Contrat de concession avec travaux en matière de traitement des déchets ménagers et assimilés

Convention de délégation de service public

Les stipulations relatives au RGPD de l'article 74.3 du contrat de concession sont remplacées par celles de l'annexe 38.3 ci-dessous.

Annexe 38. 3. Protection des données personnelles

1. Textes applicables

Les Parties se conforment à la réglementation en vigueur en matière de protection des données à caractère personnel, applicable dans le cadre de l'exécution du Contrat de concession, s'agissant notamment des textes suivants :

- Le 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, dénommé « règlement général sur la protection des données » ci-après « RGPD »,
- Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil,
- Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, modifiée par la directive 2009/136/CE du 25 novembre 2009,
- La loi n°78-17 du 6 janvier 1978 dite "loi informatique et libertés" modifiée,
- Le décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi 78-17 modifiée,

Également :

- Les lignes directrices adoptées le 4 mai 2020 par le Comité européen de la protection des données ;
- Les lignes directrices adoptées par la Commission nationale de l'informatique et des libertés par délibération.

2. Préambule

La présente annexe a pour objet de déterminer les obligations des parties aux fins de répondre aux exigences du RGPD et de garantir la protection des droits des personnes concernées.

Elle détermine plus particulièrement les droits et obligations des Parties

- En cas de responsabilité conjointe, afin de garantir le respect de l'article 26 du RGPD,
- Lorsque les Parties sont responsables de traitement autonomes.

Les clauses n'exemptent pas les Parties des obligations auxquelles elles sont soumises en vertu du RGPD ou d'autres législations.

La présente annexe sera complétée par les cinq sous-annexes suivantes :

Annexe 38. 3. Protection des données personnelles	
Sous-annexe 38.3.A. **(**)**	Eléments détaillés de l'engagement général des parties.
Sous-annexe 38.3.B. **(*)**	Identification détaillée du périmètre de responsabilité conjointe des Parties selon la typologie du RGPD.
Sous-annexe 38.3.C. **(**)**	Matrice de l'identification détaillée des traitements objets d'une responsabilité conjointe.
Sous-annexe 38.3.D.	Clauses « Sécurité et connaissance des systèmes d'information, Clausier à destination des contrats de délégation de Service public ».
Sous-annexe 38.3.E. **(**)**	Fichier (matrice) « Mesures Organisationnelles Sécurité RGPD ».

(*) Annexe dont le contenu sera délivré par les parties au cours de l'exécution du contrat.

(**) Annexe portant matrice des livrables contractuels.

3. Stipulations applicables aux cas de responsabilité conjointe des Parties

Le régime des traitements en cas de responsabilité conjointe est déterminé selon les clauses suivantes.

3.1 Principe général d'identification de la responsabilité conjointe des Parties

Certains traitements réalisés aux fins de la bonne exécution des missions de service public caractérisent une convergence décisionnelle, au sein de laquelle les décisions des Parties se complètent l'une l'autre, et sont nécessaires pour la caractérisation des traitements de données à caractère personnel. Dès lors, chaque Partie a un impact tangible sur la détermination des finalités et des moyens de ces traitements, au sens de l'article 26 du RGPD.

Les Parties sont donc responsables conjoints de ces traitements.

Ces traitements sont documentés conformément à l'article 3.9 de la présente. Cette documentation identifie les périmètres d'intervention de chaque responsable conjoint au sein d'un traitement.

Chaque Partie s'engage à établir un registre des activités de traitement au sens de l'article 30 du RGPD (ci-après le Registre) détaillant ces traitements conformément à la matrice de la sous-annexe 38.3.C. Chaque partie communique à l'autre Partie les éléments utiles à l'inscription au Registre.

Toute modification d'un traitement figurant à ce Registre, par l'une ou l'autre des Parties est réalisée en conformité avec les présentes clauses, et requiert l'information préalable de l'autre Partie, avant sa mise en production.

Cette modification est également documentée conformément à l'article 3.9 de la présente. Elle a pour effet de mettre à jour le Registre.

3.2 Principe général de pilotage par le Délégataire des traitements faisant l'objet d'une responsabilité conjointe

Dans l'hypothèse d'une responsabilité conjointe, le Délégataire est réputé garant du pilotage du traitement.

A ce titre il assure, avec l'aide du Délégant pour la part qui lui incombe :

- L'information des personnes concernées (cf. § 3.4 infra) ;
- Le traitement des demandes d'exercice des droits des personnes concernées (cf. § 3.5 infra) ;
- La gestion des violations de données (cf. § 3.6 infra) ;
- Le point de contact des personnes concernées (cf. § 3.7 infra) ;
- L'établissement des éléments permettant la tenue du Registre (cf. § 3.9 infra) ;
- La réalisation des études d'impact sur la protection des données (cf. § 3.16 infra).

3.3 Transfert de données vers des pays tiers ou à des organisations internationales

Tout transfert de données à caractère personnel effectué par les Parties ou par leurs sous-traitants vers des pays tiers ou à des organisations internationales doit toujours se faire conformément au chapitre V du RGPD.
Les transferts de données à caractère personnel vers un pays tiers, y compris, le cas échéant, l'outil de transfert prévu au chapitre V du RGPD sur lequel ils sont fondés, sont documentés dans le Registre comprenant notamment les éléments de la matrice de la sous-annexe 38.3.C.

3.4 Information des personnes concernées

Le Délégataire informe les personnes concernées conformément à la section II du chapitre III du RGPD. Il veille à leur communiquer que :

- les Parties sont responsables conjoints au sens de l'article 26 du RGPD ;
- dans ce cadre, il a un rôle de garant du traitement tel que défini au chapitre 3.2;
- leur point de contact est le Délégataire.

Le Délégataire veille également à la mise à disposition de la présente annexe ou au moins de ses grandes lignes aux personnes concernées afin qu'elles bénéficient d'une information exhaustive sur les rapports entretenus entre les responsables conjoints du traitement.

Le Délégant s'engage à transmettre au Délégataire les éléments nécessaires à l'information des personnes concernées, pour la partie du traitement qui lui incombe.
Le Délégataire n'est pas tenu de procéder à l'information des institutions représentatives des agents du Délégant, qui s'en charge.

3.5 Exercice des droits des personnes concernées.

Tenant compte de la nature du traitement, le Délégataire s'acquitte de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III du RGPD. Il est l'interlocuteur de la personne concernée, et se trouve en charge de la réponse.

Le Délégataire informe annuellement le Délégant du nombre des demandes de droits exercées, ainsi que des suites qui leur ont été données.

