CIRCULAIRE N° 3088 DU 25/03/2010

CIRCULAIRE	Informative	Administrative	~~Projet~~
OBJET	**SECURITE DES DONNEES PERSONNELLES**		
DESTINATAIRE	Direction	Secondaire ordinaire	
RESEAUX	Organisé par la Communauté française		
PÉRIODE	2010		

- Aux Chefs d'établissements d'enseignement Secondaire 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	**NON**

Équipe Sécurité de l'information de
la DGEO

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.
Il est important de s'en préoccuper 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 Chef d'établissement, 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 chefs 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 premier 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 (Signalétique Elève) sera aussi abordé puisque chaque établissement secondaire du réseau organisé par la Communauté française sera amené à y introduire ses inscriptions. Pour rappel cette application permet l'inscription en ligne de vos élèves vers la DGEO et remplacera à terme l'application GestionElèves. Les informations ainsi récoltées seront utilisées par le service du comptage des élèves, par le service du contrôle de l'obligation scolaire et à des fins statistiques.

Cette application permet de récupérer les informations sur les élèves telles qu'elles sont connues au Registre national (RN), ce qui facilite l'encodage et réduit les erreurs. L'utilisation des données du RN est strictement contrôlée par la Commission de la Protection de la Vie Privée (CPVP) et tous les établissements doivent, préalablement à l'utilisation de SIEL, obtenir l'autorisation de cette Commission.

[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.

Cela se fait à l'aide du document à l'annexe 2 intitulé ***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***. Le second objectif de cette circulaire est donc de vous accompagner dans cette démarche afin que votre établissement bénéficie de l'autorisation de la CPVP qui est nécessaire pour utiliser SIEL.

Toujours dans cet objectif, les chargés de mission de la DGEO prendront contact avec vous pour vous présenter l'application SIEL et vous accompagner dans le remplissage du questionnaire qu'ils récupèreront à la fin de leur visite pour le transmettre à l'équipe Sécurité de l'information de la DGEO.

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 chef d'établissement 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.

---

[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.

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.

Les zones de texte encadrées concernent directement l'application SIEL.

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.

Peu avant leur visite, les chargés de mission vous renverront la présente circulaire et vous inviteront à la relire, en particulier l'annexe 3 qui est un document expliquant le contenu de ce questionnaire et comment le remplir. Ainsi, avec leur aide pendant leur visite, vous devriez pouvoir remplir et signer ce document. Les chargés de mission le récupèreront à la fin de leur visite et le transmettront à l'équipe Sécurité de l'information.

3. L'organisation de la sécurité des données.

Pour garantir la protection des données, il est nécessaire d'avoir un inventaire de ses ressources en données personnelles, de définir les rôles et responsabilités de chaque utilisateur, les règles d'accès et d'utilisation des données et les procédures de gestion des incidents. Pour assurer l'efficacité de cette organisation, il convient que chaque utilisateur en soit informé.

- **Les responsabilités.**

- Le chef d'établissement : 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.

[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.

- Autre membre du personnel : il ne peut utiliser les données que selon les consignes du chef d'établissement. 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 autorisée à les traiter à 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 à l'annexe 1 de la circulaire. **Tout accès à SIEL est au préalable conditionné à la signature de cet engagement.**

- **La gestion des ressources.**

Une première étape importante à l'organisation de la sécurité est d'établir un inventaire précis de l'ensemble des données personnelles traitées dans votre établissement. Cet inventaire est une liste des divers supports papier et informatiques contenant de telles informations et de leur localisation.
Pour les supports papier, ce sont les documents administratifs comme les registres de classe, les fiches papier d'inscription d'élève, etc. Pour les supports informatiques, ce sont les ordinateurs, les serveurs de données, les supports de mémoires (CD-ROM, mémoires USB, disquettes, …).
Pour chaque support, l'inventaire doit indiquer le local où il est rangé. Sur ce point, pour diminuer les risques, il est intéressant de minimiser le nombre de locaux de stockage.

- **La gestion des accès.**

Le caractère confidentiel des données personnelles et du RN impose de s'assurer qu'elles ne sont accessibles que par les personnes autorisées. Il faut donc définir les règles et les mesures de contrôle d'accès aux divers supports contenant ces informations.
Pour les supports papier, ils peuvent être stockés dans un local fermé, les clés étant détenues par un nombre limité et connu de personne.
Pour les supports informatiques, on utilise un identifiant et un mot de passe pour accéder à l'ordinateur, à l'application ou à la base de donnée.

