L’obligation de notification des violations de données à caractère personnel à la CNIL

	L’obligation de notification des violations de données à caractère personnel à la CNIL

A l'occasion de la révision des directives « Paquet télécom » en 2009, le législateur européen a imposé aux fournisseurs de services de communications électroniques l'obligation de notifier les violations de données personnelles aux autorités nationales compétentes, et dans certains cas, aux personnes concernées.

Cette obligation de notification a été transposée en droit français à l'article 34 bis de la loi informatique et libertés. Les conditions de sa mise en œuvre ont été précisées par le décret n° 2012-436 du 30 mars 2012, ainsi que par le règlement européen n° 611/2013 du 24 juin 2013.

Dans quels cas l'article 34 bis s'applique-t-il ?
L'article 34 bis de la loi informatique et libertés s'applique lorsque plusieurs conditions sont réunies :
• condition 1 : il faut qu'un traitement de données à caractère personnel ait été mis en œuvre
• condition 2 : le traitement doit être mis en oeuvre par un fournisseur de services de communications électroniques
• condition 3 : dans le cadre de son activité de fourniture de services de communications électroniques (par exemple, lors de la fourniture de son service de téléphonie ou d'accès à d'internet)
• condition 4 : ce traitement a fait l'objet d'une violation. Selon l'article 34 bis, une violation est constituée par une destruction, une perte, une altération, une divulgation, ou un accès non autorisé à des données à caractère personnel. Elle peut se produire de manière accidentelle ou illicite, l'intention malveillante étant l'un des possibles cas de figure, mais pas le seul.

Sont, par exemple, constitutifs d'une violation :
• Une intrusion dans la base de données de gestion clientèle d'un fournisseur d'accès internet (FAI) ;
• Une faille dans la boutique en ligne d'un opérateur mobile permettant de récupérer les numéros de cartes de crédits des clients ayant commandé un nouveau téléphone associé à un forfait (car ce sont les données clients collectées en tant qu'opérateur) ;
• Un email confidentiel destiné à un client d'un FAI, diffusé par erreur à d'autres personnes ;
• La perte d'un contrat papier d'un nouveau client par un agent commercial d'un opérateur mobile dans une boutique.

Ne sont pas des violations de données personnelles au sens de l'article 34 bis :
• Toute violation ne concernant pas un traitement du FAI comme un virus informatique qui s'attaque aux PC des abonnés du FAI pour collecter des données personnelles ;
• Toute activité ne concernant pas la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public tel que le piratage du fichier des ressources humaines du FAI.

Qui doit notifier la CNIL et informer les personnes concernées par la violation ?
L'article 34 bis vise les « fournisseurs de services de communications électroniques accessibles au public ». Il s'agit des opérateurs devant être déclarés auprès de l'ARCEP (article L. 33-1 alinéa 1 du code des postes et des communications électroniques) (par exemple, les fournisseurs d'accès à internet ou de téléphonie fixe et mobile).
Les services de la société d'information, tels que les banques en ligne, les sites d'e-commerce ou les téléservices des administrations, ne sont pas concernés.

Quand et comment notifier la CNIL ?
Toute violation doit être notifiée à la CNIL, quelle que soit son niveau de gravité.
La notification doit être adressée à la CNIL dans les 24h de la constatation de la violation.
Si le fournisseur de services de communications électroniques ne peut fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, il est possible de procéder à une notification en deux temps :
Une notification initiale dans les 24 heures de la constatation de la violation ; puis
Une notification complémentaire dans le délai de 72 heures après la notification initiale.
Cette notification doit se faire par lettre remise contre signature ou via le formulaire de dépôt en ligne accessible sur le site de la CNIL, à l'aide du formulaire de notification prévu à cet effet [faire un lien vers le formulaire de notification].

Quand informer les personnes ?
L'information des personnes doit être effectuée sans retard injustifié après constat de la violation de données à caractère personnel (article 91-2 du décret).
Cependant, le fournisseur n'a pas l'obligation d'informer les personnes dans les cas suivants :
la violation n'est pas susceptible de porter atteinte aux données ou à la vie privée des personnes (un outil permettant d'évaluer le niveau de gravité d'une violation est disponible sur le site de la CNIL) ;
la violation est susceptible de porter atteinte aux données ou à la vie privée des personnes, mais le fournisseur a mis en place des mesures techniques de protection appropriées (article 91-3 du décret). Mises en place préalablement à la violation, ces mesures doivent avoir rendues les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès (voir ci-dessous).

Que sont des mesures de protection appropriées ?
Il s'agit de toute mesure technique efficace destinée à rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès. Par exemple, le fait de chiffrer les données permet de rendre les données incompréhensibles à des tiers dans la mesure où la clé de chiffrement n'a pas été compromise.
Si le fournisseur a mis en œuvre de telles mesures de protection, il doit en informer la CNIL au moment de la notification. En effet, pour que le fournisseur puisse être dispensé d'informer les personnes, la CNIL doit d'abord constater que les mesures sont appropriées et qu'elles ont été efficacement mises en œuvre.
La CNIL a deux mois pour se prononcer sur ces mesures. En cas de silence de la CNIL, elles sont considérées comme ne répondant pas aux exigences de l'article 34 de la loi informatique et libertés et le fournisseur doit avertir les personnes.

La CNIL peut-elle imposer au fournisseur d'informer les personnes ?
Oui, la CNIL peut imposer au fournisseur d'informer les personnes si elle constate que la violation porte atteinte aux données ou à la vie privée des personnes, que les mesures de protection mises ne place n'étaient pas appropriées ou que les personnes n'ont pas été ou ont été mal informé.

Comment informer les personnes ?
L'information des personnes doit être faite par tout moyen permettant d'apporter la preuve de l'accomplissement de cette formalité (par courrier électronique, par exemple). Cette information doit contenir les éléments suivants :
• le nom du fournisseur ;
• l'identité et les coordonnées du correspondant informatique et libertés ou d'un point de contact auprès duquel les personnes peuvent obtenir des informations supplémentaires ;
• le résumé de l'incident à l'origine de la violation ;
• la date estimée de l'incident ;
• la nature et la teneur des données concernées ;
• les conséquences vraisemblables de la violation pour la personne ;
• les circonstances de la violation ;
• les mesures prises pour remédier à la violation ;
• les mesures recommandées par le fournisseur pour atténuer les préjudices potentiels.
En outre, cette information doit être rédigée dans une langue claire et aisément compréhensible. Elle ne doit pas être utilisée comme un moyen de promouvoir ou d'annoncer de nouveaux services ou être associée à d'autres informations (être mentionnée sur la facture adressée aux personnes concernées, par exemple).

Quels sont les risques pris par le fournisseur qui ne notifierait pas ?
Le fournisseur encourt des sanctions pénales car le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la CNIL ou à l'intéressé est puni de cinq ans d'emprisonnement et de 300 000 € d'amende (article 226-17-1 du code pénal).
En outre, tout manquement à la loi informatique et libertés est passible de sanctions administratives, notamment financières pouvant aller jusqu'à 300 000 €.

En cas de violations, le fournisseur a-t-il d'autres obligations que la notification ?
Oui, il doit tenir à jour un inventaire des violations qui doit notamment contenir les modalités de la violation (ce qui s'est passé), l'effet de la violation (les conséquences) et les mesures prises pour remédier à la violation (les actions correctives mises en œuvre).
Ce recensement des violations peut être réalisé sous format papier ou numérique, et doit être conservé à la disposition de la CNIL.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.cnil.fr/linstitution/actualite/article/article/la-notification-des-violations-de-donnees-a-caractere-personnel