Lorsqu'une personne concernée décide d'exercer ses droits auprès du Délégant conformément à l'article 26 3 du RGPD, ce dernier transmet cette demande au Délégataire dans les meilleurs délais et dans un délai maximum de cinq (5) jours à l'adresse rvd.donnees-personnelles@veolia.com, qui fait toute diligence pour traiter la demande conformément à la réglementation.

Le Délégant s'engage à transmettre au Délégataire les éléments nécessaires au traitement de la demande de la personne concernée dans le cas où celle-ci porterait en tout ou partie sur le périmètre du Délégant.

Chaque Partie informe l'autre Partie dans les meilleurs délais de la saisine de la CNIL par une personne concernée.

3.6 Violations de données

3.6.1.

Chaque Partie, pour la part du traitement qui lui incombe s'acquitte des obligations suivantes dans les conditions prescrites par l'article 33 et 34 du RGPD :
- notifier la violation de données à caractère personnel à la CNIL, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.
-communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

Chaque partie informe le DPO (contact.CNIL@bordeaux-metropole.fr / rvd.dpo@veolia.com) et le RSSI (contact.ssi@bordeaux-metropole.fr / fr.rvd.ssi@veolia.com) de l'autre Partie dans les meilleurs délais de toute violation de données après en avoir pris connaissance, et de toute action réalisée en rapport avec la violation de données. Il communique dans les meilleurs délais à l'autre Partie toute la documentation produite à cette occasion.

Par la suite, les Parties se concertent afin de limiter au maximum la propagation de la violation, mais également afin d'évaluer la situation.

Le Délégant peut proposer des mesures visant à remédier à la violation ou le cas échéant à atténuer les éventuelles conséquences négatives. En cas d'accord avec le Délégataire les mesures doivent être mises en œuvre dès que possible.

En tout état de cause, chaque Partie s'engage à :
- procéder aux diligences d'usage aux fins d'identification de l'origine et de l'étendue de la violation de données à caractère personnel sur son périmètre,
- définir et adopter, à ses frais, toutes mesures permettant de remédier à la violation de données dans les plus brefs délais, ainsi que des mesures permettant d'éviter leur survenance dans le futur sur son périmètre.

3.6.2.
Dans le cas où la violation de données concerne tout ou partie du périmètre du Délégant, ce dernier s'engage à :
- en informer le Délégataire dans les meilleurs délais,
- procéder aux diligences d'usage aux fins d'identification de l'origine et de l'étendue de la violation de données à caractère personnel, sur son périmètre, et en informer le Délégataire dans les meilleurs délais,
- définir et adopter, à ses frais, toutes mesures permettant de remédier à la violation de données dans les plus brefs délais, ainsi que des mesures permettant d'éviter leur survenance dans le futur, sur son périmètre, et en informer le Délégataire dans les meilleurs délais.

3.7 Point de contact des personnes concernées

Le Délégataire est garant de constituer le point de contact auprès des personnes concernés, au sens de l'article 132 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

3.8 Sous-traitance

Les Parties se conforment à l'article 28 du RGPD.

Les Parties s'informent de tout changement prévu concernant l'ajout ou le remplacement de sous-traitants ultérieurs au moins 1 mois à l'avance, sauf cas de force majeure. Chaque partie apporte les modifications à son Registre conformément à l'article 3.9.

Une copie du contrat avec un sous-traitant et de ses éventuelles modifications est transmise à l'autre Partie, à sa demande, sous réserve de l'occultation des secrets protégés par la loi.

3.9 Registre

Chaque Partie s'engage à tenir à jour un registre des traitements concernés par la responsabilité conjointe, conformément à la matrice de la sous-annexe 38.3.C.

L'établissement du registre donne lieu à des échanges entre les Parties.

Chaque Partie peut accéder au registre de l'autre Partie à simple demande.

Tout au long de l'exécution du Contrat de concession, chaque Partie transmet à l'autre Partie les informations, matrices complétées et documentation nécessaires à la tenue ainsi que la mise à jour du Registre.

La documentation nécessaire à la tenue du Registre comprend le cas échéant l'analyse d'impact sur la protection des données, et dans tous les cas, le renseignement du fichier « Mesures Organisationnelles Sécurité RGPD ».

3.10 Finalités

Chaque Partie ne peut utiliser les données à caractère personnel que pour les finalités limitativement énumérées dans les sous-annexes.

Toute nouvelle finalité doit faire l'objet d'un accord préalable de l'autre Partie et exige une mise à jour du registre, y compris pour une finalité compatible au sens des articles 5 1.b) et 6 du RGPD lorsqu'elle comporte une incidence sur l'économie du Contrat. Dans ce cas la Partie proposant la nouvelle finalité a la charge de documenter et de communiquer à l'autre Partie le test de compatibilité.

3.11 Confidentialité

Les Parties s'engagent à prendre toutes précautions utiles afin de préserver la sécurité des données à caractère personnel, et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

Les Parties ne donnent accès aux données à caractère personnel traitées que sur la base du besoin d'en connaître, au profit :

- de personnes qui relèvent de leur autorité, et qui se sont engagées à respecter la confidentialité des données,

- de personnes tierces qui ont une obligation légale ou contractuelle appropriée de confidentialité.

Dans le cas où la réalisation du traitement nécessiterait l'octroi de droits d'accès à des personnes relevant de l'autorité du Délégant sur des systèmes gérés par le Délégataire, le Délégant s'engage à transmettre la liste à jour des personnes autorisées au Délégataire ainsi que les mouvements au fil de l'eau.

La liste des personnes auxquelles un accès a été accordé doit faire l'objet d'un examen à minima semestriel. Sur la base de cet examen, l'accès aux données à caractère personnel peut être retiré, si l'accès n'est plus nécessaire, et ces personnes ne peuvent donc plus avoir accès aux données à caractère personnel.

Particulièrement, les Parties s'engagent à demander à l'ensemble de leur personnel et des tierces personnes qu'elles habilitent :

- de ne prendre aucune copie des documents ou fichiers de données à caractère personnel,
- de ne pas utiliser les données à caractère personnel à d'autres fins que celles définies par le Contrat de concession listées dans les sous-annexes et figurant au Registre

- de ne pas divulguer ces informations à d'autres personnes.

Les Parties s'engagent à veiller à ce que leur personnel reçoive une information nécessaire en matière de protection des données à caractère personnel.

En particulier, les Parties veillent à apporter une formation et une sensibilisation des agents accédant aux données dans le cadre de leurs attributions, aux règles de mise en œuvre d'un système de vidéosurveillance.