L'accès à l'application SIEL se fait en utilisant un identifiant personnel c'est-à-dire lié à son utilisateur. Pour chaque établissement, il y aura un nombre limité d'identifiants disponibles déterminé par le nombre d'implantations. Un identifiant sera attribué au chef d'établissement, et les autres, à sa demande, seront attribués à des personnes en charge de l'inscription des élèves dans les autres implantations.

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

Pour chaque identifiant supplémentaire, le chef d'établissement aura dû au préalable faire parvenir à l'équipe sécurité de la DGEO l'engagement à la confidentialité signé par le futur utilisateur. Pour chaque établissement, seules les personnes à qui ont été attribués les identifiants sont autorisées à utiliser SIEL. **Ces identifiants sont personnels et intransmissibles.**

Lors d'un changement de direction, le chef d'établissement sortant doit communiquer à l'équipe sécurité de la DGEO sa date de départ pour qu'elle révoque ses autorisations d'accès à SIEL. Lors de sa prise de fonction, le nouveau chef d'établissement doit faire la demande d'un identifiant et de ses autorisations d'accès.
Le chef d'établissement doit aussi communiquer à l'équipe sécurité de la DGEO tout changement dans l'attribution d'accès à SIEL à des responsables administratifs.

- **La gestion des autorisations d'accès à SIEL.**

Les besoins et les objectifs d'utilisation de SIEL sont différents en fonction des acteurs. Les établissements scolaires envoient à l'administration les informations sur les élèves, l'administration traite ces données au sein de divers services avec des missions bien précises. Il est donc nécessaire de différencier les autorisations d'utilisations de l'application SIEL. C'est pourquoi ont été définis les profils applicatifs de SIEL, dont trois pour les utilisateurs des écoles. Il s'agit des profils Encodage, Confirmation et Transfert.

Les profils applicatifs :

Les trois profils sont définis pour que les utilisateurs d'un établissement ne puissent accéder qu'aux informations des élèves inscrits dans cet établissement.

- Profil Encodage :

Ce profil donne accès à toutes les données de la fiche d'inscription d'un élève, soit :
- les données d'identification,
- les données relatives à l'inscription,
- les données spécifiques au niveau d'enseignement,
- les données sur le(les) responsable(s) légal(aux).

Les fonctionnalités de l'application accessible par ce profil sont la création, la consultation, la modification et la clôture d'une inscription.

- Profil Confirmation :

Ce profil permet à un établissement de confirmer ses inscriptions à l'administration. C'est à partir de cette confirmation que l'administration pourra visualiser et commencer à traiter les dossiers des élèves.
Les données accessibles sont les mêmes que dans le profil précédent.

Les fonctionnalités de l'application accessible par ce profil sont la consultation et la confirmation d'une inscription.

o Profil Transfert :

Ce profil permet, à un établissement de transférer ses inscriptions à l'administration pour les dates de comptage.
Les données accessibles sont les mêmes que dans le profil précédent.

Les fonctionnalités de l'application accessible par ce profil sont la consultation et le transfert des inscriptions.

- **La gestion des incidents de sécurité.**

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

- La violation de confidentialité d'une donnée signifie qu'une personne y a eu accès sans avoir obtenu 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 chef d'établissement doit prendre contact avec l'équipe sécurité de la DGEO et l'informer de l'incident.

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.**

- Après avoir fait l'inventaire des divers supports contenant des données à caractère personnel, il est préférable de stocker ces supports 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.
- 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.

5. Conclusion.

La sécurité des données personnelles est une problématique à laquelle peu de personnes 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 : Déclaration sur l'honneur.

Située en pages 10 et 11, c'est l'engagement au respect de la confidentialité des données du Registre national.

Annexe 2 : Questionnaire d'évaluation de la CPVP.

Situé en pages 12 et 13, il doit être complété et signé par le chef d'établissement, et remis au chargé de mission lors de sa première visite concernant SIEL. L'équipe Sécurité de l'information de la DGEO se chargera d'envoyer le questionnaire à la Commission de la Protection de la Vie Privée.

Annexe 3 : Explications du questionnaire d'évaluation de la CPVP.

Situées à partir de la page 14, elles contiennent toutes les informations nécessaires pour vous permettre de répondre au mieux au questionnaire de la Commission.

Ministère de la Communauté française

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

Équipe Sécurité de l'information de
la DGEO

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

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 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.

