|  |
| --- |
| DEMANDE VISANT A OBTENIR UNE DÉLIBÉRATIONDU COMITÉ DE SÉCURITÉ DE L’INFORMATION |

|  |
| --- |
| **1. Généralités** |
| 1. Informations relatives au demandeur : dénomination, adresse complète et données de contact (à fournir par demandeur s’il y a plusieurs demandeurs)

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Type de demande
	* Nouvelle délibération
	* Modification d’une délibération existante

La demande concerne la modification de la délibération n° .../... (*numéro de référence*) du .... (*date*). Le demandeur peut obtenir un fichier WORD de la dernière version de la délibération auprès du secrétariat du Comité de sécurité de l’information (ivc@mail.fgov.be). Il est prié d’apporter lui-même les modifications souhaitées dans la version la plus récente de la délibération (en mode « *track changes* ») et de fournir à cet égard une explication détaillée (il n’est alors pas nécessaire de compléter la suite du présent document). ……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Le demandeur dispose-t-il déjà de délibérations ou de protocoles relatifs au traitement de données à caractère personnel ?

Spécifications :……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

|  |
| --- |
| 1. Le demandeur a-t-il déjà accès au registre national pour la réalisation de la finalité du traitement (conformément à une loi, un arrêté royal, une délibération du Comité sectoriel du registre national ou une décision du Ministre de l’Intérieur) ?

Spécifications :………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………Le demandeur est-il déjà autorisé à utiliser le numéro de registre national pour la réalisation de la finalité du traitement (conformément à une loi, un arrêté royal, une délibération du Comité sectoriel du registre national ou une décision du Ministre de l’Intérieur) ?Spécifications :……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Est-il fait appel à un sous-traitant (le demandeur ne traitera pas lui-même les données à caractère personnel ou ne les traitera pas complètement lui-même) ?
* Oui

Spécifications………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………Tâches concrètes qui seront réalisées par le sous-traitant dans le cadre de la présente demande :………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Non
 |

|  |
| --- |
| **2. Déroulement de la communication de données à caractère personnel** |
| 1. S’agit-il de catégories spécifiques de données à caractère personnel ?
	* Non, aucune catégorie spécifique de données à caractère personnel n’est traitée
	* Oui, des catégories spécifiques de données à caractère personnel sont (aussi) traitées
		1. données à caractère personnel relatives à la santé
		2. données à caractère personnel relatives aux condamnations pénales et aux infractions pénales ou aux mesures de sécurité y relatives
		3. autres :

………………………………………………………………………………….......………………………………………………………………………………….......……………………………………………………………………………………… |
| 1. Personnes dont les données à caractère personnel seront traitées:
* Qualité des personnes[[1]](#footnote-1) + motivation des critères de sélection[[2]](#footnote-2)

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Nombre + motivation de la nécessité de ce nombre

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Procédure de sélection

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

|  |  |  |
| --- | --- | --- |
| 1. Instances concernées (organisation qui communique les données à caractère personnel / organisation qui reçoit les données à caractère personnel)

|  |  |
| --- | --- |
| Les données proviennent * des personnes concernées
* de la BCSS / d'une institution publique de sécurité sociale du réseau primaire de la sécurité sociale
* d'une autre institution de sécurité sociale (non publique)
* de services publics et d’institutions publiques de l’autorité fédérale hors secteur social
* autres

Spécifications……………………………………….……………………………………….………………………………………. | Destinataire* les personnes concernées
* la BCSS / une institution publique de sécurité sociale du réseau primaire de la sécurité sociale
* une autre institution de sécurité sociale (non publique)
* des services publics et institutions publiques de l’autorité fédérale hors secteur social
* autres

Spécifications…………………………………….....……………………………………….………………………………………. |

 |
| 1. Données des instances auxquelles des données à caractère personnel sont demandées:

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Données des personnes de contact par instance, avec numéro de téléphone et adresse e-mail

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Aperçu schématique des flux de données + explication

