



**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*

Légifrance

Le service public de la diffusion du droit

Commission Nationale de l'Informatique et des Libertés

Délibération n°2005-213 du 11 octobre 2005

Délibération portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel.

NOR: CNIX0508839X

Etat: VIGUEUR

La Commission nationale de l'informatique et des libertés ;

Vu la convention du Conseil de l'Europe du 28 janvier 1981 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 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu l'article 9 du Code civil ;

Vu les articles 226-16 à 226-24 du Code pénal ;

Vu le code du patrimoine ;

Vu la délibération n° 88-052 du 10 mai 1988 portant adoption d'une recommandation sur la compatibilité entre les lois n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et n° 79-18 du 3 janvier 1979 sur les archives ;

Après avoir entendu M. Emmanuel de Givry, commissaire, en son rapport et Mme Catherine Pozzo di Borgo, Commissaire du gouvernement adjoint, en ses observations.

Formule les observations suivantes :

Les entreprises, organismes ou établissements privés ont l'obligation, au regard de la réglementation applicable, d'archiver nombre d'informations très détaillées sur leur activité passée, en particulier au sujet des opérations effectuées avec leurs clients, fournisseurs ou salariés. Ces informations, de tous degrés d'importance (documents internes, pièces comptables, déclarations sociales et fiscales, transactions bancaires, contrats, etc.) peuvent comporter des données à caractère personnel et sont, dès lors, protégées par les dispositions de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 relative aux fichiers, à l'informatique et aux libertés.

Face à la mémoire de l'informatique, seul le principe du "droit" à l'oubli consacré par l'article 6-5° de la loi du 6 janvier 1978 peut garantir que les données collectées sur les individus ne soient pas conservées, dans les entreprises, pour des durées qui pourraient apparaître comme manifestement excessives. La Commission nationale de l'informatique et des libertés a pour mission de veiller au respect de ce principe s'agissant, en particulier, des durées de conservation relatives aux informations collectées par les entreprises, organismes ou établissements privés mais aussi des modalités de conservation de ces informations.

Dans sa recommandation du 10 mai 1988 sur la compatibilité entre les lois n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et n° 79-18 du 3 janvier 1979 sur les archives, la CNIL a déjà précisé, pour les administrations et organismes du secteur public, les modalités relatives à l'archivage public dans le respect des dispositions de la loi "informatique et libertés". Il lui apparaît aujourd'hui nécessaire, au regard des enjeux relatifs à la protection de la vie privée des personnes, d'adopter la présente recommandation relative aux modalités d'archivage électronique, dans les entreprises, organismes ou établissements privés, de données à caractère personnel.

Par archivage électronique de données à caractère personnel, il convient d'entendre les pratiques de conservation des données visées à l'article 2 de la loi du 6 janvier 1978 modifiée, que celles-ci soient collectées, reçues, établies ou transformées sous forme électronique, par toute personne, service ou organisme privé dans l'exercice de son activité.

La présente recommandation a vocation à s'appliquer aux archives dites courantes, intermédiaires et définitives, ainsi définies :

- par archives courantes, il convient d'entendre les données d'utilisation courante par les services concernés dans les entreprises, organismes ou établissements privés (par exemple les données concernant un client dans le cadre de

l'exécution d'un contrat) ;

- par archives intermédiaires, il convient d'entendre les données qui présentent encore pour les services concernés un intérêt administratif, comme par exemple en cas de contentieux, et dont les durées de conservation sont fixées par les règles de prescription applicables ;

- par archives définitives, il convient d'entendre exclusivement les données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction.

Sur la durée de conservation des données archivées

Les archives courantes et intermédiaires doivent répondre, conformément aux articles 6-5° et 24 de la loi du 6 janvier 1978 modifiée en août 2004, à des durées de conservation spécifiques, proportionnées à la finalité poursuivie (en particulier au regard des durées de prescription définies par la réglementation commerciale, civile ou fiscale), qui doivent être précisées dans le cadre des dossiers de formalités préalables adressés à la CNIL.