Chaque partie peut demander à l'autre de prouver sur pièces que les personnes concernées relevant de son autorité sont soumises à la confidentialité mentionnée ci-dessus.

3.12 Sécurité

Les Parties s'engagent à mettre en œuvre les mesures de sécurité nécessaires pour se conformer à la réglementation en vigueur en matière de protection des données à caractère personnel et à les imposer par contrat à ses éventuels sous-traitants.

Ainsi et conformément à l'article 32 du RGPD, 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, pour les droits et libertés des personnes physiques, les Parties mettent en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Pour le périmètre qui lui échoit et identifié au Registre, chaque Partie adresse à l'autre ces mesures et toute la documentation afférente pour les traitements effectués dans le cadre de la responsabilité conjointe en renseignant le document « Mesures Organisationnelles Sécurité RGPD ».

Chaque partie doit respecter à minima l'ensemble des clauses « Sécurité et connaissance des systèmes d'information, Clausier à destination des contrats de délégation de Service public » rédigées par la Direction Générale Numérique et Systèmes d'Information de Bordeaux Métropole.

3.13 Renvoi des données au Délégant en fin de Contrat

Au terme normal ou anticipé du Contrat de concession, le Délégataire est tenu de renvoyer toutes les données à caractère personnel au Délégant et de détruire les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation de certaines de ces données à caractère personnel. Dans une telle hypothèse, le Délégataire s'engage à traiter exclusivement les données à caractère personnel pour les finalités et la durée prévues par cette législation et dans les strictes conditions applicables.

Les données de vidéosurveillance ne seront pas à renvoyer au Délégant en fin de Contrat de concession.

Le Délégataire convient avec tout fournisseur /sous-traitant, ou sous-traitant ultérieur de clauses lui permettant de s'acquitter des obligations stipulées au présent article, et notamment, de donner instruction au fournisseur/sous-traitant, ou au sous-traitant ultérieur, de supprimer ou de renvoyer les données à caractère personnel.

Ces clauses stipulent que ces prestations s'effectuent sans coût pour le Délégant.

3.15 Contrôle, audit et vérification

Pendant la durée résiduelle du contrat, s'il le juge nécessaire, le Délégant peut décider après en avoir informé le Délégataire et dans la limite d'une fois, de réaliser un audit des traitements de données à caractère personnel, sur le plan de leur conformité à la réglementation.

Le Délégataire met à la disposition du Délégant toutes les informations et la documentation nécessaires pour démontrer le respect des obligations prévues au RGPD et fixées dans la présente annexe.

Le Délégataire veille à faciliter la réalisation des audits/inspections, par le Délégant ou un autre auditeur qu'il a mandaté soumis à une obligation de confidentialité adéquate, et à contribuer à ces audits.

Sur la base des résultats de ces audits/inspections, le Délégant peut proposer au Délégataire que des mesures supplémentaires soient prises pour garantir le respect de la réglementation en matière de protection des données, ainsi que le respect du Contrat de concession. Ces mesures seront dûment justifiées par le Délégant et leurs modalités de mise en œuvre dans le cadre du Contrat seront déterminées conjointement par les Parties aux frais exclusifs du Délégataire, qu'il soit responsable de traitement conjoint ou sous-traitant, ou aux frais de sous-traitants et/ou sous-traitants ultérieurs. Ces mesures peuvent concerner tant le Délégataire que ses sous-traitants et sous-traitants ultérieurs.

Le Délégant ou son représentant a en outre accès aux lieux où le traitement de données à caractère personnel est effectué par le Délégataire, ses sous-traitants et ses sous-traitants ultérieurs, y compris les installations physiques ainsi que les systèmes utilisés pour le traitement et liés à celui-ci, afin de les inspecter, y compris physiquement.

Le Délégant prend en charge, le cas échéant, les frais qu'il a engagés aux fins de la réalisation des audits/inspections. Le Délégataire veillera à dégager les ressources (principalement le temps) raisonnables pour que le Délégant puisse y procéder, sans droit à indemnisation.

Dans le cadre de ces audits/inspections et conformément aux exigences du RGPD, le Délégant ou son représentant n'accèdent qu'aux seules données à caractère personnel strictement nécessaires à la bonne réalisation du contrôle ou de l'audit/inspection en cause, dans le respect de la réglementation applicable et de l'article 3.11 de la présente annexe.

3.16 Analyse d'impact

Le Délégataire, en collaboration avec le délégant, réalise les analyses d'impacts lorsqu'elles sont requises au sens de l'article 35 du RGPD, notamment pour les traitements relatifs à la vidéosurveillance. Il s'engage à prendre en compte les risques liés aux droits et libertés des personnes physiques inhérents à l'ensemble des processus du traitement en responsabilité conjointe, y compris ceux relevant du périmètre de traitement du Concédant éventuellement identifié, et ce, sur la base des informations transmises par le Délégant. A ce titre, le Délégant s'engage à transmettre toutes les informations nécessaires au Délégataire.

Le Délégant s'engage à faire toute diligence pour collaborer à la mise en œuvre de l'analyse d'impact.

Dans ce cadre, les traitements portant vidéosurveillance font l'objet d'une analyse d'impact conduite par le Délégataire.

La validation de l'étude d'impact et la mise en œuvre du plan d'action afférent, échoient aux parties.

Après concertation avec le Délégant, le Délégataire consulte la CNIL, préalablement à la mise en œuvre du traitement, lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

3.17 Coopération avec les autorités de contrôle (notamment : CNIL, DGCCRF, ARCEP, ANSSI)

Dans le cas d'un contrôle par une autorité compétente, les Parties s'engagent :
- à coopérer avec l'autorité de contrôle,
- à s'informer réciproquement dans les meilleurs délais. Le Délégataire informe en particulier DPO (contact.CNIL@bordeaux-metropole.fr) et le RSSI (contact.ssi@bordeaux-metropole.fr) du Délégant. Le délégant informe en particulier le : DPO (rvd.dpo@veolia.com) et DSSI (fr.rvd.ssi@veolia.com) du délégataire.
- à faire toute diligence pour permettre à ses représentants d'être présents lors du contrôle,
- à se concerter afin de fournir ensemble les informations et les documents demandés par l'Autorité.

Les parties sont tenues de fournir à l'Autorité un accès à leurs installations physiques, sur présentation d'un document d'identification approprié.