……………………………………………………………………………………………………….……………………………………………………………………………………………………….………………………………………………………………………………………………………. |

|  |
| --- |
| **3. Finalité** |
| 1. Finalités générales

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Fondement légal pour le traitement de données (avec référence à l’article précis du RGPD)
2. S’agit-il de données à caractère personnel qui ont trait aux caractéristiques suivantes de l’individu: origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, l’appartenance syndicale, données concernant la santé, ou données concernant la vie sexuelle ou l’orientation sexuelle
* OUI :
	+ - * consentement de l'intéressé
			* obligations du droit du travail, du droit de la sécurité sociale ou du droit à la protection sociale
			* en vue de la défense des intérêts vitaux de la personne concernée ou d'une personne qui n’est pas en mesure de donner son consentement
			* le traitement est effectué par une fondation, une association ou une autre instance sans but lucratif active au niveau politique, philosophique, religieux ou syndical
			* le traitement porte sur des données à caractère personnel manifestement rendues publiques par la personne concernée
			* en rapport avec une action juridique ou dans le cadre d’une compétence juridique d’un tribunal
			* motifs d’intérêt public
			* finalités de médecine préventive ou de médecine du travail
			* motifs d’intérêt public au niveau de la santé publique
			* recherche scientifique ou historique ou fins statistiques
				+ L’avis d'un comité d’éthique est-il requis ?
* Oui -> joindre l’avis lors de l’introduction de la demande
* Non
	+ - NON :
			* consentement de l'intéressé
			* en vue de l’exécution d’un contrat 🡪 (à joindre)
			* en vue de l’exécution d’obligations légales[[3]](#footnote-3)
			* en vue de la défense d’intérêts vitaux
			* en vue l'accomplissement d’une mission d'intérêt public ou d’une mission relevant de l’autorité publique
			* aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant
 |
| 1. Réglementation applicable

La référence à la réglementation (jusqu’au niveau des articles applicables) doit permettre au Comité de sécurité de l’information d’évaluer le respect des principes de *limitation des finalités* et de *minimisation des données*.……………………………………………………………………………………………………….……………………………………………………………………………………………………….……………………………………………………………………………………………………….La réglementation doit en tout cas être définitive[[4]](#footnote-4). En principe, la délibération n’entre en vigueur qu’à la date d’entrée en vigueur de la réglementation. Ce n’est qu’à partir de cette date qu’il est permis de traiter des données à caractère personnel sur la base de la délibération.Ce n’est qu’à titre exceptionnel (!) que le demandeur peut demander au Comité de sécurité de l’information de pouvoir traiter déjà des données à caractère personnel réelles à des fins de test avant la date d’entrée en vigueur de la base juridique.Dans la mesure où les tests peuvent être réalisés au moyen de données fictives ou brouillées, il y a lieu d'opter pour cette méthode de travail. Ce n’est que lorsque cela s’avère impossible que des tests avec des données à caractère personnel réelles peuvent être réalisés aux conditions suivantes :* + il s’agit de données à caractère personnel d'une population limitée ;
	+ les données à caractère personnel sont uniquement utilisées à des fins de test et non pour l’octroi de droits ;
	+ les données à caractère personnel doivent être supprimées à l’issue des tests ;
	+ le traitement des données à caractère personnel à des fins de test fait l'objet d'une journalisation.

Le cas échéant, le demandeur expose de manière circonstanciée les raisons pour lesquelles les tests ne peuvent être exécutés au moyen de données fictives ou brouillées et la manière dont il satisfait aux quatre conditions précitées.……………………………………………………………………………………………………….……………………………………………………………………………………………………….………………………………………………………………………………………………………. |

|  |
| --- |
|  **4. Traitement ultérieur (utilisation de données initialement collectées pour d’autres finalités)** |
| * Oui

Description de l’utilisation initiale des données à caractère personnel par l’instance qui fournira les données:………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Non
 |

|  |
| --- |
| **5. Transparence** |
| 1. Communication d'informations aux personnes concernées (avec indication des articles 13 ou 14 du RGPD) ?
* Oui, comment? Ajouter document

