Circulaire n°4577 du 23/09/2013

Protection de la vie privée et sécurité des données

Réseaux et niveaux concernés

☐ Fédération Wallonie- Bruxelles

☐ Libre subventionné
- ☐ libre confessionnel
- ☐ libre non confessionnel)

☒ Officiel subventionné

☒ Niveaux :
Fondamental et secondaire ordinaire
Fondamental et secondaire spécialisé

Type de circulaire

☐ Circulaire administrative

☒ Circulaire informative

Période de validité

☐ A partir du

☐ Du au

Documents à renvoyer

☐ Oui

☐ Date limite :

☐ Voir dates figurant dans la circulaire

Mot-clé :

SIEL - CPVP

Destinataires de la circulaire

- Aux Pouvoirs organisateurs des établissements de l'enseignement officiel fondamental ou secondaire, ordinaire ou spécialisé, subventionné par la Fédération Wallonie-Bruxelles ;
- Aux Directions des établissements de l'enseignement officiel fondamental ou secondaire, ordinaire ou spécialisé, subventionné par la Fédération Wallonie-Bruxelles.

Signataire

Administration : AGERS – Direction générale de l'Enseignement obligatoire
Madame Lise-Anne Hanse, Directrice générale

Personnes de contact

Service : AGERS – DGEO – Direction d'Appui

Nom et prénom	Téléphone	Email
Dubost Guillaume	02/690 85 44	guillaume.dubost@cfwb.be

Madame, Monsieur,

Que ce soit pour la gestion quotidienne de votre école ou dans vos relations avec l'administration, vous récoltez, traitez et transmettez des données à caractère personnel concernant les élèves de votre établissement et/ou leurs représentants légaux. L'utilisation de ces informations est soumise à la législation sur la protection de la vie privée, qui garantit un équilibre entre l'utilisation légitime de ces données et la garantie de leur protection.

L'évolution vers la simplification administrative, avec l'utilisation croissante de l'outil informatique, augmente aussi le risque qui pèse sur la protection de la vie privée et, par conséquent, la prise en considération de la sécurité des données doit devenir toujours plus importante.

Parmi les données que vous traitez et que vous transmettez à l'administration, se trouvent celles issues du Registre national comme le numéro national, par exemple dans le cadre du comptage des élèves. C'est aussi le cas avec les inscriptions dans la base de données SIEL (SIgnalétique ELève), que ce soit directement par l'application Internet ou au travers des webservices via une application locale. Pour plus d'information sur SIEL vous pouvez consulter la circulaire n° 4058 du 18 juin 2012.

L'utilisation des données du Registre national dans SIEL permet de garantir l'authenticité des données relatives aux élèves. La législation impose des contraintes très strictes en matière de traitement de ces données, et la Commission de la Protection de la Vie Privée (CPVP) est chargée d'en assurer le contrôle.

L'entrée d'un établissement scolaire dans le système SIEL nécessite au préalable l'autorisation de la CPVP. Même si votre établissement ne rentre pas immédiatement dans SIEL, il est vivement recommandé de commencer maintenant à se mettre en ordre vis-à-vis de la CPVP.

Afin de vous aider dans cette démarche, cette circulaire explique la démarche, les documents de la CPVP et les informations nécessaires pour obtenir cette autorisation.

Mes services restent évidemment à votre disposition pour toute information complémentaire.

Je vous pris d'agréer, Madame, Monsieur, l'expression des mes meilleures salutations.

Pour la Directrice générale absente,
La Directrice générale adjointe,

Claudine LOUIS

Généralités

Afin de pouvoir intégrer dans la base de données SIEL les données du Registre national, la Direction générale de l'Enseignement obligatoire a obtenu l'autorisation de la CPVP, sous la forme des délibérations RN n°08/2006 du 22 mars 2006 et RN n°15/2010 du 14 avril 2010.

Ces délibérations précisent que pour que les établissements scolaires et les Pouvoirs organisateurs puissent bénéficier de l'autorisation d'utiliser SIEL, ils doivent au préalable renseigner à la CPVP le conseiller en sécurité de l'information qui a été désigné pour ces entités, et qu'ils doivent aussi compléter et lui envoyer le questionnaire relatif à l'état de la sécurité de l'information.

