non	Documentation communicable : ☐ Politique de gestion des habilitations ☐ PAS en tout ou partie
	Oui / Non	Documentation communicable : ☐ Politique de gestion des habilitations ☐ PAS en tout ou partie
	Oui / Non	Documentation communicable : ☐ Politique de gestion des mots de passe ☐ PAS en tout ou partie
	Oui / Non	Documentation communicable : ☐ Politique de traçabilité ☐ PAS en tout ou partie

LES MESURES ORGANISATIONNELLES & DE SÉCURITÉ À METTRE EN ŒUVRE PAR LE SOUS-TRAITANT

2

Obligatoire ST | Analyse au cas par cas en fonction du tr

N°	Questions ?	Commentaires (Dont Références RGPD)
11	Contrôle d'intégrité	Art. 32
12	Archivage	Art. 32
13	Sécurité des documents papier	Art. 32
14	Destruction des données/documents	Art. 28-3
15	Réversibilité (restitution des données ou transmission à des tiers)	Art. 28-3
	Mesures de sécurité organisationnelles	
16	Sensibilisation/formation du personnel à la sécurité	Quels sont les moyens organisationnels mis Art. 32
17	Gestion des projets/Tests	Tests réalisés sur des données fictives ou a Art. 32 du RGPD
	Mesures de sécurité organisationnelles	

TABLEAU DE MESURES DE SÉCURITÉ

raitement et de la sensibilité des données

		Motivations (Juridiques, techniques, pratiques...)
	Oui / Non	Documentation communicable : ☐ PAS en tout ou partie
	Oui / Non	Documentation communicable : ☐ PAS en tout ou partie ☐ PAS tiers archiveur ☐ Politique de conservation
	Oui / Non	Documentation communicable : ☐ PAS en tout ou partie ☐ Politique de conservation des documents papier
	Oui / Non	Documentation communicable : ☐ PAS en tout ou partie ☐ Procédure de destruction des données (schéma) ☐ PV de destruction des données/documents
	Oui / Non	Documentation communicable : ☐ PAS en tout ou partie ☐ Plan de réversibilité
en place ?	Oui / Non	Exemple : Fréquence des : – Sensibilisations/ formations – moyens – périmètre formation/ sensibilisation – Évaluations du personnel
nonymes	Oui / Non	Documentation communicable : ☐ PAS en tout ou partie

LES MESURES ORGANISATIONNELLES & DE SÉCURITÉ À METTRE EN ŒUVRE PAR LE SOUS-TRAITANT

2

Obligatoire ST | Analyse au cas par cas en fonction du tr

N°	Questions ?			Commentaires (Dont Références RGPD)
18	Gestion des audits			Quels sont les moyens organisationnels mis permettre au RT de réaliser les inspections traitements de DCP confiés au ST ?
19	Gestion des risques			Avez-vous une cartographie des risques cor les DCP ? (atteinte à la confidentialité, à la d et à l'intégrité). Cette cartographie doit perr les mesures de sécurité applicables aux trai des DCP. Art. 32
20	Gestion des incidents et Violations de données			Disposez-vous d'une procédure d'escalade ? Art. 32

