C/M/S/ Bureau Francis Lefebvre

L’optimisation de la gestion des données personnelles ou les valeurs des entreprises « data friendly »

Antoine Gendreau, Marie-Pierre Schramm, Anne-Laure Villedieu

C/M/S/ Bureau Francis Lefebvre

Anne-Laure Villedieu

Des conditions générales sans clauses abusives

Les conditions générales sanctionnées

- Dix-huit clauses des Conditions de Vente en ligne d' Amazon.com ont été jugées abusives comme contraires à la loi Informatique et Libertés
- Sanction : 30 000 euros de dommages-intérêts
- Quatre d'entre elles concernaient le traitement des données personnelles
- TGI Paris, 28/10/2008

Et la finalité ?

- Amazon.fr partage les *“informations avec Amazon.com Inc et les filiales qu’Amazon.com Inc contrôle et qui se conforment à la présente politique ou appliquent des règles aussi protectrices que celles mentionnées dans la présente politique”*

- Jugé que cette clause impose au consommateur une diffusion de ses coordonnées sans indication de l’usage et de l’utilité de ce partage d’information

Et l'opt-in ?

- "*nous envoyons de temps en temps des offres à certaines catégories de clients Amazon.fr pour le compte d'autres sociétés*"

- L'article L. 121-20-5 du Code de la consommation n'autorise la prospection directe par voie électronique que lorsqu'elle est réalisée par la même personne morale qui avait originairement collecté les données

Et l'information ?

- *"nous divulgons"* [les données] "...*si cette divulgation est nécessaire pour exécuter et faire appliquer nos conditions générales de vente ou tout autre accord, ou pour protéger les droits d'Amazon ou des tiers"*

- Jugé que les expressions *"tout autre accord* et "*ou des tiers*" laissent le consommateur dans l'ignorance de la destination et de l'usage qui sera fait de ses données

Et les interconnexions ?

- *“à l’avenir nous pourrions être amené à proposer des offres commerciales ou services en co-branding ou en partenariat avec un tiers comme nous vous le proposons aujourd’hui sur le site Amazon”*

- La clause ne spécifiant pas l’objet de la prospection directe possible et introduisant un tiers dans la prospection est jugée abusive comme contraire à l’article L. 121-20-5 du Code de la consommation

Se prémunir

- Respecter le principe de proportionnalité
- Définir en amont les finalités des traitements
- Identifier les destinataires réels des données
- Informer les personne concernée
- Recueillir le consentement à la prospection commerciale directe
- Faire accepter les interconnections
- Et, plus généralement, éviter les clauses « fourre tout »

C/M/S/ Bureau Francis Lefebvre

Marie-Pierre Schramm

La cybersurveillance raisonnée des salariés dans le respect des libertés individuelles

Introduction

- Augmentation des plaintes, auprès de la CNIL, sur les systèmes de contrôle de l'activité des salariés

- Nécessité de concilier les contraintes de sécurité pour l'entreprise et les droits fondamentaux du salarié

Les principes essentiels à respecter (1/4)

- Le principe de proportionnalité : article L. 1121-1 du Code du Travail

  « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché »

Les principes essentiels à respecter (2/4)

- Le principe du respect des droits des personnes :
  - Respect de la vie privée : un principe ancien figurant dans diverses dispositions
  - Secret des correspondances : article L. 226-15 du Code Pénal
  - Droit à l'information

Les principes essentiels à respecter (3/4)

- Une finalité légitime : les données à caractère personnel ou les procédures suivies doivent avoir un usage défini et pertinent

Les principes essentiels à respecter (4/4)

- La consultation des institutions représentatives du personnel :
  - Article L. 2323-13 du Code du Travail sur l'introduction de nouvelles technologies
  - Article L. 2323-32 du Code du Travail notamment sur la mise en œuvre de techniques de contrôle de l'activité des salariés

Les nouvelles technologies et la jurisprudence (1/3)

- La cybersurveillance est un droit mais aussi un devoir pour l'employeur (article 1384 du Code Civil) :
  - Cour d'appel d'Aix-en-Provence du 13 mars 2006
  - Cour de cassation, 2ème C Civ. Du 19 juin 2003

Les nouvelles technologies et la jurisprudence (2/3)

- Dans le respect des droits et des procédures :
  - Cour de cassation, arrêt NIKON du 2 octobre 2001
  - Notion de fichiers personnels et Cour de Cassation du 19 octobre 2006
  - A défaut, risque de récusation des moyens de preuve en cas de licenciement

Les nouvelles technologies et la jurisprudence (3/3)

- Etant précisé par ailleurs que le doute profite aux salariés :
  - Problème d'identification du salarié soi-disant fautif

Déclarations et autorisations (1/2)

- La procédure CNIL
  - Déclaration normale
  - Déclaration simplifiée
  - Autorisation

Déclarations et autorisations (2/2)

- Le CIL (correspondant informatique et libertés)
  - Sa mission
  - Les conséquences de sa désignation

Prescription/archivage/bulletin dématérialisé

- Loi du 17 juin 2008
- Durée de conservation des documents sociaux
- Loi du 28 avril 2009

