

Explication du formulaire de demande CSI V4.0

La Commission de la sécurité de l'information est composée de deux chambres : la Chambre de la sécurité sociale et santé et la Chambre du gouvernement fédéral.

Candidatures à la Chambre du gouvernement fédéral

Le fonctionnement de la Chambre du gouvernement fédéral de la Commission de la sécurité de l'information est régi par les (nouveaux) articles 35/1 à 35/5 de la loi du 15 août 2012 relative à la création et à l'organisation d'un intérateur de services fédéraux.

La Chambre du gouvernement fédéral délibère sur la communication de données à caractère personnel par les autorités publiques et les établissements publics du gouvernement fédéral à des tiers qui ne sont pas des institutions de sécurité sociale, dans la mesure où les responsables concernés ne parviennent pas à un accord ou si au moins un responsable du traitement demande une délibération.

La communication de données à caractère personnel par les autorités publiques et les établissements publics du gouvernement fédéral aux établissements publics de sécurité sociale et aux services publics fédéraux en charge de l'application de la sécurité sociale nécessite une délibération des chambres conjointes de la commission de la sécurité de l'information, mais uniquement dans la mesure où les responsables de traitement concernés ne parviennent pas à un accord ou qu'au moins un responsable de traitement demande une délibération.

La communication de données personnelles par les services publics et les institutions publiques du gouvernement fédéral à d'autres institutions de sécurité sociale nécessite toujours une délibération des chambres conjointes de la commission de la sécurité de l'information.

La communication de données à caractère personnel par les autorités fédérales (autres que le Registre national) à des tiers autres que les institutions de sécurité sociale ne nécessite qu'une délibération de la Chambre du gouvernement fédéral, dans la mesure où les responsables du traitement de l'autorité communicante et de l'autorité destinataire ne sont pas en mesure de conclure un protocole.

Voir <https://bosa.belgium.be/fr/themes/administration-numerique/cooperation-et-partage-des-connaissances/comite-de-securite-de>

Demandes d'admission à la Chambre de la sécurité sociale et santé

Quand faut-il introduire une demande auprès de la Chambre SS&S ?

La compétence de la Chambre de la sécurité sociale et santé de la Commission de la sécurité de l'information est incluse dans la loi BCSS, art.46 :

Pour les données de santé

La Chambre de la Sécurité Sociale et Santé de la Commission de la Sécurité de l'Information est compétente pour délibérer en matière de communication de données à caractère personnel concernant la santé, dans la mesure où ces délibérations sont imposées par l'article 42 de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé ou par une autre disposition établie par la loi ou en vertu de celle-ci.

L'article 42 §2, 3° de la loi du 13 décembre 2006 dispose :

3° l'octroi d'une autorisation de principe à l'égard de toute communication de données à caractère personnel concernant la santé, sauf dans les cas suivants :

- si la communication est faite entre des professionnels de santé tenus au secret professionnel et qui participent personnellement à la réalisation d'actions diagnostiques, préventives ou de soins à l'égard d'un patient ;

- si la communication est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance et après avis de l'APD

- dans les cas déterminés par le Roi, par un décret adopté après consultation en Conseil des ministres et après avis de l'APD

- si les données sont communiquées entre les autorités d'une même Communauté ou Région qui n'utilisent pas les services de base de la plateforme eHealth, visés à la loi du 21 août 2008 relative à la création et à l'organisation de la plateforme eHealth et à diverses dispositions.

Références au formulaire

1. Généralités

1.1. Le demandeur

Le demandeur est le sous-traitant ultime des données demandées. Il initie la demande à le CSI.

Le demandeur agira en tant que responsable du traitement des données (RGPD art.4.7) lorsqu'il déterminera la finalité et les moyens du traitement. Si l'objet et les moyens sont déterminés conjointement avec d'autres parties, ces parties sont coresponsables du traitement et doivent également être mentionnées sur le formulaire.

Les responsabilités précises de chaque coresponsable du traitement doivent être documentées.

1.2. Type de demande

Si le demandeur n'a pas encore obtenu l'autorisation de l'IRPC pour le traitement en question, il s'agit d'une nouvelle demande.

