



PANDEMIE GRIPPALE : DEPLOYER UN PLAN DE CONTINUTE DE L'ACTIVITE CONFORME A LA LOI « I ET L »

Elaborer un plan de continuité d'activité (PCA)

- De nombreuses entreprises et collectives territoriales établissement actuellement, sous l'impulsion des pouvoirs publics, un plan de continuité d'activité (PCA) afin de **faire face à une épidémie grippale** de grande ampleur.
- L'élaboration d'un PCA ayant pour objectif de **maintenir l'activité économique** au niveau le plus élevé possible tout en protégeant les personnels exposés est d'ailleurs imposé aux administrations de l'Etat et établissements publics placés sous sa tutelle par la **circulaire du 3 juillet 2009**.
- Dans le cadre de la préparation et de la mise en place de leur plan de continuité en cas de passage de la France en niveau d'alerte 6 concernant le virus H1N1, ces entités vont être amenés à **collecter des données à caractère personnel** concernant leurs salariés.
- Cette collecte, bien que légitime et **recommandée par la fiche technique G.1** intitulée « Recommandations aux entreprises et aux administrations pour la continuité des activités économiques et des services publics et la prévention sanitaire en période de pandémie » accompagnant la circulaire, doit être entourée de précautions et réalisée dans le respect des exigences issues de la **loi Informatique et libertés**.

Les actions recommandées

- La conformité du traitement à la loi I et L impose, sous peine de sanctions pénales pouvant aller jusqu'à 5 ans de prison et 300 000 € d'amende, les actions suivantes :
 - A1 : réaliser les **formalités préalables auprès de la Cnil**. Si la collecte se borne à recenser les coordonnées personnelles des salariés ainsi que les moyens de transport utilisés, les traitements sont couverts par la déclaration Cnil de gestion du personnel ou introduits dans la liste des traitements tenue par le Cil. Pour la collecte d'informations liées à la santé, une déclaration normale doit être faite à la Cnil, sous réserve d'avoir recueilli le consentement exprès des salariés concernées. A défaut, le traitement sera soumis à autorisation préalable de la commission.
 - A2 : recueillir le **consentement exprès des salariés** à la collecte et au traitement des données relatives à leur santé ;
 - A3 : **informer les salariés** notamment de la finalité du traitement, des destinataires des données et des droits qu'elles tiennent au titre de la loi Informatique et libertés ;
 - A4 : garantir aux personnes concernées un **droit** d'interrogation, **d'accès**, de rectification et d'opposition pour motifs légitimes ;
 - A5 : assurer la **sécurité** et la **confidentialité** des données. S'agissant en particulier de leurs modalités de recueil (renvoi direct sous pli ou par mail à la personne désignée au sein du service des ressources humaines) ;
 - A6 : déterminer une **politique de durée de conservation** des données ;
 - A7 : encadrer, le cas échéant, les **flux transfrontières** de données.

L'enjeu

Collecter en toute légalité, des données à caractère personnel concernant les salariés afin de mettre en place un plan de continuité d'activité en cas de pandémie.

(1) [Circulaire DGT 2009/16du 3 juillet 2009](#).

Les conseils

- ▶ La mention de recueil du consentement doit figurer en bas des formulaires papiers ou électroniques de collecte de données ou dans un document remis aux salariés en caractères apparents (8 minium) et être précédée d'une case à cocher.
- ▶ L'accès à ces données doit être exclusivement réservé aux personnes habilitées du service des ressources humaines et/ou à la cellule de crise de l'entreprise.

