CIRCULAIRE N° 2256 DU 03/04/2008

CIRCULAIRE	~~Informative~~	Administrative	~~Projet~~
OBJET	SECURITE DES DONNEES PERSONNELLES		
DESTINATAIRE	Direction	Fondamental ordinaire (mat/prim)	
RESEAUX	Organisé par la Communauté française		
PÉRIODE	2008		

- Aux Directeurs des établissements d'enseignement fondamental ordinaire organisés par la Communauté française;

ÉMETTEUR	Administration - Direction générale de l'Enseignement obligatoire (DGEO)
SIGNATAIRE	Lise-Anne HANSE
CONTACT	Dubost Guillaume (02 690 85 44, guillaume.dubost@cfwb.be)
DOCUMENTS A RENVOYER	OUI
DATE LIMITE D'ENVOI	A l'expiration des 2 semaines qui suivent la formation à SIEL.

Équipe Sécurité de l'information

Tél. +32 (2) 690.85.44 – Fax +32 (2) 690.85.83
+32 (2) 690.86.18
Administration générale de l'Enseignement et de la Recherche scientifique
Direction générale de l'Enseignement obligatoire

1. Introduction.

Dans le cadre de la gestion interne de votre établissement et de votre relation avec l'Administration, vous récoltez auprès de vos élèves et/ou de leurs représentants légaux un certain nombre d'informations les concernant : ce sont leur date de naissance, leur adresse, leur numéro de téléphone, leur numéro du Registre national, …
Ces informations sont des données à caractère personnel et leur utilisation est soumise à la législation sur la protection de la vie privée. Elle tend à garantir pour chaque personne physique la protection de ses libertés et droits fondamentaux en délimitant l'utilisation de ces informations.
Ceci est essentiel à une époque, où des données personnelles nous concernant sont stockées dans de nombreux organismes, publics ou privés, et s'échangent de plus en plus facilement grâce aux avancées dans les technologies de communication.

Conformément à la loi « vie privée », en tant que directeur de l'école fondamentale, vous êtes considéré comme le responsable du traitement [1] des données qui vous ont été confiées. C'est alors à vous que revient la charge d'en assurer la protection en mettant en place les mesures de sécurité adéquates. Le sujet de la sécurité des données étant vaste et complexe, une équipe Sécurité de l'information a été créée à la Direction Générale de l'Enseignement Obligatoire, avec dans ses missions, l'accompagnement des directeurs d'établissements à la protection des données.

Coordonnées et composition de l'équipe Sécurité de l'information :

Direction générale de l'Enseignement obligatoire
Service des Affaires générales et des Relations internationales
Rue Lavallée, 1 – 1080 Bruxelles

E-mail : securite.dgeo@cfwb.be
M. Guillaume Dubost – Correspondant en sécurité de l'information
☎ : 02/690 85 44 - 🖹 : 02/690 85 83
M. Sébastien Fioroni – Gradué
☎ : 02/690 86 18 - 🖹 : 02/690 85 83

La présente circulaire a pour objectif de vous préciser les grands principes de cette législation et de vous donner des méthodes concrètes pour protéger les données que vous détenez.

Le cas de l'application SIEL sera aussi abordé puisque chaque établissement fondamental du réseau organisé par la Communauté française y introduira ses inscriptions à partir de la rentrée 2008. Cette application vous a été brièvement présentée dans un courrier (réf. LAH/pj/06/2008) envoyé début février. Pour rappel cette application permet l'inscription en ligne de vos élèves vers la DGEO. Les informations ainsi récoltées seront utilisées par les services du comptage des élèves et par les services du contrôle de l'obligation scolaire.
Les zones de texte encadrées concernent directement l'application SIEL.

Lors de leur passage pour la formation à l'application SIEL, les chargés de mission aborderont avec vous le sujet de la sécurité des données et vous accompagneront dans les quelques démarches à mettre en œuvre pour votre établissement.