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Non, motivation:
	+ la personne concernée dispose déjà des informations
	+ en cas de collecte indirecte : l’obtention ou la communication des données sont expressément prévues par le droit de l’Etat membre:

……………………………………………………………………………………….……………………………………………………………………………………….……………………………………………………………………………………….* + la fourniture de ces informations se révèle impossible ou exigerait des efforts disproportionnés (à motiver)

motivation……………………………………………………………………………………….……………………………………………………………………………………….………………………………………………………………………………………. |

|  |
| --- |
| 1. **Type de données**
 |
| 1. Nature des données:
* non pseudonymisées - les personnes sont-elles désignées par leur nom ou NISS (numéro de registre national ou numéro Banque Carrefour)?

Qui est en mesure d’identifier les personnes? ……………………………………………………* pseudonymisées - les données ayant trait à l’identité de la personne, telles que le nom, le NISS (numéro de registre national ou numéro Banque Carrefour) et l’adresse sont-elles supprimées?
	1. Est-il nécessaire de conserver le lien entre la série de données pseudonymisées et l’identité des personnes ?
* Oui

Qui conserve ce lien?………………………………………………………………………………….Motivation………………………………………………………………………………….………………………………………………………………………………….………………………………………………………………………………….* Non
* données anonymes (pas de données à caractère personnel au sens étroit du terme)
 |
| 1. Set de données demandé, à mentionner par source de données (exhaustif - en termes compréhensibles – dans la mesure où les données sont décrites dans la réglementation, les termes spécifiques de la réglementation doivent être utilisés tout en renvoyant aux articles concernés – la liste des données demandées peut éventuellement être ajoutée en annexe)

Le demandeur doit veiller à décrire les mesures de pseudonymisation mises en place (par exemple, communication de dates relatives)……………………………………………………………………………………………….……………………………………………………………………………………………………………….……………………………………………………………………………………………………….………………………………………………………………………………………………………. |
| 1. Données d'identification (NISS, registre national, registres Banque Carrefour, registre d'attente, ...)
* utilisation du NISS (numéro d'identification de la sécurité sociale: numéro de registre national ou numéro Banque Carrefour)
* communication de données du Registre national ou accès à ces données
* communication de données des registres Banque Carrefour ou accès à ces données
* communication de données du registre d'attente ou accès à ces données
* communication de données du registre des cartes d’identité ou accès à ces données
* communication de données du registre des cartes pour étrangers ou accès à ces données
* pas d’application
 |
| 1. En ce qui concerne les données d'identification précitées:
* Accès aux modifications apportées dans le passé aux données demandées (historique):
	1. Données concernées

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* 1. Période de l’historique

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* 1. Justification

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………* Réception automatique de modifications futures aux données auxquelles l’accès est demandé:
1. Données concernées

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………1. Justification

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………1. À quel intégrateur de services faites-vous appel à cet effet ?

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

|  |
| --- |
| **7. Proportionnalité / Minimisation des données** |
| 1. Durée de validité de la délibération + motivation[[5]](#footnote-5)

……………………………………………………………………………………………………….……………………………………………………………………………………………………….………………………………………………………………………………………………………..……………………………………………………………………………………………………….. |
| 1. Délai de conservation + motivation[[6]](#footnote-6)

……………………………………………………………..………………………………………………………………………………………………..………………………………………………………………………………………………………………………………………………………….………………………………………………………………………………………………………. |
| 1. Justification de la proportionnalité par catégorie de données et par source de données[[7]](#footnote-7)

……………………………………………………………….……………………………………………………………………………………………………………………………………………….……………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Fréquence de la consultation des données + motivation
* ponctuelle
* périodique (à intervalles réguliers). Période de consultation:
	+ annuelle
	+ semestrielle
	+ trimestrielle
	+ mensuelle
	+ hebdomadaire
	+ quotidienne
	+ autre
* permanente
 |
| 1. Utilisateurs internes au niveau du demandeur et, le cas échéant, mise en place de la séparation de fonction au sein de l’instance demanderesse.