Les durées de conservation déclarées à la CNIL doivent être respectées sous peine de sanction prévue par l'article 226-20 du code pénal.

Il est rappelé qu'en application de l'article 36 alinéa 2 de la loi du 6 janvier 1978 modifiée, les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives dans le cadre du livre II du code du patrimoine sont dispensés des formalités préalables à la mise en oeuvre des traitements prévues au chapitre IV de la loi précitée.

Recommande par conséquent que le responsable de traitement établisse, dans le cadre de ses moyens d'archivage, des procédures aptes à gérer des durées de conservation distinctes selon les catégories de données qu'il collecte et soit en mesure d'effectuer, le cas échéant, toute purge ou destruction sélective de données.

Sur la sécurité des données archivées

En application de l'article 34 de la loi du 6 janvier 1978 modifiée, le responsable du traitement doit mettre en oeuvre les mesures techniques et d'organisation appropriées pour protéger les données archivées contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. Ces mesures doivent assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger. Le non-respect de l'obligation de sécurité est sanctionné par l'article 226-17 du code pénal.

L'article 35 de la loi du 6 janvier 1978 modifiée dispose par ailleurs que le responsable du traitement, lorsque l'archivage est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces mesures. La réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable de traitement et qui prévoit notamment que le soustraitant n'agit que sur la seule instruction du responsable de traitement et que les obligations en matière de sécurité incombent également à celui-ci.

Recommande

. s'agissant des archives intermédiaires, que l'accès à celles-ci soit limité à un service spécifique (par exemple un service du contentieux) et qu'il soit procédé, a minima, à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations).

. s'agissant des archives définitives, que celles-ci soient conservées sur un support 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 consulter ce type d'archives (par exemple la direction des archives de l'entreprise).

Recommande, afin de garantir l'intégrité des données archivées, de mettre en oeuvre des dispositifs sécurisés lors de tout changement de support de stockage des données archivées.

Recommande de mettre en oeuvre des dispositifs de traçabilité des consultations des données archivées.

Sur le droit d'accès aux données archivées

Les archives courantes et intermédiaires sont soumises au droit d'accès.

L'article 39-I-4° de la loi du 6 janvier 1978 modifiée dispose que : "Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir (...) la communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci".

Le responsable de traitement doit, par conséquent, prévoir la possibilité d'une demande de droit d'accès aux données archivées et doit être en mesure d'y répondre favorablement.

L'article 39 II de la loi du 6 janvier 1978 modifiée dispose néanmoins que : "Les dispositions du présent article ne s'appliquent pas lorsque les données à caractère personnel sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées et pendant une durée n'excédant pas celle nécessaire aux seules finalités d'établissement de statistiques ou de recherche scientifique ou historique. Hormis les cas mentionnés au deuxième alinéa de l'article 36, les dérogations envisagées par le responsable du traitement sont mentionnées dans la demande d'autorisation ou dans la déclaration adressée à la Commission nationale de l'informatique et des libertés".

Dès lors que le traitement des archives définitives se limite à assurer la conservation à long terme de documents d'archives, et sauf demande spéciale motivée, soumise le cas échéant, à l'appréciation de la Commission, le responsable du traitement n'est pas tenu de donner suite aux demandes concernant les informations archivées et n'a pas le notifier préalablement à la CNIL.

Néanmoins le responsable de traitement doit, dans ce cas, être en mesure de justifier que les moyens d'archivage employés sont de nature à exclure manifestement tout risque d'atteinte à la vie privée des personnes concernée.

Recommande par conséquent d'utiliser, en particulier en cas de données sensibles au sens de l'article 8 de la loi "Informatique et Libertés" modifiée, des procédés d'anonymisation.

Recommande enfin que les entreprises, organismes ou établissements privés définissent, dans le cadre de procédures formalisées, des règles d'archivage répondant à l'ensemble des préconisations précitées et qu'une information puisse être fournie sur ces règles, en cas de demande exprimée de leur part, aux individus faisant l'objet des traitements archivés.

Le président, Alex TURK.

Nature de la délibération: Recommandation

Date de la publication sur legifrance: 14 octobre 2015