[CHLOE TORRES](#)



TRANSPORT ET BILLETTE PAR CARTE RFID : ATTENTION AUX LIBERTES INDIVIDUELLES DES USAGERS

Le respect de l'anonymat des usagers

- La Cnil a procédé à un **contrôle sur place** auprès de la société délégataire du service public des transports urbains de la ville de Rennes, mettant en œuvre ce dispositif de **billettique par carte RFID**.
- C'est le dépôt de deux plaintes d'usagers des transports urbains rennais, fondées sur le **défaut d'information** sur le passe de transport urbain Korrigo anonyme et la différence de prix entre ce passe et le passe nominatif qui ont alerté la Cnil.
- Le contrôle de la Cnil a révélé des conditions de commercialisation et d'exploitation du passe Korrigo rendant quasiment **impossibles** les **déplacements anonymes** par transports urbains dans la ville de Rennes.
- En outre, les conditions d'exploitation du passe nominatif étaient **contraires** à un certain nombre de principes fondamentaux en matière de **protection des données** à caractère personnel issus de la réglementation Informatique et libertés.

Le passe Korrigo des transports urbains de Rennes sanctionné par la Cnil

- Le contrôle de la Cnil a débouché sur un **avertissement** à l'encontre de la société rennaise exploitant ce dispositif de billettique (1).
- En l'espèce, la possibilité de **circuler de façon anonyme** avait été volontairement quasiment **annihilée** dans la mesure où :
 - seule la **publicité** du passe nominatif Korrigo était assurée ; les intéressés n'étaient pas informés de la possibilité d'utiliser des titres de transports anonymes alors même que l'autorisation unique n° 15 prévoit cette obligation (2) ;
 - le **coût** du passe anonyme pour un usager régulier était nettement supérieur à celui du passe Korrigo nominatif .
- En outre, la Cnil a constaté que les données à caractère personnel collectées et conservées **sans limitation de durée**, étaient ensuite utilisées pour **d'autres finalités** que la gestion des fiches clients (gestion des impayés) sans que les usagers en soient informés.
- Enfin, la société qui par délégation de service public gérait le passe Korrigo nominatif n'avait pas établi de **politique de sécurité interne** ni sensibilisé son personnel aux mesures de sécurité à mettre en œuvre pour assurer la sécurité des données à caractère personnel.
- Ce n'est pas tant la **sanction** qui rend ce cas intéressant mais l'impossibilité volontaire de déplacement anonyme des usagers, le nombre de manquements à la protection des données à caractère personnel et surtout le caractère symptomatique de ce cas d'espèce.
- En effet, ce cas est particulièrement représentatif d'une très nette tendance actuelle au **sacrifice** trop systématique de la **liberté d'aller et venir** de façon anonyme au profit d'intérêts divers pouvant tenir à des **impératifs de sécurité** publique, ou plus grave, **d'intérêts privés**.

Les enjeux

L'atteinte à la liberté d'aller et venir de façon anonyme et plus largement à la vie privée des usagers des transports urbains.

Les conseils

- La possibilité de circuler de façon anonyme doit, dans tous les cas, être préservée.
- Chaque responsable de traitement qui met à disposition des usagers des titres nominatifs de transport doit également prévoir de leur laisser le choix d'utiliser des titres de transport anonymes.

(1) [Délibération n°2009-002 du 20 janvier 2009.](#)

(2) [Délibération n° 2008-161 du 3 juin 2008.](#)

CAROLINE
DOULCET



La collecte d'informations personnelles auprès des salariés est-elle autorisée ?

Source

▪ **Oui** dès lors que les salariés sont bien **informés de la finalité** du recueil et des destinataires de ces informations, par exemple le plan de continuité de l'activité (PCA) des entreprises dans le cadre du risque de pandémie grippale.

A cet effet, la Cnil propose un modèle de mention d'information à faire figurer sur le formulaire de collecte :

« Afin d'établir le « plan de continuité d'activité » (PCA) de l'entreprise, préconisé par les pouvoirs publics dans le cadre du plan national de prévention et de lutte « pandémie grippale », nous souhaitons recueillir vos coordonnées personnelles afin de pouvoir vous joindre (téléphone fixe ou portable, email personnel) ainsi que les moyens de transport que vous utilisez pour vous rendre sur votre lieu de travail.