[1] Art. 1 §4 de la Loi du 8/12/92 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

2. La protection de la vie privée. [2]

Le texte législatif traitant de la vie privée est la loi du 8/12/92 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. La loi du 8/08/83 organisant un registre national des personnes physiques est d'application dès que l'on fait usage des données du Registre national. Les mesures et les principes de protection définis dans les deux textes sont très similaires et la Commission de la Protection de la Vie Privée tend à considérer le traitement de données personnelles de la même manière que le traitement de celles du Registre national. Pour tout complément d'information, le site web de la Commission est accessible à l'adresse : http://www.privacycommission.be

La loi « vie privée » impose un devoir de transparence et des règles d'utilisation des données à caractère personnel. Elle instaure des droits pour les personnes à qui se rapportent ces données. L'application de cette législation doit aboutir à un équilibre entre l'utilisation légitime et proportionnée de ces informations et la protection de la vie privée des personnes concernées.
La collecte et l'utilisation de ces données doivent être transparentes, ce qui signifie, dans votre cas, que la collecte doit se faire directement auprès de la personne concernée, ou de son représentant légal. Cette personne doit pouvoir être informée de l'utilisation que vous en ferez et à qui vous les transmettrez.
Les données récoltées doivent être utilisées pour la réalisation de finalités bien définies, légitimes et proportionnelles. En d'autres mots, il doit y avoir un équilibre entre votre intérêt à les utiliser et l'intérêt des personnes concernées à préserver leurs droits et leurs libertés. Dans le cas d'une école, le traitement de données est légitime[3]. Il convient donc de les protéger contre toute utilisation qui ne répondrait pas à ces finalités.

La loi « vie privée » impose à tout responsable de traitement de mettre en place des mesures qui doivent garantir la confidentialité, la disponibilité et l'intégrité des données. Il s'agit donc de les protéger contre toute curiosité ou contre des manipulations non-autorisées et malveillantes. Le directeur de l'école fondamentale doit assurer leur protection. Les personnes travaillant sous sa responsabilité ne pourront utiliser que les données dont elles ont besoin pour exercer leurs fonctions. Il prendra des mesures de sécurité contre des atteintes accidentelles ou malintentionnées, à l'intégrité de ces données.

Les mesures de sécurité[4] à prendre sont de deux ordres : des mesures organisationnelles et des mesures techniques. Les mesures organisationnelles définissent les règles de gestion de la sécurité des données : quelle personne peut y accéder, ce qu'elle peut en faire, qui informer en cas d'incident, etc.
Les mesures techniques donnent les moyens pratiques de la mise en œuvre des règles organisationnelles, c'est en partie de la sécurité informatique. Ces deux aspects de la sécurité sont développés dans les points suivants.

---

[2] Voy. Le document *La protection des données à caractère personnel* sur le site web de la Commission, http://www.privacycommission.be.
[3] Art. 5 de la Loi du 8/12/92 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
[4] Voy. Le document *Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel* sur le site web de la Commission, http://www.privacycommission.be.

3. L'organisation de la sécurité des données.

Pour garantir la protection des données, il est nécessaire de définir les rôles de chaque utilisateur, les règles d'utilisation des données, les procédures d'attribution d'accès ou de gestion des incidents. Pour assurer l'efficacité de cette organisation, il convient que chaque utilisateur en soit informé.

- Les responsabilités.

- Le directeur de l'école fondamentale : il est le responsable du traitement car il détermine pour son établissement les objectifs et les moyens d'utilisation des données. Il est donc responsable de leur protection au sein de son établissement et de leur exactitude quand il les envoie vers l'extérieur. Cette responsabilité inclut l'information de son personnel sur les mesures de sécurité à appliquer. Pour toute question, il peut s'adresser à l'équipe sécurité de l'information de la DGEO.
- Autre membre du personnel : il ne peut utiliser les données que selon les consignes du directeur de l'école fondamentale. S'il est amené à traiter des données provenant du Registre national (comme c'est le cas dans SIEL), il devra signer un engagement au respect de la confidentialité.

L'engagement à la confidentialité.

L'application SIEL utilise des informations provenant du Registre national, la loi en vigueur dans ce cas impose[5] à toute personne les utilisant de signer un document par lequel elle s'engage à préserver le caractère confidentiel de ces données et à ne pas les utiliser à des fins autres que professionnelles. Un exemplaire de cet engagement à la confidentialité se trouve en annexe de la circulaire. Tout accès à SIEL est au préalable conditionné à la signature de cet engagement.

