Déclaration sur l'honneur

Cercle de confiance (Circle-of-Trust - CoT)

Introduction

Dans le cadre du traitement de données à caractère personnel pseudonymisées provenant notamment du Datawarehouse marché du travail et protection sociale, il faut qu'il existe des garanties au niveau de la sécurité de l'information. Le principe du Cercle de confiance (« Circle of trust - CoT ») est dès lors appliqué.

Le concept de « cercle de confiance » concerne un groupe d'utilisateurs d'une instance (*en l'occurrence, l'instance qui a besoin des données à caractère personnel pour la réalisation d'études utiles à la connaissance, à la conception et à la gestion de la protection sociale*), pour lequel cette instance prend elle-même, à plusieurs niveaux, des mesures de sécurité de l'information et veille à leur respect, de sorte qu'une autre instance (*en l'occurrence, la Banque Carrefour de la sécurité sociale*) puisse raisonnablement avoir confiance que ces mesures de sécurité de l'information soient respectées et qu'elle ne doive dès lors pas les organiser ou les contrôler elle-même.

Pour que des instances autres que l'instance qui met en place un cercle de confiance, puissent légitimement y faire confiance, des critères sont fixés auxquels doit satisfaire l'instance qui souhaite organiser un cercle de confiance. Ces critères renvoient, dans toute la mesure du possible, à la législation belge et européenne actuelle, telle 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, et abrogeant la directive 95/46/CE* (Règlement général sur la protection des données). Ces critères ne portent pas atteinte à cette réglementation, qui reste pleinement applicable, mais ils précisent dans certains cas comment il y a lieu de satisfaire à cette réglementation. Les critères se présentent sous la forme d'un règlement. Le présent règlement vise à offrir aux instances qui traitent ce type de données à caractère personnel pseudonymisées en vue de la réalisation d'études utiles à la connaissance, à la conception et à la gestion de la protection sociale, un cadre standard dans lequel ce traitement peut être réalisé dans le respect de la réglementation en vigueur, en particulier le Règlement général relatif à la protection des données.

Pour qu'une instance puisse être considérée comme un cercle de confiance, elle doit satisfaire aux 11 critères qui ont été validés dans un Règlement qui a été approuvé par le Comité de sécurité de l'information. L'instance doit prendre les mesures utiles en vue du respect de ces critères. Ces critères peuvent être consultés sur https://ksz-bcss.fgov.be/fr/dwh/dwh_page/content/websites/datawarehouse/menu/cercle-de-confiance.html

Les instances concernées peuvent déclarer qu'elles satisfont à ce cadre standard. Dans ce cas, le projet de délibération soumis par la Banque Carrefour de la sécurité sociale au Comité de sécurité de l'information fait référence à ce cadre standard et à cette déclaration, de sorte que les mesures à prendre ne doivent pas à chaque fois être décrites de manière ad hoc dans la délibération. Cela responsabilise les instances qui reçoivent les données à caractère personnel pseudonymisées et simplifie le traitement du dossier au sein du Comité de sécurité de l'information. Toutefois, l'instance

qui demande les données concernées est invitée à décrire, pour toute demande, les mesures par lesquelles elle garantit que les données demandées constituent des données anonymes ou des données à caractère personnel pseudonymisées au sens du Règlement général relatif à la protection des données et que le principe de la minimisation des données est appliqué.

Il est important de garantir que les données à caractère personnel sont exclusivement traitées pour des finalités légitimes, par des personnes qui ont effectivement besoin de données à caractère personnel pseudonymisées relatives aux personnes concernées pour la réalisation de ces finalités. Dans un système de traitement de données à caractère personnel par de nombreux acteurs - en l'occurrence, les organisations qui mettent ces données à caractère personnel à la disposition en tant que sources authentiques, la Banque Carrefour de la sécurité sociale qui les enregistre dans son Datawarehouse marché du travail et protection sociale et finalement les organisations qui les utilisent pour la réalisation d'études utiles à la connaissance, à la conception et à la gestion de la protection sociale - l'offre de ce type de garantie requiert que les responsabilités de chacun soient clairement définies.

La Banque Carrefour de la sécurité sociale enregistre le « statut CoT » dans un *cadastre* dès qu'une organisation déclare qu'elle satisfait aux 11 critères qui sont applicables au principe du Cercle de confiance.

