BANQUE CARREFOUR
D'ÉCHANGE DE DONNÉES

BCED-WI - Engagement de confidentialité des utilisateurs

1. Contexte

La Banque Carrefour d'Echange de Données (BCED) met en place des services d'accès hautement sécurisés afin d'assurer le transport fiable et la distribution des données dans le respect des bonnes pratiques de la sécurité des systèmes d'information. La BCED se préoccupe tout particulièrement de la sécurité dans le cadre du partage de données à caractère personnel.

Les données sont traitées conformément aux dispositions du 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 (RGPD). Pour rappel, la notion de données à caractère personnel ne se limite pas aux informations relatives à la vie privée des personnes mais couvre toute information se rapportant à une personne physique identifiée ou identifiable, de manière directe ou indirecte. Ainsi, même les informations qui se rapportent à la vie professionnelle ou publique d'une personne physique sont considérées comme des « données à caractère personnel ».

Ce document définit les règles et bonnes pratiques à respecter par les utilisateurs du système d'information BCED-WI, mis à disposition par la BCED. Ce document est un des composants du Référentiel de Sécurité qui regroupe l'ensemble des règles standard devant être appliquées pour garantir, de manière cohérente et efficace, la politique de sécurité de la BCED et de l'outil BCED-WI.

2. Comportement général

1.1. Comportement attendu des utilisateurs

Chaque utilisateur est personnellement responsable de l'usage qu'il fait des ressources informatiques auxquelles il a accès. Il a la charge de contribuer par son comportement à la sécurité générale des systèmes d'information mis à disposition par la BCED.

Le comportement inadéquat d'un seul utilisateur peut gravement compromettre la confidentialité d'informations concernant des personnes physiques ou morales, ainsi que la disponibilité des ressources informationnelles.

Une attention particulière doit être accordée au respect des règles de sécurité. La prudence et la vigilance sont de nécessité absolue afin d'éviter tout comportement facilitant la divulgation d'informations confidentielles.
L'utilisateur doit verrouiller les sessions actives de son poste de travail chaque fois qu'il ne peut en assurer la surveillance physique (même pour un délai très bref).

1.2. Limitation des accès aux ressources informationnelles

La BCED est particulièrement attentive aux principes qui régissent les protocoles / autorisations d'accès aux données à caractère personnel, notamment :

- **la finalité** : Les données à caractère personnel ne peuvent être recueillies et traitées que pour un ou plusieurs usages déterminés et légitime ;
- **la proportionnalité** : Seules doivent être accédées les informations pertinentes et nécessaires à l'accomplissement des finalités ;
- **la sécurité des traitements** : L'accès des utilisateurs aux données fournies par l'intermédiaire de l'outil BCED-WI doit être encadré par des mesures de sécurités techniques et organisationnelles appropriées pour garantir la sécurité des données à caractères personnel, notamment contre les risques de traitements non autorisés ou illicites).

Concrètement, cela signifie notamment que :

- les données à caractère personnel ne peuvent être recueillies et traitées que dans le cadre strict des conditions fixées par l'autorisation de la source authentique, du Comité de sécurité de l'information (sur base de la demande que vous avez introduite) ou du protocole d'accord directement conclu avec le fournisseur de données authentiques;

- les données à caractère personnel ne peuvent jamais être communiquées à des tiers[1] ni utilisées à d'autres fins que celles reprises dans l'autorisation ou le protocole d'accord ;
- les données à caractère personnel ne peuvent être recueillies et traitées que par les agents dument identifiés auprès de la BCED comme utilisateurs et qui ont signé le présent engagement de confidentialité, à l'exclusion de tout autre agent, y compris à l'intérieur de votre service ;
- même si l'outil mis à disposition par la BCED permet l'accès à d'autres données que celles énumérées dans l'autorisation ou le protocole , ces données ne peuvent en aucun cas être utilisées. L'agent reste le seul responsable d'une utilisation non conforme des données.