Ces démarches se font avec les documents suivants :

- *Proposition de désignation d'un conseiller en sécurité de l'information*, disponible sur le site web de la CPVP à l'adresse internet :

http://www.privacycommission.be/fr/questionnaire-evaluation-candidat-conseiller-en-securite

Ce document permet à la CPVP d'évaluer l'indépendance et les compétences de la personne désignée, cette évaluation reposant sur le principe de proportionnalité entre le besoin de sécurité et les moyens disponibles.

- *Déclaration de conformité relative à la sécurité du système d'information faisant l'objet de la demande d'autorisation d'accès ou de connexion au registre national*, disponible à l'adresse internet :

http://www.privacycommission.be/fr/node/15233 pour la version word du document.
http://www.privacycommission.be/fr/node/15142 pour la version pdf du document.

Ce document permet à la CPVP d'évaluer la mise en œuvre de la sécurité dans les différents domaines organisationnels et informatiques.

Le conseiller en sécurité de l'information

Le conseiller en sécurité pour une organisation est la personne de référence sur la sécurité de l'information. Son rôle est d'abord de fournir des avis et des recommandations au responsable de l'organisation 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.

Une même personne peut-être être conseiller en sécurité pour plusieurs entités, ce qui signifie qu'un Pouvoir organisateur (PO) peut alors désigner la même personne pour lui-même et pour ses écoles. Mais il faut pour chacune des entités déclarer à la CPVP l'identité de cette personne à l'aide du document téléchargeable à l'adresse internet http://www.privacycommission.be/fr/questionnaire-evaluation-candidat-conseiller-en-securite .

Ce document peut être complété, signé et envoyé aussi bien électroniquement que manuellement.

La CPVP a édité un document explicatif du formulaire *Proposition de désignation d'un conseiller en sécurité de l'information* que vous pouvez trouver à l'adresse internet :
http://www.privacycommission.be/fr/node/15140

La mise en conformité relative à la sécurité de l'information

Une fois que le conseiller en sécurité a été désigné, il peut, avec le responsable du traitement de l'organisation, commencer à répondre aux questions de la *Déclaration de conformité relative à la sécurité du système d'information faisant l'objet de la demande d'autorisation d'accès ou de connexion au registre national*.

Ce document contient 14 questions qui portent sur les aspects organisationnels et informatiques de la sécurité du système d'information, auxquelles il faut répondre par oui ou non. Si pour l'une ou l'autre question, il ne peut pas être répondu par la positive, il convient de mettre en œuvre la ou les mesures nécessaires afin de pouvoir obtenir l'autorisation de la CPVP.

Ce document est disponible à l'adresse internet :
- http://www.privacycommission.be/fr/node/15233 pour la version word du document.
- http://www.privacycommission.be/fr/node/15142 pour la version pdf du document.

Vous trouverez ci-dessous une explication de ces questions.

Question 1 : Un *conseiller en sécurité de l'information a été chargé de veiller à la mise en application de la politique de sécurité lors de l'exécution de ce traitement.*

Voir plus haut : **Le conseiller en sécurité de l'information**

Question 2 : *L'évaluation des risques*
Une évaluation des risques encourus par les données à caractère personnel traitées a été réalisée et les besoins de sécurité ont été définis en conséquence.

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, 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 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.

Question 3 : *La politique de sécurité de l'information*
Un document écrit – la politique de sécurité de l'information – précisant les stratégies et mesures retenues pour sécuriser les données à caractère personnel traitées a été élaboré.

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, …

Question 4 : *L'identification des supports*
Tous les supports, quels qu'ils soient et impliquant les données à caractère personnel traitées, ont été identifiés.

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 identifier qui peut donner accès à des données à caractère personnel (SIEL, application locale…)

Question 5 : *L'information du personnel*
Le personnel interne et externe impliqué dans ce traitement a été informé de ses devoirs de confidentialité et de sécurité vis-à-vis des données à caractère personnel traitées découlant aussi bien des différentes exigences légales que de la politique de sécurité.

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.