-

4. Obligations des Parties lorsqu'elles se trouvent responsables de traitement autonome

Chaque partie est responsable de traitement autonome pour les traitements réalisés dans le cadre de ce Contrat de concession qui ne sont pas mentionnés en responsabilité conjointe de traitement dans l'annexe 38.3.B.A ce titre, les Parties reconnaissent que chacune est responsable de son propre Traitement et que leurs Traitements respectifs demeureront strictement séparés pendant toute la durée de l'exécution du Contrat.

Chaque Partie déclare par ailleurs que l'utilisation et le traitement des Données à Caractère Personnel qu'elle collecte pour ses activités s'opère et continuera à s'opérer conformément à la Législation en Vigueur sur la Protection des Données.
Chacune des Parties sera dès lors l'unique Responsable de ses propres Traitements en particulier à l'égard des personnes physiques dont les Données à Caractère Personnel sont collectées et traitées, notamment pour leur information et l'exercice des droits qui leur sont reconnus par la Loi en Vigueur sur la Protection des Données (droit d'accès, de rectification, d'effacement…).

Chaque Partie garantit l'autre Partie en cas de réclamation ou de litige en lien avec leurs traitements de ces données. En tout état de cause, les Parties coopéreront de bonne foi, et en particulier, s'obligent à transmettre dans les meilleurs délais toute demande qu'elles recevraient mais qui serait destinée à l'autre Partie.

SOUS-ANNEXE 38.3.A.

ELEMENTS DETAILLES DE L'ENGAGEMENT GENERAL DES PARTIES

A.1. Protocole détaillé de gestion du Registre des traitements :

[PROTOCOLE DE GESTION DU REGISTRE]

[LOGICIEL DE GESTION DU REGISTRE]

[PROTOCOLE D'ECHANGE AVEC LE DELEGANT AUX FINS DE LUI FACILITER LA COMPLETION DE SON REGISTRE MIROIR EN TANT QUE RESPONSABLE CONJOINT]

A.2. Protocole détaillé de gestion des violations de données :

[PROTOCOLE DE GESTION DES VIOLATIONS DE DONNEES]

[PROTOCOLE D'INFORMATION ET D'ECHANGE AVEC LE CONCEDANT EN CAS DE VIOLATIONS DE DONNEES]

A.3. Protocole détaillé de gestion des demandes d'exercice de droit des personnes concernées :

[PROTOCOLE DE GESTION DES DEMANDES D'EXERCICE DE DROIT DES PERSONNES CONCERNEES]

[PROTOCOLE D'INFORMATION PERIODIQUE DU CONCEDANT QUANT AUX DEMANDES D'EXERCICE DE DROIT DES PERSONNES CONCERNEES]

SOUS-ANNEXE 38.3.B.

IDENTIFICATION DETAILLEE DU PERIMETRE DE RESPONSABILITE CONJOINTE DES PARTIES SELON LA TYPOLOGIE DU RGPD

Le tableau ci-dessous dresse l'inventaire détaillé des responsabilités des Parties au regard des traitements en responsabilité conjointe générés par le Contrat, selon la typologie du RGPD :

Tableau récapitulatif des traitements				
N°	**Traitement**	**Délégant**	**Délégataire**	**BLOC SI**
	[FINALITÉ DU TRAITEMENT] [SOUS-FINALITES DU TRAITEMENT [NATURE DU TRAITEMENT]	Choisir : a. Conjoint non garant (principe) b. Responsable Conjoint garant (exception)	Choisir : a. Conjoint garant (principe) b. Responsable Conjoint non garant (exception)	Choisir : #1 #2 #3
NOTA : CES ÉLÉMENTS DOIVENT ÊTRE COMPLÉTÉS POUR CHACUN DES TRAITEMENTS.				
1	**VIDEO SURVEILLANCE DES SITES Bègles et Cenon (hors contrôle vidéo du Décret 2021-345 du 30 mars 2021 codifié à l'article D. 541-48-1 du code de l'environnement)** **Finalité du traitement :** **Nature du traitement :** **Accès aux données**	**a) Délégant Responsable Conjoint non garant**	**a) Délégataire Responsable Conjoint garant.** - Assurer la sécurité du site, des biens et des personnes (ex : accident, intrusion, incendie, etc.) - Veiller au fonctionnement des machines industrielles - Gestion flux de circulation des véhicules, entrées et sorties Vidéosurveillance des sites VALBOM Bègles et Cenon, dont notamment : collecte, enregistrement, conservation, consultation, extraction, rapprochement, communication, modification, suppression. **OUI**	#2

SOUS-ANNEXE 38.3.C.

MATRICE D'IDENTIFICATION DETAILLEE DES TRAITEMENTS CONCERNES PAR LA RESPONSABILITE CONJOINTE.

C1. Le responsable conjoint garant du traitement est :

[RESPONSABLES CONJOINTS]

[RESPONSABLE CONJOINT GARANT].

[NOTE: PAR PRINCIPE LE DELEGATAIRE EST LE GARANT DU TRAITEMENT EN CAS DE RESPONSABILITE CONJOINTE.]

C2. La finalité du traitement est :

[FINALITÉ DU TRAITEMENT].

C3. Le traitement des données concerne principalement (la nature du traitement) :

[NATURE DU TRAITEMENT].

C4. Le traitement de données a pour fondement légal :

[FONDEMENT LEGAL DU TRAITEMENT].

C5. Le traitement comprend les types suivants de données à caractère personnel relatives aux personnes concernées :

[TYPE DE DONNÉES À CARACTÈRE PERSONNEL TRAITÉES].

C6. Le traitement comprend les catégories de personnes concernées suivantes :

[CATÉGORIES DE PERSONNES CONCERNÉES].

C7. Sécurité du traitement

Le niveau de sécurité doit tenir compte :
[RENSEIGNEMENT IMPERATIF DU FICHIER « Mesures Organisationnelles Sécurité RGPD »]
[EN TENANT COMPTE DE LA NATURE, DE LA PORTÉE, DU CONTEXTE ET DES FINALITÉS DES ACTIVITÉS DE TRAITEMENT AINSI QUE DES RISQUES POUR LES DROITS ET LIBERTÉS DES PERSONNES PHYSIQUES, DESCRIPTION DES ÉLÉMENTS ESSENTIELS POUR LE NIVEAU DE SÉCURITÉ]

C8. Durée de conservation/procédures relatives à l'effacement

[PÉRIODE DE CONSERVATION/LES PROCÉDURES RELATIVES À L'EFFACEMENT]

9. Lieu du traitement

[LIEU DU TRAITEMENT]

[DELEGANT, DELEGATAIRE OU LE SOUS-TRAITANT UTILISANT L'ADRESSE EN QUESTION]