Déclaration

En signant le présent document, je déclare que l'instance respecte le règlement relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel, et satisfait aux 11 critères ci-après qui s'appliquent au principe du Cercle de confiance.

Je suis d'accord avec le fait que le non-respect des 11 critères par l'instance peut donner lieu à un retrait de l'enregistrement du Cercle de confiance

L'instance s'engage à veiller au respect permanent des éléments repris dans la déclaration. Lors de tout changement substantiel de ses processus, en particulier les processus informatiques, elle s'engage à vérifier le respect de l'ensemble des critères repris dans le présent document et à signaler immédiatement le fait qu'elle n'est plus en mesure d'y satisfaire.

Nom de l'instance:

Adresse :

Coordonnées du responsable :

Coordonnées du délégué à la protection de données:

Date, nom et signature du responsable :

Ce formulaire doit être transmis à la Banque Carrefour de la sécurité sociale. L'instance doit pouvoir prouver, à tout moment, le respect de la protection de la vie privée à l'autorité de protection des données compétente.

- CRITÈRE 1: LÉGITIMITÉ

L'organisation destinatrice fonde la licéité du traitement des données à caractère personnel du datawarehouse marché du travail et protection sociale sur l'article 6, 1, alinéa premier, c) ou e), du Règlement général sur la protection des données (respectivement la nécessité du « respect d'une obligation légale à laquelle le responsable du traitement est soumis » et la nécessité pour « l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement »).

- CRITÈRE 2: LIMITATION DES FINALITÉS

Le datawarehouse marché du travail et protection sociale a été créé en application de l'article 5 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, dans le seul but de permettre à la Banque Carrefour de la sécurité sociale de répondre de manière efficace à des demandes de traitement de données à caractère personnel pour la réalisation d'études utiles à la connaissance, à la conception et à la gestion de la protection sociale. L'organisation qui reçoit les données à caractère personnel peut uniquement les traiter dans ce cadre. Elle est tenue de respecter en tout temps les dispositions des délibérations applicables de la chambre sécurité sociale et santé du Comité de sécurité de l'information, rendues en application de l'article 15 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.

- CRITÈRE 3: PROPORTIONNALITÉ ET LIMITATION DU TRAITEMENT

Les données à caractère personnel du datawarehouse marché du travail et protection sociale peuvent uniquement être traitées par les utilisateurs au sein de l'organisation qui, en raison de leur fonction spécifique, doivent pouvoir les traiter pour les finalités de traitement légitimes. L'organisation définit les possibilités de traitement de manière suffisamment granulaire de sorte que l'utilisateur puisse uniquement traiter les données à caractère personnel dont il a effectivement besoin de par sa fonction et ce uniquement pour la durée nécessaire du chef de sa fonction. L'organisation s'abstient de toute tentative de conversion des données à caractère personnel pseudonymisées reçues de la part de la Banque Carrefour de la sécurité sociale en données à caractère personnel non-pseudonymisées.

Il est interdit à l'organisation de communiquer les données à caractère personnel reçues de la Banque Carrefour de la sécurité sociale en tout ou en partie à des tiers ou au promoteur de l'étude. Les résultats de son étude peuvent uniquement être intégrés sous forme anonyme dans des publications scientifiques.

Dans la mesure où l'organisation communique elle-même, préalablement à son étude utile à la connaissance, à la conception et à la gestion de la protection sociale, des données à caractère personnel non-pseudonymisées à la Banque Carrefour de la sécurité sociale (à titre d'input) que la Banque Carrefour de la sécurité sociale lui renvoie ensuite (couplées à d'autres données à caractère personnel) sous forme de données à caractère personnel pseudonymisées (à titre d'output), elle prévoit une stricte séparation de fonctions entre les sections/facultés concernées. La section/faculté qui reçoit et traite l'output, doit être différente de la section/faculté qui fournit l'input et ne peut pas avoir accès à l'input.

L'organisation conserve les données à caractère personnel pseudonymisées qui ont été communiquées pour la durée nécessaire à la réalisation de l'étude utile à la connaissance, à la conception et à la gestion de la protection sociale et au plus tard jusqu'à la date fixée, le cas échéant, par la chambre sécurité sociale et santé du Comité de sécurité de l'information. Elle les détruit ensuite irrévocablement.

Lors de sa demande de données, l'organisation prend toutes les mesures pour formuler elle-même des propositions de minimisation des données et de pseudonymisation adéquate.

- CRITÈRE 4: AUTHENTIFICATION DE L'IDENTITÉ DE L'UTILISATEUR

L'organisation authentifie l'identité de la personne physique qui traite les données à caractère personnel (« l'utilisateur »).

Cette authentification intervient soit

- par un moyen intégré dans le Federal Authentication Service (FAS) de niveau 400 ou supérieur,
- soit par un système d'authentification propre à l'organisation
    - 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 de niveau 400 ou supérieur
    - 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[1] et
    - à condition que le moyen d'authentification utilisé dans le système d'authentification propre au prestataire et son processus d'activation répondent aux conditions d'un niveau de garantie « faible », tel que précisé au point 2.2.1. élément 1 et au point 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.

L'usage unique d'un moyen d'authentification intégré dans le FAS pour enregistrer l'identité de l'utilisateur n'implique pas que le FAS doive être utilisé à cet effet. La carte d'identité électronique peut par exemple aussi être demandée afin de comparer visuellement la photo avec le détenteur de la carte ou de la lire au moyen d'une implémentation propre à l'organisation concernée. Le système d'authentification propre à l'organisation doit répondre 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 être un moyen d'authentification qui a recours à un seul facteur d'authentification (p.ex. numéro d'utilisateur et mot de passe).

- CRITÈRE 5: LOGGING

L'accès électronique aux données à caractère personnel fait l'objet d'une prise de traces (logging) par l'organisation. Le système de gestion des loggings doit au moins permettre à l'organisation de déterminer, de manière simple et rapide, quelle personne physique a obtenu accès, à quel moment et de quelle façon, à quelles données à caractère personnel de la Banque Carrefour de la sécurité sociale et d'identifier de manière univoque la personne qui a traité les données à caractère personnel. L'organisation dispose des outils nécessaires pour permettre aux personnes autorisées d'exploiter les données de logging. Elle conserve les données de logging pendant minimum dix ans (pendant 6 mois en ligne et pendant 9 ans et 6 mois dans une archive).

- CRITÈRE 6: JOURNAL D'AUDIT

Suite à une plainte, en cas d'enquête, menée à l'initiative de la Banque Carrefour de la sécurité sociale ou d'un organe de contrôle, l'organisation veille à ce qu'une reconstruction complète puisse avoir lieu en vue de déterminer quelle personne physique a eu accès à quelles données à caractère personnel, quand et de quelle façon. Par ailleurs, l'organisation consent explicitement à ce que des représentants de la Banque Carrefour de la sécurité sociale aient, à tout moment, accès aux locaux où les données à caractère personnel communiquées par cette dernière sont conservées, afin de veiller au respect des dispositions de la réglementation applicable

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1502&from=FR

et, le cas échéant, des délibérations rendues par la chambre sécurité sociale et santé du Comité de sécurité de l'information.

- CRITÈRE 7: INFORMATION, FORMATION ET SENSIBILISATION

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

- CRITÈRE 8: CONTRÔLE INTERNE

L'organisation organise un contrôle interne régulier quant au respect des critères contenus dans le présent document et des directives visant à les implémenter. Elle conserve les résultats de ce contrôle interne pendant 2 ans. Elle prévoit aussi des sanctions dissuasives à l'égard des utilisateurs au sein du cercle de confiance qui ne respectent pas les critères.

- CRITÈRE 9: RESPECT DES DÉLIBÉRATIONS DU COMITÉ DE SÉCURITÉ DE L'INFORMATION

L'organisation assure respecter 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 de la chambre sécurité sociale et santé du Comité de sécurité de l'information, rendues en application de l'article 15 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale.

- CRITÈRE 10: DOCUMENTATION PUBLIQUE

L'organisation publie sur son site web, en des termes compréhensibles, les finalités pour lesquelles elle traite des données à caractère personnel du datawarehouse marché du travail et protection sociale ainsi que les directives implémentant le principe de proportionnalité.

- CRITÈRE 11: CONTRÔLE EXTERNE

Les documents et directives élaborés par l'organisation en vue du respect de ces conditions, ainsi que les résultats du contrôle interne sont tenus à la disposition des organes de contrôle par l'organisation.