Comité de sécurité de l'information
Chambre sécurité sociale et santé

CSI/CSSS/25/034

**DÉLIBÉRATION N° 25/016 DU 14 JANVIER 2025 PORTANT SUR LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA POSSIBILITÉ D'EMPLOI SOUS UN RÉGIME SPÉCIAL DE COTISATIONS DE SÉCURITÉ SOCIALE PAR L'OFFICE NATIONAL DE SÉCURITÉ SOCIALE À DES EMPLOYEURS POTENTIELS, À DES MANDATAIRES SOCIAUX ET À DES BUREAUX DE RECRUTEMENT ET DE SÉLECTION DANS LE CADRE D'UNE RELATION PRÉCONTRACTUELLE, SUR LA BASE D'UN MANDAT ACCORDÉ PAR L'INTÉRESSÉ**

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, en particulier l'article 15, § 1er ;

Vu la demande de l'Office national de sécurité sociale ;

Vu le rapport de la Banque Carrefour de la sécurité sociale ;

Vu le rapport du président.

## A. OBJET

**1.** Par la délibération n° 24/222 du 3 décembre 2024, la chambre sécurité sociale et santé du Comité de sécurité de l'information a décidé, suite à une question des institutions de sécurité sociale concernées, que la communication de données à caractère personnel du réseau de la sécurité sociale par une institution de sécurité sociale à une organisation, une entreprise ou un professionnel individuel, sur la base d'un mandat accordé par une personne physique, doit toujours s'effectuer selon les dispositions de cette délibération. La délibération précitée constitue un cadre général qu'il y a lieu de respecter, sans toutefois porter préjudice à la compétence du Comité de sécurité de l'information de se prononcer, au cas par cas, dans des situations concrètes sur ce type de traitement de données à caractère personnel.

**2.** Conformément à la délibération n° 24/222 du 3 décembre 2024, la communication de données à caractère personnel dans le cadre d'une relation s'effectue moyennant un mandat standardisé accordé par l'intéressé. La portée de chaque (type) de mandat susceptible d'être accordé doit est approuvée par le Comité de sécurité de l'information.

**3.** Cette délibération spécifique porte sur la communication de certaines données à caractère personnel par l'Office national de sécurité sociale à des employeurs potentiels afin qu'ils puissent vérifier, dans la phase précontractuelle, sur la base d'un mandat accordé par

l'intéressé, si celui-ci peut être employé ou non en application de certains régimes en matière de cotisations de sécurité sociale.

**4.** L'intéressé peut accorder ce mandat de type « données à caractère personnel précontractuelles » à trois catégories de mandataires : des employeurs potentiels, des mandataires désignés par les employeurs dans le cadre de l'administration sociale et des agences de recrutement et de sélection.

**5.** La première catégorie (employeurs potentiels) concerne toutes les entités qui disposent d'un numéro d'entreprise. Dans la phase précontractuelle, ils ne doivent pas nécessairement déjà être inscrits comme employeur auprès de l'Office national de sécurité sociale. Il peut par exemple s'agir d'un travailleur indépendant (personne physique) qui souhaite engager un premier travailleur salarié. Les agences d'intérim agréées relèvent également de la catégorie des employeurs potentiels. Les agences d'intérim agréées qui vont à la recherche d'un emploi adéquat pour les personnes qui sont inscrites auprès d'elles, doivent par exemple pouvoir vérifier, moyennant un mandat de l'intéressé, si celui-ci peut être employé ou non dans le cadre d'un régime spécial en matière de cotisations de sécurité sociale. Dans ce cadre, les parties fixent par écrit, dans une déclaration d'intention, leur intention de conclure un contrat de travail intérimaire (conformément à l'article 8, § 2, de la loi du 24 juillet 1987 *sur le travail temporaire, le travail intérimaire et la mise de travailleurs à la disposition d'utilisateurs*.

**6.** Une deuxième catégorie de mandataires concerne les mandataires sociaux qui sont désignés par un employeur dans le cadre de son administration sociale, visés à l'article 31ter de la loi du 29 juin 1981 *établissant les principes généraux de la sécurité sociale des travailleurs salariés*. Cette catégorie comprend deux types de mandataires sociaux : d'une part, les secrétariats sociaux agréés et, d'autre part, les prestataires de services sociaux non-agréés qui sont enregistrés auprès de l'Office national de sécurité sociale.