Question 6 : *La sécurisation physique des accès*
Des mesures de sécurité adéquates ont été mises en place afin de prévenir les accès physiques inutiles ou non autorisés aux supports contenant les données à caractère personnel traitées.

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, en respectant la législation très stricte sur ce sujet
- …

Question 7 : *La sécurité physique et environnementale*
Les mesures de sécurité nécessaires ont été mises en place afin de prévenir les dommages physiques pouvant compromettre les données à caractère personnel traitées.

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 l'entreprise Vinçotte 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.

Question 8 : *La sécurisation des réseaux*
Les différents réseaux auxquels sont reliés les équipements traitant les données à caractère personnel ont été protégés.

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 version plus récentes) 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.

Question 9 : *La liste des personnes habilitées*
Une liste actualisée des différentes personnes habilitées à accéder aux données à caractère personnel dans le cadre de ce traitement, reprenant leur niveau d'accès respectif (création, consultation, modification, destruction), a été établie.

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 de votre organisation qui accèdent à ces sources de données, quel que soit le support (papier ou informatique). Il faut établir une liste de ces personnes, en indiquant quelles actions elles peuvent effectuer, c'est-à-dire créer, consulter, modifier, détruire. Cela conduit à la définition des accès.

Il faut, au moment de changement de personnel, et au moins de manière régulière, reconsidérer les utilités de ces accès (applications locales ou web, dossiers 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 type d'accès respectif.

Question 10 : *La sécurisation logique des accès*
Un mécanisme d'autorisation d'accès conçu de façon à ce que les données à caractère personnel traitées et les traitements les concernant ne soient accessibles qu'aux personnes et applications explicitement autorisées a été mis en place.

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 stockées 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 par la confidentialité des données à caractère personnel, il faut que cet identifiant soit personnel (lié à une personne précise) et que 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, différent 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.

Question 11 : *La journalisation des accès*
Le système d'information a été conçu de façon à permettre une journalisation, un traçage et une analyse permanents des accès des personnes et entités logiques aux données à caractère personnel traitées.

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. Pour la base de données SIEL, l'ETNIC assure une journalisation des accès.

Question 12 : *La surveillance, la révision et la maintenance*
Un contrôle de la validité et de l'efficacité dans le temps des mesures techniques ou organisationnelles mises en place a été prévu.

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.

Question 13 : *La gestion d'urgence des incidents de sécurité de l'information*
Des procédures de gestion d'urgence des incidents de sécurité impliquant les données à caractère personnel traitées ont été mises en place.

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 (dont obligatoirement le conseiller en sécurité) et ce qui doit être fait.

Question 14 : *La documentation*
Une documentation suffisante concernant l'organisation de la sécurité de l'information dans le cadre du traitement en question a été constituée et sera tenue à jour.

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.

Personnes de contacts pour plus d'information

Si vous avez besoin d'information complémentaire sur la mise en conformité avec la CPVP, vous pouvez contacter les personnes reprises ci-dessous :

- Guillaume DUBOST, correspondant en sécurité de la DGEO : 02/690 85 44 – guillaume.dubost@cfwb.be
- Alain DELSOIR, chef de projet SIEL : 02/690 84 92 – alain.delsoir@cfwb.be
- Martine GARNIER, chargée de mission SIEL – PRIMVER : 02/690 83 63 – martine.garnier@cfwb.be
- Carine GEUNS, chargée de mission SIEL – PRIMVER : 02/690 83 18 – carine.geuns@cfwb.be
- Christian DEGLIM, chargé de mission SIEL – PRIMVER : 02/690 84 29 – christian.deglim@cfwb.be
- Vincent GILSON, chargé de mission SIEL – PRIMVER : 02/690 83 06 – vincent.gilson@cfwb.be
- Olivier HONNORÉ, chargé de mission SIEL – PRIMVER : 02/690 86 25 – olivier.honnore@cfwb.be
- Lucien NOIRHOMME, chargé de mission SIEL – PRIMVER : 02/690 84 20 – lucien.noirhomme@cfwb.be
- Benoît TAQUET, chargé de mission SIEL – PRIMVER : 02/690 83 79 – benoit.taquet@cfwb.be