Lorsque les chargés de mission passeront dans votre établissement pour la formation à SIEL, ils vous demanderont de signer ce document en deux exemplaires. Le premier est pour vous, le second sera remis par les chargés de mission à l'équipe Sécurité de l'information de la DGEO.
Par la suite, lors d'un changement de direction par exemple, le nouveau directeur devra demander à l'équipe Sécurité de l'information de lui fournir le document. Il lui suffira ensuite de leur renvoyer un des exemplaires signés aux coordonnées indiquées plus haut.

- La gestion des accès.

Comme évoqué plus haut, un des principes importants pour garantir la protection des données est de définir précisément les règles d'accès et d'utilisation de ces données et d'en informer les personnes concernées.

L'accès à l'application SIEL se fait en utilisant un identifiant qui est lié à l'établissement. Pour chaque établissement, il y a deux identifiants disponibles : le premier est attribué au directeur et le second, à la demande du directeur, à un autre membre de son personnel. Pour ce deuxième identifiant, le directeur devra communiquer à l'équipe sécurité de la DGEO l'identité de cette personne. Pour chaque établissement, seules les deux personnes à qui ont été attribuées les

[5] Art. 12 de la Loi du 08/08/1983 organisant un registre national des personnes physiques.

identifiants ont l'autorisation d'utiliser SIEL. Ces identifiants sont personnels et intransmissibles.
Lors d'un changement de direction, le directeur sortant doit communiquer à l'équipe sécurité de la DGEO sa date de départ pour qu'elle révoque temporairement son identifiant. Lors de sa prise de fonction, le nouveau directeur doit faire la demande de réactivation de l'identifiant. Une fois la demande traitée, à sa première connexion le directeur pourra choisir le mot de passe associé à l'identifiant.
De même lors d'un changement d'attribution du second identifiant, l'équipe Sécurité de la DGEO doit en être informée.

- La gestion des incidents de sécurité.

On entend par incident de sécurité tout évènement qui compromet une des trois caractéristiques suivantes : la confidentialité, la disponibilité et l'intégrité.

- La violation de confidentialité d'une donnée signifie qu'elle a été accessible à une personne n'en ayant pas l'autorisation.
- La perte de disponibilité d'une donnée signifie qu'elle n'est plus accessible à un utilisateur autorisé. Les causes d'un tel incident sont multiples : problème avec le réseau informatique, problème avec la base de données, problème avec l'application, perte du mot de passe, ...
- La perte d'intégrité d'une donnée signifie qu'elle a été modifiée sans autorisation et/ou qu'elle est incorrecte.

Dans les trois cas le directeur de l'école fondamentale doit prendre contact avec l'équipe sécurité de la DGEO et l'informer de l'incident.

- L'autorisation de la Commission de la Protection de la Vie Privée (CPVP).

Pour que l'Administration et les établissements scolaires bénéficient de données officielles et authentiques sur les élèves, l'application SIEL utilise un lien avec le Registre national. L'utilisation de ce lien est soumise à l'autorisation de la CPVP, qui doit être accordée à chaque établissement.

La demande d'autorisation se fait à la CPVP par le biais de son *Questionnaire d'évaluation destiné à tout demandeur d'accès ou de connexion au Registre National et concernant les mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel* (http://www.privacycommission.be/fr/static/pdf/questionnaire-rn-vs-01.pdf).
Vous trouverez ce questionnaire en annexe de la circulaire.

Lors de leur passage, les chargés de mission vous remettront un document expliquant le contenu de ce questionnaire et comment le remplir. Par la suite vous pouvez vous adresser à l'équipe Sécurité de l'information.