Mentionnez toujours, par catégorie d’utilisateurs internes, le service, la fonction et le motif d’accès. Ces données doivent être communiquées pour l’ensemble des catégories d’utilisateurs internes qui ont accès aux données demandées en remplissant la rubrique ci-dessous. En cas d’utilisateurs internes multiples, vous devez ajouter une annexe contenant les données demandées par catégorie d’utilisateurs internes supplémentaire.1. Service

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………1. Fonction

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………1. Raison …………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |
| 1. Des tiers ont-ils accès aux données demandées?
* Non
* Oui, répondez aux questions ci-après.
1. Les données sont-elles communiquées à des tiers?
* Non
* Oui
1. Nom de l’instance

…………………………………………………………………………………………………………………………………………………………………………………………………………1. Raison de la communication

…………………………………………………………………………………………………………………………………………………………………………………………………………1. L’instance dispose-t-elle d’une délibération ?
* Non
* Oui→ ajouter
 |

|  |
| --- |
| **8. Politique de sécurité** |
| 1. Délégué à la protection des données

Nom : ………………………………………………………………………………………….Organisation : ……………………………………………..……………………………………. |
| 1. Questionnaire à questions fermées (ne doit pas être rempli par des organisations appartenant au réseau de la sécurité sociale)
 |

|  |  |  |  |
| --- | --- | --- | --- |
| ***Formulaire d’évaluation*** | ***oui*** | ***non*** | ***commentaire ou renvoi à des documents joints en annexe*** |
| 1. Disposez-vous d’un délégué à la protection des données? Dans l’affirmative, veuillez remplir la rubrique précitée. |  |  |  |
| 2. Avez-vous évalué les risques et les besoins de protection qui sont inhérents à votre organisation et qui concernent le traitement de données à caractère personnel? |  |  |  |
| 3. Disposez-vous d’une version écrite de votre politique de sécurité et votre politique de protection des données à caractère personnel y est-elle intégrée? Dans l’affirmative, veuillez joindre une copie de cette politique en annexe de la demande. |  |  |  |
| 4. Avez-vous identifié les divers supports de votre organisation contenant des données à caractère personnel? |  |  |  |
| 5. Le personnel interne et externe concerné par le traitement de données à caractère personnel est-il suffisamment informé des obligations de confidentialité et de protection en lien avec ces données , découlant à la fois des différentes dispositions légales et du plan de sécurité? |  |  |  |
| 6. Avez-vous pris des mesures de gestion pour empêcher tout accès physique inutile ou non autorisé aux supports contenant les données à caractère personnel? |  |  |  |
| 7. Avez-vous pris des mesures pour éviter tout dommage physique qui pourrait compromettre les données à caractère personnel ? |  |  |  |
| 8. Avez-vous pris des mesures de gestion pour protéger les différents réseaux auxquels sont connectés les appareils qui traitent les données à caractère personnel? |  |  |  |
| 9. Disposez-vous d’une liste actuelle des différentes personnes compétentes qui ont accès aux données à caractère personnel et de leur niveau d’accès respectif (création, consultation, modification, destruction)? |  |  |  |
| 10. Avez-vous installé un mécanisme d'autorisation d'accès sur vos systèmes d’information de sorte que les données à caractère personnel traitées et les traitements qui y ont trait, soient uniquement accessibles aux personnes et applications qui y sont expressément autorisées? |  |  |  |
| 11. Votre système d'information est-il conçu de telle sorte qu’il enregistre en permanence l'identité des personnes qui accèdent aux données à caractère personnel ? |  |  |  |
| 12. Avez-vous prévu de contrôler la validité et l'efficacité des mesures organisationnelles et techniques à travers le temps afin de garantir la protection des données à caractère personnel ? |  |  |  |
| 13. Avez-vous prévu des procédures d'urgence et de rapportage en cas d'incidents de sécurité impliquant des données à caractère personnel ? |  |  |  |
| 14. Disposez-vous d'une documentation mise à jour concernant les différentes mesures de gestion mises en place en vue de la protection des données à caractère personnel et des différents traitements qui y ont trait ? |  |  |  |

|  |
| --- |
| 1. Si d’application, une analyse d'impact relative à la protection des données spécifique en application de l’article 23 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel a-t-elle été réalisée?
* Oui
* Non, date envisagée pour l’exécution de l’analyse d'impact relative à la protection des données spécifique