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 Certificat en management de la sécurité des systèmes d'information
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 ?					
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***

Annexe 3 - Explications des questions contenues dans le Questionnaire d'évaluation de la Commission de la Protection de la Vie Privée à destination des directions d'écoles.

Introduction.

Tel que cela est défini dans la législation, tout organisme qui souhaite recevoir communication et traiter des données du Registre national, doit au préalable obtenir l'autorisation du Comité sectoriel du Registre national de la CPVP.
Dans le cadre du projet SIEL de la Communauté française, d'envoi des données relatives à l'inscription des élèves via Internet, le Comité sectoriel du RN a accordé aux directions d'école une autorisation suspensive. Pour rendre effective cette autorisation, les directions d'école doivent remplir le ***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***. L'équipe sécurité de l'information de la DGEO se charge de collecter et transférer au Comité sectoriel du RN (CSRN) les questionnaires des écoles organisées par la CF. Les réponses seront analysées par le Comité qui décidera si l'autorisation peut devenir effective.

Le sens de ces questions n'est pas évident à comprendre par tout le monde, surtout si l'on est peu ou pas sensibiliser à la problématique de la sécurité de l'information. L'objectif de ce document est de palier cette difficulté en décryptant au mieux possible les quatorze questions. De plus, quand cela est possible, des pistes vous seront données sur où et comment trouver les réponses, car dans certains cas, cela pourrait être en dehors de votre périmètre de responsabilité. Pour compléter ces informations nous vous recommandons vivement de lire le document ***Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel*** que vous pouvez trouver à l'adresse :
www.privacycommission.be/fr/static/pdf/mesures-de-r-f-rence-vs-01.pdf

Ce questionnaire doit être signé par le chef d'établissement car selon la loi « vie privée », il est le responsable du traitement des données à caractère personnel.

1ère question : Disposez-vous d'un conseiller en sécurité ?

Le conseiller en sécurité pour un organisme est la personne de référence sur la sécurité de l'information. Son rôle est d'abord de fournir des avis et recommandations au responsable du traitement sur ce qui doit être mis en œuvre comme mesures de sécurité. Pour cela il se base sur une évaluation des risques existants pour déterminer les besoins en sécurité. Cela détermine alors un plan d'action qui doit être validé par le responsable du traitement. Le conseiller en sécurité doit ensuite veiller à sa mise en œuvre au sein de l'organisation.

Cette mise en œuvre comprend la définition de l'organisation de la sécurité, l'établissement de procédures et de mesures techniques et l'information des personnes traitant des données sur cette sécurité.

Réponse : OUI. Pour les établissements du réseau organisé par la Communauté française, le conseiller en sécurité est celui de la Direction générale de l'Enseignement obligatoire (DGEO).

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 Certificat en management de la sécurité des systèmes d'information
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 DGEO
Temps pouvant être consacré à sa mission de sécurité :	100%
Autres fonctions éventuelles :	Aucune

2ème question : 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 ?

L'évaluation des risques pesant sur les données d'un organisme consiste à déterminer quelles sont les menaces existantes, leur probabilité d'occurrence et l'impact qu'elles ont sur l'organisme et des tiers. Une fois cette évaluation faite, il est possible de déterminer les besoins en sécurité de l'organisme. Ces besoins se concrétisent en mesures de sécurité qui diminuent la probabilité d'occurrence ou l'impact des menaces.

Les risques portant sur les données sont tout ce qui peut compromettre l'intégrité, la disponibilité et la confidentialité des données.
L'intégrité correspond à l'exactitude et l'authenticité des données. Elle n'est assurée que si celles-ci ne peuvent être créées et modifiées que par une action volontaire et légitime.
La disponibilité est l'aptitude à pouvoir obtenir les données demandées et à accomplir les traitements nécessaires.
La confidentialité définit le caractère réservé d'une donnée dont l'accès est limité aux seules personnes admises à la connaître.

L'évaluation et la gestion des risques impliquent dans la plupart des cas une connaissance à la fois des aspects fonctionnels et des aspects techniques. C'est pourquoi une coopération entre le responsable du traitement et le prestataire technique est souhaitable chaque fois que des aspects relevant de la technologie de l'information sont présents.

Le risque peut être	*Le risque peut*
• *Accidentel*	• *pénaliser l'école et son personnel*
• *Volontaire*	• *altérer le matériel informatique, le support papier*

Il faut analyser les risques et mettre en place les solutions indispensables à la sauvegarde des actifs « données ».