10. Transfert de données à caractère personnel vers des pays tiers

[IDENTIFICATION DU TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL VERS UN PAYS TIERS OU À UNE ORGANISATION INTERNATIONALE]

[BASE JURIDIQUE POUR LE TRANSFERT EN VERTU DU CHAPITRE V DU RGPD]

11. Sous-traitants

Dès l'entrée en vigueur des **présentes clauses**, le Délégant recourt aux sous-traitants suivants :

NOM	**Nº D'ENTREPRISE**	**ADRESSE**	**DESCRIPTION DU TRAITEMENT**

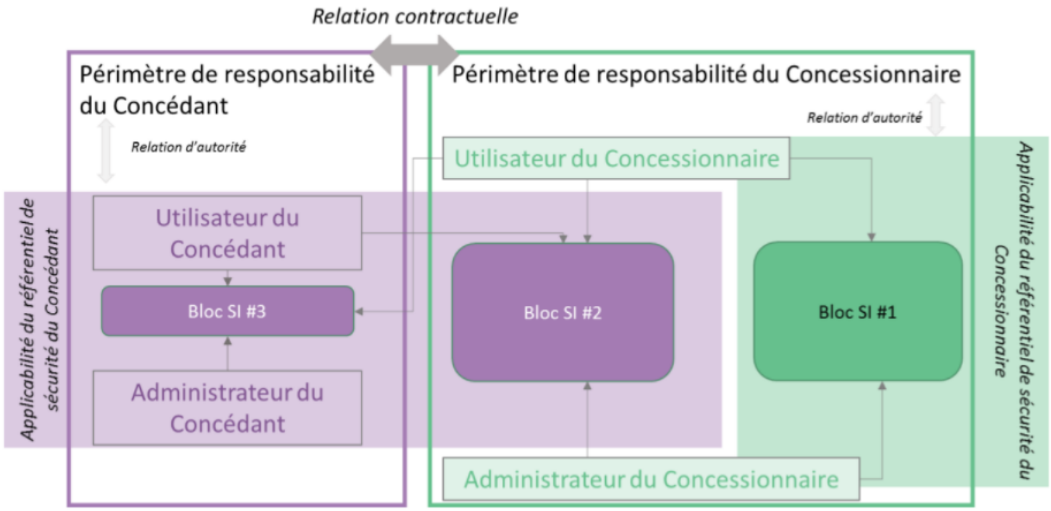
DGNSI - Service commun

Annexe 38.3.D - SECURITE ET CONNAISSANCE DES SYSTEMES D'INFORMATION

Clausier à destination des contrats de délégation de service public

Table des matières

1 Périmètre de responsabilité



Les clauses de sécurité de ce présent document s'appliquent au bloc SI#2 uniquement.

2 Analyse de risque et Plan d'Assurance Sécurité

Le délégataire doit conduire, dans les 8 mois suivant le démarrage de la délégation, une analyse de risques de sécurité de l'information sur les systèmes d'information sous sa responsabilité.

Dans le cadre de cette analyse de risque, il produit un radar de maturité basé sur les exigences ISO27001.

Le délégataire doit revoir cette analyse de risques initiale et le radar de maturité SSI au minimum tous les deux ans et en cas d'évolution majeure de son contexte ou de celui de la prestation.

L'analyse de risque et la constitution du radar de maturité doivent être menées par un prestataire reconnu par l'ANSSI

Livrables :

- Résultat de l'analyse des risques : basée sur la méthode EBIOS RM de préférence et en prenant comme référence les échelles internes de Bordeaux Métropole qui sont précisées dans sa Politique Générale de Sécurité du Système d'Information Mutualisé (PGSSI) en vigueur au moment de l'analyse de risque.

- Radar de maturité : sur les axes évalués, le niveau de maturité attendu est à 3 (Référence CMMI : https://fr.wikipedia.org/wiki/Capability_Maturity_Model_Integration)

- Schéma Directeur du Système d'Information (SDSI) : le délégataire fournit son SDSI présentant sa démarche pour atteindre les objectifs et les exigences précisées par Bordeaux Métropole.

- Proposition d'un plan d'action à détailler dans un document "Plan d'Assurance Sécurité". Le PAS est destiné à servir d'outil de pilotage entre le délégataire et Bordeaux Métropole sur les chantiers liés à la sécurité des SI. Le PAS présente les projets à mener dans le cadre de la délégation pour assurer un niveau de sécurité conforme aux exigences et permettant de répondre aux conclusions de l'analyse de risque. Les projets sont classés par axe thématiques et présentent des éléments budgétaire (cout estimé et suivi), des éléments de suivi de mise en place (statut) et des éléments de gouvernance (responsabilités liées au projet). Le PAS est présenté dans un format à valider par les deux parties.

3 Hébergement des systèmes d'information

Le délégataire précise sa stratégie vis-à-vis de l'hébergement des systèmes d'information sous sa responsabilité, notamment en ce qui concerne l'utilisation des services de cloud.

Il se base pour cela sur les informations transmises par Bordeaux Métropole dans les annexes au contrat qui concernent les systèmes d'information.

Cette stratégie est proposée à Bordeaux Métropole pour validation.

Livrable : note décrivant l'approche mise en place

4 Exigences de sécurité

4.1 Organisation et politiques de la sécurité

4.1.1 Politiques de sécurité

Le délégataire rédige et met à jour des politiques de sécurité qui s'appliquent aux SI sous sa responsabilité.

Sur les SIIV : respect de la règle "1. Règle relative à la politique de sécurité des systèmes d'information" de l'arrêté sectoriel du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Transports terrestres » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense.

4.1.2 Rôles liés aux aspects sécurité du contrat

Le délégataire doit désigner une personne garante du respect des clauses contractuelles liées à la sécurité des systèmes d'information désignée par "Responsable sécurité des systèmes d'information du contrat".

Il décrit son organisation interne en termes de management de la sécurité : fonctions et équipes liées à la sécurité. Il précise notamment son organisation en termes de SOC.

Livrable : note décrivant l'approche mise en place

4.1.3 Pilotage de la sécurité

Le délégataire propose une gouvernance dédiée à la gestion du PAS :

- COTECH PAS : comité de suivi des actions du PAS, focus sur sujets particuliers à la demande de Bordeaux Métropole ou du Délégataire (ex : résultats exercices PRA, résultats de tests de vulnérabilités), arbitrages à mener, présentation d'indicateurs de sécurité, etc. La fréquence, les participants et la structure des supports de ces comités sont définis et validés par les deux parties.

