Commission nationale de l'informatique et des libertés

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 (AU-046)

NOR : *CNIL1603455X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 9 et 25-I-3° ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la décision n° 2004-499 DC du 29 juillet 2004 du Conseil constitutionnel ;

Après avoir entendu Mme Marie-France MAZARS, commissaire, en son rapport, et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

Dans le cadre d'une activité régulière, les personnes physiques et les personnes morales peuvent être contraintes de défendre leurs intérêts en justice, notamment pour obtenir la réparation d'un préjudicie subi. Pour faire valoir leurs droits, elles peuvent ainsi être amenées à préparer et à gérer des contentieux.

Dans certains cas, en particulier au sein des personnes morales, il est souvent nécessaire de mettre en œuvre un traitement de données à caractère personnel pour atteindre cet objectif légitime.

Les traitements de données à caractère personnel mis en œuvre pour préparer et gérer des contentieux sont, par nature, susceptibles de porter sur des données relatives à des infractions et condamnations pénales, ou sur des mesures de sûreté.

Il y a par conséquent lieu de faire application des dispositions du 3° du I de l'article 25 de la loi du 6 janvier 1978 modifiée qui prévoient que les traitements, automatisés ou non automatisés, portant sur des données à caractère personnel relatives aux infractions, condamnations ou mesures de sûreté, ne peuvent être mis en œuvre qu'après une autorisation de la commission.

La commission relève, à cet égard, que les personnes morales et les personnes physiques sont fondées, en application de l'article 9 de la loi du 6 janvier 1978 modifiée et de la décision n° 2004-499 DC du 29 juillet 2004 du Conseil constitutionnel, à traiter de telles données en qualité de victime d'une infraction. Par une réserve d'interprétation, le Conseil a en effet estimé que la déclaration d'inconstitutionnalité du 3° de l'article 9 de la loi du 6 janvier 1978 modifiée ne saurait être interprétée comme privant d'effectivité le droit d'exercer un recours juridictionnel dont dispose toute personne physique ou morale, s'agissant des infractions dont elle a été victime.

En application des dispositions du II de l'article 25 de la loi du 6 janvier 1978 modifiée, la commission peut autoriser par une décision unique une catégorie de traitements qui répondent aux mêmes finalités, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires.

Les traitements automatisés de données à caractère personnel mis en œuvre par les personnes physiques et les personnes morales à des fins de préparation et de gestion de contentieux sont de ceux qui peuvent, sous certaines conditions, relever de cette définition.

Les responsables de traitement qui adressent à la Commission une déclaration comportant un engagement de conformité pour les traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à les mettre en œuvre.

Tout traitement de données à caractère personnel qui excède le cadre ou les exigences définis par la présente autorisation unique doit en revanche faire l'objet d'une demande d'autorisation spécifique.

Art. 1er. – *Finalité du traitement.*

Seuls peuvent faire l'objet d'un engagement de conformité en référence à la présente autorisation unique les traitements, automatisés ou non automatisés, impliquant notamment le traitement de données relatives à des infractions ou condamnations pénales ou à des mesures de sûreté et mis en œuvre par une personne morale de droit privé ou de droit public, ou par une personne physique, aux fins de préparer, d'exercer et de suivre une action disciplinaire ou un recours en justice et, le cas échéant, de faire exécuter la décision rendue.

Art. 2. – *Données collectées et traitées.*

A titre liminaire, la commission rappelle que des données à caractère personnel ne peuvent être collectées que si elles sont adéquates, pertinentes et non excessives au regard de la finalité poursuivie.

Le responsable de traitement doit dès lors être en mesure de justifier du caractère nécessaire des données à caractère personnel effectivement collectées.

Sous cette réserve, pour préparer et gérer un contentieux, une personne physique ou une personne morale peut collecter et traiter des données relatives à :

- l'identification des personnes mises en cause, des victimes, des témoins et des auxiliaires de justices mandatés dans la procédure (nom ; nom d'usage ; prénoms ; sexe ; date et lieu de naissance ; nationalité ; adresse, numéros de téléphone et de fax ; adresse électronique) ;
- des infractions, condamnations ou mesure de sûreté, en particulier :
  - les faits litigieux à l'origine de la procédure ;
  - les informations, documents et pièces recueillis tendant à établir des 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 ;
  - les 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 ;
  - la date, la nature, les motifs, les montants et les éventuels échelonnements des condamnations ;
  - les commentaires relatifs à la description et au suivi de la procédure.