PREVENTION – PROTECTION

Comment réagir et surtout comment anticiper les réactions si :
• Un employé a volé les données du RN ?
• Le feu s'est déclaré dans l'école ravageant toutes les installations informatiques ?
Les collaborateurs n'ont pas toujours conscience de la valeur des informations manipulées et de l'importance de la sécurité et des responsabilités qui en découlent. La sécurité ne doit pas être considérée comme une charge, mais bien comme un investissement qui assure la pérennité des données et qui diminue les risques opérationnels.
Exemples concrets

- Risque de vandalisme
  - Prévention : alarme intrusion et connexion vers la zone de police ; on protège ainsi l'école et son contenu (données, matériel, …)
- Risque informatique (prise de contrôle de l'ordinateur à distance)
  - Prévention : anti-virus, spyware pour protéger la machine
- Risque par rapport au personnel
  - Prévention : formation du personnel et ainsi meilleure utilisation et protection des données

Il faut toujours évaluer le risque maximum possible dans les 3 axes concernés

- la confidentialité,
- la disponibilité
- l'intégrité des données

et considérer les impacts au niveau

- de l'image de l'école,
- de l'aspect social et humain,
- de l'aspect juridique
- de l'aspect financier

afin de limiter les menaces.
La mise en place de mesures préventives assure une meilleure protection.

Réponse : OUI. La DGEO a réalisé une évaluation des risques avec plusieurs chefs d'établissement. Elle est bien entendu générale mais donne une bonne idée des besoins en sécurité d'un établissement. Une évaluation précise pour votre établissement peut être réalisée si nécessaire.

3ème question : 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 ?

La Politique de sécurité est un document publié par le responsable du traitement qui définit ses attentes en matière de sécurité de l'information. Les principes qui y sont énoncés doivent être respectés par l'ensemble du personnel. Elle sert de base de référence pour toutes les mesures organisationnelles et techniques qui visent à assurer la sécurité des traitements effectués. On y retrouve donc la définition de l'organisation de la sécurité, les procédures à utiliser dans cette organisation, les mesures à mettre en œuvre, …

Réponse : OUI. La DGEO a rédigé une politique de sécurité pour l'application SIEL dont le périmètre inclut les écoles organisées par la Communauté française. Elle a été rédigée au 15/05/2007. Les éléments de cette politique applicables aux écoles se retrouvent dans la circulaire **Sécurité des données personnelles**.

4ème question : Avez-vous identifié les divers supports impliquant des données à caractère personnel dans votre organisme ?

On entend par support tout élément physique sur lequel peuvent être inscrites des données. Cela peut être des supports papier comme les registres ou des supports informatiques comme les disques durs des ordinateurs, les disques externes, les CD, les clés de mémoire USB, les serveurs, …

Ce qu'il faut faire :

- Dans la mesure du possible, répartir les données à caractère personnel dans un nombre limité de locaux
- Localiser et lister l'emplacement des Registres, des dossiers d'élèves et autres listings contenant des données à caractère personnel.
- Localiser et lister l'ensemble de l'équipement informatique présent dans l'école et qui peut donner accès à des données à caractère personnel (SIEL, application locale…)

Réponse : OUI, si les supports en question ont été identifiés et localisés.

5ème question : 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 les différentes exigences légales que de la politique de sécurité ?

La sécurité des données est aussi assurée par le personnel impliqué dans le traitement des données à caractère personnel. Il faut alors que ce personnel soit bien informé de son devoir de confidentialité et de sécurité vis-à-vis de ces données. De plus pour que les procédures définies dans la politique de sécurité soient correctement appliquées et que les mesures soient efficaces, le personnel doit être informé de l'existence de ces procédures et mesures, et de la manière de les appliquer. Un moyen de limiter les risques au niveau des utilisateurs, est de limiter le nombre de personnes qui ont accès aux données.

Il peut donc être utile, en début de chaque année, que le directeur d'école ou le responsable du PO fasse un rappel à son personnel des exigences légales, des procédures et des mesures à appliquer.

Réponse : En cours, il est de la responsabilité du directeur d'informer son personnel :

- de leur engagement au respect de la confidentialité des données ;
- de traiter ces données uniquement dans le cadre de leurs activités professionnelles et pour les besoins de leurs fonctions.

