Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel[1]

Version 1.0

Le présent document reprend une liste d'onze domaines d'actions liées à la sécurité de l'information pour lesquels tout organisme - personne morale[2], entreprise ou administration -qui conserve, traite ou communique des données à caractère personnel doit prendre des mesures.

Vu l'extrême diversité des situations concrètes rencontrées, il n'est pas possible de définir précisément les actions à entreprendre pour chaque cas.

Chacune des mesures de référence ci-dessous devra donc être adaptée au contexte et aux spécificités de chaque organisme et nécessitera la mise en œuvre de solutions pratiques dont le niveau de détail ou de complexité devra être proportionnel aux besoins réels de l'organisme, en tenant compte :

- de la nature des données à caractère personnel traitées et de leurs traitements ainsi que des exigences en matière de confidentialité, intégrité et disponibilité ;
- des exigences légales ou règlementaires qui seraient d'application ;
- de la dimension 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 personnelles sont traitées,
- ainsi que `de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures'[3].

La sécurité de l'information étant un domaine en perpétuelle évolution, ces mesures de référence seront adaptées progressivement aux différentes évolutions légales, techniques ou autres.

---

[1] Le présent document est destiné aux responsables de traitement dans le but de les aider à mettre en place un environnement sécurisé conformément à l'obligation prévue à l'article 16 de la Lo i relative à la protection des données à caractère personnel du 8 décembre 1992.

[2] Ceci ne dispense pas les personnes physiques de l'obligation de se conformer à l'article 16 de la Loi relative à la protection des données à caractère personnel du 8 décembre 1992, lequel prévoit des obligations en matière de sécurité applicables à tout responsable de traitement. 3 Loi relative à la protection des données à caractère personnel du 8 décembre 1992.

[3] Loi relative à la protection des données à caractère personnel du 8 décembre 1992.

1. Politique de sécurité de l'information

Tout organisme traitant des données à caractère personnel doit rédiger un document écrit – la politique de sécurité de l'information – précisant les stratégies et mesures retenues pour sécuriser ces données.

Afin de déterminer adéquatement ces dernières, l'organisme doit initier sa démarche de sécurisation par une réflexion à propos des menaces potentielles pesant sur les données à caractère personnel traitées et une évaluation des risques réellement encourus par celles-ci.

La politique de sécurité de l'information comprendra :

- l'exposé de la démarche d'analyse des risques relatifs aux données à caractère personnel ;
- les priorités retenues et les mécanismes mis ou à mettre en place consécutivement à cette analyse des risques ;
- le planning de mise en œuvre ;
- la description des différentes responsabilités et des règles organisationnelles mises en place ;
- la description du processus de gestion des incidents de sécurité ;
- la description du processus de sensibilisation de l'organisme à cette politique ;
- les dispositions retenues afin de maintenir à jour le système de sécurisation une fois installé.

Cette politique de sécurité de l'information doit être approuvée par le plus haut niveau de la hiérarchie ainsi que par les divers responsables et suffisamment diffusée au sein de l'organisme afin d'être connue de tous.

Elle doit être actualisée au moins une fois par année, ou en cas de modification ou de réévaluation.

2. Organisation de la sécurité de l'information

En fonction de la nature des données à caractère personnel utilisées/traitées et des termes de l'autorisation accordée, un conseiller en sécurité de l'information doit être désigné au sein de l'organisme en tant que responsable de l'exécution de la politique de sécurité de l'information.

Il rapporte directement à la direction de l'organisme et doit disposer des moyens suffisants (en temps, en ressources humaines et matérielles et en budget) et avoir accès, sans contraintes, aux informations nécessaires à sa fonction, pour autant qu'il reste dans le cadre de la politique de sécurité de l'information.

Il veillera à ce que les différentes responsabilités en matière de sécurité de l'information (prévention, surveillance, détection et traitement) soient clairement identifiées et que les personnes en charge de la sécurité de l'information puissent agir en toute indépendance à l'abri des pressions d'intérêts particuliers et contradictoires.

Il devra disposer des compétences et formations nécessaires et ne pourra exercer de fonction(s) ou de responsabilité(s) incompatible(s) avec celles de conseiller en sécurité de l'information.