Nous vous recommandons de nous transmettre ces informations afin de pouvoir vous prévenir et organiser la continuité de notre activité, en cas de pandémie grippale avérée, conformément aux préconisations des pouvoirs publics.

Les destinataires de ces données sont exclusivement les personnes habilitées du service du personnel (ou de la cellule de crise).

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous pouvez accéder à ces informations et les faire rectifier en vous adressant à (Veuillez préciser le service et l'adresse) » (1).

Ce modèle devra notamment être complété par une mention visant à recueillir le consentement express des personnes concernées pour la collecte et le traitement de leurs données de santé.

Doit-on déclarer à la Cnil les traitements relatifs au plan de continuité de l'activité (PCA) ?

Non si le recueil de ces informations se limite aux **coordonnées personnelles** des salariés et à la seule indication des moyens de transport utilisés. Dans ce cas, il n'y a pas lieu de déclarer les fichiers ainsi constitués dès lors que l'entreprise a désigné un correspondant informatique et libertés ou a déclaré son fichier de gestion du personnel (2).

Oui dans le cas contraire et notamment si le recueil porte sur des **données de santé**. Une déclaration normale doit être faite à la Cnil, sous réserve d'avoir recueilli le consentement exprès des salariés concernées. A défaut, le traitement sera soumis à autorisation préalable de la commission.

L'entreprise est-elle responsable des données traitées en télétravail ?

▪ **Oui** La protection des données utilisées et traitées par le télétravailleur incombe à l'employeur conformément aux prescriptions de la Commission nationale de l'informatique et des libertés (Cnil).

Le règlement intérieur de l'entreprise peut prévoir les limites à l'utilisation du matériel et les sanctions encourues. Son éventuelle modification se fait dans les conditions habituelles de consultation du comité d'entreprise et de décision de l'inspecteur du travail (3).

(1) [Communiqué Cnil du 11 août 2009.](#)

(2) [Norme simplifiée n°46.](#)

(3) [Fiche G.3 – Travail à distance.](#)

Informatique et libertés : impact du bilan d'activité de la Cnil sur les entreprises : 16 septembre 2009

▪ **Alain Bensoussan** animera un petit-déjeuner débat consacré au dernier rapport d'activité de la Cnil et à son impact sur les entreprises.

En 2008, la Commission a multiplié les actions de contrôle sur place visant à vérifier le respect de la réglementation Informatique et Libertés par les entreprises et établissements publics. Avec 218 contrôles effectués, elle accroît son activité de + 33 % par rapport à 2007. Elle a adressé 126 mises en demeure, prononcé un avertissement et 9 sanctions financières et effectué cinq dénonciations au Parquet.

L'année a aussi été marquée par la multiplication des sanctions pécuniaires prononcées à l'encontre des entreprises (9 pour un total de 137 100 €), en particulier lorsque la Cnil a constaté des commentaires abusifs dans les zones « blocs notes » des applications relatives à la gestion commerciale et aux ressources humaines.

De même, le développement des technosurveillances en entreprise (géolocalisation, vidéosurveillance, contrôles d'accès, biométrie, etc.) s'est amplifié jusqu'à envisager d'élargir les compétences de la Cnil en matière de vidéosurveillance.

Enfin, 2008 a vu naître un groupe de travail sur le traçage électronique, rebaptisé « groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques » suite aux recommandations du Sénat en mai 2009.

Nous vous proposons, au cours d'un petit-déjeuner, de faire le point sur les plans de mise en conformité qui s'imposent aux entreprises.

▪ **Inscription gratuite** : Nous vous remercions de bien vouloir confirmer votre présence avant le 1er septembre 2009 par courrier électronique en indiquant vos coordonnées et le nombre de personnes qui assisteront au petit déjeuner débat à l'adresse suivante : invitation-conference@alain-bensoussan.com ou en faxant le [bulletin d'inscription](#) au 01 41 33 35 36.