6ème question : Avez-vous mis en place des mesures de sécurité afin de prévenir les accès physiques inutiles ou non autorisés aux supports contenant les données à caractère personnel ?

Il s'agit de mesures qui empêchent toute personne non-autorisée de s'approcher physiquement des équipements informatiques (supports mobiles, ordinateurs, serveurs) et papier qui contiennent des données à caractère personnel.

Quelques possibilités …

- Verrouiller les portes et fenêtres des locaux dans lesquels se trouvent les documents qui contiennent des données à caractère personnel

- Equiper de serrures ou cadenas les armoires contenant des données à caractère personnel
- Fermer armoires, portes et fenêtres d'accès au local à clé, lorsque vous quittez celui-ci
- Identifier les propriétaires des différentes clés dans l'école
- Installer des caméras de surveillance
- …

Réponse : OUI, si les mesures nécessaires sont en place.

7ème question : Avez-vous mis en place des mesures destinées à prévenir les dommages physiques pouvant compromettre les données à caractère personnel ?

Les causes des dommages physiques sont multiples : vandalisme, incendie, inondation, … Les mesures en question doivent permettre de se prémunir contre ces dommages.

Mesures de prévention :

- Eviter les entreposages d'archives en sous-sol ;
- Assurer la mise en conformité des bâtiments (après contrôle effectué par Vincotte ou tout autre organisme agréé) et veiller à faire effectuer régulièrement une visite de contrôle par les pompiers : les recommandations communiquées constitueront une base de prévention efficace.
- Envisager des mesures de sécurisation des locaux en fonction des besoins locaux : placement de vitrages de sécurité, de grillages aux fenêtres, de serrures et portes classiques ou de sécurité renforcée, d'alarmes passives ou actives…
- Et peut-être le plus important, avoir un système de backup (sauvegarde) sur un site distant qui permettra de récupérer les données en cas de perte totale sur le site principal. Ce site doit disposer des mêmes mesures de protection que le site initial.

Pour les données de SIEL, il existe un site de sauvegarde géré par l'ETNIC.

Réponse : OUI, si les mesures nécessaires sont en place.

8ème question : 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 ?

Les équipements informatiques utilisant les données confidentielles sont connectés à l'internet. Ils doivent donc être protégés contre les menaces provenant de l'Internet comme les logiciels malveillants, les tentatives d'intrusion dans les ordinateurs, …

Ce qu'il faut faire dans le périmètre de l'école-PC locaux :

- Installation et mises à jour régulières d'un pare-feu (firewall) : entrant (Windows XP &+) ou mieux, entrant et sortant ;
- Installation et mises à jour régulières d'un anti-virus automatisé ;
- Mises à jour recommandées par les fournisseurs des logiciels utilisés : Windows, Office, messagerie… (Alerte de sécurité)
- Sécurisation des réseaux filaires & sans-fil (Wi-Fi) :
    - Autorisations d'accès limitées : clé réseau ;
    - Autorisations d'accès limitées en nombre ;
    - Autorisations d'accès limitées par identification physique des ordinateurs (portables) utilisés (Adresses Mac).

Réponse : OUI, si les mesures nécessaires sont en place.

9ème question : 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) ?

A la question 4, on vous demande de lister les sources de données à caractère personnel au sein de votre organisation. La question 9 vise plus particulièrement les personnes, dans votre organisation, qui accèdent à ces sources de données quelque soit le support (papier ou informatique). Il faut établir une liste de ces personnes, en indiquant quelles actions elles peuvent effectuer dessus, c'est-à-dire créer, consulter, modifier, détruire. Cela conduit à la définition de profils applicatifs.
Il faut au moment de changement de personnel, et au moins de manière régulière, reconsidérer les utilités de ces accès (applications locales ou web, dossier papier). Ils doivent être limités et/ou supprimés en fonction des besoins réels de chacun. La liste du personnel habilité à accéder aux données doit être mise à jour conformément à ces changements, en ce compris leur profil applicatif respectif.

Réponse : OUI. Le chef d'établissement devra établir une liste nominative des utilisateurs de l'application SIEL. Cette liste devra être tenue à jour et communiquée à l'équipe sécurité de l'information de la DGEO.

10ème question : 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 ?

