



Services de la direction générale
Correspondant Informatique et Libertés

NOTICE TECHNIQUE

D n°4B • 18 mars 2008
Rédacteur : Dominique Chaumet

Traitements de données à caractère personnel

Mise en œuvre de l'Instruction Générale 518

La présente notice technique annule et remplace la notice technique D n°4 du 19 novembre 1981.

Les définitions sont celles de l'I.G.518

1. Formalités préalables à la mise en service d'un traitement

Un traitement de données à caractère personnel ne peut être mis en service avant la réalisation de la formalité préalable qui lui correspond au regard de la loi Informatique et Libertés. Les formalités possibles sont:

- la dispense de déclaration et de demande d'autorisation,
- la demande d'autorisation de la CNIL, d'un ministère, ou du Conseil d'Etat,
- la déclaration au correspondant Informatique et Libertés de la RATP, contre récépissé.

Elles doivent être accomplies pour tout traitement nouveau ou toute modification de traitement.

1.1 La détermination de la formalité pertinente

La formalité préalable à accomplir est déterminée dès l'avant-projet du traitement, afin de ne pas risquer de le remettre en cause après sa mise au point. Lors de cette phase d'avant-projet, le responsable du traitement ou son représentant fait parvenir au correspondant Informatique et Libertés un mémo comportant:

- une description sommaire du traitement,
- une liste des destinataires du traitement,
- une liste prévisionnelle des données à caractère personnel objet du traitement,
- un descriptif sommaire des principes de sécurité envisagés pour assurer la protection de ces données.

En retour, le correspondant Informatique et Libertés indique la formalité préalable à laquelle devra procéder le responsable du traitement avant la mise en service de celui-ci. Le cas échéant, il propose des évolutions pouvant amener à simplifier la future formalité (dispense, norme simplifiée, autorisation unique, etc.). Le responsable du traitement n'a pas obligation à accepter ces propositions. Si nécessaire, le correspondant Informatique et Libertés fait part de ses observations quant à la proportionnalité des données et de leur durée de conservation aux finalités du traitement. Le responsable du traitement intègre ces remarques dans le développement du projet.

1.2 Les interdictions

1.2.1 Il est interdit de collecter et de traiter les données dites "sensibles", c'est-à-dire les données concernant:

- les origines raciales ou ethniques
- les opinions politiques
- les opinions philosophiques ou religieuses
- l'appartenance syndicale

- la santé
- la vie sexuelle

1.2.2 Par dérogation, les données sensibles peuvent cependant être collectées et traitées, dans les cas suivants:

1.2.2.1 sur autorisation de la CNIL

- si le traitement est nécessaire à la recherche dans le domaine de la santé, hors études menées par les médecins de soin,
- ou si une anonymisation rapide des données est effectuée.

La procédure à appliquer dans ce cas est décrite à l'article 1.4

1.2.2.2 contre récépissé de déclaration au correspondant Informatique et Libertés

- si la personne concernée a donné son consentement exprès et éclairé, et que la loi ne s'y oppose pas,
- ou si la personne n'a pas pu donner son consentement, mais que le traitement est nécessaire à la sauvegarde de la vie humaine,
- ou si les données ont été rendues publiques par la personne,
- ou si le traitement est nécessaire à l'exercice d'un droit en justice,
- ou si le traitement est nécessaire à l'exercice de la médecine préventive ou de soin, et qu'il est mis en œuvre par un membre d'une profession de santé soumis à l'obligation du secret professionnel,
- ou si le traitement est nécessaire à des études menées par les médecins de soin et destinées à leur usage exclusif.

La procédure à appliquer dans ce cas est décrite à l'article 1.5

1.3 Les dispenses

Sont dispensés de formalité préalable à leur mise en service les traitements destinés exclusivement à la tenue d'un registre obligatoire et ouvert à la consultation publique.

Sont aussi dispensés de formalité préalable les traitements respectant strictement les spécifications de la CNIL éditées dans les documents suivants, et sous réserve que leurs données ne fassent pas l'objet d'un transfert hors de l'Union Européenne:

- n°1: traitement de la paye,
- n°3: dématérialisation des marchés publics (fichiers comportant les noms des acheteurs et des vendeurs/candidats),
- n°4: fichiers des fournisseurs comportant des personnes physiques,
- n°7: fichiers d'adresses pour communication externe, hors sollicitation commerciale.

Enfin, sont dispensés de formalité préalable spécifique les traitements respectant strictement l'une des déclarations transversales déjà effectuées et ayant fait l'objet d'un récépissé. La liste de ces déclarations transversales est disponible sur Argos (Espace Infos & Services >> Informatique et Libertés).

Ces traitements peuvent être mis en service sans formalité préalable au regard de la loi Informatique et Libertés. Afin de permettre au correspondant Informatique et Libertés d'assurer le droit d'accès des personnes concernées conformément aux dispositions du chapitre 2, le responsable d'un traitement lui transmet une fiche descriptive succincte (modèle joint en annexe 1).