- Ateliers de travail sur des sujets nécessitant la participation des deux parties. Ils portent sur des points d'attention remontés notamment lors des COTECH. Ils réunissent les experts de BM et du Délégataire sur des sujets particuliers. Ils ont pour objectif de déterminer des plans d'action (qui seront intégrés dans le plan d'action global suivi en comité) ou de présenter des éléments factuels en vue d'un arbitrage.

- Production d'indicateurs : le délégataire propose une liste d'indicateurs relatifs au pilotage de la sécurité pour validation. Il produit et met à disposition ces indicateurs qui peuvent être commentés lors des Cotech. Ils portent notamment sur : les incidents de sécurité, la gestion des vulnérabilités et le déploiement des correctifs et mises à jour, les droits d'accès et les authentifications des utilisateurs du SI dont le délégataire a la responsabilité, les opérations de sensibilisation sur la sécurité, etc. (Note : sur les SIIV, respect de la règle "20. Règle relative aux indicateurs" de l'arrêté sectoriel)

4.1.4 Respect des exigences de sécurité et responsabilité

Le délégataire s'engage à respecter l'ensemble des exigences de sécurité de l'information de Bordeaux Métropole, décrites dans la PGSSI (Politique Générale de Sécurité du Système d'Information mutualisé de Bordeaux Métropole) et à les faire respecter par des tiers intervenants sur le SI.

Il porte la responsabilité du respect des clauses de ce contrat, y compris lorsqu'il fait appel à des tiers pour la fourniture de services et produits prévus au contrat.

Le délégataire s'engage à faire respecter par les personnes sous sa responsabilité les obligations relatives à la confidentialité, notamment :

- Ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la présente prestation prévue au contrat, l'accord préalable du maître du fichier est nécessaire ;

- Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;

- Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;

- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;

- Prendre toutes mesures de sécurité, notamment matérielle, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;

- au terme du marché et/ou de la prestation concernée à procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies, et à ne divulguer aucune de ces informations de quelque manière que ce soit, et ce, sans limitation de durée, sauf accord écrit de Bordeaux Métropole.

4.1.5 Exigences légales et réglementaires

Le délégataire doit s'assurer du respect des exigences légales et réglementaires en vigueur dans le cadre de l'exécution du présent contrat. En particulier, ces exigences légales et réglementaires prévalent sur toute autre clause du présent contrat.

4.1.6 Homologation

Le délégataire doit vérifier la conformité du traitement de l'information et des procédures dont il est chargé au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité.

Si des SI sous sa responsabilité sont concernés par des homologations réglementaires (ex : LPM, NIS), il en informe Bordeaux Métropole pour valider les modalités, notamment en ce qui concerne les audits associés et les modalités de l'homologation (autorité et commission d'homologation)

Sur les SIIV : respect de la règle "2. Règle relative à l'homologation de sécurité" de l'arrêté sectoriel

4.1.7 Sensibilisation des utilisateurs

Le délégataire doit définir et mettre en œuvre un plan de sensibilisation à la sécurité de l'information. Il peut être amené à présenter sa démarche et des indicateurs de résultats d'opération de sensibilisation au cours de COTECH.

4.2 Gestion des actifs

4.2.1 Cartographie et inventaire

Le délégataire définit et met à jour au minimum de façon annuelle :

Processus métier :

-Cartographie des processus métier qui doit établir le lien entre ses activités et les composants des systèmes d'information qui les supportent.

Applications :

-Inventaire des composants logiciels des SI sous sa responsabilité : son identifiant unique, son éditeur, son numéro de version lorsqu'applicable, sa description fonctionnelle, ses échanges avec les autres composants des systèmes d'information (fournisseur et consommateur de l'information traitée), la nature fonctionnelle des informations manipulées, la liste des composants matériels que le supportent. Cet inventaire doit être complété par les services logiciels fournis par des prestataires et utilisés dans le cadre des processus métier du délégataire

-Cartographie applicative fonctionnelle (basée sur l'inventaire des composants logiciels).

Composants matériels :

-Inventaire des composants matériels des SI sous sa responsabilité : sa typologie, son identifiant unique, son fabricant, son modèle, la version de son système d'exploitation, ses principaux paramètres de configuration, des informations relatives à sa localisation.

-Cartographie technique des composants matériels (basée sur l'inventaire des composants matériels).

Données :

- Inventaire des données utilisées et traitées dans le cadre de ses processus métiers : sa nature fonctionnelle, les processus contribuant à leur cycle de vie (création / collecte, enrichissement, traitement, utilisation, archivage, destruction).

- En complément de son inventaire des données, le délégataire doit préciser pour chaque type de donnée inventorié son éligibilité (a priori) à sa mise en ligne, conformément aux lois et règlements relatifs à l'Open Data. Lorsque l'éligibilité à la mise en ligne de données est avérée et que la mise en ligne de ces données est réalisée par Bordeaux Métropole, le délégataire doit périodiquement mettre à disposition de Bordeaux Métropole ces données dans un format conforme aux exigences légales et réglementaires en vigueur. Il est précisé que, lorsque nécessaire, l'anonymisation des données sera réalisée par Bordeaux Métropole.

- Note : Les données nécessaires à la fourniture du service par le délégataire pour le compte de Bordeaux Métropole sont considérées comme des biens de retours.

Le délégataire doit mettre à disposition de Bordeaux Métropole les informations relatives aux cartographies et inventaires sous la forme de données structurées. Il s'appuie pour cela sur les outils définis par Bordeaux Métropole.

Sur les SIIV : respect de la règle "3. Règle relative à la cartographie" de l'arrêté sectoriel

4.2.2 Contrôle de l'utilisation des SI

Le délégataire doit contrôler l'utilisation des systèmes d'information sous sa responsabilité afin de détecter : les comportements inappropriés, notamment ceux contraires aux règles de bon usage, les tentatives de fraude et les fraudes avérées.

Il peut être amené à présenter sa démarche (méthode et outils) au cours de COTECH.

4.2.3 Protection des informations stockées sur des équipements mobiles

Le délégataire doit s'assurer que les informations sensibles stockées sur des équipements mobiles sont chiffrées (terminaux, support de stockage amovibles).

4.2.4 Protection des terminaux

Le délégataire doit s'assurer que les terminaux permettant d'accéder aux systèmes d'information sous sa responsabilité sont munis d'un dispositif antiviral actif, mis à jour

régulièrement ainsi que d'un dispositif de filtrage de flux (pare-feu). En cas de contraintes techniques majeures, le délégataire devra mettre en œuvre des solutions alternatives permettant de réduire les risques d'infection virale.

