CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

MANQUEMENTS RELEVÉS ET RECOMMANDATIONS SUITE AUX CONTRÔLES EFFECTUÉS PAR LA CNIL SUR LES TRAITEMENTS MIS EN ŒUVRE PAR LES ASSOCIATIONS DE SUIVI D'AUTEURS D'INFRACTIONS

1. Sur la nécessité de mettre en place un registre des traitements et d'effectuer une étude d'impacts

Le Règlement Général sur la Protection des Données (RGPD) n° 2016/679 du 27 avril 2016 est applicable depuis le 25 mai 2018, ainsi que les dispositions de la Directive (UE) n° 2016/680 qui ont été transposées en droit national. Le règlement européen et la directive européenne modifient la Loi « Informatique et Libertés » du 06 janvier 1978 modifiée et renforcent la protection des données à caractère personnel, droit fondamental reconnu à chaque personne. Aussi, j'attire votre attention sur la nécessité de veiller au respect de leurs dispositions.

Les associations de suivi d'auteurs d'infractions et de personnes mises en cause reçoivent mandat de magistrats pour la mise en œuvre de missions prévues par le code de procédure pénale, et notamment ses articles 41, 41-1 et 81.

Dans ce cadre, elles sont amenées à traiter un volume important de données, à la fois au format papier et numérique, portant sur une grande diversité de données (appréciations sur les difficultés sociales des personnes, données relatives à des infractions, condamnations et mesures de sûreté, données sensibles relevant de l'article 9 de la loi du 6 janvier 1978 modifiée, dont les exigences sont reprises à l'article 10 du RGPD.

Dès lors qu'un traitement de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, l'article 35 du RGPD prévoit dans certaines circonstances que la conduite d'une analyse d'impact relative à la protection des données est requise. Au regard de la nature de ces données, de tels traitements étaient soumis à autorisation de la CNIL avant l'application du RGPD. Certains étaient d'ailleurs susceptibles d'être encadrés par les délibérations portant autorisation unique adoptées par la CNIL pour ce secteur (notamment AU-048). Le RGPD ne prévoit plus l'obligation de procéder à des formalités préalables, les organismes mettant en œuvre des traitements de suivi d'auteurs d'infractions peuvent néanmoins utilement s'appuyer sur ces normes qui constituent des cadres de référence pour la mise en œuvre de vos traitements de données à caractère personnel et le cas échéant, pour mener votre analyse d'impacts.

Le règlement prévoit notamment l'obligation pour de nombreux organismes de désigner un « délégué à la protection des données » (DPD). La désignation de ce délégué contribue, en tout état de cause, à réduire vos risques juridiques tout en bénéficiant de l'accompagnement de la CNIL.

Toutes les informations utiles sont accessibles sur le site de la CNIL (www.cnil.fr) ou en contactant le service des DPO à l'adresse suivante servicedpo@cnil.fr ou par téléphone au 01.53.73.22.22 (de 10h à 12h, sauf le mercredi).

2. Sur la durée de conservation des données

Les contrôles effectués par la CNIL ont mis en évidence des pratiques inégales s'agissant des durées de conservation appliquées aux données papiers conservées par les associations sur les auteurs et personnes mises en cause pour lesquelles elles ont été mandatées par l'autorité judiciaire.

En conséquence, **il appartient à ces associations de mettre en œuvre une politique de durée de conservation des données qu'elles traitent** qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées, comme le prévoit l'article 6-5° de la loi n°78-17 du 6 janvier 1978 modifiée, dont les exigences sont reprises à l'article 5-e) du règlement européen (UE) 2016/679 sur la protection des données.

Le cycle de conservation des données à caractère personnel peut être divisé en trois phases successives distinctes qui sont : la base active ; l'archivage intermédiaire ; l'archivage définitif.

La base active constitue la durée d'utilisation courante des données ou autrement dit, la durée nécessaire à la réalisation de la finalité du traitement.

Pour les archives intermédiaires, le choix du mode d'archivage est laissé à l'appréciation du responsable du fichier. Des données peuvent ainsi être archivées : soit dans une base d'archive spécifique, distincte de la base active, avec des accès restreints aux seules personnes ayant un intérêt à en connaitre en raison de leurs fonctions (par exemple, le service du contentieux) ; soit dans la base active, à condition de procéder à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) pour les rendre inaccessibles aux personnes n'ayant plus d'intérêt à les traiter.

Pour les archives définitives (c'est- à-dire les données conservées dans l'intérêt public), il est recommandé de les conserver sur un support physique indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à les consulter (par exemple, la direction des archives lorsqu'elle existe).

Les associations mettant en œuvre des traitements de suivi d'auteurs d'infractions peuvent consulter la délibération n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel. Cette délibération de la CNIL précise notamment les règles d'archivage intermédiaire appliquées aux données conservées pour répondre à une obligation légale ou à des fins probatoires et dont les durées de conservation sont fixées par les règles de prescription applicables.

3. Sur la sécurité et la confidentialité des données

Les contrôles ont également mis en évidence des manquements graves à l'obligation d'assurer la sécurité et la confidentialité des données, prévues aux articles 34 et 35 de la loi n°78-17 du 6 janvier 1978 modifiée dont les exigences sont reprises aux article 5-1-f), 30-2-d), 32 et 33 du règlement européen (UE) 2016/679 sur la protection des données.