Veuillez renvoyer ce questionnaire, complété et signé, au plus tard 2 semaines après le passage des chargés de mission, à :

Direction Générale de l'Enseignement Obligatoire
Service des Affaires générales et des Relations internationales
à l'attention de Monsieur Guillaume Dubost
Rue A. Lavallée, 1
1080 Bruxelles

4. Les mesures de sécurité technique.

Une fois que l'organisation de la sécurité des données a été définie, il faut mettre en œuvre les mesures pour l'appliquer. Ces mesures doivent protéger les ressources sensibles, c'est-à-dire les supports (informatiques ou papier) où sont stockées les données à caractère personnel et le matériel informatique servant à traiter ces données. Ce sont des mesures techniques, qui se divisent en deux catégories : les mesures de sécurité physique et les mesures de sécurité informatique. Les mesures de sécurité physique ont pour objectif d'empêcher toute personne non-autorisée de s'approcher physiquement des ressources sensibles (informatiques ou autres). Les mesures de sécurité informatique ont pour objectif d'empêcher cette même personne d'utiliser les ressources informatiques sensibles. Ces deux catégories sont bien entendu complémentaires.

- Les mesures de sécurité physique.

- Il faut tout d'abord localiser précisément l'ensemble de l'équipement informatique (ordinateur, serveur, support de mémoire) et des archives papier servant dans le traitement de données à caractère personnel, et qui constitue les ressources sensibles. Il est préférable que ces ressources sensibles soient réparties dans un nombre limité de locaux, si possible dans un seul.
- Une fois que les locaux où sont situées les ressources sensibles ont été identifiés, il faut s'assurer que leurs accès soient sécurisés, c'est-à-dire que les portes et les fenêtres puissent être verrouillées.
- Il faut naturellement, en dehors des heures de travail, que les portes et les fenêtres de ces locaux soient verrouillées.
- Durant les heures de travail, l'accès à ces locaux doit être contrôlé. Idéalement, seules les personnes autorisées à traiter des données à caractère personnel doivent pouvoir y pénétrer. Il faut alors en cas d'absence temporaire verrouiller les portes, ou à tout le moins, verrouiller l'ordinateur (cf. annexe 1).
- Les archives papier et les supports de mémoire doivent être stockés dans des armoires ou tiroirs fermant à clé.

- Les mesures de sécurité informatique.

Elles ont pour objectif de protéger les informations contenues dans un ordinateur. Les menaces potentielles ont des origines indirectes et directes. Elles peuvent provenir du réseau de communication auquel est connecté l'ordinateur. Mais cela peut aussi être une personne qui s'installe devant l'ordinateur pour y récupérer son contenu. La sécurité informatique fournit des moyens pour se protéger contre ces menaces.
La mise en œuvre de cette sécurité se fait par l'utilisation d'outils informatiques agissant sur des menaces précises, ainsi que par une configuration et une utilisation adéquates de l'ordinateur. Ces différents points nécessitant une description plus pratique, ils font l'objet d'une annexe à cette circulaire.

5. Conclusion.

La sécurité des données personnelles est une problématique à laquelle peu de personne sont familiarisées. Elle peut donc apparaitre comme une contrainte supplémentaire. Il n'est toutefois pas possible de l'ignorer : tout organisme traitant des données personnelles est dans l'obligation de la mettre en œuvre. De plus, ceci permet de protéger le responsable du traitement en cas d'incident lié aux données.
Cette sécurité se base avant tout sur le bon sens et conduit à une pratique de « bon père de famille ». Une fois son organisation bien assimilée et la bonne pratique intégrée au quotidien, elle devient alors un élément à part entière dans le traitement de l'information.
Selon des études, le facteur ayant le plus grand impact sur la protection des données, est le facteur humain. Un utilisateur bien informé sur le respect de la confidentialité et avec une bonne pratique dans le traitement des données, garantit alors un niveau de sécurité élevé.

Je vous remercie de votre collaboration.

La directrice générale

Lise-Anne Hanse

Annexe 1 : les mesures de sécurité informatique.

Utilisation du matériel informatique :

Antivirus et pare-feu.

Il est important que chaque ordinateur qui est connecté vers l'extérieur soit protégé contre les logiciels malveillants qui circulent sur l'Internet. Ces logiciels sont des virus, des vers informatiques, des chevaux de Troie … Les logiciels de protection qui doivent être installés et actifs sur l'ordinateur sont un antivirus et un pare-feu.
L'antivirus doit être régulièrement mis à jour pour qu'il puisse reconnaître les nouveaux virus. Les ordinateurs administratifs qui sont fournis par l'ETNIC sont équipés de l'antivirus Sophos. Vous devez juste vous assurer qu'il est actif et à jour, sachant que la mise à jour doit idéalement se faire de manière automatisée.
Il est important d'utiliser régulièrement l'antivirus pour faire une analyse de l'ordinateur à la recherche de logiciels malveillants.