La commission précise qu'il est possible, pour établir des faits susceptibles d'être reprochés, de traiter des données relatives à la vie professionnelle, à la vie personnelle, à des informations économiques et financières ou à la santé, sous réserve que les données en question soient indispensables pour atteindre l'une des finalités prévues à l'article 1er de la présente délibération.

Art. 3. – *Durée de conservation des données.*

La commission rappelle que des données à caractère personnel ne peuvent être conservées, conformément à l'article 6-5° de la loi du 6 janvier 1978 modifiée, que le temps strictement nécessaire à l'accomplissement de la finalité pour laquelle elles ont été collectées.

Les données collectées et traitées dans le cadre de la gestion d'un précontentieux doivent ainsi être supprimées dès le règlement amiable du litige ou, à défaut, dès la prescription de l'action en justice correspondante.

Les données collectées et traitées dans le cadre d'un contentieux doivent quant à elles être supprimées lorsque les voies de recours ordinaires et extraordinaires ne sont plus possibles contre la décision rendue.

A l'expiration de ces périodes, les données sont supprimées de manière sécurisée ou, le cas échéant, archivées dans des conditions définies en conformité avec les dispositions du code du patrimoine relatives aux obligations d'archivage des informations du secteur public pour les organismes soumis à ces dispositions, d'une part, ou conformément aux dispositions de la délibération de la commission no 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique de données à caractère personnel pour les organismes relevant du secteur privé, d'autre part.

A cet égard, la commission estime que les décisions prononcées peuvent être conservées par le responsable de traitement à titre d'archive définitive en raison d'un intérêt historique.

Art. 4. – *Destinataires et personnes pouvant accéder aux données.*

La commission rappelle, à toutes fins utiles, que le responsable d'un traitement de données à caractère personnel est tenu, en application de l'article 34 de la loi du 6 janvier 1978 modifiée, de prendre toutes les garanties utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher que des tiers non autorisés y aient accès.

A ce titre, le responsable d'un traitement de données à caractère personnel doit, avant de transmettre des données à un tiers, opérer un tri parmi ces dernières pour s'assurer que ce dernier accède aux seules données adéquates, pertinentes et non excessives au regard de la justification de la communication.

Dans les limites de leurs attributions respectives, et chacun pour ce qui le concerne, peuvent accéder aux données visées par la présente décision unique :

- 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 ;
- les sous-traitants du responsable de traitement ;
- les auxiliaires de justice et officiers ministériels ;
- l'autorité saisie d'un litige.

La commission rappelle, par ailleurs, que les autorités légalement habilitées sont susceptibles, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, de demander au responsable de traitement la communication de données à caractère personnel dans les conditions prévues par le texte fondant leur demande.

Art. 5. – *Information des personnes.*

Le responsable du traitement procède, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée, à l'information des personnes concernées par un traitement mis en œuvre en référence à la présente autorisation unique au moyen d'un affichage, de l'envoi ou de la remise d'un document, ou par tout autre moyen équivalent, en précisant notamment à cette occasion l'identité du responsable de traitement ou 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 rendues nécessaires pour éviter la dissimulation ou la destruction de preuves, cette information peut être délivrée après l'adoption des mesures conservatoires indispensables.

A toutes fins utiles, la commission rappelle qu'un 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, conformément aux dispositions de l'article 32 précité, tels que par exemple les dispositifs de vidéosurveillance ou les outils de sécurisation des ressources informatiques.

Art. 6. – *Droits d'accès, de rectification et d'opposition pour motif légitime.*

Les droits d'accès, de rectification et d'opposition définis au chapitre V de la loi du 6 janvier 1978 modifiée s'exercent directement auprès du ou des services que le responsable de traitement doit impérativement désigner.

Lorsque des règles spéciales régissent la communication de pièces dans une procédure, l'exercice du droit d'accès prévu par l'article 39 de la loi du 6 janvier 1978 modifiée doit intervenir conformément aux règles spéciales en vigueur.