Si le traitement implique un ajustement ou une extension d'un traitement antérieur pour lequel il existe déjà une délibération, le demandeur doit demander cette délibération et proposer les ajustements nécessaires dans le suivi des modifications.

1.3. Délibérations en cours

Mentionnez les délibérations pertinentes que le demandeur a déjà reçues dans le passé ou les protocoles qui ont été conclus pour un traitement similaire.

1.4. Accès au Registre national et utilisation du numéro du Registre national

L'accès aux données du registre national et l'utilisation du numéro du registre national font l'objet d'une autorisation distincte.

Si cet accès et/ou cette utilisation est nécessaire à la réalisation du traitement prévu, l'origine de l'autorisation doit être indiquée ici.

Si le traitement est effectué exclusivement sur la base de données pseudonymisées, il n'est pas nécessaire qu'une telle autorisation soit nécessaire. Par exemple, BCSS relie des données provenant de différentes sources sur la base du numéro de registre national, mais le demandeur reçoit des pseudonymes. Dans ce cas, le demandeur n'a pas besoin d'avoir l'autorisation de consulter le registre national ou d'utiliser le numéro de registre national.

Conformément à la loi du 8 août 1983 portant réglementation du Registre national des personnes physiques, modifiée par la loi du 25 novembre 2018 portant diverses dispositions relatives au Registre national et aux registres de la population, l'accès aux données du Registre national est autorisé par le ministre ayant l'Intérieur dans ses attributions.

Voir <https://www.ibz.rrn.fgov.be/fr/registre-national/demande-dacces-au-registre-national/>

1.5. Processeur

Le demandeur peut faire appel à un ou plusieurs sous-traitants au sens de l'article 4.8 du RGPD pour le traitement final.

Dans ce cas, c'est toujours le responsable du traitement qui détermine la finalité et les moyens du traitement. Le sous-traitant travaille pour le compte et sous la supervision du responsable du traitement.

Un accord doit être conclu entre le responsable du traitement et le sous-traitant qui respecte les exigences de l'article 28 du RGPD.

L'accord doit documenter l'étendue exacte et les tâches du sous-traitant.

2. Procédure de communication des données à caractère personnel

2.1. Catégories spéciales

Ces catégories spéciales se réfèrent aux articles 9 et 10 du RGPD. Ces catégories sont soumises à des exigences spécifiques qui permettent le traitement. Le CSI veut vérifier dans quelle mesure le demandeur peut répondre à ces exigences.

Article 9 :

Traitement de données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, et traitement de données génétiques, de données biométriques aux fins d'identifier de manière unique une personne, ou de données relatives à la santé, ou de données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Article 10 :

Données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sécurité y afférentes.

2.2. Personnes dont les données personnelles seront traitées

Les critères limites pour le traitement prévu doivent être documentés en détail ici. Quels groupes cibles ou catégories de personnes sont inclus dans le traitement et selon quels critères de sélection.

2.3. Autorités concernées

Ici, il est documenté qui sont les détenteurs des données et qui sont les destinataires des données.

2.4. Détenteurs de données

Liste de tous les organismes qui fourniront des données en tant que détenteurs de données.

2.5. Contacts

Données des personnes de contact par autorité (titulaires et destinataires des données) qui ont connaissance du traitement des données prévu.

2.6. Flux

Vue d'ensemble schématique des flux de données des détenteurs de données vers les destinataires des données en passant par les Trusted Third Party (TTP).

Explication de chaque flux mentionné dans le schéma.

Cette note explicative clarifie les liens prévus entre les flux de données et les mesures intermédiaires prises par le TTP pour pseudonymiser/anonymiser l'identification des personnes concernées.

3. Irrévocabilité

3.1. Usages généraux

Décrire les finalités générales du traitement prévu

3.2. Base juridique du traitement

« OUI » fait référence à l'article 9.2 du RGPD pour le traitement de catégories particulières de données personnelles. En principe, ce traitement est interdit, sauf si une ou plusieurs des conditions spécifiées sont remplies.

