BCED-WI - Engagement de confidentialité des utilisateurs

1. Contexte

La Banque Carrefour d'Echange de Données (BCED) assure le transport fiable et la distribution des données par des services d'accès hautement sécurisés dans le respect des bonnes pratiques de la sécurité des systèmes d'information. La BCED se préoccupe tout particulièrement de la problématique de la sécurité dans le cadre du partage de données à caractère personnel. Dans ce cas, les données sont traitées conformément aux dispositions de la loi du 8 décembre 1992 relative au traitement de données à caractère personnel.

Pour rappel, cette notion ne se limite pas aux informations relatives à la vie privée des personnes. Même les informations qui se rapportent à la vie professionnelle ou publique de quelqu'un d'une personne sont considérées comme des "données à caractère personnel».

Ce document a pour objectif de définir 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

2.1. Comportement attendu des utilisateurs

Chaque utilisateur est responsable de l'usage qu'il fait des ressources informatiques auxquelles il a accès. Il a aussi la charge, à son niveau, 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.

Le respect des règles de sécurité, mais aussi la prudence et la vigilance sont donc d'absolues nécessités. Une attention particulière doit être accordée aux conditions d'utilisation facilitant la divulgation d'informations confidentielles. A ce titre, l'utilisateur doit verrouiller les sessions actives de sa station de travail lorsqu'il ne peut en assurer la surveillance physique.

2.2. Limitation des accès aux ressources informationnelles

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

- la finalité (Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime)
- la proportionnalité (Seules doivent être accédées les informations pertinentes et nécessaires pour leur finalité).

Concrètement, cela signifie notamment que :

- les données à caractère personnel ne peuvent être recueillies et traitées que dans le strict but de répondre à l'autorisation obtenue de la CPVP sur base de la demande introduite par votre service ;
- les données à caractère personnel ne seront pas communiquées à des tiers ni utilisées à d'autres fins que celle correspondant à la demande d'autorisation ;
- les données à caractère personnel ne peuvent être recueillies et traitées que par vous et 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 que la BCED met à votre disposition permet l'accès à d'autres données que celles initialement approuvées, vous restez le seul responsable de l'utilisation de ces informations à des fins opposées aux principes de finalité et de proportionnalité.

3. Principes généraux de gestion

3.1. Gestion des droits d'accès

Les utilisateurs reçoivent des identifiants et des moyens d'authentification dépendant de leur contexte d'utilisation des ressources. Ces données sont individuelles et la confidentialité des moyens d'authentification doit être préservée. Les moyens d'authentification sont strictement personnels et doivent être tenus secrets.

3.2. Gestion des données et des informations

Le traitement des données à caractère personnel est soumis aux règles de la Loi Vie privée. 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 sous la responsabilité de la BCED font l'objet de traces pour la gestion et la surveillance des systèmes. Ces traces peuvent contenir des données à caractère personnel vous concernant. Dans ce cadre, la BCED s'engage à prendre les meilleures mesures de sécurité afin d'éviter que des tiers n'abusent des données à caractère personnel que vous avez communiquées, par votre accès à l'outil mis à disposition par la BCED. 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.

5. Incidents

On entend par « incident de sécurité » tout évènement potentiel ou avéré impactant ou présentant une probabilité forte d'impacter la sécurité de l'information dans ses critères de Disponibilité, d'Intégrité, de Confidentialité et/ou de Preuve. Un incident de sécurité peut correspondre à une action malveillante délibérée, 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.

Tout incident lié à la sécurité de l'information devra être notifié dans les meilleurs délais au conseiller en sécurité de votre organisme, ainsi qu'au conseiller en sécurité de la BCED.

6. Sanctions en cas de non-respect

Les enfreintes aux règles de la BCED et aux lois régissant la sécurité de l'information sont passibles de sanctions disciplinaires, qui peuvent être appliquées conformément à la loi ou au règlement de travail. Le cas échéant, la responsabilité civile et/ou pénale individuelle peut être engagée. Certaines fautes peuvent relever de la criminalité informatique ou d'autres dispositions d'ordre pénal ; elles peuvent alors donner lieu à des poursuites judiciaires.

Je soussigné, ……..,
déclare avoir lu et accepté l'engagement de confidentialité lié à l'usage de l'outil BCED-WI.

(Date et signature)