………………………………………………………………………………………………….…………………………………………………………………………………………………. |
| 1. L’utilisation du numéro de registre national ainsi que le transfert automatisé de données à caractère personnel à des tiers sont-ils poursuivis par une interconnexion des systèmes d’information qui utilisent le numéro de registre national de la personne concernée en tant que clé?
* Non
* Oui
	1. Raison de la communication des données

………………………………………………………………………………………………………………………………………………………………………………………………* 1. Destinataire

………………………………………………………………………………………………………………………………………………………………………………………………* 1. Le destinataire dispose-t-il d’une autorisation pour utiliser le numéro de registre national?
		1. Oui, référence: …………………………………...............................................
		2. Non
	2. Le flux de données (fourniture de données autres que le numéro de registre national) a-t-il été couvert par une ou plusieurs délibérations antérieures du Comité de sécurité de l’information, d’un des anciens Comités sectoriels ou de la Vlaamse Toezichtscommissie ?
		1. Oui, référence: …………………………………………………………………….
		2. Non
 |
| 1. Organisation intermédiaire
* Oui
	1. Quelle organisation
		+ Plate-forme eHealth
		+ BCSS
		+ Intégrateur de services fédéral
		+ ……………………………………………………………………………………...…………………………………………………………………………………...…

Preuve de l’accord (en annexe)* 1. TTP (*trusted third party*)
		+ Couplage
		+ Pseudonymisation
		+ Anonymisation
	2. Autres
* Non

Si le demandeur est d’avis que l’intervention de la BCSS prévue par la réglementation n'offre pas de valeur ajoutée, il peut demander au Comité de sécurité de l’information d’accorder une dispense de l’intervention de la BCSS. Il fournit à cet effet une explication circonstanciée.……………………………………………………………………………………………………….……………………………………………………………………………………………………….……………………………………………………………………………………………………….……………………………………………………………………………………………………….En cas d’intervention de la Plate-forme eHealth en tant que TTP, le demandeur doit prendre contact avec le service eHealth TTP pour s’assurer que la communication de données est techniquement réalisable. Le demandeur communique une copie de cet accord. |
| 1. SCRA prévue (analyse de risque *small cell*) ?
* Oui
	1. Quelle organisation……………………………………………………………………….

Preuve de l’accord (en annexe)* Non (motivation pourquoi pas)
 |
| 1. Tous les collaborateurs sont-ils soumis à un devoir de confidentialité?
* Oui, régi par:
	1. Obligation légale:

Titre et article de la disposition légale : ……………………………………………* 1. Obligation statutaire (joindre statut):
	2. Obligation contractuelle (joindre contrat):
* Non
 |
| 1. Dans la mesure où des données relatives à la santé sont traitées, il convient de désigner un professionnel des soins de santé responsable.

Nom : ………………………………………………………………………………………………………Fonction: ………………………………………………………………………………………………………Organisation ……………………………………………………………………………………………………… |

|  |
| --- |
| **9. Utilisation des services de sécurité** |
| * Oui
* Boîte aux lettres électronique sécurisée
* Certificats eHealth
* Pseudonymisation, anonymisation & trusted third party
* ConsultRN
* Coordination de sous-processus électroniques
* Horodatage électronique (timestamping)
* Gestion des loggings
* Gestion intégrée des utilisateurs et des accès
* Répertoire des références
* Site portail
* Système de chiffrement de bout-en-bout
* Non