Par défaut le pare-feu installé est celui de Windows, vous pouvez vérifier qu'il est activé par la procédure suivante : cliquez sur démarrer, menu Paramètre, cliquez sur Panneau de configuration. Dans la fenêtre qui s'ouvre, double-cliquez sur Centre de sécurité, choisissez ensuite Pare-feu Windows. Dans la nouvelle fenêtre, la case Activé, à côté du symbole vert doit être cochée.

Démarrage et verrouillage de l'ordinateur.

Il est important que les ordinateurs soient configurés de manière à ce qu'un mot de passe soit demandé au démarrage. Ainsi pour chaque ordinateur, seul le détenteur du mot de passe peut l'allumer. Si pour des raisons fonctionnelles, l'accès à l'ordinateur doit être partagé entre plusieurs utilisateurs, il est préférable de configurer cet ordinateur avec plusieurs comptes d'utilisateurs et donc un mot de passe par compte. Cette configuration se fait en allant dans le Panneau de configuration et en choisissant Comptes d'utilisateurs. Vous pouvez vous adresser au Helpdesk de l'ETNIC (02/800 1010) pour être assisté dans cette configuration.

Avant de vous éloigner de votre ordinateur, pensez à le verrouiller ; ainsi, il sera nécessaire d'entrer le mot de passe pour le réactiver et donc empêcher qu'il soit utilisé pendant votre absence.
Pour verrouiller votre ordinateur, pressez en même temps les touches L et Logo Windows de votre clavier. La touche Logo Windows est située en bas à gauche du clavier entre les touches Ctrl et Alt.

Touche Logo Windows : 

Pour déverrouiller l'ordinateur, pressez en même temps les 3 touches Ctrl, Alt et Delete, vous devez ensuite introduire le mot de passe et votre ordinateur est déverrouillé.

Les sauvegardes de récupération des données.

Il peut arriver que vous perdiez une partie ou la totalité de vos dossiers sauvegardés sur l'ordinateur. Cela peut être dû à un dysfonctionnement informatique, à la destruction de l'ordinateur ou à son vol. Une telle situation peut se révéler catastrophique s'il n'existe aucun double de ces dossiers. C'est pourquoi il est fortement recommandé de régulièrement faire des sauvegardes de récupération (ou double) de vos documents sur un support mémoire tel qu'une disquette, un cd ou une mémoire USB. Ce support doit être stocké dans un lieu différent de l'ordinateur pour éviter que les données du support soient perdues en même temps que celles de l'ordinateur.

Les logiciels malveillants.

Ceux-ci peuvent parfois franchir les barrières de protection de l'ordinateur en exploitant leurs faiblesses. Ces logiciels peuvent être hébergés sur des sites web (à leur insu ou non) et tentent la contamination dès que l'on se connecte au site. Avant de se connecter et visiter un site, il convient donc de s'interroger au préalable sur le degré de confiance que l'on peut lui accorder. Préférez par exemple les sites officiels, ou encore ceux qui vous ont été recommandés par une connaissance fiable.

Un autre moyen utilisé par ces logiciels est de s'introduire par le courriel : soit au travers d'une adresse mail qui vous est inconnue, soit au travers de l'adresse mail d'un de vos contacts qui a déjà été contaminé.
C'est pourquoi il est recommandé :

- de supprimer tous les mails d'origine inconnue avant même d'ouvrir les fichiers qui leur seraient attachés.
- de vérifier que les noms des fichiers attachés correspondent à des documents que vous attendez ou que vous avez l'habitude de recevoir.

Les spams.

Les spams sont des courriels à buts commerciaux et/ou d'arnaque qui sont envoyés en masse. En soi, ils ne sont pas dangereux mais peuvent devenir très incommodants. Il y a deux règles principales pour se prémunir :

- Ne communiquez votre adresse mail qu'aux personnes et organismes en qui vous avez confiance.
- Ne répondez jamais à un spam, le seul résultat serait d'en recevoir plus.