**7.** La troisième catégorie concerne les agences de recrutement et de sélection qui aident les intéressés à trouver un emploi et/ou qui aident les employeurs à trouver des travailleurs adéquats. Les médias qui diffusent des offres d'emploi, les prestataires de services ICT des agences de recrutement et de sélection, ... ne tombent pas sous cette catégorie.

## B. EXAMEN

**8.** Le Comité de sécurité de l'information estime qu'il convient de souligner l'essence du mandat de l'intéressé, accordé conformément au cadre général décrit dans la délibération n° 24/222 du 3 décembre 2024 : la communication de données à caractère personnel par une institution de sécurité sociale moyennant un mandat de l'intéressé, dans le cadre d'une relation, s'effectue sur la base du consentement éclairé de l'intéressé en ce qui concerne les modalités d'un tel mandat.

**9.** Le Comité de sécurité de l'information constate que les quatre documents qui lui sont soumis concernant la communication de la série de « données à caractère personnel précontractuelles » par l'Office national de sécurité sociale sur la base d'un mandat de l'intéressé, fixent les conditions d'accès à ces données à caractère personnel, ce qui permet aux employeurs potentiels, mandataires sociaux et agences de recrutement et de sélection d'obtenir uniquement accès aux données à caractère personnel nécessaires à la

réalisation de la finalité précitée. Ceci répond par ailleurs au principe de partage minimal de données.

## C. CONCLUSION

La chambre sécurité sociale et santé du Comité de sécurité de l'information approuve les documents suivants, joints en annexe, qui font partie intégrante de la présente délibération:

- le document précisant les modalités d'octroi d'un mandat par l'intéressé en ce qui concerne l'accès aux « données à caractère personnel précontractuelles » ;

- le document contenant les modalités d'accès aux « données à caractère personnel précontractuelles » par le mandataire ;

- le règlement d'utilisation pour l'accès via le service en ligne aux données sociales à caractère personnel sur la base d'un mandat accordé par une personne physique ;

- le règlement établissant les critères pour l'application d'un cercle de confiance par une organisation, une entreprise ou un professionnel individuel dans le cadre de l'échange de données sociales à caractère personnel sur la base d'un mandat accordé par une personne physique.

Le Comité de sécurité de l'information approuve dès lors les conditions décrites en matière d'accès, via *application programming interface* (API), à certaines données à caractère personnel de l'Office national de sécurité sociale (en ce qui concerne la possibilité d'emploi sous un régime spéciale de cotisations de sécurité sociale) par des employeurs potentiels, des mandataires sociaux et des agences de recrutement et de sélection, sur la base d'un mandat accordé par l'intéressé.

La présente délibération entre en vigueur le 29 janvier 2025.

Michel DENEYER
Président

**Annexe 1**

## Conditions du mandat pour l'accès aux données précontractuelles

Vous consentez à ce que les destinataires (mandataires) approuvés par vous puissent consulter certaines données selon les conditions établies ci-après, sur la base de votre mandat, dans le cadre d'une sollicitation.

Pour votre contingent d'étudiant, votre mandat est valable pendant maximum 3 mois à compter de la date d'enregistrement de votre consentement. Pour les flexi-jobs, votre mandat est valable pendant maximum 1 mois à compter de la date d'enregistrement de votre mandat.

Vous pouvez toujours retirer votre mandat via : https://toegangtotmijndata.fgov.be/XXXX.

L'octroi ou la révocation d'un mandat font l'objet d'un enregistrement électronique. Un aperçu de vos mandats actifs est disponible ici.

### Responsable du traitement

Le destinataire des données à caractère personnel s'engage, en tant que responsable du traitement, à respecter les dispositions pertinentes en matière de protection des données, notamment le Règlement général relatif à la protection des données (RGPD).

### Données à caractère personnel

Votre mandat est valable pour la consultation des données à caractère personnel suivantes :

- pour le travail d'étudiant : le nombre d'heures disponibles du contingent de travail d'étudiant avec application de la cotisation de solidarité.
- pour les flexi-jobs : la réponse à la question de savoir si vous répondez ou non aux conditions d'emploi ou de pension.

