Recommandation n° 01/2013 du 21 janvier 2013

Objet : Recommandation d'initiative relative aux mesures de sécurité à respecter afin de prévenir les fuites de données (CO-AR-2013-001)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 30 ;

Vu le rapport de M. F. Robben, Mme F. D'Hautcourt et M. E. Gheur ;

Émet la recommandation suivante, le 21 janvier 2013 :

I. OBJET DE LA RECOMMANDATION

1. Suite à plusieurs événements concrets[1] qui se sont produits récemment et qui ont été abondamment commentés dans les médias, la Commission a considéré qu'il convenait d'entreprendre immédiatement une action pour mettre fin à des fuites de données involontaires et illicites, appelées *data breaches*, dont elle a constaté qu'elles étaient généralement dues à une sécurisation insuffisante des données.

2. L'évolution de la technologie et de l'interconnexion entre les systèmes d'informations, la dématérialisation de ces dits systèmes ainsi que de leurs supports et la multiplication des informations numériques ne font qu'accroître le risque de divulgation de données à des personnes qui n'ont pas à y avoir accès.

3. La disponibilité inadéquate de données à caractère personnel sur Internet constitue un problème majeur, et ce d'autant plus que ces données peuvent avoir une valeur marchande et que leur diffusion en devient incontrôlable à l'heure actuelle si des mesures de sécurité appropriées ne sont pas prises par chaque responsable du traitement.

4. À cet égard, une structure informatique défaillante se trouve souvent à l'origine du problème et, combinée à un manque de moyens de contrôle suffisamment intégrés (le principe des quatre yeux) et à l'absence d'un système qui détecte et rectifie les erreurs à temps, elle constitue le terreau idéal pour des fuites de données. Dans un souci permanent de prévenir de telles situations, la Commission formule dès lors les recommandations suivantes.

II. MESURES DE SECURITÉ

2.1. LA SECURITE DES SYSTEMES EN GENERAL : ÉVALUATION DES RISQUES ET POLITIQUE DE SECURITE

5. La sécurité de l'information consiste à protéger les informations traitées par une organisation d'une multitude de risques, qu'il s'agisse de menaces (actions extérieures ou intérieures malveillantes) ou de vulnérabilités (risques propres aux systèmes et applications), et permet ainsi de garantir la confidentialité, l'intégrité ainsi que la disponibilité des données.

[1] Publication en ligne via Google de la liste de clients de SNCB Europe concernant 1.500.000 personnes le 22 décembre 2012, publication d'une liste de 500 collaborateurs de la Défense le 3 janvier 2013 et publication similaire le 8 janvier 2013 des données salariales de 15.000 personnes sur la base d'une enquête sur les salaires réalisée par Jobat.

6. Cette sécurité doit être assurée par la mise en œuvre de mesures adéquates regroupant structures organisationnelles, règles, processus, procédures mais également systèmes techniques.
   L'ensemble de ces mesures doivent être déterminées et documentées, implémentées, auditées et améliorées aussi souvent que nécessaire, et ce de manière à atteindre les objectifs spécifiques en matière de sécurité de l'information.

7. Les mesures de sécurité publiées par la Commission et la norme ISO/IEC 27002 peuvent offrir à cet égard un cadre de référence général adéquat.

8. De plus, ces mesures doivent être élaborées, en concertation avec le reste des processus business de l'organisation (les utilisateurs des applications), à partir de l'identification des exigences en matière de sécurité de l'information. Ces exigences sont issues :

- de l'évaluation méthodique des risques liés à l'entité et aux traitements des données ;
- des aspects légaux applicables ;
- des principes et exigences métier en matière de traitement de l'information.

9. L'analyse de risques doit considérer à la fois la sécurité physique, la sécurité au niveau système, la sécurité au niveau applicatif, la sécurité au niveau réseau et communication (y compris, la sécurité des systèmes de stockage tels que USB, …).

10. La mise en place de la sécurité de l'information doit être à l'initiative, au support et à la responsabilité du management de l'entreprise, mais nécessite la participation de l'ensemble des acteurs impliqués dans le traitement de l'information : informaticiens, responsables administratifs des procédures et membres de la direction.

11. La politique de sécurité prévoira d'informer de manière continue les collaborateurs de l'organisation des risques encourus en termes de sécurité de l'information ainsi que de leurs obligations légales dans le cadre de la collecte, du stockage et de la manipulation de données à caractère personnel.

2.2. ARCHITECTURE INFORMATIQUE

12. L'architecture informatique doit garantir la sécurisation des systèmes de traitement de l'information ainsi que des données accessibles, et plus particulièrement celles accessibles à partir d'Internet.