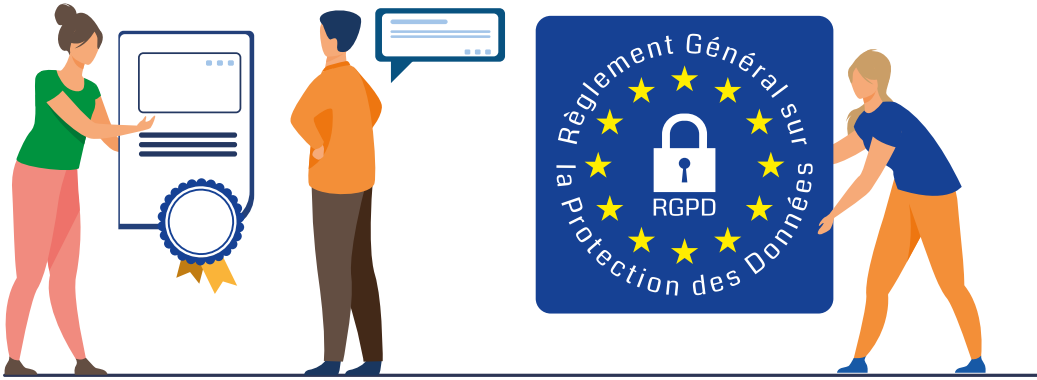


TABLEAU DE MESURES DE SÉCURITÉ

raitement et de la sensibilité des données

		Motivations (Juridiques, techniques, pratiques...)
en place pour relatives aux	Oui / Non	Exemple : Fréquence et périmètre des audits – externes/ internes
ncernant isponibilité mettre d'ajuster itements	Oui / Non	Documentation communicable : ☐ PAS en tout ou partie ☐ PCA ☐ PRA ☐ Politique et/ou procédure de sauvegarde
?	Oui / Non	Documentation communicable : ☐ PAS en tout ou partie ☐ Politique de gestion des Violations

Partie 3 - Modèles de Registres du Sous-Traitant

Une approche par Client/Responsable du traitement (Version 1 du registre)

Une approche par finalité du traitement (Version 2 du registre)

3

LE REGISTRE DES TRAITEMENTS DU SOUS-TRAITANT

Les modèles de registre proposés par la Fédération sont conçus pour être adaptés aux besoins de leurs utilisateurs, en fonction de leurs contraintes, de leur activité et de leurs propres obligations légales et contractuelles, ainsi :

→I **La V1 du modèle de registre** a été élaborée suivant une approche classique qui prévoit une fiche par Client/Responsable de traitement. Dans ce cas, le prestataire (ST) créera une fiche pour chaque client (responsable de traitement) pour le compte duquel il effectue des opérations de traitement.

→I **La V2 du modèle de registre** a été élaborée suivant une approche « Finalité du traitement », et s'adresse spécifiquement aux Sous-Traitants qui effectuent des traitements similaires sur le même type de DCP, pour un nombre important de clients : par exemple, un prestataire ayant plusieurs centaines ou milliers de clients utilisant la version standard de sa solution.

→I **Tous les modèles de tableaux proposés sur les pages 25 à 27 sont téléchargeables sur le lien suivant :** https://fntc-numerique.com/modeles-de-registres-de-sous-traitant/

Une approche par Client/Responsable de traitement (V1) : →I Modèle téléchargeable

Ce modèle de registre est adapté aux prestataires dont les opérations de traitement et/ou leur finalité, sont semblables pour tous leurs clients - ne s'appliquent qu'à un nombre limité de clients.

CLIENT / RESPONSABLE DE TRAIT					
Dénomination sociale / nom de l'entité (OBLIGATOIRE : art. 30-2) Adresse / N° SIREN / Forme juridique / capital social				Représentant Légal (OBLIGATOI Nom & Prénom / Fonction / N° d	
FINALITÉ DU					
Exécution par XXX des prestations définies dans le contrat de XXX. Exemple					
Activité de					
Catégories de traitements effectués pour le compte du CLIENT (OBLIGATOIRE : art. 30-2)	Instructions données par le client	Objet du traitement / finalités (10)	Outil / Application utilisée pour le traitement	Type de données personnelles	Durée du traitement / Durée de conservation (11)
Catégorie 1 : Transmission au client					
Catégorie 2 : Accès donné au client					
Catégorie 3 : Transmission au tiers					
Catégorie 4 : Accès donné au tiers					

propres à chaque client, ainsi qu'aux prestataires dont la finalité et les opérations de traitement - bien que

TEMENT (OBLIGATOIRE : ART. 30-2)

RE : art. 30-2)
e téléphone / E-mail

Délégué à la Protection des Données ou équivalent (OBLIGATOIRE : art. 30-2)
Nom & Prénom / Fonction / N° de téléphone / E-mail

TRAITEMENT

: Déploiement et mise en œuvre de la solution XXX pour le compte du client

traitement

Date de suppression	Catégorie de personnes concernées [12]	Destinataires [13]	Description des mesures de sécurité techniques et Organisationnelles mises en œuvre [14] (OBLIGATOIRE : art. 30-2)	Transferts hors UE : OUI/NON (OBLIGATOIRE : art. 30-2)	Garantie entourant le transfert hors UE [15] (OBLIGATOIRE : art. 30-2)

LE REGISTRE DES TRAITEMENTS DU SOUS-TRAITANT

3

CLIENT / RESPONSABLE DE TRAIT	
Dénomination sociale / nom de l'entité (OBLIGATOIRE : art. 30-2) Adresse / N° SIREN / Forme juridique / capital social	Représentant Légal (OBLIGATOI Nom & Prénom / Fonction / N° d

FINALITÉ DU					
Exécution par XXX des prestations définies dans le contrat de XXX. Exemple					
Activité de					
Catégories de traitements effectués pour le compte du CLIENT (OBLIGATOIRE : art. 30-2)	Instructions données par le client	Objet du traitement / finalités [10]	Outil / Application utilisée pour le traitement	Type de données personnelles	Durée du traitement / Durée de conservation [11]
Catégorie 5 : Structuration [1]					
Catégorie 6 : Stockage [2]					
Catégorie 7 : Consultation					
Catégorie 8 : Utilisation					
Catégorie 9 : Sauvegarde [3]					
Catégorie 10: Déplacement [4]					
Catégorie 11 : Extraction [5]					

VERSION 1

TEMENT (OBLIGATOIRE : ART. 30-2)

RE : art. 30-2)
e téléphone / E-mail

Délégué à la Protection des Données ou équivalent (OBLIGATOIRE : art. 30-2)
Nom & Prénom / Fonction / N° de téléphone / E-mail

TRAITEMENT

: Déploiement et mise en œuvre de la solution XXX pour le compte du client

traitement

Date de suppression	Catégorie de personnes concernées[12]	Destinataires[13]	Description des mesures de sécurité techniques et Organisationnelles mises en œuvre[14] (OBLIGATOIRE : art. 30-2)	Transferts hors UE : OUI/NON (OBLIGATOIRE : art. 30-2)	Garantie entourant le transfert hors UE[15] (OBLIGATOIRE : art. 30-2)

REGISTRE DES TRAITEMENTS DU SOUS-TRAITANT

3

CLIENT / RESPONSABLE DE TRAIT	
Dénomination sociale / nom de l'entité (OBLIGATOIRE : art. 30-2) Adresse / N° SIREN / Forme juridique / capital social	Représentant Légal (OBLIGATOI Nom & Prénom / Fonction / N° d

FINALITÉ DU					
Exécution par XXX des prestations définies dans le contrat de XXX. Exemple					
Activité de					
Catégories de traitements effectués pour le compte du CLIENT (OBLIGATOIRE : art. 30-2)	Instructions données par le client	Objet du traitement / finalités [10]	Outil / Application utilisée pour le traitement	Type de données personnelles	Durée du traitement / Durée de conservation [11]
Catégorie 12 : Restauration [6]					
Catégorie 13 : Destruction [7]					
Catégorie 14 : Restitution [8]					
Catégorie 15 : Interconnexion [9]					

(1) Organisation des données de manière à en faciliter le traitement ou l'utilisation
(2) Conservation des données dans un espace dédié, en vue par exemple d'en permettre l'usage
(3) Conservation des données sur un support afin d'en permettre la récupération en cas de perte ou d'endommagement
(4) Modification de la localisation physique/géographique des données
(5) Transfert permanent ou temporaire des données sur un autre support, par quelque moyen ou sous quelque forme que ce soit
(6) Récupération de données perdues à la suite d'un incident, d'une erreur ou d'une défaillance
(7) Suppression des données à l'issue de la durée de conservation ou sur demande.
(8) Remise des données à l'issue du contrat ou sur demande
(9) Croisement de fichiers de données

VERSION 1

TEMENT (OBLIGATOIRE : ART. 30-2)

RE : art. 30-2)
e téléphone / E-mail

Délégué à la Protection des Données ou équivalent (OBLIGATOIRE : art. 30-2)
Nom & Prénom / Fonction / N° de téléphone / E-mail

TRAITEMENT

: Déploiement et mise en œuvre de la solution XXX pour le compte du client

traitement

Date de suppression	Catégorie de personnes concernées (12)	Destinataires (13)	Description des mesures de sécurité techniques et Organisationnelles mises en œuvre (14) (OBLIGATOIRE : art. 30-2)	Transferts hors UE : OUI/NON (OBLIGATOIRE : art. 30-2)	Garantie entourant le transfert hors UE (15) (OBLIGATOIRE : art. 30-2)

