CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

AU 46

Gestion de contentieux dans les secteurs privés et publics

Suite à l'entrée en application du RGPD, les normes adoptées par la CNIL n'ont plus de valeur juridique depuis le 25 mai 2018.

Dans l'attente de la production de référentiels RGPD, les responsables de traitement peuvent s'en inspirer pour orienter leurs premières actions de conformité.

La CNIL attire toutefois l'attention sur la nécessité de veiller au respect des nouvelles règles.

Gestion de contentieux dans les secteurs privés et publics

(Déclaration N° 46)

Suite à l'entrée en application du RGPD, les autorisations uniques adoptées par la CNIL n'ont plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables de traitement d'orienter leurs premières actions de mise en conformité.

L'autorisation unique n° 46 encadre la collecte et traitement de données relatives à des infractions, condamnations et mesures de sûreté pour préparer, exercer et suivre une action disciplinaire ou un recours juridictionnel et, le cas échéant, faire exécuter la décision rendue.

TEXTE OFFICIEL

Délibération n° 2016-005 du 14 janvier 2016 portant autorisation unique de traitements de données à caractère personnel mis en œuvre par les organismes publics et privés pour la préparation, l'exercice et le suivi de leurs contentieux ainsi que l'exécution des décisions rendues.

Objectif(s) poursuivi(s) par le traitement (finalités)

Préparation, exercice et suivi d'une action disciplinaire ou d'un recours en justice et, le cas échéant, exécution de la décision rendue.

Données personnelles concernées

1. Données d'identification des mis en cause, des victimes, des témoins et des auxiliaires de justices (nom ; nom d'usage ; prénoms ; sexe ; date et lieu de naissance ; nationalité ; adresse, numéros de téléphone et de fax ; adresse électronique).

2. Données relatives à des infractions, condamnations ou mesure de sûreté, en particulier :

- **faits litigieux ;**
- **informations, documents et pièces recueillis tendant à établir les faits susceptibles d'être reprochés** : constat ; témoignage ; attestation ; mise en demeure ; compte rendu d'une enquête consécutive à une alerte professionnelle ; images extraites d'un dispositif de vidéosurveillance ; « logs » extraits d'un outil de sécurisation des ressources informatiques ; fiche de constat des faits ; dépôt de plainte ; certificat médical ;
- **caractéristiques du contentieux** : date de début et de clôture du litige, juridiction saisie, date de l'assignation, date d'audience, état de la procédure, nature et objet des demandes, griefs, argumentations, observations et avis des représentants légaux, date du jugement ;
- **date, nature, motifs, montants et éventuels échelonnements des condamnations ;**
- **commentaires relatifs à la description et au suivi de la procédure.**

Durée de conservation des données

Les données traitées pour gérer un précontentieux doivent être supprimées dès le règlement amiable du litige ou, à défaut, dès la prescription de l'action en justice correspondante.

Les données traitées pour gérer un contentieux doivent être supprimées lorsque les recours ne sont plus possibles contre la décision rendue pour la faire exécuter.

À l'expiration de ces périodes, les données sont supprimées de manière sécurisée ou archivées dans les conditions prévues par le code du patrimoine, d'une part, ou conformément à la délibération de la Commission n° 2005-213 du 11 octobre 2005 concernant l'archivage électronique pour les organismes du secteur privé, d'autre part.

Les décisions prononcées peuvent être conservées par le responsable de traitement à titre d'archive définitive en raison d'un intérêt historique.

Destinataires des données

Dans les limites de leurs attributions, peuvent accéder aux données :

- les employés du responsable de traitement habilités à préparer et gérer des contentieux dans le cadre de leurs fonctions ; les autres personnes chargées de traiter les données en raison de leurs fonctions (commissaires aux comptes, …) ;
- les sous-traitants du responsable de traitement ;
- les auxiliaires de justice et officiers ministériels (avocats, huissiers, notaires, …) ;
- l'autorité saisie d'un litige.

Les autorités légalement habilitées peuvent, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, demander la communication de données à caractère personnel dans les conditions prévues par le texte fondant leur demande.

Information des personnes et respect des droits « informatique et libertés »

Le responsable du traitement doit informer les personnes concernées par affichage, envoi ou remise d'un document, ou par tout autre moyen équivalent, en précisant notamment son identité ou celle de son représentant, la finalité poursuivie, les destinataires ou catégories de destinataires des données et les modalités d'exercice des droits des personnes (droits d'accès, de rectification et d'opposition pour motif légitime).

Lorsque des mesures conservatoires sont nécessaires pour éviter la dissimulation ou la destruction de preuves, cette information peut être délivrée après l'adoption des mesures conservatoires.

Le responsable de traitement, le cas échéant, doit également informer les personnes concernées de l'existence des traitements permettant de mettre en lumière des comportements susceptibles d'être reprochés ou de contrôler l'activité de son personnel tels que, par exemple, les dispositifs de vidéosurveillance ou les outils de sécurisation des ressources informatiques.

Sécurité et confidentialité

Le responsable de traitement doit prévoir une authentification des utilisateurs respectant les recommandations de la CNIL, un mécanisme de gestion des habilitations, une sécurisation du stockage et des échanges de données, un mécanisme de journalisation des accès à l'application et des opérations effectuées et sécuriser les interventions de maintenance.

Il doit également définir une politique de sécurité, adaptée aux risques présentés par ses traitements et à la taille de l'organisme, décrivant les objectifs de sécurité ainsi que les mesures de sécurité physiques, logiques et organisationnelles permettant de les atteindre.

Transferts des donnes hors de l'union européenne

Il est possible de réaliser des transferts de données :

- vers un pays reconnu par une décision de la Commission européenne comme assurant un niveau de protection suffisant ;
- ou garantissant un niveau suffisant de protection de la vie privée, ainsi que les droits et libertés fondamentaux des personnes, par la mise en œuvre des clauses contractuelles types adoptées par la Commission européenne, ou par l'adoption de règles internes d'entreprise (BCR) ;
- ou justifiés par l'exception du 3° de l'article 69 de la loi du 6 janvier 1978 modifiée, c'est-à-dire le respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice.

Le recours aux exceptions prévues par l'article 69 de la loi du 6 janvier 1978 modifiée n'est pas possible pour les transferts répétitifs, massifs ou structurels de données qui doivent quant à eux faire l'objet d'un encadrement spécifique (BCR ou clauses contractuelles types).