Votre adresse administrative (ec00xxxx@adm.cfwb.be) doit exclusivement être utilisée pour communiquer avec l'administration.

Accès à l'application SIEL.

Identifiant et mot de passe.

Pour accéder à l'application SIEL (https://www.geste.cfwb.be), vous utilisez un identifiant (EC00….) et un mot de passe. Le mot de passe permet de vérifier votre identité. Une fois identifié, au travers de votre identifiant et authentifié au travers de votre mot de passe, toute

action effectuée dans SIEL est associée à l'identifiant et donc à la personne à qui il est attribué. Cela signifie que cet identifiant et ce mot de passe vous sont personnels et sous votre responsabilité. Par conséquent, ces deux éléments sont intransmissibles.

Gestion du mot de passe.

Lors de votre premier accès à SIEL, il vous sera demandé de choisir un mot de passe. Par la suite, il vous sera régulièrement demandé de choisir un nouveau mot de passe.
Si vous deviez perdre votre mot de passe, ou aviez des doutes sur sa confidentialité, veuillez prendre contact avec l'équipe sécurité de la DGEO. Votre mot de passe sera réinitialisé et vous devrez en choisir un nouveau.
Si vous gardez une trace écrite de votre mot de passe, il ne doit pas être possible de l'associer à l'application SIEL et à votre identifiant.

Choix du mot de passe.

Le mot de passe doit être composé de 4 à 8 caractères alphanumériques (lettres et chiffres). Bien entendu, plus il est long, plus il est sûr. Il n'est pas sensible aux minuscules/majuscules. Il ne peut pas être identique à votre identifiant. Il est conseillé que ce mot de passe ne soit pas un mot du dictionnaire, ni un nom propre, ni une date associée à un événement personnel. Les mots de passe les plus sûrs sont des séquences incompréhensibles de chiffres et de lettres. Vous pouvez par exemple partir d'un nom commun ou propre, dans lequel vous remplacez certaines lettres par des chiffres.

Annexe 2 : Déclaration sur l'honneur.

Située en page 11 et 12, c'est l'engagement au respect de la confidentialité des données du Registre national.

Annexe 3 : Questionnaire d'évaluation de la CPVP.

Situé en page 13 et 14, il doit être complété et signé par le directeur de l'école fondamentale, puis renvoyé à l'équipe Sécurité de l'information de la DGEO dans les deux semaines qui suivent la formation à SIEL. Cette équipe se chargera d'envoyer le questionnaire à la Commission de la Protection de la Vie Privée.

Déclaration sur l'honneur.

Je, soussigné, ……..
membre du personnel de l'établissement ……..,
avec la fonction de ……, par la présente et en toute circonstance, m'engage à préserver le caractère confidentiel des informations obtenues du Registre National via la banque de données SIEL. En conséquence, en dehors des besoins pour l'accomplissement de ma fonction, je m'interdis formellement de divulguer à qui que ce soit ou d'utiliser à mon profit personnel, directement ou indirectement, cesdites informations.
Je suis averti que toute contravention de ma part à cet engagement est susceptible d'entraîner des poursuites pénales à mon encontre.

Fait en 2 exemplaires* à ……..
Le ……

Mention « Lu et approuvé »
Nom et signature :

* un pour l'équipe Sécurité de l'information de la DGEO et un pour le signataire.

Extrait de la **Loi organisant un registre national des personnes physiques** du 8 août 1983 :

Art. 12. <Rétabli par L 2003-03-25/30, art. 9, 013; En vigueur : 07-04-2003> § 1er. La Commission de la protection de la vie privée, instituée par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, est chargée de tenir un registre dans lequel sont mentionnées toutes les autorisations. Ce registre est rendu accessible au public par la Commission.

§ 2. Les autorités publiques, les organismes publics ou privés et les personnes qui ont obtenu l'accès aux informations du Registre national ou la communication desdites informations sont tenus :

1° de désigner nominativement leurs organes ou préposés qui, en raison de leurs attributions, ont obtenu l'accès aux informations ou la communication desdites informations et de les informer conformément à l'article 16, § 2, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel; ils sont tenus de dresser une liste de ces organes ou préposés;

2° de faire signer par les personnes effectivement chargées du traitement des informations une déclaration par laquelle elles s'engagent à préserver le caractère confidentiel des informations.