4.2.5 Postes d'administration

Le délégataire doit s'assurer que les opérations d'exploitation et d'administration sont réalisées à partir de terminaux dédiés à ces tâches. L'environnement logiciel pour effectuer ces opérations ne doit pas être utilisé à d'autres fins, comme l'accès à des sites ou serveurs de messagerie sur internet.

Sur les SIIV : respect de la règle "15. Règle relative aux systèmes d'information d'administration" de l'arrêté sectoriel.

4.3 Contrôle d'accès

4.3.1 Accès et authentification

Le délégataire met en œuvre une politique des accès qui s'applique au SI sous sa responsabilité. Cette politique aborde notamment les sujets suivants :

- Un processus permettant de gérer les droits d'accès des personnes accédant aux systèmes d'information sous sa responsabilité, quel que soit leur statut et ceci en cohérence avec leur cycle de vie (arrivée, changement de poste, absence longue durée, départ) est défini.

- Les accès aux applications se font par SSO.

- Les accès se font par des identifiants uniques et personnels.

- Les mots de passe d'accès aux applications respectent à minima les exigences en vigueur de la CNIL (https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires).

- Les flux d'accès aux applications sont chiffrés.

- Le modèle de moindre privilège est appliqué pour l'exécution et l'accès aux applications.

- Les utilisateurs doivent avoir uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation.

- Une revue périodique des comptes et des droits d'applicatifs est réalisée.

- Des dispositifs empêchant l'accès direct aux systèmes d'information sous sa responsabilité depuis l'extérieur sont en place.

- Le mécanisme d'authentification aux terminaux doit être protégé contre les attaques par force brute et les sessions doivent se verrouiller automatiquement après une période d'inactivité donnée.

- L'allocation et l'utilisation des droits d'accès à privilèges doivent être restreintes et contrôlées.

Livrable : politique associée ou note décrivant l'approche mise en place

Sur les SIIV : respect des règles "11. Règle relative à l'identification", "12. Règle relative à l'authentification", "13. Règle relative aux droits d'accès", "18. Règle relative aux accès à distance" de l'arrêté sectoriel.

4.3.2 Comptes d'administration et avec privilèges

Le délégataire dispose d'un politique ou charte consacrée à la gestion des comptes d'administration et avec privilèges et les applique sur les SI sous sa responsabilité.

Livrable : politique / charte associée ou note décrivant l'approche mise en place

Sur les SIIV : respect de la règle "14. Règle relative aux comptes d'administration" de l'arrêté sectoriel

4.4 Développement, maintenance et exploitation

4.4.1 Procédures d'exploitation

Le délégataire doit définir et mettre à jour des procédures documentées relatives aux tâches d'exploitation et d'administration des systèmes d'information sous sa responsabilité.

4.4.2 Maintenance préventive et corrective

Le délégataire doit définir et mettre en œuvre une stratégie de maintenance préventive et corrective pour les composants des systèmes d'information sous sa responsabilité.

4.4.3 Maintien en condition opérationnelle

Le délégataire met en place une stratégie de MCO sur le SI dont il a la responsabilité permettant de gérer le cycle de vie des composants qui le constitue. Notamment, il procède aux montées de version de l'ensemble des logiciels afin qu'il n'y en ait aucun dont la fin de support annoncée par son éditeur arrive à échéance sous moins d'un an et il procède au remplacement de l'ensemble des matériels afin qu'en fin de concession in n'y en ait aucun dont la fin de support arrive à échéance sous moins d'un an.

4.4.4 Supervision

Le délégataire doit superviser les systèmes d'information sous sa responsabilité notamment afin d'anticiper et de réagir efficacement aux dysfonctionnements et aux dépassements de ses capacités.

Il peut être amené à présenter sa démarche (méthode et outils) au cours de COTECH.

4.4.5 Journalisation des évènements et exploitation des traces

Le délégataire met en place sur les SI sous sa responsabilité un système de journalisation portant notamment sur :

- Tentatives d'accès

- Actions liées à la gestion des comptes et des droits d'accès

- Accès aux ressources

- Modification des règles de sécurité

- Opérations métier sensibles

- Activités des administrateurs

- Etc.

Les traces générées doivent être exploitables et analysées afin de produire des alertes de sécurité le cas échéant.

L'intégrité de ces traces doit être maintenue et celles-ci doivent être conservées dans la limite des durées fixées par la législation et la réglementation applicable.

Le délégataire doit tenir ces traces à disposition de Bordeaux Métropole, notamment dans le cadre de l'auditabilité du présent contrat, et d'investigations numériques.

Livrable : politique associée ou note décrivant l'approche mise en place (organisation / équipes en place, évènements journalisés, contenu des traces, centralisation / conservation / protection des traces, corrélation et analyse des traces, etc.)

Sur les SIIV : respect des règles "5. Règle relative à la journalisation", "7. Règle relative à la détection", "6. Règle relative à la corrélation et l'analyse de journaux" de l'arrêté sectoriel.

4.4.6 Gestion des vulnérabilités

Le délégataire doit définir et mettre en œuvre un processus de gestion des vulnérabilités sur les SI sous sa responsabilité :

- Veille, remontée d'information de la part des collaborateurs, évaluation de la criticité, qualification et déploiement des correctifs

- Réalisation d'audit de sécurité et mise en œuvre priorisée de recommandations

- Communication à destination de Bordeaux Métropole sur les vulnérabilités détectées et les mesures prises

Il peut être amené à présenter sa démarche (méthode et outils) et des indicateurs de suivi au cours de COTECH.

Livrable : politique associée ou note décrivant l'approche mise en place

Sur les SIIV : respect de la règle "4. Règle relative au maintien en conditions de sécurité" de l'arrêté sectoriel.

4.4.7 Sécurité dans les projets

Le délégataire s'engage à appliquer des principes de Security & Privacy by design dans sa gestion de projet et dès le démarrage du projet.

4.5 Réseaux et communication

4.5.1 Accès à internet

Le délégataire doit s'assurer que les accès Internet depuis les systèmes d'information sous sa responsabilité se font au moyen des services qu'il fournit aux utilisateurs sous sa responsabilité. Ces services doivent limiter les risques d'infections virales par la mise en œuvre de dispositifs de filtrage et de cloisonnement.

Il peut être amené à présenter sa démarche (méthode et outils) au cours de COTECH.

4.5.2 Connexion entre systèmes d'information

Le délégataire doit restreindre au strict nécessaire les connexions entre : les systèmes d'information de Bordeaux Métropole sous sa responsabilité, ses propres systèmes d'information, les autres systèmes d'information qu'il utilise (par exemple : Internet, système d'information partenaire ou d'entités du groupe auquel il appartient). Le délégataire doit également assurer la confidentialité des données sensibles échangées entre ces systèmes d'information.

Sur les SIIV : respect des règles "17. Règle relative au filtrage" et "16. Règle relative au cloisonnement" de l'arrêté sectoriel

4.6 Relation avec les tiers

4.6.1 Sécurité dans les relations avec les fournisseurs

Le délégataire intègre des clauses et des exigences de sécurité dans les contrats passés portant sur le SI sous sa responsabilité. Il les propose à Bordeaux Métropole pour validation.

Si le délégataire souhaite sous-traiter des prestations de services ou des travaux qui lui sont confiés, il en informe Bordeaux Métropole pour validation.

Par ailleurs, il privilégie des solutions françaises et locales dans le choix des outils et des prestations.

Livrable : annexe contractuelle présentant les exigences de sécurité

4.7 Continuité et reprise d'activité, gestion des incidents et des crises

4.7.1 Continuité et reprise d'activité

Le délégataire définit sa stratégie de continuité et de reprise d'activité.

Il identifie au préalable les activités métiers et les SI éligibles à la mise en place de PCA / PRA pour validation auprès de Bordeaux Métropole. Sur ces activités il précise, en coordination avec Bordeaux Métropole, les PDMA (Perte de Données Maximale Admissible) et DMIA (Durée Maximale d'Interruption Admissible).

Cette stratégie aborde notamment la gestion des sauvegardes : les procédures de sauvegarde doivent garantir la confidentialité des données sensibles. Dans le cas où Bordeaux Métropole met à disposition du délégataire plusieurs sites, les supports de sauvegarde doivent être stockés sur un site différent de celui hébergeant les systèmes d'information sous sa responsabilité.

Il procède à des tests annuels de reprise d'activité et communique les résultats lors de Cotech.

Livrable : politique associée ou note décrivant l'approche mise en place.

4.7.2 Redondances

Le délégataire met en œuvre des architectures suffisamment redondées pour répondre aux exigences de disponibilité.

Livrable : note décrivant l'approche mise en place

4.7.3 Gestion des incidents de sécurité et gestion de crise

Le délégataire doit définir et mettre en œuvre un processus de gestion des incidents de sécurité.

Ce processus est partagé avec Bordeaux Métropole et doit aborder au minimum les sujets suivants :

- Qualification de l'incident

- Chronologie de l'incident et réponses apportées

- Modalités de remontée des informations auprès de Bordeaux Métropole

- Actions à mettre en place pour limiter la reproduction

En cas d'incident qualifié de majeur par le délégataire, une procédure de gestion de crise est mise en œuvre.

Livrable : politique associée ou note décrivant l'approche mise en place

Sur les SIIV : respect des règles "8. Règle relative au traitement des incidents de sécurité" et "10. Règle relative à la gestion de crises" de l'arrêté sectoriel

Annexe 38.3.E

CADRE DE REPONSE RGPD - Pièce Contractuelle

	Le prestataire renseigne dans cet onglet les sous-traitants (ST) ultérieurs auxquels il fait appel et les transferts internationaux de données (transmission délibérée ou accès, consultation à distance des données d'un destinataire relevant de la juridiction d'un État hors EEE) qu'il effectue					
N°	**Domaine**	**Libellé mesure**	**Sous-détail**	**Engagement à réaliser la mesure ou présentation de la mesure adoptée (Oui / Non / Sans objet)**	**Justification (si mesure traitée)**	**Commentaire (si mesure non traitée ou sans objet)**
1	Sous-traitant ultérieurs.	Quels sont les destinataires des données autres que sous-traitants	Editeur Filiales de l'éditeur (si oui, préciser) Partenaire de l'éditeur (si oui, préciser) Autres (si oui, préciser)			
2	Sous-traitant ultérieurs.	Quels sont les sous-traitants ultérieurs auxquels vous envisagez de faire appel ?	1/ Identité, coordonnées des sous-traitants ultérieurs			
3	Sous-traitant ultérieurs.	Quels sont les sous-traitants ultérieurs auxquels vous envisagez de faire appel ?	2/ Finalités du traitement et nature des opérations effectuées dans le cadre du traitement			
4	Sous-traitant ultérieurs.	Quels sont les sous-traitants ultérieurs auxquels vous envisagez de faire appel ?	3/ Type de données concernées.			
5	Sous-traitant ultérieurs.	Quels sont les sous-traitants ultérieurs auxquels vous envisagez de faire appel ?	4/ Durée du contrat de sous-traitance ultérieure			
6	Sous-traitant ultérieurs.	Modalités de transfert des données hors EEE	Y a-t-il un transfert de données à un sous-traitant ultérieur situé hors Espace économique européen (EEE) ?			
7	Sous-traitant ultérieurs.	Modalités de transfert des données hors EEE	Quels sont les outils juridiques de transfert prévues par le sous-traitant qui encadrent ces transferts, conformément au chapitre V du RGPD ?			
8	Sous-traitant ultérieurs.	Modalités de transfert des données hors EEE	Quelles sont les mesures de sécurité au titre de l'article 32 du RGPD pour assurer qu'un niveau de protection approprié des données soit appliqué lors du transfert ?			
9	Sous-traitant ultérieurs.	Modalités de transfert des données hors EEE (CJUE, arrêt Schrems II, 2020, C-211/18 ; Recommandations 01/2020 du Comité européen de la protection des données (CEPD) sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'Union européenne, adoptées le 18 juin 2021)	Quelles sont les mesures supplémentaires pertinentes pour garantir un niveau de protection des données équivalent à celui garanti dans l'EEE dès lors qu'il existe une atteinte susceptible de la législation/pratique du pays destinataire à l'efficacité des garanties appropriées visées à l'article 46 du RGPD sur lesquelles les transferts s'appuient ?			
10	Sous-traitant ultérieurs.	Modalités de transfert des données hors EEE (CJUE, arrêt Schrems II, 2020, C-211/18 ; Recommandations 01/2020 du Comité européen de la protection des données (CEPD) sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'Union européenne, adoptées le 18 juin 2021)	Lorsque les sous-traitants ultérieurs sont situés au sein de l'EEE mais soumis à un droit extraterritorial tiers pouvant impliquer des transferts portant atteinte au niveau de protection des données : Quelles sont les mesures supplémentaires pertinentes pour garantir le respect du niveau de protection requis par le droit de l'Union européenne ?			