Les données à caractère personnel sous forme informatisée sont généralement traitées à l'aide d'une application informatique. Cette application peut-être locale et alors les données sont stockée directement sur l'ordinateur, ou être en ligne et dans ce cas les données sont stockées sur un serveur distant.
Quelle que soit votre application, il est important de pouvoir contrôler qui y accède et donc qui accède aux données. Pour cela on met en place un mécanisme d'autorisation d'accès, qui peut-être l'utilisation d'un identifiant (ou login) et d'un mot de passe pour pouvoir utiliser l'application et les données. De part la confidentialité des données à caractère personnel, il faut que cet identifiant soit personnel (lié à une personne précise) et le mot de passe soit intransmissible, et donc ne peut être retrouvé à proximité du PC. Ce mot de passe doit être d'une qualité suffisante en terme de sécurité, par exemple être constitué d'au moins 8 caractères, mélangeant chiffres et lettres, différant de l'identifiant, …
Un mécanisme de contrôle d'accès plus sûr comme un token, un certificat numérique ou la carte d'identité électronique (eID) peuvent aussi être utilisés.

Réponse : OUI. A chaque ouverture d'une session SIEL, il sera demandé à l'utilisateur d'introduire son identifiant et son mot de passe. Ce mécanisme est entièrement géré par la DGEO.

11ème question : Votre système est-il conçu de manière à enregistrer de façon permanente l'identité des entités ayant accédé aux données à caractère personnel ?

Il peut être nécessaire de savoir a posteriori qui a fait quoi et quand dans l'application de traitement des données. Pour cela, il faut donc avoir gardé des traces des actions des différents utilisateurs. Le système d'information, en lien avec l'application de traitement de données, doit être conçu pour pouvoir enregistrer quand un identifiant se connecte à l'application ainsi que les différentes actions effectuées par cet identifiant.
La base de données ainsi constituée représente un journal des accès aux données qu'il convient aussi de protéger.

Réponse : OUI. L'application SIEL est conçue pour enregistrer de façon permanente les identifiants des utilisateurs accédant à l'application SIEL, ainsi que les actions réalisées par ces identifiants.

12ème question : 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 ?

Régulièrement (une fois par an par exemple), il est intéressant de faire un bilan de la sécurité mise en œuvre. Cela consiste à évaluer pour chaque mesure opérationnelle son efficacité dans la protection des données. Il pourra alors apparaître que certaines mesures doivent être modifiées, et même que de nouvelles doivent être mises en place.
Le résultat de ce travail doit alors être transposé dans une mise à jour du plan d'action de la politique de sécurité.

Réponse : OUI ou EN COURS, s'il a été prévu une évaluation des mesures de sécurité.

13ème question : Avez-vous mis en place des procédures de gestion d'urgence des incidents de sécurité impliquant les données à caractère personnel ?

Quand un incident de sécurité est constaté, c'est-à-dire que l'intégrité, la disponibilité ou la confidentialité de certaines données sont compromises, il est important de savoir ce qu'il y a à faire. C'est ce que l'on retrouve dans les procédures de gestion d'urgence des incidents. Elles doivent définir, en fonction de l'incident, quelles sont les personnes à prévenir dans l'organisation (et obligatoirement le conseiller en sécurité) et ce qui doit être fait.

Réponse : OUI. Les procédures de gestion des incidents sont expliquées dans la circulaire **Sécurité des données personnelles**.
Il faut prévenir le conseiller en sécurité de la DGEO lors d'un incident portant atteinte aux données personnelles.

14ème question : Disposez-vous d'une documentation actualisée concernant les différentes mesures de sécurité mises en place afin de protéger les données à caractère personnel et les différents traitements les concernant ?

L'ensemble des documents liés à la sécurité des données comme l'analyse des risques, la politique de sécurité, les mesures techniques et organisationnelles, les listes du personnel habilité à accéder aux données, leur profil applicatif, leur engagement à la confidentialité, les différentes procédures de sécurité, … doivent être rassemblés et conservés par le responsable du traitement ainsi que par son conseiller en sécurité.
Cette documentation doit être mise à jour régulièrement en fonction des évolutions.

Réponse : OUI. Cette documentation comprend la circulaire sécurité, la liste des utilisateurs, tout document lié à la sécurité et tout document que le directeur jugera nécessaire de rédiger, par exemple pour l'information de son personnel.

Information pratique :

En complément des informations qui vous ont été communiquées dans ce document, vous pouvez aussi consulter le site suivant de l'Agence Wallonne des Télécommunications :
http://www.awt.be/web/sec/index.aspx
Vous y trouverez, par exemple, un guide « sécurité informatique ».