### Finalité

Le destinataire peut uniquement traiter vos données à caractère personnel pour vérifier, dans le cadre d'une sollicitation, si vous répondez aux conditions pour être employé en tant que travailleur flexi-job ou étudiant avec cotisation de solidarité et, si oui, pour combien d'heures ou de jours.

### Délai de conservation

Le destinataire peut uniquement traiter ces données pour la durée du délai nécessaire pour décider s'il vous emploiera ou non via le statut d'étudiant jobiste ou flexi-job. Si le destinataire décide de ne pas vous engager, il est tenu de détruire vos données sans délai.

**Protection des informations**

L’accès à vos données à caractère personnel s’effectue toujours de manière sécurisée par la voie électronique. Le destinataire est tenu de respecter les mesures en matière de protection des informations définies par le Comité de sécurité de l’information :

- en cas de consultation via service en ligne : le règlement d'utilisation suivant
- en cas de consultation via API : le « cercle de confiance » suivant (CoT).

**Annexe 2**

## Conditions mandataire accès aux données précontractuelles

Vous vous engagez à respecter les conditions déterminées ci-après en vertu desquelles vous obtenez un accès à certaines données relatives au candidat-travailleur (mandant), qui vous octroie à cet effet un mandat dans le cadre d'un entretien d'embauche.

En ce qui concerne le contingent étudiants, votre accès est valable pendant au maximum 3 mois à compter de l'enregistrement du mandat du candidat-travailleur.

En ce qui concerne les flexi-jobs, votre accès est valable pendant 1 mois au maximum à compter de l'enregistrement du mandat du candidat-travailleur.

Le candidat-travailleur peut retirer son mandat à tout moment. Pour obtenir une liste des mandats actifs, veuillez cliquer sur ce lien.

## Responsable du traitement

En tant que responsable du traitement, vous vous engagez à respecter les dispositions pertinentes relatives à la protection des données, dont le Règlement général relatif à la protection des données (RGPD).

## Données à caractère personnel

Le mandat est valable pour la consultation des données à caractère personnel suivantes du candidat-travailleur:

- pour le travail étudiant: le nombre d'heures disponibles du contingent travail étudiant avec application de la cotisation de solidarité,
- pour les flexi-jobs: la réponse à la question de savoir si le candidat-travailleur satisfait ou non aux conditions d'emploi ou de mise à la retraite.

## Finalité

Vous pouvez uniquement traiter ces données à caractère personnel dans le cadre d'un entretien d'embauche pour vérifier que le candidat-travailleur entre en considération pour un emploi comme travailleur en flexi-job ou comme étudiant avec cotisation de solidarité, et dans l'affirmative, pour combien d'heures ou de jours restants.

## Délai de conservation

Vous pouvez uniquement traiter ces données pendant la période nécessaire pour décider si vous engagerez ou non ce candidat sous le statut d'étudiant jobiste ou de travailleur en flexi-job. Dès que vous avez décidé ne pas engager ce candidat, vous devez immédiatement détruire les données.

**Protection des informations**

L'accès aux données à caractère personnel a toujours lieu par la voie électronique sécurisée. Vous devez respecter les mesures de protection de l'information qui ont été déterminées par le Comité de sécurité de l'information:

- lors de la consultation au moyen d'un service en ligne: le règlement des utilisateurs suivant
- lors de la consultation au moyen d'une API: le « cercle de confiance » (CoT) suivant

**Annexe 3**

# Règlement d'utilisation pour l'accès à des données sociales à caractère personnel sur la base d'un mandat accordé par une personne physique

## Article 1er. Champ d'application

Ce règlement concerne l'accès à des données sociales à caractère personnel, désignées comme données à caractère personnel, qui ont été obtenues d'une institution de sécurité sociale moyennant un mandat accordé par une personne physique à une organisation, une entreprise ou un professionnel individuel, et le traitement de ces données.

Ce règlement comporte des obligations complémentaires et ne porte pas atteinte aux obligations prévues dans le "Règlement à l'usage des utilisateurs en vue de l'accès et de l'utilisation du système d'information des autorités fédérales et des institutions publiques de sécurité sociale par les entreprises et leurs mandataires"[1].

## Article 2 – Définitions

Intéressé : une personne physique qui accorde l'accès, sur la base d'un mandat, à une série de données à caractère personnel qui la concernent dans le chef d'une instance tierce.