Art. 13. (Est puni d'un emprisonnement de huit jours à un an et d'une amende de cent euros à deux mille euros, ou d'une de ces peines seulement, celui qui, en qualité d'auteur, de coauteur ou de complice, contrevient aux dispositions des articles 8, § 2, et 12, § 2, de la présente loi.

Est puni d'un emprisonnement de trois mois à cinq ans et d'une amende de mille euros à vingt mille

Équipe Sécurité de l'information

Tél. +32 (2) 690.85.44 – Fax +32 (2) 690.85.83
+32 (2) 690.86.18
Administration générale de l'Enseignement et de la Recherche scientifique
Direction générale de l'Enseignement obligatoire

euros, ou d'une de ces peines seulement, celui qui, en qualité d'auteur, de coauteur ou de complice, contrevient aux dispositions de l'article 11 de la présente loi.) <L 2003-03-25/30, art. 10, 013; En vigueur : 07-04-2003>

Les peines encourues par les complices des infractions visées aux alinéas 1er et 2, n'excéderont pas les deux tiers de celles qui leur seraient appliquées s'ils étaient l'auteur de ces infractions.

S'il existe des circonstances atténuantes, les peines d'emprisonnement et d'amende pourront respectivement être réduites sans qu'elles puissent être inférieures aux peines de police.

Extrait de la **Version coordonnée de la loi relative à la protection des données à caractère personnel du 8 décembre 1992. Version coordonnée (janvier 2006).**

Art. 16. (§ 1er. Lorsque le traitement est confié à un sous-traitant, le responsable du traitement ou, le cas échéant, son représentant en Belgique, doit :
1° choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements;
2° veiller au respect de ces mesures notamment par la stipulation de mentions contractuelles;
3° fixer dans le contrat la responsabilité du sous-traitant à l'égard du responsable du traitement;
4° convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu en application du paragraphe 3;
5° consigner par écrit ou sur un support électronique les éléments du contrat visés aux 3° et 4° relatifs à la protection des données et les exigences portant sur les mesures visées au paragraphe 3.

§ 2. Le responsable du traitement ou, le cas échéant, son représentant en Belgique, doit :
1° faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 4 à 8;
2° veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service;
3° informer les personnes agissant sous son autorité des dispositions de la présente loi et de ses arrêtés d'exécution, ainsi que de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel;
4° s'assurer de la conformité des programmes servant au traitement automatisé des données à caractère personnel avec les termes de la déclaration visée à l'article 17 ainsi que de la régularité de leur application.

§ 3. Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.) <L 1998-12-11/54, art. 23, 004; En vigueur : 01-09-2001>

(§ 4.) Afin de garantir la sécurité des données à caractère personnel, le (responsable du traitement et, le cas échéant, son représentant en Belgique, ainsi que le sous -traitant doivent prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel) contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. <L 1998-12-11/54, art. 23, 004; En vigueur : 01- 09-2001>
Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.
Sur avis de la Commission de la protection de la vie privée, le Roi peut édicter des normes appropriées en matière de sécurité informatique pour toutes ou certaines catégories de traitements.

Équipe Sécurité de l'information

Tél. +32 (2) 690.85.44 – Fax +32 (2) 690.85.83
+32 (2) 690.86.18
Administration générale de l'Enseignement et de la Recherche scientifique
Direction générale de l'Enseignement obligatoire

Questionnaire d'évaluation destiné à tout demandeur d'accès ou de connexion au Registre National et concernant les mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel

Organisme demandeur	
nom :	
Adresse officielle :	