(10) Objectif précis de la catégorie de traitement envisagé
(11) Durée du traitement: durée de l'opération sur les données. Durée de conservation : Durée de rétention des données. La durée de conservation peut ou pas correspondre à la durée du traitement
(12) Employés, clients, utilisateurs, usagers, cocontractants, bailleurs, locataires, étudiants, stagiaires…
(13) Entités internes (services…) ou externes à l'organisme, ayant accès aux données , ou à qui les données sont transmises
(14) Contrôle d'accès physique et logique, cloisonnement des données, engagements de confidentialité, chiffrement, sauvegarde sur support sécurisés…
(15) Décision d'adéquation de l'UE, Règles d'entreprise contraignantes (BCR), Clauses Contractuelles Types (CCT) Consentement documenté des personnes concernées

LE REGISTRE DES TRAITEMENTS DU SOUS-TRAITANT

Une approche par finalité du traitement (V2) : → Modèle téléchargeable

Ce modèle de registre est adapté aux prestataires pour lesquels il n'est pas possible de remplir une fiche
Cette partie décrit la finalité du traitement (commune à tous les responsables de traitement) et reprend la

				FINALITÉ DU
Exécution par la Société X des prestations définies dans le contrat standard				
				Clients / Responsa
N°	Date d'inscription au registre	Dénomination sociale / Nom de l'entité / N° SIREN (OBLIGATOIRE : art. 30-2)	Forme juridique / Capital social	Nom et coordonnées du représentant légal (OBLIGATOIRE : art. 30-2)
1				
2				
3				
4				
5				
7				
8				
9				
10				

par client. Il comprend deux parties - par exemple, pour les prestations «standard».
a liste de tous les clients concernés ainsi que les informations qui leur sont propres.

TRAITEMENT				
Définition de la prestation				
bles du traitement				
Nom et coordonnées du DPO (OBLIGATOIRE : art. 30-2)	Date de mise en œuvre du traitement	Date de fin / Durée de conservation des données	Date de suppression	Instructions / Mises à jour

REGISTRE DES TRAITEMENTS DU SOUS-TRAITANT

Activités de traitement : →I Modèle téléchargeable

Cette partie décrit les traitements standard réalisés pour le compte des clients identifiés dans la V2.

					Activité de
Catégories de traitements effectués pour le compte du CLIENT (OBLIGATOIRE : art. 30-2)	Instructions OUI/NON	Objet du traitement/ finalités	Outil / Application utilisée pour le traitement	Durée du traitement/ Durée de conservation	Date de suppression
Catégorie 1 : Transmission au client		Exemple : Communication au Client d'un rapport par e-mail sécurisé	Exemple : Application d'envoi de courrier, d'e-mail sécurisé		
Catégorie 2 : Accès donné au client		Exemple : Accès à son coffre-fort électronique	Exemple : Outil de gestion des habilitations/ contrôles d'accès		
Catégorie 3 : Transmission au tiers		Exemple : Communication au partenaire d'un client	Exemple : Application d'envoi de courrier, d'e-mail sécurisé		
Catégorie 4 : Accès donné au tiers		Exemple : Maintenance, contrôle par un Administrateur	Exemple : Outil de gestion des habilitations/ contrôles d'accès		
Catégorie 5 : Structuration		Exemple : Classification par ordre chronologique, alphabétique...	Exemple : Logiciel de gestion de base de données		
Catégorie 6 : Stockage		Exemple : Hébergement / Création et mise à la disposition du Client d'un coffre-fort électronique	Exemple : Cloud public/ privé		
Catégorie 7 : Consultation		Exemple : Mise en œuvre du support Client	Exemple : Application d'exécution du support		

traitement

Type de données personnelles	Catégorie de personnes concernées	Destinataires	Description des mesures de sécurité techniques / organisationnelles mises en œuvre (OBLIGATOIRE : art. 30-2)	Transferts hors UE : OUI/NON (OBLIGATOIRE : art. 30-2)	Garantie entourant le transfert (OBLIGATOIRE : art. 30-2)
		Exemple : Organisme chargé de la maintenance, Administrateur			
		Exemple : Hébergeur			
		Exemple : Service en charge du support			