Instance tierce : une organisation, une entreprise ou un professionnel individuel qui obtient accès, sur la base d'un mandat accordé par l'intéressé, à des données à caractère personnel de cet intéressé.

## Article 3 - Licéité et principe de limitation de la finalité

L'instance tierce dispose, pour les activités de traitement concernant les intéressés ayant accordé un mandat, d'un registre des activités de traitement tel que visé à l'article 30 du Règlement général sur la protection des données (RGPD), qui mentionne les finalités de traitement légitimes des activités de traitement. Il s'agit donc également des traitements de données à caractère personnel obtenues sur la base d'un mandat accordé par chacun des intéressés.

## Article 4 - Principe de proportionnalité : limitation du traitement

Les données à caractère personnel relatives aux intéressés peuvent uniquement être traitées par des utilisateurs de l'instance tierce qui doivent pouvoir les traiter du chef de leur fonction pour des finalités de traitement légitimes et telles que définies dans la délibération spécifique qui détermine la portée du mandat accordé et la finalité.

[1] https://www.socialsecurity.be/site_fr/general/rules/rules_employer_F.pdf

## Article 5 – Information, formation et sensibilisation

L'organisation tierce rédige les directives nécessaires afin de répondre aux conditions prévues dans le présent document, les met à la disposition, d'une manière généralement accessible, de l'ensemble des utilisateurs qui ont accès aux données fournies, offre à ce sujet une formation permanente adéquate à ces utilisateurs et les sensibilise en permanence concernant le respect des directives.

## Article 6 - Respect des délibérations du Comité de sécurité de l'information

L'instance tierce confirme qu'elle respecte l'ensemble des mesures en matière de sécurité de l'information et de protection de la vie privée qui sont contenues dans les délibérations applicables du Comité de sécurité de l'information.

## Article 7 - Enregistrement de l'acceptation et application du présent règlement par l'instance tierce

L'instance tierce déclare qu'elle est d'accord avec les conditions mentionnées dans le présent document et les applique dans son organisation. Cette déclaration s'effectue dans le système de gestion des accès de la sécurité sociale par les personnes habilitées à cet effet par les responsables de l'organisation.

**Annexe 4**

# Règlement fixant les critères en vue de l'application d'un cercle de confiance par une organisation, une entreprise ou un professionnel individuel dans le cadre de l'échange de données sociales à caractère personnel sur la base d'un mandat accordé par une personne physique

## OBJECTIF DU RÈGLEMENT

Le présent règlement concerne le traitement de données sociales à caractère personnel, dénommées données à caractère personnel, obtenues d'une institution de sécurité sociale au moyen d'un mandat accordé par une personne physique, appelée ci-après la personne concernée, à une organisation, à une entreprise ou à un professionnel individuel, dénommé(e) ci-après la tierce organisation.

Le traitement de données à caractère personnel doit intervenir dans le respect des mesures relatives à la sécurité de l'information et à la protection de la vie privée. Un aspect essentiel dans ce contexte est la garantie que les données à caractère personnel sont uniquement traitées

- pour des finalités légitimes et
- par des personnes qui, pour pouvoir réaliser ces finalités, ont besoin de traiter des données à caractère personnel relatives à la personne concernée.

Dans un système où les données à caractère personnel sont obtenues au moyen d'un mandat accordé par la personne concernée à une tierce organisation, l'offre de ce type de garantie requiert que les responsabilités de chacun soient clairement définies.

Le présent règlement entend y contribuer en précisant le concept des 'cercles de confiance'. Un 'cercle de confiance' est un groupe d'utilisateurs d'une organisation pour lequel cette organisation prend, à plusieurs niveaux, des mesures relatives à la sécurité de l'information et en surveille le respect correct, de sorte que d'autres organisations et la personne concernée puissent raisonnablement avoir confiance que ces mesures de sécurité de l'information sont respectées et qu'elles ne doivent pas les organiser ou les contrôler elles-mêmes.

Pour que des organisations autres que l'organisation qui crée un cercle de confiance et la personne concernée puissent légitimement y avoir confiance, le règlement fixe des critères auxquels doit satisfaire toute organisation qui souhaite organiser ce type de cercle de confiance. Ces critères renvoient, dans toute la mesure du possible, à la législation belge et européenne actuelle telle le Règlement général sur la protection des données (RGPD). Ils ne portent pas préjudice à cette réglementation qui reste pleinement en vigueur, mais ils précisent dans certains cas comment il y a lieu de satisfaire à cette réglementation.