3. Organisation et aspects humains de la sécurité de l'information

L'organisme doit définir clairement les responsabilités et processus de gestion en matière de sécurité des données à caractère personnel et les intégrer adéquatement dans son organisation générale et son fonctionnement.

Des moyens organisationnels, techniques et financiers, suffisants et adaptés, doivent être affectés à l'organisation de la sécurité de l'information.

Afin de sécuriser efficacement les données à caractère personnel, l'organisme doit veiller à mettre en place des procédures de classification[4] de l'information permettant d'inventorier et de localiser toutes les données à caractère personnel traitées, et ce, quel qu'en soit le support.

La réussite de la sécurisation d'un système d'information dépendant fortement de l'information correcte des différents acteurs, l'organisme doit prendre les mesures nécessaires afin que toute personne (interne ou externe) intervenant dans le traitement des données personnelles soit constamment suffisamment informée de ses devoirs et responsabilités lors de ces traitements et suffisamment et correctement formée à l'exercice de sa fonction et de ses responsabilités de sécurité de l'information.

D'éventuels suivis disciplinaires doivent être prévus en cas de non-respect des règles édictées et un engagement de confidentialité requis lorsque les risques le justifient.

Lorsque l'organisme sous -traite tout ou partie de ses traitements de données à caractère personnel, il doit veiller à répercuter, dans le contrat de sous-traitance, les mêmes obligations de sécurité de l'information que celles en vigueur au sein de l'organisme lui-même.

4. Sécurité physique et de l'environnement

L'organisme doit prendre les mesures qui s'imposent pour garantir la protection physique des données à caractère personnel.

Pour cela, il doit s'assurer que les supports des données à caractère personnel et les systèmes informatiques les traitant, soient placés, conformément à leur classification, dans des locaux identifiés et protégés et dont l'accès est limité aux seules personnes autorisées et aux seules heures justifiées par leur fonction.

Au cas où une continuité des services s'avère nécessaire, des dispositifs de prévention, de détection et de traitement de dangers physiques tels que les incendies ou les inondations doivent être installés et

[4] 'Classification' est à prendre ici dans son sens premier de classement, tel qu'utilisé habituellement en sécurité des systèmes d'informations, c'est-à-dire qualification de l'information et non pas tel que prévu dans la loi du 11 décembre 1998 – Loi relative à la classification et aux habilitations, attestations et avis de sécurité.

régulièrement contrôlés. L'organisme doit aussi prendre les mesures de sauvegarde (back up) nécessaires afin de pouvoir contrer la perte ou l'altération accidentelle de données à caractère personnel.

5. Sécurisation des réseaux

L'organisme doit s'assurer que les réseaux auxquels sont connectés les équipements impliqués dans le traitement des données à caractère personnel garantissent la confidentialité et l'intégrité de celles-ci.

Lorsque le réseau interne de l'organisme est connecté à un réseau externe public, l'organisme doit prendre les mesures nécessaires afin de protéger le ou les réseaux impliqué(s) dans le traitement des données à caractère personnel contre tout accès non autorisé (intrusions, codes malveillants, etc.).

6. Sécurisation logique des accès

L'organisme doit s'assurer que les données à caractère personnel ne soient accessibles, conformément à leur classification, qu'aux personnes et aux applications qui en ont explicitement l'autorisation.

Il maintiendra à jour une liste actualisée des différentes personnes habilitées à accéder et traiter ces données et de leurs pouvoirs respectifs (création, consultation, modification, destruction).

Ces différentes autorisations doivent être traduites en dispositifs techniques et contrôles d'accès aux différents éléments informatiques (programmes, procédures, éléments de stockage, équipements de télécommunication, etc.) intervenant dans le traitement des données à caractère personnel.

Ces dispositions techniques doivent inclure les activités en amont (développement applicatif) et en aval (gestion des exemplaires de sauvegarde).

Si le niveau de sécurité l'impose, l'identification des intervenants sera complétée par une procédure d'authentification.

7. Journalisation, traçage et analyse des accès

L'organisme doit mettre en œuvre des mécanismes de journalisation et de traçage.

Ces derniers doivent permettre de retrouver, en cas de nécessité, l'identité de l'auteur de tout accès aux données à caractère personnel ou de toute manipulation de celles-ci. L'enregistrement de ces informations de contrôle peut concerner, suivant les cas, l'accès physique, l'accès logique ou les deux.