2.2.1. ARCHITECTURE INFORMATIQUE LOCALE

13. Elle sera basée sur le principe des couches de sécurité, en implémentant une segmentation logique et/ou physique des zones. L'accès direct aux systèmes applicatifs depuis Internet sera contrecarré par l'utilisation simultanée de divers moyens disponibles selon les cas, par exemple des serveurs relais tels "Proxy/Reverse Proxy", par la translation des adresses IP, par un pare-feu (firewall) ou un routeur convenablement paramétrés.

14. Il est impératif, dans une version minimale, de séparer le réseau local des machines accessibles depuis Internet, par exemple en mettant en œuvre firewall/proxy et DMZ. Un système permettant le filtrage des flux entre ces zones doit être implémenté et ses alertes doivent être suivies et traitées dans des délais raisonnables.
    Une option pour atteindre le but est d'implémenter une structure plus solide, ayant au minimum trois zones "DMZ", une par niveau :

    - Proxy/Reverse Proxy ;
    - Application Web ;
    - Système de base de données contenant des données à caractère personnel.

    D'autres options garantissant la séparation complète des flux sont possibles et donc tout aussi acceptables.

15. Parallèlement, un système permettant l'analyse et la vérification des requêtes venant de l'Internet en direction des serveurs de contenu doit être envisagé afin de limiter l'exposition à des vulnérabilités détectées dans la logique applicative ("Web Application Firewall"). Les vulnérabilités les plus courantes, comme le "SQL injection", doivent avoir été corrigées.

16. En fonction des ressources disponibles, la mise en place et le suivi d'un système de détection (et de prévention) d'intrusion ("IDS/IPS") sont un plus permettant de repérer des activités anormales ou suspectes.

17. Tous ces dispositifs assurant la sécurité doivent être documentés et l'organisation doit réaliser de manière régulière des tests de sécurité de ses infrastructures.

2.3. SECURITE DES DONNEES A CARACTERE PERSONNEL

18. Les systèmes de base de données contenant des données à caractère personnel ne peuvent être accessibles qu'à partir d'applications sécurisées dédiées, et ce d'autant plus s'il est possible d'accéder aux applications et donc à ces données depuis une zone non sécurisée.

19. Les serveurs détenant ces données ne peuvent être publiquement accessibles sur Internet. L'indexation par les robots liés aux moteurs de recherche tels que Google, Bing, etc. sera limitée à ce qui est légitime (voir ci-après).

20. Les échanges de données sensibles ou à caractère personnel avec des tiers ne peuvent se faire qu'avec des systèmes sécurisés[2].

21. Enfin, les extractions de données qualifiées/classifiées d'un système de base de données de production doivent être limitées et contrôlées.

2.4. CYCLE DE DEVELOPPEMENT/PRODUCTION

22. Il s'agit de réaliser une stricte séparation des environnements de développement, test, acceptation/intégration et production et de n'accorder des accès à l'environnement de production qu'aux gestionnaires systèmes dûment autorisés et identifiés.

23. Afin d'assurer une bonne ségrégation des fonctions et accès aux systèmes d'information, la Commission recommande :

- d'interdire l'accès aux systèmes d'application et de contenu en production aux développeurs ;
- de mettre en place des procédures pour que la mise en production de contenus, d'applications, voire de données soit réalisée par une équipe dédiée (Release Management). Lors de la mise en production de contenu tant statique que dynamique (application), il s'agira d'exercer une stricte vérification des pages web et des fichiers y associés et de contrôler les fichiers accessibles en ligne, même et surtout si ces derniers ne sont pas associés à une page web ;
- d'associer les utilisateurs aux vérifications avant la mise en production ;

[2] Tels que l'application eBox utilisée pour les échanges de données entre institutions de la sécurité sociale.

- de limiter, en fonction de la qualification des données, les accès des gestionnaires de bases de données. L'introduction du principe des quatre yeux est recommandée pour la gestion et la consultation des données à caractère personnel.

2.5. GESTION DES INCIDENTS

24. L'organisme doit disposer de procédures d'alertes connues et documentées à appliquer en cas d'incidents portant atteinte à la sécurité des informations à caractère personnel. Ces procédures doivent mentionner l'identification et les coordonnées des responsables à contacter au niveau technique et au niveau management.

25. Une attribution claire des responsabilités de sécurité, que ce soit en régime et/ou en cas d'incident, doit être établie au sein de toute organisation.

26. Plus particulièrement, en cas d'incident public, les autorités compétentes (Commission vie privée) doivent être informées des causes et des dommages endéans les 48 heures.