3. Principes généraux de gestion des accès

2.1. Gestion des droits d'accès

Chaque utilisateur reçoit un identifiant unique en lien avec son contexte d'utilisateur lui permettant de s'authentifier sur l'outil BCED-Wi.. Ces données sont strictement personnelles et la confidentialité des moyens d'authentification doit être absolue. Par conséquent, il est absolument interdit de partager ces données.

2.2. Gestion des données et des informations

Le traitement des données à caractère personnel est soumis au RGPD ainsi qu'aux autres législations belges ou européennes applicables (loi du 30 juillet 2018, textes légaux spécifiques à une base de données déterminée,…).

Sont inclus dans le terme « traitement » : la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

4. Traces et contrôles

Les accès aux systèmes et aux données via BCED-Wi se font sous le contrôle et la responsabilité de la BCED. Dès lors, ils font l'objet de prise de traces pour la gestion et la surveillance des systèmes. Ces traces peuvent contenir des données à caractère personnel concernant l'utilisateur. Dans ce cadre, la BCED est elle-même soumise aux obligations issues du RGPD et s'engage à prendre toutes les mesures de sécurité adéquates afin de préserver la confidentialité de ces données.

L'accès aux traces respecte les prescrits de la politique de sécurité de la BCED en la matière, qui garantit la confidentialité des traces informatiques contenant des données à caractère personnel.

Seul le Délégué à la protection des données et son représentant auprès de la BCED ou le conseiller en sécurité de la BCED peuvent avoir accès à ces traces.

5. Incidents

On entend par « incident » tout incident de sécurité ou toute violation de données personnelles.

Est considéré comme tel tout évènement potentiel ou avéré impactant ou présentant une probabilité forte d'impacter l'information dans ses critères de Disponibilité, d'Intégrité, de Confidentialité et/ou de Preuve.

Un incident peut correspondre à une action malveillante délibérée ou non, au non-respect de la politique de sécurité ou du présent engagement, ou d'une manière générale à toute atteinte aux informations, à toute augmentation des menaces sur la sécurité de l'information ou à toute augmentation de la probabilité de compromission des opérations liées à l'activité de traitement des informations.

L'incident peut entraîner, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

[1] Par tiers, on entend toute personne externe à l'entité
Selon le RGPD, il s'agit d'une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel

Tout incident ou suspicion d'incident devra être notifié dans les meilleurs délais – et au plus tard dans les 72h de sa découverte – :

- au supérieur hiérarchique
- au conseiller en sécurité ou au délégué à la protection des données de votre organisme,
- au représentant du délégué à la protection des données de la BCED ainsi qu'au conseiller en sécurité de la BCED.

La notification de l'incident auprès du conseiller en sécurité de la BCED ne vous libère en aucun cas de vos obligations de notification de l'incident à l'Autorité de protection des données et, le cas échéant, de communication auprès des personnes physiques dont les données ont été violées, en vertu des articles 33 et 34 du RGPD.

6. Sanctions en cas de non-respect

Le non-respect des règles contenues dans le présent engagement ainsi que dans les conditions générales d'utilisation de BCED-WI peuvent entrainer une clôture temporaire ou définitive de votre accès au système d'information BCED-WI.

En outre, ces violations peuvent constituer une infraction à l'autorisation ou au protocole qui justifie votre accès aux données. Dans de tel cas, l'autorité détentrice des données (source authentique) peut décider de suspendre ou mettre fin à votre accès.

Enfin, ces infractions peuvent également constituer, dans le chef du responsable du traitement, une violation des législations spécifiques encadrant la sécurité de l'information (RGPD, loi du 30 juillet 2018, …) et sont, à ce titre, passibles de poursuites administratives (devant l'Autorité de Protection des Données), civiles (devant le Président du Tribunal de première instance), et pénales. Le cas échéant, la responsabilité civile et/ou pénale individuelle de l'agent qui s'est rendu coupable d'une violation de ces normes peut être engagée.