Déclarer ses fichiers à la CNIL : 25 septembre 2009

▪ **Chloé Torres** animera une formation organisée en partenariat avec Francis Lefebvre Formation.

Les objectifs de cette formations sont multiples :

- traiter les données à caractère personnel dans l'entreprise et les formalités à accomplir ;
- savoir quelles sont les données autorisées, interdites, sensibles ;
- apprendre à choisir entre les déclarations, les demandes d'autorisation, les déclarations simplifiées ;
- réaliser les annexes de déclaration et demande d'autorisation ;
- savoir présenter une demande d'autorisation et réaliser un dossier d'accompagnement précisant les fondamentaux juridiques, techniques et économiques à l'appui de sa demande.

Cette formation s'adresse avant tout aux DSI, responsables des données, administrateurs du système d'information, juristes.

Plus généralement, elle s'adresse également à toute personne ayant à prendre en charge la conformité juridique de traitements de données à caractère personnel.

[Télécharger le programme et les conditions Francis Lefebvre Formation](#)

▪ **Inscription payante** auprès de Francis Lefebvre Formation.

▪ Lieu de la formation : Paris.

Biométrie sur le lieu de travail autorisée par la Cnil

- La Cnil a adopté une **autorisation unique** de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur le lieux de travail.
- Elle considère que la gestion des **contrôles de l'accès physique** à l'entrée des lieux de travail et dans les zones limitativement identifiées de l'organisme faisant l'objet d'une restriction de circulation, peuvent s'effectuer grâce à la biométrie (1).

Source

(1) [Autorisation unique AU-019 du 7-5-2009](#), JO du 21 juin 2009.

Procédures judiciaires américaines dite de « DISCOVERY »

- La Cnil a publié des recommandations concernant la communication d'informations à titre de preuve dans les procédures judiciaires américaines dite de « Discovery » **excluant la communication dans le cadre d'affaires pénales** (2).
- La procédure de « Discovery » est une phase d'investigation et d'instruction préalable au procès civil ou commercial, essentielle pour **toute action en justice aux Etats-Unis**, faisant obligation à chaque partie de divulguer à l'autre tous les éléments de preuve pertinents au litige dont elle dispose, même si elles lui sont contraires, quelles que soient leur localisation et leur forme.

(2) [Cnil, Délib. n° 2009-474 du 23 juillet 2009](#).

Collecte d'informations statistiques par la Banque centrale européenne

- Le **contrôleur européen** de la protection des données vient de rendre un avis sur la recommandation pour un règlement du Conseil modifiant le règlement (CE) n° 2533/98 du 23 novembre 1998 concernant la collecte d'informations statistiques par la Banque centrale européenne (3).

(3) [Avis paru au JOUE C 192 du 15 août 2009](#).

Grippe AH1N1 : Recommandations de la CNIL

- La Cnil a publié des recommandations pratiques sur les plans de continuité de l'activité (PCA) des entreprises face au risque de pandémie grippale (4).

(4) [Communiqué Cnil du 11 août 2009](#).

Règles applicables aux réseaux sociaux : le G29 se prononce

- Afin de préciser et d'**harmoniser les règles européennes**, le G29 (groupe des CNIL européennes) a adopté un avis sur les réseaux sociaux sur internet (5).

(5) Avis du G29 sur les réseaux sociaux ([version anglaise](#)).

Notation des avocats et des médecins : la CNIL veille

- La CNIL a adopté une **mise en demeure** à l'encontre du site internet de notation de professionnels (avocats, médecins, etc.) Palmares.com (6).

(6) [Cnil, délib. n° 2009-329 du 4 juin 2009](#).

Directeur de la publication : Bensoussan Alain
Rédigée par les avocats et juristes de ALAIN BENSOUSSAN SELAS
Animée par Chloé Torres et Isabelle Pottier, avocat
Diffusée uniquement par voie électronique
ISSN 1634-0698
Abonnement à : paris@alain-bensoussan.com