27. Une campagne d'information au public doit aussi être réalisée 24 à 48 heures au plus tard après notification aux autorités.

2.6. SOUS-TRAITANCE (ARTICLE 16 DE LA LVP)

28. Lorsque le traitement est confié à un sous-traitant, pour une partie ou la totalité de ses services informatiques, l'organisation doit notamment veiller au respect des règles et politiques de sécurité applicables au traitement de l'information par son (ses) sous-traitant(s), tout en clarifiant les rôles et responsabilités de chaque intervenant.

III. CADRE JURIDIQUE

29. L'obligation pour le responsable du traitement de prendre les mesures techniques et organisationnelles requises pour garantir la sécurité des données à caractère personnel traitées est explicitement reprise à l'article 16, § 4 de la LVP, pris en exécution de l'article 17 de la Directive européenne 95/46/CE du 24 octobre 1995 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et de la libre circulation de ces données*. Malgré tout, la Commission constate que dans la pratique, le responsable du traitement n'y est pas assez attentif, avec les conséquences inhérentes et indéniablement néfastes pour les données à caractère personnel des personnes concernées.

30. Bien que la Commission ait déjà pris l'initiative de publier les "Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel" et les "Lignes directrices pour la sécurité de l'information de données à caractère personnel" qui sont déjà destinées à servir de fil conducteur pour le responsable du traitement en vue de la mise en œuvre d'une politique de sécurité efficace en exécution de l'article 16, § 4 de la LVP, les événements récents amènent également la Commission à conclure que le cadre réglementaire existant doit être renforcé, à savoir en complétant l'article 16, § 4 de la LVP de sorte que la Commission ne soit pas seulement compétente pour formuler des recommandations relatives aux mesures de sécurité, mais aussi pour les rendre juridiquement contraignantes. À cette fin, la Commission entend s'adresser au législateur.

31. Du point de vue de la protection de la vie privée, non seulement le manque de garanties de sécurité (article 16, § 4 de la LVP) constitue un problème fondamental, mais l'article 4, § 1, 2° et l'article 9 de la LVP sont également en cause.

32. L'article 4, § 1, 2° de la LVP ne permet pas que des données dont dispose un responsable du traitement soient réutilisées pour une finalité incompatible avec la finalité pour laquelle il a initialement obtenu ces données. Il va de soi que la publication en ligne de données qui n'y étaient pas destinées au départ constitue un traitement de données impliquant une infraction à ce prescrit, laquelle est en outre pénalement sanctionnée par l'article 39, 1° de la LVP.

33. Dans ce contexte, il convient également d'attirer l'attention sur l'article 9 de la LVP. Cette disposition impose au responsable du traitement l'obligation d'informer les personnes concernées des finalités pour lesquelles les données seront utilisées. S'il apparaît ultérieurement que le responsable du traitement a utilisé les données pour une finalité incompatible avec la finalité initiale et à propos de laquelle il n'a fourni aucune information aux personnes concernées, il aura commis une infraction punissable sur la base de l'article 39, 4° de la LVP.

34. Vu l'importance évidente de prévoir les garanties nécessaires en matière de protection des données, la Commission insiste dès lors auprès des responsables du traitement pour que les recommandations ci-avant (point II) relatives aux mesures de sécurité soient scrupuleusement respectées. Mieux encore, en cas de non respect de ces recommandations, la Commission s'engage à mettre en œuvre tous les moyens légaux disponibles permettant de mettre en cause la responsabilité du responsable de traitement, lui faisant encourir le

risque d'être poursuivi. En effet, sauf si la loi en dispose autrement, la Commission dénonce au procureur du Roi les infractions dont elle a connaissance (article 32, § 2 de la LVP).

35. Cet ensemble de règles constitue donc les règles de l'art à respecter par tout responsable du traitement afin d'assurer une sécurité de l'information optimale et partant, de garantir la sécurisation des données à caractère personnel des personnes concernées.

36. La présente recommandation permettra également aux autorités judiciaires, lorsque celles–ci sont saisies de dénonciations ou lorsqu'elles s'en saisissent d'office, d'apprécier tout fait constitutif d'une infraction au sens de la LVP et d'en évaluer la gravité.

37. Enfin, la Commission rappelle que le responsable du traitement est responsable du dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la LVP.
    Il n'est exonéré de sa responsabilité que s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable (article 15*bis* de la LVP).

PAR CES MOTIFS,

la Commission recommande

que tout responsable du traitement respecte scrupuleusement les recommandations ci-dessus et les applique selon les règles de l'art, de manière à appliquer une politique de sécurité par laquelle il se conforme à la norme du bon père de famille.

L'Administrateur f.f., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere