https://www.observatoire-collectivites.org/spip.php?article7671

Atteinte à la sécurité des données de demandeurs de logements : une association sanctionnée par la CNIL

- Jurisprudence -

Date de mise en ligne : jeudi 21 juin 2018

Copyright © Observatoire Smacl des risques de la vie territoriale & associative - Tous droits réservés

Une association peut-elle être sanctionnée pour avoir insuffisamment protégé les données personnelles de ses utilisateurs sur son site internet bien que celui-ci ait été développé par un prestataire professionnel ?

Oui : une association peut être sanctionnée par la CNIL en tant que responsable de traitement suite à un incident de sécurité sur son site internet rendant librement accessibles les données personnelles de ses utilisateurs, et ce, alors même que le site a été développé par une société prestataire. L'ampleur de la violation (plus de 40 000 documents accessibles) et le degré de sensibilité des données concernées (références bancaires, numéros de sécurité sociale, salaires, passeports...) ont justifié la décision prise par la CNIL de sanctionner l'association à hauteur de 75 000 euros et de rendre publique cette décision, alors même que celle-ci était de bonne foi et faisait preuve de coopération avec ses services.

Une association de mise à disposition de logements dans des résidences et foyers, notamment pour des étudiants, familles monoparentales et travailleurs migrants, propose aux demandeurs de logements d'effectuer leurs démarches d'inscription en ligne.

Ils doivent ainsi déposer leurs pièces justificatives sur le site de l'association : avis d'imposition, titres de séjours, passeports, cartes d'identité, bulletins de salaires, attestations CAF, numéro de sécurité sociale, références bancaires, date de naissance, nombre d'enfants, versement d'aides au logement et allocations aux adultes handicapés...

En juin 2017, la CNIL est informée de l'existence d'un incident de sécurité sur le site. Via un contrôle en ligne, elle s'aperçoit qu'une simple modification du chemin de l'adresse URL affichée dans le navigateur permet d'accéder à des documents enregistrés par d'autres demandeurs. Alertée, l'association indique avoir demandé à la société qui a développé le site de remédier au problème.

Quelques jours plus tard, la CNIL se rend dans les locaux de l'association pour effectuer un second contrôle et constate que les données sont toujours librement accessibles.

Estimant que l'association avait manqué à son obligation de préserver la sécurité et la confidentialité des données personnelles des utilisateurs, la formation restreinte de la CNIL prononce à son encontre une sanction pécuniaire de 75 000 euros.

La CNIL estime que les mesures élémentaires de sécurité suivantes auraient dû être prises en amont du développement du site :

– mise en place d'un dispositif permettant d'éviter la prévisibilité des URL (exemple : URL composée d'une chaîne de caractères aléatoires et ne comportant pas la dénomination de la pièce fournie par la personne).
– mise en place d'une procédure d'identification et d'authentification des utilisateurs du site internet.

Copyright © Observatoire Smacl des risques de la vie territoriale & associative

La formation restreinte de la CNIL a tenu compte de la bonne coopération de l'association avec ses services, mais a néanmoins considéré que la gravité de la violation était constituée en raison de la nature particulièrement intime des données rendues librement accessibles et du nombre de documents concernés (plus de 40 000 documents en libre accès). Pour ces raisons, elle a décidé de rendre publique sa décision.

A noter :

Les manquements reprochés ont été commis préalablement à l'entrée en application de la nouvelle règlementation relative aux données personnelles (RGPD). Pour les manquements désormais commis sous l'empire du RGPD (à compter du 25 mai 2018), il faut tenir compte des éléments suivants :

– en cas de violation sur les données personnelles, le responsable de traitement doit en informer la CNIL dans les 72 heures à partir du moment où il en a pris connaissance ;

– la responsabilité des sous-traitants est renforcée et il est nécessaire de rappeler dans un contrat les obligations de celui-ci en matière de protection des données personnelles (mesures de sécurité, protection des données dès la conception et par défaut, collaboration...).
Leur responsabilité peut être engagée par le responsable de traitement en cas de manquement, ainsi que par les personnes concernées sur le plan délictuel en cas de dommage subi. La CNIL peut également les sanctionner directement.

Depuis l'introduction de la loi pour une République numérique, la CNIL a la possibilité de prononcer une sanction pécuniaire sans mise en demeure préalable, notamment lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure.
Ce qui était le cas en l'espèce puisque la CNIL a considéré que les effets du manquement constaté ne pouvaient être corrigés par le biais d'une mise en demeure (à savoir la libre accessibilité des données personnelles pendant la durée de l'incident de sécurité) mais que le manquement pouvait être directement sanctionné.