Conclusion

- L’intérêt d’un guide – livret – charte : « Mieux vaut prévenir que guérir »
- La portée d’un tel document

C/M/S/ Bureau Francis Lefebvre

Antoine Gendreau

L’archivage des données à caractère personnel

Archivage et données nominatives (1/6)

- Contrainte : Marier deux exigences contradictoires :
  - Respect de l'obligation d'archivage d'informations détaillées sur l'activité
  - Respect du principe du «droit à l'oubli» : les données archivées sur les clients, fournisseurs ou salariés ne doivent pas être conservées, pour des durées manifestement excessives; la purge des données concilie droits des individus et saine gestion de l'entreprise
  - les modalités pratiques de cet archivage garantissent les personnes contre, notamment, tout détournement de finalité
- La CNIL a adopté une recommandation 11 octobre 2005 sur l'archivage

Archivage et données nominatives (2/6)

- Classification (1/2)
  - Archives courantes
    - *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)*
  - Archives intermédiaires
    - *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*

Archivage et données nominatives (3/6)

- Classification (2/2)
  - Archives définitives
    - *les données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction.*

Archivage et données nominatives (4/6)

- Règle n°1 : Conservation des archives courantes et intermédiaires pendant une durée proportionnelle à la finalité précisée déclarée à la CNIL :
  - Exemple : durées de prescription définies par la réglementation
  - Conséquence : Etablissement de procédures permettant
    - De gérer des durées
    - De purger de façon sélective les données

Archivage et données nominatives (5/6)

- Règle n°2 : accès aux archives intermédiaires limité exclusivement aux personnes qui ont à connaître des informations (par exemple un service du contentieux) ; isolement des données intermédiaires archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations)

- Règle n°3 : archives définitives conservées sur un support indépendant non accessible par les systèmes de production (avec procédures d'accès obéissant à des règles de motivation) ; dispositifs sécurisés lors de tout changement de support de stockage des données archivées et des dispositifs de traçabilité des consultations des données archivées

Archivage et données nominatives (6/6)

- Conséquences :
  - Formalisation de procédures
  - Permet :
    - D'avoir une visibilité sur les pratiques de l'entreprise et d'en évaluer la conformité
    - De corriger les pratiques
    - De se préparer à un éventuel contrôle

C/M/S/ Bureau Francis Lefebvre

Anne-Laure Villedieu

Auditer ses traitements de données à caractère personnel

Qu’est-ce qu’un audit ?

- *« Un examen systématique et indépendant permettant de déterminer si les activités impliquant un traitement de données à caractère personnel sont menées conformément aux procédures de protection des données à caractère personnel de l’entité, et si ces traitements remplissent les conditions de la loi Informatique et Libertés au sens large »*

Pourquoi un audit ?

- Evaluer le niveau de conformité de l'entreprise à la loi Informatique et Libertés
- Evaluer la conformité des pratiques de l'entreprise avec ses propres règles
- Identifier les lacunes possibles et les faiblesses du système

Catégories d'audits

- Audit interne : l'entreprise procède elle-même de manière régulière à un audit de ses propres traitements
- Audit des contractants : l'entreprise ou ses consultants auditent les contractants de l'entreprise afin de s'assurer que ceux-ci satisfont à la loi Informatique et Libertés
- Audit externe : audit externe de l'entreprise par un consultant ou sous-traitant indépendant

Les méthodes d'audit

- Audit documentaire : vérifier que les règlements, codes d'usages, documents internes et procédures documentées sont conformes à la loi

- Audit de conformité :
  - vérifier que les pratiques de l'entreprise sont conformes aux fondamentaux :
    - Audit fonctionnel ou vertical (un seul service)
    - Audit de traitement ou horizontal (audit d'un traitement)

Interaction avec les salariés

- Questionnement du personnel
- Entretiens sur la sensibilisation du personnel à la protection des données (interviews en face à face ou groupes ciblés)

Méthodologie de l'audit documentaire (1/2)

- Réunion introductive
- Délais : avant l'audit de conformité (minimum 2 à 3 semaines) afin de régulariser les déficiences mineures des documents
- Etude des documents :
  - politique de l'entreprise
  - Codes d'usage
  - Directives
  - Procédures documentées
  - Conséquences de l'audit documentaire

Méthodologie de l’audit de conformité (2/2)

- Réunion introductive
- Détermination de l’environnement de l'audit
- Réalisation de l’audit
- Compte-rendu :
  - Enregistre les données de référence clé
  - Récapituler les principales constatations
  - Suggérer les documents pour l’action corrective
  - Inscrire la nature et les délais de suivi

Les avantages de l'audit

- Les audits permettent de faciliter la mise en conformité à la loi Informatique et Libertés
- Ils établissent la mesure et aident à l'amélioration de la conformité au systèmes de protection des données de l'entreprise
- Ils augmentent le niveau de sensibilisation du management et des salariés à la protection des données personnelles
- Ils améliorent la satisfaction des clients par la réduction des possibilités d'erreurs génératrices de plaintes