Les critères mêmes se concrétisent sous la forme d'un règlement. Pour une bonne compréhension, des précisions sont apportées à certains critères. Ces précisions sont données à titre purement indicatif.

## LISTE DES CRITÈRES

### THÈME 1: PRINCIPE DE LÉGITIMITÉ ET DE LIMITATION DE LA FINALITÉ

#### CRITÈRE 1: REGISTRE DES ACTIVITÉS DE TRAITEMENT

L'organisation dispose, pour les activités de traitement concernant les personnes concernées qui ont accordé un mandat, d'un registre des activités de traitement tel que visé à l'article 30 du Règlement général sur la protection des données (RGPD), qui mentionne les finalités de traitement légitimes des activités de traitement. Il s'agit donc aussi de traitements de données à caractère personnel obtenues au moyen d'un mandat accordé par chaque personne concernée.

### THÈME 2: PRINCIPE DE PROPORTIONNALITÉ

#### CRITÈRE 2: LIMITATION DU TRAITEMENT

Les données à caractère personnel relatives aux personnes concernées peuvent uniquement être traitées par des utilisateurs de la tierce organisation, qui doivent pouvoir les traiter, dans le chef de leur fonction, pour les finalités de traitement légitimes telles que décrites dans le registre des activités de traitement et comme précisé dans la délibération spécifique qui définit la portée du mandat et sa finalité. Les possibilités de traitement sont modulées de façon suffisamment détaillée, de sorte que tout utilisateur ne puisse traiter que les seules données à caractère personnel relatives aux personnes concernées pour lesquelles ce traitement est nécessaire dans le cadre de sa fonction et pendant la période pendant laquelle ce traitement est nécessaire dans le cadre de sa fonction.

### THÈME 3: GESTION DES ACCÈS ET DES UTILISATEURS

#### CRITÈRE 3: AUTHENTIFICATION DE L'IDENTITÉ DE L'UTILISATEUR

La tierce organisation authentifie l'identité de la personne physique qui traite les données à caractère personnel obtenues (l'utilisateur).

Cette authentification intervient soit

- par un moyen intégré dans le Federal Authentication Service (FAS) d'un niveau identique ou supérieur au niveau 400;
- par un système d'authentification propre à l'organisation, pour des applications internes
    - à condition que l'enregistrement de l'identité soit effectué au moyen d'un usage unique d'un moyen d'authentification intégré dans le FAS d'un niveau identique ou supérieur au niveau fixé par le Comité de gestion de la Banque Carrefour de la sécurité sociale et
    - à condition que le moyen d'authentification propre à l'organisation satisfasse aux conditions d'un niveau de garantie « substantiel », tel que précisé dans les points 2.1., 2.2.1 élément 2, 2.2.3., 2.2.4., 2.3.1. (à l'exception de l'élément 1) et 2.4. de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS et

- à condition que le moyen d'authentification utilisé dans le système d'authentification propre à l'organisation et que son processus d'activation satisfassent aux conditions d'un niveau de garantie « faible », tel que précisé dans les points 2.2.1. élément 1, et 2.2.2. de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS et qu'il ait été conçu de la sorte que l'on peut présumer qu'il ne sera utilisé que par la personne à laquelle il appartient.

*Commentaire explicatif*

*L'usage unique d'un moyen d'authentification intégré dans le FAS afin d'enregistrer l'identité de l'utilisateur n'implique pas que le FAS même doive être utilisé à cet effet. La carte d'identité électronique peut par exemple aussi être demandée pour comparer visuellement la photo avec le détenteur de la carte ou lue au moyen d'une implémentation propre à l'organisation concernée. Le système d'authentification propre à l'organisation doit satisfaire aux conditions du niveau de garantie « substantiel » de l'annexe au Règlement d'exécution (UE) 2015/1502 du Règlement EIDAS, en ce sens que le moyen d'authentification peut effectivement être un moyen d'authentification qui fait usage de seulement un facteur d'authentification (par exemple, numéro d'utilisateur et mot de passe).*

## THÈME 4: LOGGING

### CRITÈRE 4: LOGGING INTERNE

L'accès électronique aux données à caractère personnel fait l'objet d'une prise de traces (logs). La gestion des logs doit au moins répondre aux objectifs suivants

- permettre de déterminer rapidement et de manière aisée quelle personne physique a eu accès à quelles données à caractère personnel relatives à quelle personne, à quel moment et de quelle manière;
- pouvoir identifier de manière univoque la personne qui a traité des données à caractère personnel et la personne concernant laquelle les données à caractère personnel sont traitées;
- mettre les outils nécessaires à la disposition afin de permettre une exploitation des données de logging par des personnes autorisées;
- conserver les données de logging au moins pendant 10 ans.

### CRITÈRE 5: AUDIT TRAIL

Étant donné que le traitement électronique de données à caractère personnel implique l'accès à des données à caractère personnel, il y a lieu de garantir, en cas d'investigation à l'initiative de la Banque Carrefour de la sécurité sociale, ou d'un organe de contrôle, suite à une plainte, qu'une reconstitution complète puisse avoir lieu dont le but est de déterminer quelle personne physique a eu accès à quels types de données à caractère personnel concernant quelles personnes, à quel moment et de quelle manière.

Si pour le logging conservé en application du critère 4, toutes les informations mentionnées dans ce critère sont disponibles dans un seul fichier de logging, cette reconstitution peut avoir lieu conformément à ce fichier de logging.

Des méthodes permettant cette reconstitution complète sont décidées sous la coordination de la Banque Carrefour de la sécurité sociale.

## THÈME 5: INFORMATION, FORMATION, SENSIBILISATION, CONTRÔLE ET SANCTION

### CRITÈRE 6: INFORMATION, FORMATION ET SENSIBILISATION

La tierce organisation rédige les directives nécessaires afin d'exécuter les critères prévus dans le présent document, les met à la disposition, d'une manière généralement accessible, de l'ensemble des utilisateurs qui font partie du cercle de confiance, offre une formation permanente adéquate à ces utilisateurs et les sensibilise en permanence concernant le respect des directives.

### CRITÈRE 7: CONTRÔLE INTERNE

L'organisation organise un contrôle interne régulier quant au respect des critères contenus dans le présent document et des directives qui les exécute. Pour les organisations occupant plus de [10] personnes qui ont accès à des données à caractère personnel traitées par des tiers, cette surveillance régulière se traduit par un contrôle interne formel. L'organisation conserve les résultats de cette surveillance interne ou de ce contrôle interne pendant 2 ans. L'organisation prévoit des sanctions dissuasives vis-à-vis des utilisateurs qui font partie du cercle de confiance qui ne respecteraient pas les critères ou les directives qui les exécutent.

## THÈME 6: RESPECT DES DÉLIBÉRATIONS DU COMITÉ DE SÉCURITÉ DE L'INFORMATION

### CRITÈRE 8: Respect des délibérations du Comité de sécurité de l'information

La tierce organisation assure respecter l'ensemble des mesures relatives à la sécurité de l'information et à la protection de la vie privée qui sont contenues dans les délibérations applicables du Comité de sécurité de l'information.

## THÈME 7: VÉRIFICATION

### CRITÈRE 9: Enregistrement de l'adhésion de la tierce organisation en tant qu'organisation mettant en place un cercle de confiance dans le système de gestion des accès de la sécurité sociale

La tierce organisation notifie qu'elle met en place un cercle de confiance, conformément aux conditions mentionnées dans le présent document, et confirme à cet égard qu'elle satisfait à chacune de ces conditions. Cette notification est réalisée dans le système de gestion des accès de la Sécurité sociale par les personnes autorisées à cet effet par les responsables de l'organisation.

### CRITÈRE 10: CONTRÔLE EXTERNE

La tierce organisation tient le registre des activités de traitement et les documents et politiques qu'elle élabore en vue du respect de ces conditions, ainsi que les résultats de la surveillance interne ou du contrôle interne, à la disposition des organes de contrôle.