Pour aller plus loin :

Sécurité des sites web : les 5 problèmes les plus souvent constatés

De nombreuses failles de sécurité pourraient être aisément évitées. La CNIL donne la **liste des 5 problèmes les plus souvent constatés** et les solutions pour les éviter :

1- un mot de passe trop simple ;

2- l'absence d'authentification à un compte ;

3- un compte client accessible depuis une URL incrémentale (le changement d'un seul caractère de URL d'un compte client, amène sur le compte d'un autre client et donne accès à toutes ses informations.) ;

4- l'absence de chiffrement des données ;

Copyright © Observatoire Smacl des risques de la vie territoriale & associative

5- l'indexation des données dans un moteur de recherche

Préparer la mise en conformité des associations au RGPD :

La CNIL a publié un guide complet rappelant les précautions élémentaires à prendre, avec des fiches et des outils pratiques pour aider les organisations à se mettre en conformité.

Voici les 6 étapes essentielles pour démarrer sa mise en conformité :

1- Désigner un pilote : si les associations n'ont pas forcément l'obligation de désigner un délégué à la protection des données, il est fortement recommandé de désigner une personne chargée de s'assurer de la mise en conformité au RGPD.

2- Cartographier vos traitements de données personnelles : commencez par recenser de façon précise les traitements de données personnelles que vous mettez en œuvre (par finalités et catégories de données). La tenue d'un registre des traitements vous permet de faire le point (un modèle est à disposition sur le site de la CNIL).

3- Prioriser les actions : identifiez les traitements les plus à risque pour les droits des personnes et leur vie privée et définissez des actions prioritaires à mener (minimisation des données, information…). La CNIL donne une liste de points d'attention nécessitant une vigilance particulière.

4- Gérer les risques : pour les traitements de données identifiés comme susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées (ex : données bancaires, médicales, convictions politiques…), il faudra établir une étude d'impact sur la protection des données qui permettra de déterminer les mesures à prendre pour les protéger au mieux (mesures de sécurité, chiffrement…).

5- Organiser les processus internes : il s'agit de mettre en place des procédures internes, des sensibilisations, des remontées d'information… qui permettront de vérifier que les réflexes de la protection des données sont acquis et appliqués en interne.

6- Documenter la conformité : il faut constituer et regrouper la documentation qui permettra de prouver la conformité au règlement (registre, contrats avec les sous-traitants, mentions d'information, analyses de risques…).

Délibération CNIL nÂ°2018-003 du 21 juin 2018

Post-scriptum :

– La CNIL peut sanctionner un responsable de traitement (association ou autre organisme public ou privé) suite à un incident de sécurité sur un site entraînant une violation de données, et ce, même si le site a été développé par une société prestataire.

– La CNIL tient compte de la bonne foi de l'organisme et de la coopération avec les services de contrôle pour fixer le niveau de la sanction.

– Le montant de la sanction et sa publicité sont en l'espèce justifiés par l'ampleur de la violation (plus de 40 000 documents en libre accès) et par le degré de sensibilité des données concernées (références bancaires, numéros de sécurité sociale, revenus, dates de naissance, pièces d'identité...).

Copyright © Observatoire Smacl des risques de la vie territoriale & associative

– Il faut faire attention dans le choix de son fournisseur/prestataire et définir les obligations de chacun dans un contrat (analyse d'impact, mesures de sécurité, coopération...)

Textes de référence

– **Loi nÂ° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**

– **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016**

– **Directive (UE) 2016/680 du parlement européen et du conseil du 27 avril 2016**

– **Loi nÂ° 2016-1321 du 7 octobre 2016 pour une République numérique**

Pour aller plus loin

– **Guide complet de la CNIL : Se préparer au RGPD en 6 étapes** (source : site de la CNIL)

– **Sites internet : liste des 5 problèmes les plus souvent constatés** (source : site de la CNIL)

Etes-vous sûr(e) de votre réponse ?

– **A défaut de mentions légales indiquant le nom du directeur de la publication sur un journal ou un blog associatif, le droit de réponse exercé par un tiers peut-il être valablement adressé au président de l'association ?**

– **Un maire peut-il utiliser les données du recensement pour mettre à jour le fichier population ?**

Plus de décisions de justice intéressant les associations

Copyright © Observatoire Smacl des risques de la vie territoriale & associative