La recherche scientifique sur des expériences sur des êtres humains et sur du matériel humain reproductif nécessite des conseils éthiques fondés sur un protocole de recherche.

« NON » fait référence à l'article 6.1 du RGPD qui définit les conditions de traitement licite.

Remarque : quelques exceptions aux dossiers de l'article 9.2 implicites sur l'article 6.1 (consentement, intérêts vitaux, intérêt public). S'il n'y a pas de mappage implicite, il doit toujours exister une base juridique pour le traitement basée sur l'article 6.1. Ce dernier s'applique également aux traitements fondés sur l'article 10.

3.3. Réglementation applicable

L'article 5 du RGPD définit les principes régissant le traitement des données à caractère personnel. Il s'agit de la licéité, de l'équité, de la transparence, de la limitation des finalités, de la minimisation des données, de l'exactitude, de la limitation de la conservation, de l'intégrité et de la confidentialité.

Lorsque ces principes trouvent leur origine dans des réglementations, celles-ci doivent être énoncées en détail ici (au niveau de l'article).

4. Traitement ultérieur

Lorsque des données sont traitées qui ont été initialement collectées à d'autres fins, il faut indiquer ici pour chaque détenteur de données quelles données ont été collectées et à quelles fins.

5. Transparence

Les articles 13 et 14 du RGPD déterminent les informations à fournir aux personnes concernées lorsque les données ont été collectées auprès des personnes concernées (art.13) ou non (art.14).

« OUI » Celle-ci doit indiquer comment les personnes concernées sont informées. Cela peut se faire, par exemple, via le Formulaire Informed Consent (FIC) dans lequel l'étendue exacte du traitement est indiquée.

« NON » Si les données n'ont pas été collectées auprès de la personne concernée, il est possible d'indiquer (de manière motivée) l'une des options indiquées.

6. Type de données

6.1. Type de données

L'article 89.1 du RGPD indique que le traitement doit être effectué sur des données anonymes si les finalités peuvent être atteintes. Dans le second cas, le traitement doit être effectué sur des données pseudonymisées si les finalités peuvent être atteintes. Uniquement lorsque les finalités ne peuvent être atteintes que sur la base de données identifiables.

Les critères d'anonymat sont indiqués au considérant 26 du RGPD.

6.2. Jeu de données demandé

Alors que dans la version 2.6, les flux de données schématiques ont été clarifiés, une description exhaustive de chaque source de données doit être donnée ici.

Il s'agit donc d'une liste de champs d'information avec leur signification, par détenteur de données, par ensemble de données. Il faut indiquer quels champs sont pseudonymisés et de quelle manière.

6.3. Identification

Identifiez toutes les données d'identification répertoriées ici qui apparaissent dans un ensemble de données répertorié à la section 6.2.

6.4. Réception des modifications

Cette section s'applique lorsque les données d'identification de 6.3 sont obtenues par l'intermédiaire d'un intégrateur de services, par exemple BCSS.

Le premier point indique si l'on a besoin d'accéder à l'historique des modifications apportées aux données d'identification à partir de 6.3.

Le deuxième point indique si les modifications futures des données d'identification de 6.3 doivent être automatiquement communiquées au sous-traitant. Cette communication est effectuée par l'intégrateur de services et est utile pour un ensemble de données qui doit être conservé à long terme par le sous-traitant.

7. Proportionnalité / minimisation des données

7.1. Durée de validité du débat

L'application peut servir à atteindre certains objectifs une fois. Dans ce cas, la délibération aura une durée de validité temporaire. Si les objectifs doivent être atteints à long terme ou s'ils sont de nature répétitive, les délibérations peuvent être d'une durée permanente.

Dans tous les cas, la durée de validité demandée doit être justifiée et justifiée sur la base de la réglementation applicable.

7.2. Durée de conservation

L'article 5.1.e du RGPD prescrit la limitation de la conservation.

Pour cela, il faut déterminer combien de temps les données seront stockées après avoir atteint les objectifs ponctuels ou intermédiaires. Si les données sont conservées pendant une période plus longue, cela doit être justifié par rapport à la réglementation applicable.