Art. 7. – *Sécurité des données et traçabilité des actions.*

Le responsable de traitement doit prendre toutes les précautions utiles au regard des risques présentés par le traitement pour préserver la sécurité des données. Il doit, notamment au moment de leur collecte, durant leur transmission et leur conservation, empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès.

A cet égard, le responsable de traitement doit notamment s'assurer :

– que les utilisateurs s'authentifient avec un identifiant et un mot de passe respectant les recommandations de la CNIL, ou par tout autre moyen d'authentification apportant au moins le même niveau de sécurité ;
– qu'un mécanisme de gestion des habilitations régulièrement mis à jour permet de garantir que seules les personnes habilitées peuvent accéder aux données nécessaires à la réalisation de leurs missions ;
– que les mesures techniques adéquates garantissent la sécurité des données stockées ou échangées, en particulier lors d'échanges sur internet ;
– de la mise en place d'un mécanisme de journalisation des accès à l'application et des opérations effectuées et de la conservation des données de journalisation pendant une durée de six mois glissants.

Le responsable de traitement définit une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'organisme. Cette politique devra décrire les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre.

Le responsable de traitement prend les mesures nécessaires pour assurer la maintenance du matériel. Ainsi, les interventions de maintenance doivent faire l'objet d'une traçabilité et le matériel remisé ne devra plus contenir de données à caractère personnel.

La commission rappelle que l'usage d'outils ou de logiciels développés par des tiers dans le cadre de la mise en œuvre d'un traitement de données à caractère personnel reste sous la responsabilité du responsable de traitement, qui doit notamment vérifier que ces outils ou logiciels respectent l'ensemble des obligations que la loi du 6 janvier 1978 modifiée met à sa charge.

Elle rappelle également qu'un responsable de traitement conserve la responsabilité des données à caractère personnel communiquées ou gérées par ses sous-traitants et, le cas échéant, que le contrat établi entre les parties doit mentionner les objectifs de sécurité qu'un sous-traitant doit respecter.

La commission rappelle enfin que l'exigence de sécurité prévue par l'article 34 de la loi du 6 janvier 1978 modifiée nécessite la mise à jour des mesures de sécurité au regard de la réévaluation régulière des risques.

Art. 8. – *Transfert de données.*

Un transfert de données à caractère personnel à destination d'un pays tiers à l'Union européenne et non membre de l'Espace économique européen peut être effectué lorsque l'une des conditions suivantes est réunie :

– le transfert s'effectue à destination d'un pays reconnu par une décision de la Commission européenne comme assurant un niveau de protection suffisant ;
– le traitement garantit un niveau suffisant de protection de la vie privée, ainsi que les droits et libertés fondamentaux des personnes, par la mise en œuvre de clauses contractuelles rédigées sur les modèles de clauses élaborés par la Commission européenne relatives aux transferts de données, d'une part, ou par l'adoption de règles internes d'entreprise (« Binding Corporate Rules » ou BCR) adoptées par le responsable de traitement et reconnues par la commission nationale de l'informatique et des libertés et les autorités de protection des données personnelles compétentes comme offrant un cadre juridique satisfaisant pour effectuer des transferts de données en dehors de l'Union européenne, d'autre part ;

– le transfert est justifié par l'exception prévue par le 3° de l'article 69 de la loi du 6 janvier 1978 modifiée, à savoir le respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice.

La commission rappelle que le recours aux exceptions prévues par l'article 69 de la loi du 6 janvier 1978 modifiée n'est possible que pour les transferts dont le champ d'application est limité à des cas ponctuels et exceptionnels. Les transferts répétitifs, massifs ou structurels de données doivent quant à eux faire l'objet d'un encadrement juridique spécifique, par l'intermédiaire de BCR ou de clauses contractuelles types.

Le responsable de traitement s'engage, sur simple demande d'une personne concernée, à apporter une information complète sur la finalité du transfert, les données transférées, les destinataires exacts des informations et les moyens mis en œuvre pour encadrer ce transfert.

Art. 9. – *Publication.*

La présente délibération sera publiée au *Journal officiel* de la République française.

La présidente,
I. Falque-Pierrotin