COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE (CPVP) – Comité sectoriel pour l'Autorité fédérale

DÉCLARATION DE CONFORMITÉ RELATIVE À LA SÉCURITÉ DU SYSTÈME D'INFORMATION FAISANT L'OBJET D'UNE DEMANDE D'AUTORISATION OU D'ADHÉSION

Cette déclaration de conformité concerne :

☐ une nouvelle demande d'autorisation

☐ une autorisation déjà accordée par la délibération …. ……. / ……. du …. / ….. / ……..

☐ une demande d'adhésion à l'autorisation générale accordée par la délibération …. ……. / ……. du …. / ….. / ……..

Organisme demandeur responsable du traitement	
Nom :	
Abréviation officielle :	
Adresse officielle :	
Numéro entreprise (BCE) :	
Numéro de l'unité d'établissement (BCE) :	

Responsable de la gestion journalière :	
Coordonnées	
Titre :	
Nom :	
Prénom :	
Adresse de contact :	
Téléphone	
E-mail :	
Langue :	

Je soussigné, **responsable de la gestion journalière du traitement** de données à caractère personnel faisant directement l'objet de la demande d'autorisation ou d'adhésion à une autorisation générale, ci-après : 'le traitement en question',

certifie que, pour le traitement en question, et conformément aux obligations prévues par la Loi Vie Privée et les autres lois en vigueur, et comme le recommandent les Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel éditées par la CPVP,

les mesures techniques et organisationnelles appropriées ont été mises en place de façon à être opérationnelles, au plus tard pour la date de mise en exécution de ce traitement, de manière à assurer un niveau de protection adéquat des données à caractère personnel traitées tout en tenant compte,

- de la nature des données à caractère personnel traitées et de leur traitement ainsi que des exigences en matière de confidentialité, intégrité et disponibilité ;
- des exigences légales ou réglementaires qui seraient d'application ;
- de la taille de l'organisme (incluant le nombre et le profil des personnes susceptibles d'accéder aux données) ;
- de l'importance et de la complexité des systèmes d'information, systèmes informatiques et applications concernés ;
- de l'ouverture de l'organisme vers l'extérieur ainsi que des accès depuis l'extérieur ;
- des risques encourus tant pour l'organisme lui-même que pour les personnes dont les données à caractère personnel sont traitées ;
- de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures ;

certifie que, au plus tard pour la date de mise en exécution de ce traitement, les aspects suivants de la sécurité auront été finalisés (cocher la case correspondante) :

1. Un conseiller en sécurité de l'information ayant déjà reçu une approbation pour cet organisme a été chargé de veiller à la mise en application de la politique de sécurité lors de l'exécution de ce traitement. OUI ☐ / NON ☐

Coordonnées du conseiller en sécurité de l'information	
Nom :	
Prénom :	
Date de naissance :	

Ce conseiller en sécurité de l'information a déjà reçu une approbation pour cet organisme par une autorité de contrôle OUI ☐ / NON ☐

Si non, l'identité et le profil du conseiller en sécurité de l'information proposé ont été communiqués à la CPVP pour accord via le questionnaire d'évaluation ad hoc[1] OUI ☐ / NON ☐

[1] http://www.privacycommission.be/sites/privacycommission/files/documents/explications-questionnaire-evaluation-conseiller-en-securite-af_0.pdf

2. L'évaluation des risques OUI ☐ / NON ☐

   Une évaluation des risques encourus par les données à caractère personnel traitées a été réalisée et les besoins de sécurité ont été définis en conséquence.

3. La politique de sécurité de l'information OUI ☐ / NON ☐

   Un document écrit – la politique de sécurité de l'information – précisant les stratégies et mesures retenues pour sécuriser les données à caractère personnel traitées a été élaboré.

4. L'identification des supports OUI ☐ / NON ☐

   Tous les supports, quels qu'ils soient et impliquant les données à caractère personnel traitées, ont été identifiés.

5. L'information du personnel OUI ☐ / NON ☐

   Le personnel interne et externe impliqué dans ce traitement a été informé de ses devoirs de confidentialité et de sécurité vis-à-vis des données à caractère personnel traitées découlant aussi bien des différentes exigences légales que de la politique de sécurité.

6. La sécurisation physique des accès OUI ☐ / NON ☐

   Des mesures de sécurité adéquates ont été mises en place afin de prévenir les accès physiques inutiles ou non autorisés aux supports contenant les données à caractère personnel traitées.

7. La sécurité physique et environnementale OUI ☐ / NON ☐

   Les mesures de sécurité nécessaires ont été mises en place afin de prévenir les dommages physiques pouvant compromettre les données à caractère personnel traitées.

8. La sécurisation des réseaux OUI ☐ / NON ☐

   Les différents réseaux auxquels sont reliés les équipements traitant les données à caractère personnel ont été protégés.

9. La liste des personnes habilitées OUI ☐ / NON ☐

   Une liste actualisée des différentes personnes habilitées à accéder aux données à caractère personnel dans le cadre de ce traitement, reprenant leur niveau d'accès respectif (création, consultation, modification, destruction), a été établie.

10. La sécurisation logique des accès OUI ☐ / NON ☐

    Un mécanisme d'autorisation d'accès conçu de façon à ce que les données à caractère personnel traitées et les traitements les concernant ne soient accessibles qu'aux personnes et applications explicitement autorisées a été mis en place.

11. La journalisation des accès OUI ☐ / NON ☐

    Le système d'information a été conçu de façon à permettre une journalisation, un traçage et une analyse permanents des accès des personnes et entités logiques aux données à caractère personnel traitées.

Le cas échéant, une attention suffisante aura été portée aux aspects suivants de la sécurité.

12. La surveillance, la révision et la maintenance OUI ☐ / NON ☐

    Un contrôle de la validité et de l'efficacité dans le temps des mesures techniques ou organisationnelles mises en place a été prévu.

13. La gestion d'urgence des incidents de sécurité de l'information OUI ☐ / NON ☐

    Des procédures de gestion d'urgence des incidents de sécurité impliquant les données à caractère personnel traitées ont été mises en place.

14. La documentation OUI ☐ / NON ☐

    Une documentation suffisante concernant l'organisation de la sécurité de l'information dans le cadre du traitement en question a été constituée et sera tenue à jour.

Je certifie sur l'honneur que les renseignements fournis sont conformes à la réalité[2].

Date : Signature :

[2] Toute déclaration non conforme à la réalité peut être considérée comme un faux en écriture engageant la responsabilité pénale du responsable du traitement.

Les documents sont tenus à la disposition du Comité qui peut en demander copie ou procéder à un examen sur place pour vérifier l'état de la sécurité de l'information.