7.3. Proportionnalité

La version 6.2 explique les ensembles de données demandés. Il doit indiquer pour chaque donnée ou bloc de données pourquoi il est nécessaire d'atteindre les objectifs, en référence à la réglementation applicable. Les critères de sélection appliqués et les mesures prises pour éviter la réidentification des personnes impliquées sont également expliqués.

7.4. Fréquence

La fréquence de la demande de données dépend de la durée de validité des délibérations (voir 7.1).

7.5. Utilisateurs internes

Qui (service, poste) aura accès aux données demandées et pourquoi.

Il est possible que l'autorité destinataire des données traite également des données similaires sur la base d'obligations légales ou contractuelles. Le cas échéant, une entité distincte doit être mise en place au sein de l'autorité pour le traitement des données demandées afin de créer une séparation suffisante des tâches.

7.6. Utilisateurs externes

Si les données demandées sont également accessibles ou communiquées à des tiers, ces autorités doivent être mentionnées ici et doivent également disposer d'une autorisation.

8. Politique de sécurité

8.1. Délégué à la protection des données

Le délégué à la protection des données doit être mentionné ici pour chaque autorité, destinataire des données.

8.2. Questionnaire

Ce questionnaire vérifie la politique de sécurité de chaque autorité qui reçoit des données. Les institutions appartenant au réseau de sécurité sociale n'ont pas à remplir ce questionnaire car elles doivent soumettre une liste d'évaluation annuelle à la BCSS sur la base des normes minimales.

8.3. AIPD

Sur le site web de l'APD, vous pouvez également consulter la liste des traitements (n° 01/2019 du 16 janvier 2019) pour lesquels l'APD a indiqué qu'une analyse d'impact relative à la protection des données (AIPD) doit toujours être réalisée.

Les articles 35.1 et 35.3 du RGPD doivent également être pris en compte.

8.4. Relier les systèmes d'information

Cette section ne s'applique que lorsque les systèmes d'information sont reliés les uns aux autres pour transmettre des informations à des tiers et que le numéro de registre national des personnes concernées est utilisé comme moyen d'identification.

8.5. Organisation intermédiaire

Conformément à la loi sur la Banque-Carrefour, certains types de demandeurs doivent échanger des données avec l'intervention du CBSS. Toutefois, une exemption peut être

obtenue si BCSS ne peut pas offrir de valeur ajoutée. Cela doit être justifié ici si nécessaire.

Un Trusted Third Party (TTP) sera souvent tenu de pseudonymiser ou d'anonymiser les données d'identification. Un TTP différent peut être nécessaire pour relier des ensembles de données provenant de différents détenteurs de données, sur la base de ces pseudonymes. En règle générale, eHealth et BCSS sont choisis respectivement comme TTP pour le traitement des données de santé.

8.6. SCRA

Les sections 6.2 et 7.3 tenaient déjà compte de la réduction des possibilités de réidentification des personnes concernées, par exemple par des limitations dans les critères de sélection, l'utilisation de champs calculés au lieu de microdonnées, l'évitement des dates ou l'utilisation de dates relatives, l'évitement des données de localisation ou des combinaisons d'autres données qui permettraient la réidentification.

Le CSI peut imposer une Small Cell Risk Analysis (SCRA) supplémentaire afin de prendre des mesures supplémentaires dans le cadre de l'enquête sur une éventuelle réidentification.

Le pool SCR coordonné par l'Agence fédérale des données de santé (ADS) peut être sollicité si la capacité nécessaire est disponible.

8.7. Obligation de confidentialité

L'article 9 de la loi du 30 juillet 2018 régit l'obligation de confidentialité des salariés concernés qui participent au traitement prévu. Si cet article s'applique, l'obligation de confidentialité doit être justifiée ici.

8.8. Données de santé

Pour chaque autorité qui reçoit des données, le professionnel de santé responsable doit être désigné.

9. Utilisation des services de sécurité

Il s'agit des services disponibles de la plateforme eHealth qui peuvent ou non être utilisés dans le cadre de la réalisation des liens à réaliser et de la livraison des données.