REGISTRE DES TRAITEMENTS DU SOUS-TRAITANT

3

					Activité de
Catégories de traitements effectués pour le compte du CLIENT (OBLIGATOIRE : art. 30-2)	Instructions OUI/NON	Objet du traitement/ finalités	Outil / Application utilisée pour le traitement	Durée du traitement/ Durée de conservation	Date de suppression
Catégorie 8 : Utilisation		Exemple: Mise en œuvre du support Client, Opérations marketing, Réalisation de statistiques	Exemple : Outil d'élaboration de statistiques, d'IA, tableaux de bord, analyse et rapprochements		
Catégorie 9 : Sauvegarde		Exemple: Mise en place d'une sauvegarde	Exemple : Serveur redondant		
Catégorie 10: Déplacement		Exemple: Transfert à une filiale			
Catégorie 11 : Extraction		Exemple: Mise en œuvre de l'export CSV			
Catégorie 12 : Restauration		Exemple: Exécution du support (demande de restauration en cas de suppression accidentelle)	Hébergeur		
Catégorie 13 : Destruction		Exemple: Suppression à la fin de la durée contractuelle	Exemple : Outil de suppression logique des données		
Catégorie 14 : Interconnexion		Exemple: Croisement de deux fichiers de données complémentaires pour en obtenir un troisième			
Catégorie 15 : Restitution					

VERSION 2

traitement

Type de données personnelles	Catégorie de personnes concernées	Destinataires	Description des mesures de sécurité techniques / organisationnelles mises en œuvre (OBLIGATOIRE : art. 30-2)	Transferts hors UE : OUI/NON (OBLIGATOIRE : art. 30-2)	Garantie entourant le transfert (OBLIGATOIRE : art. 30-2)
		Exemple : Direction Marketing			
		Exemple : Hébergeur			
		Exemple : Filiale			
		Exemple : Prestataire d'un service complémentaire			

CONCLUSION

Ce livrable est le résultat des sessions de travail du GT RGPD organisées par la FnTC depuis 2018. Son objectif est de synthétiser les questionnements des participants - majoritairement des Sous-Traitants au sens du RGPD - sur les concepts et les principes juridiques issus du RGPD.

Le livrable entend également partager les retours d'expérience des différents participants (juristes, avocats, consultants en cybersécurité, DPO…) pour accompagner les membres de la FnTC dans leur mise en conformité réglementaire.

Ainsi, il propose les outils opérationnels suivants :

- des tableaux permettant de distinguer les réponses obligatoires aux questions posées par le Responsable du Traitement pour sélectionner son Sous-Traitant (les « garanties suffisantes » requises par l'article 28 du RGPD), de celles relevant de bonnes pratiques encouragées par la FnTC ;
- deux modèles de « Registre du Sous-Traitant ».

Le dispositif issu du RGPD reste complexe à mettre en œuvre, en particulier pour les TPE/PME. Nous sommes heureux de partager ce livrable… À consommer sans modération !

fntc
Fédération des Tiers de Confiance du Numérique

NOTES

Cet espace vous est dédié pour prendre des notes.

REMERCIEMENTS

Mars 2023

Comité de rédaction

Isabelle CANTERO – *Cabinet Caprioli & Associés*
Nathalie KRIEF – *Sellsy*
Coralie PELUCHON – *ChamberSign*

Membres du groupe ayant contribué à l'élaboration du livrable

Björn Andreas - Worldline
Franklin Brousse - Rgpdcheck
Isabelle Cantero - Cabinet Caprioli & Associés
Véronique Dumond - Worldline
Gabriel Gil - GLI Services
Thierry Hasson - Silae
Nathalie Krief - Sellsy
Sébastien Lode - Carte Blanche Partenaires
Pierrette Ngo Bakodock - WeProov
Coralie Peluchon - Chambersign
Andréa Philippe - Primobox
Guillaume Vallini - Aamex
Eric Zeyl - MyDataisRich

Fédération des Tiers de Confiance du numérique
14 rue de Bruxelles
75009 – PARIS
Tél. : 01 47 50 00 50

infos@fntc-numerique.com
www.fntc-numerique.com

FÉDÉRATION DES TIERS DE CONFIANCE DU NUMÉRIQUE