Les loggings permettent de déterminer quelle personne a traité quelles données à quel moment pour quelle finalité (« *qui-quand-quoi-pourquoi* ») et permettent de reconstituer la chaîne des opérations. Le demandeur explique ci-après le rôle de chacun des intervenants sur ce plan et de quelle manière il est possible de vérifier globalement ce qui s’est passé dans chaque phase avec les données d'une personne.………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………A travers l'inscription d'une personne dans le répertoire des références, une organisation indique qu’elle tient un type de dossier déterminé au sujet d'une personne. Les données peuvent en effet uniquement être échangées dans la mesure où tant l’instance qui les communique que l’instance qui les reçoit connaissent l’intéressé dans le contexte approprié. Le demandeur précise ci-après sous quelles codes qualité les intéressés sont inscrits dans quelles répertoires des référence[[8]](#footnote-8).……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

|  |
| --- |
| **10. Principe de collecte et enregistrement uniques de données à caractère personnel** |
| Dans la mesure où les données à caractère personnel ont déjà été recueillies et sont disponibles auprès d'une source authentique, elles ne peuvent être collectées une deuxième fois auprès des personnes concernées, mais elles doivent être obtenues auprès de cette source authentique.Il ne peut être question d'un enregistrement multiple redondant de données à caractère personnel pour les mêmes finalités. Le demandeur ne peut pas enregistrer structurellement les données à caractère personnel qu'il consulte auprès de la source authentique.Le demandeur explique comment il respecte, lors du traitement de données à caractère personnel, le principe de collecte et enregistrement uniques de données à caractère personnel ou il expose les motifs pour lesquels ce n’est pas le cas.……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………… |

|  |
| --- |
| **11. Aperçu des documents** |

1. Le demandeur communique au Comité de sécurité de l’information le(s) groupe(s) spécifique(s) de personnes dont il souhaite traiter des données, en fournissant soit une description précise, soit une énumération exhaustive des catégories. [↑](#footnote-ref-1)
2. Dans la mesure où il s’agit d'une demande d’une entité fédérée, le demandeur précise, le cas échéant, les raisons pour lesquelles il a également besoin de données de personnes en provenance d'autres entités fédérées pour la réalisation de la finalité du traitement. [↑](#footnote-ref-2)
3. Si la demande émane d'une organisation publique (indépendamment du niveau de pouvoir), il y a lieu en principe de faire référence à cette base légale. La réglementation applicable doit être explicitement mentionnée dans la demande jusqu’au niveau des articles (voir infra). [↑](#footnote-ref-3)
4. La signature définitive par les instances compétentes suffit à cet égard. La publication de la réglementation au Moniteur belge n’est pas requise. Dans la mesure où la réglementation n’est pas (encore) publiée au Moniteur belge, le demandeur joint le texte de la réglementation à sa demande. [↑](#footnote-ref-4)
5. Le demandeur précise durant quelle période les données seront nécessaires pour réaliser les finalités du traitement. Il fournit une argumentation claire avec une référence à la réglementation applicable. [↑](#footnote-ref-5)
6. Le demandeur précise pendant combien de temps les données seront conservées après réception. Il indique explicitement la période (avec le nombre de mois / d’années après réception des données) et fournit une motivation concrète à cet égard, avec une référence à la réglementation applicable. [↑](#footnote-ref-6)
7. Le demandeur expose, par donnée ou du moins par bloc logique de données, les raisons pour lesquelles il en a besoin pour la réalisation des finalités du traitement, avec une référence à la réglementation applicable (jusqu’au niveau de l’article). [↑](#footnote-ref-7)
8. Cela est particulièrement important lorsque des données du réseau de la sécurité sociale sont communiquées à une organisation d'une entité fédérée. Dans ce cas, la question est en effet de savoir si la référence à l’organisation destinatrice est reprise dans le répertoire des références de la BCSS ou dans le répertoire des références de l’instance compétente de l’entité fédérée. [↑](#footnote-ref-8)