Conseiller en sécurité	
nom :	DUBOST
prénom :	Guillaume
adresse de contact :	Rue Adolphe Lavallée, 1 - 1080 Bruxelles
téléphone :	02/690.85.44
fax :	02/690.85.83
e-mail :	guillaume.dubost@cfwb.be
Qualifications :	Ingénieur Civil Electricien spécialisé en télécommunication
Statut :	Agent de niveau 1
Description de la fonction :	Correspondant en sécurité de l'information de la DGEO
Position dans l'organigramme :	Attaché à la directrice générale de la Direction générale de l'Enseignement obligatoire (DGEO)
Temps pouvant être consacré à sa mission de sécurité :	100%
Autres fonctions éventuelles :	Aucune

Ce questionnaire est destiné à permettre une évaluation du respect de la Loi Vie Privée en ce qui concerne la sécurité des systèmes d'information traitant des données à caractère personnel[6]*.*

Il se réfère aux "Mesures de référence de sécurité applicables à tout traitement de données à caractère personnel" préconisées par la Commission de la protection de la vie privée.

Celles-ci sont présentées ici sous forme de questions auxquelles il s'agit de répondre par « oui » ou « non » ou éventuellement « sans objet ».

Il est également possible d'indiquer « prévu pour le » au cas où des développements relatifs à la question auraient été planifiés ou seraient en cours.

La colonne « Commentaires » sert à expliquer plus précisément de quelle façon une exigence particulière est respectée ou pour quelle raison elle ne l'est pas. Elle peut également servir à communiquer des références particulières qui font autorité ou toute autre information requise.

Ce questionnaire doit être daté et signé par le responsable de traitement.

[6] Il s'agit de considérer ici les systèmes d'information concernés par les données à caractère personnel en provenance du registre national et ceux qui leur seraient liés dans le cadre du traitement de ces données

Questionnaire d'évaluation	***Sans objet***	***Oui***	***En cours - Prévu pour le***	***Non***	***Commentaires ou Référence aux commentaires annexés***
1. Disposez-vous d'un conseiller en sécurité ? Si oui, pouvez-vous compléter le cadre prévu à cet effet ?					
2. Avez-vous réalisé une évaluation des risques et des besoins de sécurité propres à votre organisme et concernant vos traitements de données à caractère personnel ?					
3. Disposez-vous d'une version écrite de votre politique de sécurité intégrant votre politique de protection des données à caractère personnel ? Si oui, pouvez-vous nous indiquer en « commentaire » la date de sa dernière actualisation ?					15/05/2007
4. Avez-vous identifié les divers supports impliquant des données à caractère personnel dans votre organisme ?					
5. Est-ce que le personnel interne et externe impliqué dans le traitement des données à caractère personnel est informé de ses devoirs de confidentialité et de sécurité vis-à-vis de ces données et découlant aussi bien des différentes exigences légales que de la politique de sécurité ?					
6. Avez-vous mis en place des mesures de sécurité afin de prévenir les accès physiques inutiles ou non autorisés aux supports contenant des données à caractère personnel ?					
7. Avez-vous mis en place des mesures destinées à prévenir les dommages physiques pouvant compromettre des données à caractère personnel ?					
8. Avez-vous mis en place des mesures de sécurité afin de protéger les différents réseaux auxquels sont raccordés les équipements traitant les données à caractère personnel ?					
9. Disposez-vous d'une liste actualisée des différentes personnes habilitées à accéder aux données à caractère personnel et de leur niveau d'accès respectif (création, consultation, modification, destruction) ?					
10. Avez-vous mis en place, sur vos systèmes d'information, un mécanisme d'autorisation d'accès conçu de façon à ce que les données à caractère personnel et les traitements les concernant ne soient accessibles qu'aux personnes et applications explicitement autorisées?					
11. Votre système d'information est-il conçu de façon à enregistrer de façon permanente l'identité des entités ayant accédé aux données à caractère personnel ?					
12. Avez-vous prévu de contrôler la validité et l'efficacité dans le temps des mesures techniques ou organisationnelles mises en place pour assurer la sécurité des données à caractère personnel ?					
13. Avez-vous mis en place des procédures de gestion d'urgence des incidents de sécurité impliquant des données à caractère personnel ?					
14. Disposez-vous d'une documentation actualisée concernant les différentes mesures de sécurités mises en place afin de protéger les données à caractère personnel et les différents traitements les concernant ?					

Fait à : ***le :*** ***Signature du responsable de traitement***