La granularité des enregistrements, la localisation et la durée de conservation de ceux-ci, la fréquence et le type des manipulations effectuées sur ceux-ci dépendent du contexte. Des mécanismes supplémentaires de détection d'intrusion pourraient être requis. Le conseiller en sécurité de l'information doit être en mesure de justifier la politique adoptée.

Les données de traçage étant elles-mêmes des données à caractère personnel, tout traitement de celles-ci doit s'accompagner des mesures de sécurité adéquates.

8. Surveillance, revue et maintenance

L'organisme doit s'assurer que les mesures de sécurité techniques ou organisationnelles sont validées et font l'objet de révisions régulières.

Les besoins de maintenance de la sécurité doivent pouvoir être détectés par une surveillance portant sur les traitements, l'évolution des ressources et l'analyse des journaux de traçage.

Les systèmes d'information et les risques auxquels ils sont exposés étant en constante évolution, l'organisme s'assurera régulièrement (au moins une fois par an) que les objectifs initialement poursuivis et les mesures de sécurité mises en place consécutivement restent d'actualité afin d'y apporter les éventuels correctifs, si nécessaire.

Dans tous les cas de réorganisation de l'organisme ou de modification de son infrastructure, une réactualisation des mesures de sécurité sera effectuée.

9. Gestion des incidents de sécurité et de la continuité

L'organisme doit posséder un plan de gestion des incidents de sécurité.

En cas d'incidents mettant en péril la confidentialité et l'intégrité des données à caractère personnel, la rapidité d'intervention est primordiale pour réduire les conséquences d'une telle situation. Pour ce faire, l'organisme doit avoir prévu les procédures spécifiant la marche à suivre en cas de détection d'incident de sécurité relatifs aux données à caractère personnel ainsi que les personnes responsables pour gérer l'incident et restaurer une situation saine.

En outre, les conditions de l'incident doivent être analysées afin d'en déduire les mesures préventives ou correctrices destinées à éviter la reproduction de ce genre d'incident ou de permettre un retour plus rapide à une situation normale.

Les organismes, contraints d'assurer la continuité de leurs services, doivent :

- prévoir les plans de recouvrement et de continuité permettant de couvrir les incidents de sécurité pouvant provoquer des interruptions de service dépassant les délais acceptables ;
- veiller particulièrement à ce que la confidentialité et l'intégrité des données personnelles soient toujours assurées lors de l'exécution de ces divers plans.

10. Respect des dispositions légales et normatives

Tout organisme doit respecter à tout moment les règles et lois en vigueur en matière de traitement et de protection des données à caractère personnel. Cette législation est toujours disponible sur le site Internet de la Commission vie privée, dans la rubrique "Législation et normes".

Ainsi, la Loi vie privée stipule très précisément les conditions et les circonstances d'un traitement ou d'un transfert de données à caractère personnel. Tout organisme a l'obligation de vérifier au préalable du traitement si l'exécution du traitement, étant donné la nature délicate des données, n'est pas sujet à un autorisation et il doit toujours veiller à ce que les conditions de cette autorisation soient respectées.

L'organisme doit régulièrement organiser un audit relatif à la sécurité des données à caractère personnel utilisées/traitées.

11. Documentation

L'organisme doit disposer d'une documentation complète et régulièrement mise à jour concernant la sécurité des informations.

Toute la documentation nécessaire à la bonne gestion de la sécurité des données à caractère personnel doit être constituée par l'organisme. Elle doit être complète, formalisée, proportionnelle à ses besoins de sécurité, continuellement mise à jour, et répertoriée de manière à pouvoir être disponible en temps utile à qui de droit.

Cette documentation doit comprendre au moins :

- l'identité du conseiller en sécurité de l'information ;
- la politique de sécurité de l'information ;
- le plan de mise en œuvre des mesures de sécurité ;
- l'inventaire des données à caractère personnel traitées, de leurs localisations et des traitements effectués ;
- la liste nominative des organes ou préposés ayant accès à ces données ;
- la configuration des systèmes et des réseaux ;
- la documentation technique des mesures de sécurité mises en place ;
- le calendrier des opérations planifiées
- la politique de traçage retenue ;
- les plans de tests des mesures de sécurité ;
- les rapports d'incidents ;
- les éventuels rapports d'audit.