En conséquence, **il convient de prendre toute mesure nécessaire pour garantir la sécurité et la confidentialité des données à caractère personnel traitées par ces associations**, notamment :

En ce qui concerne la sécurité physique et la confidentialité des données :

- veiller à sécuriser l'accès aux locaux de l'association, afin que seules les personnes habilitées à y accéder puissent pénétrer dans les zones non accessibles au public (au moyen par exemple, de portes verrouillables à clé ou de contrôle d'accès par badge) et en veillant à ce que ces locaux soient dument fermés et verrouillés en dehors de leurs horaires d'ouverture ;
- veiller à sécuriser l'accès aux dossiers papiers de l'association (par exemple, en les plaçant dans des armoires fermées et verrouillées dont seules les personnes habilitées disposent de les clés), et à ne pas stocker de dossiers de l'association dans des locaux ouverts et/ou partagés avec des tiers ;
- cesser d'utiliser des documents issus de précédents dossiers de l'association et contenant des données nominatives comme papier brouillon.
- veiller à ce que les fenêtres des bureaux situés en rez-de-chaussée soient dotées de rideaux occultant ou de filtres de confidentialité.

En ce qui concerne la sécurité logique des données :

- veiller à ce que chaque utilisateur soit doté d'un compte individuel ;
- interdire le partage de compte entre plusieurs personnes et les identifiants génériques (du type « secrétariat ») ; si l'utilisation d'un identifiant générique ou partagé est incontournable, exiger une validation de la hiérarchie et mettre en œuvre des moyens pour les tracer ;
- mettre en œuvre une politique de gestion des mots de passe contraignante pour l'authentification sur les postes de travail, notamment en termes de complexité (12 caractères minimum, 4 types de caractères, à savoir des majuscules, des minuscules, des chiffres et des caractères spéciaux) et de renouvellement périodique (imposé par le système, tous les six mois, par exemple). La complexité de ces mots de passe pourra être réduite si des mesures compensatrices visant à assurer un niveau de sécurité équivalent sont mises en place, conformément à la recommandation « mots de passe » (délibération n° 2017-012 du 19 janvier 2017 modifiée le 22 juin 2017) ;
- mettre en place un verrouillage automatique des postes informatiques en cas d'inactivité prolongée (au bout de 10 minutes, par exemple) avec demande de saisie du mot de passe à la reprise ;
- veiller à chiffrer les données conservées sur des supports de stockage nomades (clé USB, disques durs externes) et à n'utiliser de tels supports pour la conservation de données sensibles qu'à titre exceptionnel et temporaire ;
- interdire le recours à du matériel personnel de salariés pour stocker des données de l'association (ordinateur portable et/ou clé USB) ; => pas de BYOD
- veiller à ne pas conserver de données concernant des personnes suivies par l'association sur du matériel informatique situé dans des locaux ouverts et/ou partagés avec des tiers.

En ce qui concerne la sécurité des applications web :

- ne pas permettre l'enregistrement de l'identifiant et du mot de passe par les applications dédiées aux activités de l'association sur les postes informatiques (fonction permettant le renseignement automatique des identifiants lors de la prochaine connexion);
- exiger des mots de passe de 12 caractères minimum, comprenant 4 types de caractères (des majuscules, des minuscules, des chiffres et des caractères spéciaux). La complexité de ces mots de passe pourra être réduite si des mesures compensatrices visant à assurer un niveau de sécurité équivalent sont mises en place, conformément à la recommandation « mots de passe » (délibération n° 2017-012 du 19 janvier 2017 modifiée le 22 juin 2017) ;

En ce qui concerne la sécurité de l'accès aux applications et aux bases de données locales :

- cesser d'adresser les mots de passe aux utilisateurs de manière non sécurisée, notamment par courrier électronique ; lors de la création du compte, le mot de passe devra être communiqué à l'utilisateur via un canal différent de celui qui est utilisé pour communiquer l'identifiant. Par exemple, si l'identifiant est envoyé par courriel, le mot de passe pourra être communiqué par téléphone, par courrier ou par SMS. Ce mot de passe devra être personnalisé par l'utilisateur lors de la première connexion.
- doter chaque utilisateur d'un compte individuel à l'exclusion de tout compte générique (sauf exception, laquelle nécessite une validation de la hiérarchie et des moyens pour assurer la traçabilité des connexions concernées) soumis à des restrictions d'accès à certaines fonctionnalités dudit logiciel en fonction du niveau d'habilitation de chacun ;
- effectuer une revue régulière des comptes d'accès afin de supprimer les éventuels comptes des personnes ayant quitté l'association.

En ce qui concerne les clauses de confidentialité avec des prestataires :

Il convient de prévoir dans le contrat liant l'association avec son(ses) prestataire(s) accédant à des données à caractère personnel, des clauses permettant de définir les obligations incombant à ce(s) dernier(s) en matière de protection de la sécurité et de la confidentialité des données et d'y préciser que le(s) prestataire(s) ne peut(vent) agir que sur instruction du responsable de traitement, conformément aux dispositions de l'article 35 de la loi du 6 janvier 1978 modifiée dont les exigences sont notamment reprises au point b) du 3ème alinéa de l'article 28 du règlement européen (UE) 2016/679.

Un guide pratique sur la « Sécurité » est disponible sur le site internet de la CNIL (www.cnil.fr).