## ANNEXE : GLOSSAIRE

### AUTHENTIFICATION DE L'IDENTITÉ

Le processus permettant de vérifier que l'identité qu'une entité prétend posséder pour pouvoir faire appel à un service électronique, est l'identité exacte. L'authentification de l'identité peut intervenir sur la base d'un contrôle

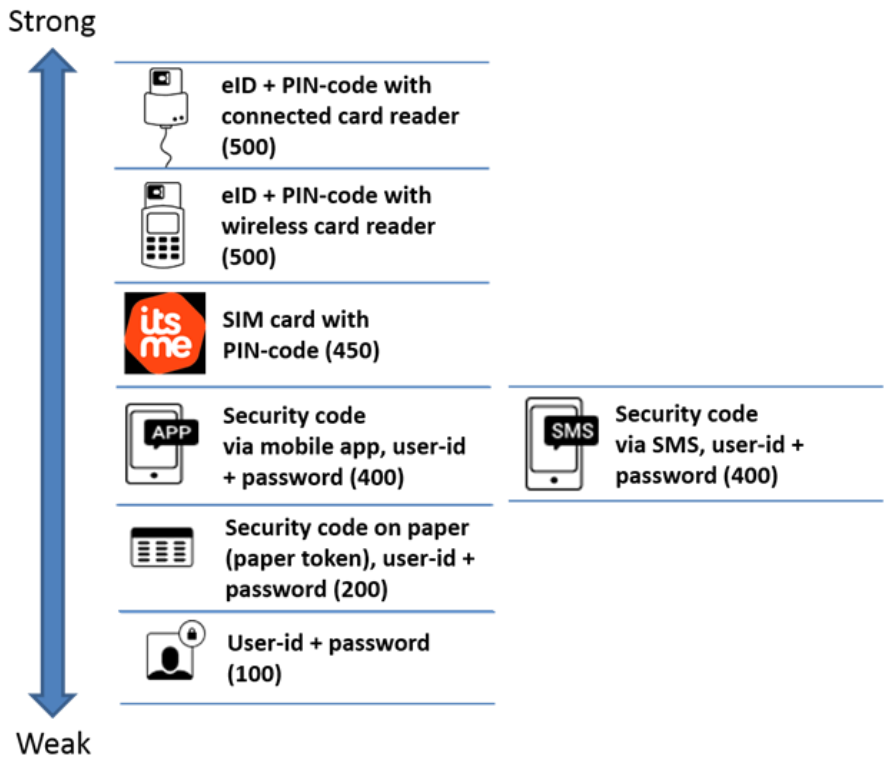
- des connaissances (p.ex. un mot de passe);
- d'une possession (p.ex. un certificat sur une carte lisible par la voie électronique);
- d'une ou des caractéristiques biométriques;
- d'une combinaison d'un ou plusieurs de ces moyens.

### CERCLE DE CONFIANCE

Un cercle de confiance est un groupe d'utilisateurs d'une organisation pour lequel l'organisation même prend, à plusieurs niveaux, des mesures relatives à la sécurité de l'information et en surveille le respect correct, de sorte que d'autres organisations puissent raisonnablement avoir confiance que ces mesures de sécurité de l'information sont respectées et qu'elles ne doivent pas les organiser ou les contrôler elles-mêmes.

### FEDERAL AUTHENTICATION SERVICE (FAS)

Un service offert par le SPF BOSA permettant aux utilisateurs de services électroniques d'authentifier leur identité par différents moyens dont le niveau de sécurité est croissant. Le FAS fait partie du CSAM, un service offrant une solution générale pour tous les aspects de la gestion des utilisateurs et des accès pour les services publics en ligne. Voir https://iamapps.belgium.be/sma/generalinfo?view=home




## NUMÉRO D'IDENTIFICATION DE LA SÉCURITÉ SOCIALE (NISS)

Clé d'identification unique par personne physique utilisée dans les secteurs public, social et de la santé. Pour les personnes enregistrées dans le Registre national, il s'agit du numéro de registre national qui est mentionné sur la carte d'identité électronique. Pour les autres personnes, il s'agit d'un numéro qui est attribué par la Banque Carrefour de la sécurité sociale et géré dans une banque de données, appelée registres BCSS.

## RÈGLEMENT EIDAS

Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE et Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

Voir https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32014R0910

## RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

Voir https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

## RÈGLEMENT D'EXÉCUTION (UE) 2015/1502 DU RÈGLEMENT EIDAS

Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

Voir https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32015R1502&from=FR

## UTILISATEUR

L'utilisateur est la personne qui traite des données à caractère personnel.

## COMITÉ DE SÉCURITÉ DE L'INFORMATION

Le Comité de sécurité de l'information institué par la loi du 5 septembre 2018.