1.4 Les demandes d'autorisation à la CNIL

Outre les cas cités au 1.2.2.1, l'autorisation de la CNIL est nécessaire pour pouvoir mettre en service:

- les traitements de données génétiques hors médecine préventive ou de soin,
- les traitements de données relatives aux infractions,
- les traitements susceptibles d'aboutir à l'exclusion du bénéfice d'un droit,
- les traitements comportant une interconnexion de fichiers relevant d'intérêts publics différents,
- les traitements comportant une interconnexion de fichiers dont les finalités principales sont différentes,
- les traitements impliquant un transfert de données en dehors de l'Union Européenne,
- les traitements comportant une appréciation sur les difficultés sociales des personnes,
- les traitements nécessaires à la recherche dans le domaine de la santé (hors études effectuées par la médecine de soin),
- les traitements ayant pour objet l'évaluation des pratiques du corps médical,
- les traitements liés à la sûreté de l'État,
- les traitements requérant le NIR (Numéro d'Inscription des personnes au Répertoire national d'identification),
- les traitements de données biométriques nécessaires à l'identification des personnes, y compris la vidéosurveillance sur le domaine privatif de la RATP.

Dans les 3 derniers cas, l'autorisation est délivrée par un ministère ou par le Conseil d'État sur avis de la CNIL

Le responsable du traitement remplit un formulaire de déclaration normale à la CNIL accompagné des annexes nécessaires et les transmet au correspondant Informatique et Libertés. Ces formulaires sont disponibles sur le site Internet de la CNIL. Après enregistrement, le correspondant Informatique et Libertés envoie le formulaire et ses annexes à la CNIL pour examen. La CNIL dispose de 2 à 4 mois pour autoriser la mise en service du traitement (ATTENTION: le silence de la CNIL vaut refus de mise en service). Le correspondant Informatique et Libertés avise le responsable du traitement de la décision de la CNIL.

cas particulier: lorsque le traitement est couvert par une "autorisation unique" (spécification éditée par la CNIL pour des traitements identiques mis en œuvre par de nombreuses entreprises), le correspondant Informatique et Libertés en informe le responsable du traitement dès la phase d'avant-projet. La demande d'autorisation à la CNIL se fait alors au moyen du formulaire de déclaration simplifiée, en lieu et place du formulaire de déclaration normale. La CNIL fournit un récépissé par retour du courrier, qui vaut autorisation.

1.5 Les déclarations au correspondant Informatique et Libertés

Tous les autres traitements de données à caractère personnel font l'objet d'une déclaration au correspondant Informatique et Libertés de la RATP. Le responsable du traitement remplit un formulaire de déclaration normale RATP (modèle joint en annexe 2) et le transmet au correspondant Informatique et Libertés. Si nécessaire, le correspondant Informatique et Libertés demande au responsable du traitement ou à son représentant désigné les informations complémentaires permettant d'apprécier le dossier.

Lorsque le dossier est satisfaisant, le correspondant Informatique et Libertés inscrit le traitement sur le registre de la liste des traitements automatisés de la RATP et en informe le responsable du traitement par courrier. Celui-ci peut alors procéder à la mise en service du traitement.

cas particulier: lorsque le traitement est couvert strictement par une "norme simplifiée" (spécification éditée par la CNIL pour des traitements identiques mis en œuvre par de nombreuses entreprises), le correspondant Informatique et Libertés en informe le responsable du traitement dès la phase d'avant-projet. La déclaration se fait alors au moyen du formulaire de déclaration simplifiée RATP (modèle joint en annexe 3), en lieu et place du formulaire de déclaration normale. Le correspondant Informatique et Libertés inscrit immédiatement le traitement sur le registre de la liste des traitements automatisés et en informe le responsable du traitement par courrier. La liste des normes simplifiées et le détail de leurs spécifications sont fournis sur le site Internet de la CNIL.

1.6 Les obligations

1.6.1 consentement et information

Un traitement de données doit avoir reçu le consentement de la personne concernée ou satisfaire à:

- une obligation légale,
- la sauvegarde de la vie de la personne,
- l'exécution d'une mission de service public,
- l'exécution d'un contrat dont la personne est partie prenante.

Dans les cas où le consentement de la personne n'est pas expressément requis, celle-ci doit néanmoins être avisée que des données la concernant sont susceptibles d'être traitées et qu'elle bénéficie d'un droit d'accès et de rectification (voir article 2.1).

1.6.2 proportionnalité des données et de leur durée de conservation

Les données collectées et/ou traitées doivent être strictement proportionnées aux besoins du traitement. Les données qui ne sont pas indispensables aux finalités du traitement ne doivent pas y être intégrées.

De même, la durée de conservation des données doit être celle juste nécessaire au traitement. La notion de conservation (maintien dans la base des données pour utilisation par le traitement) est à différencier de celle d'archivage (enregistrement sur un support séparé non accessible par un traitement automatisé): la durée de l'archivage est laissée à la discrétion du responsable.

Ce document est la propriété de la RATP. Il ne peut être reproduit, même partiellement sans son autorisation.

1.6.3 sécurité des données

Dans tous les cas de figure, y compris la dispense de déclaration, le responsable d'un traitement doit tout mettre en œuvre pour garantir l'intégrité des données à caractère personnel, ainsi que leur confidentialité (sécurité matérielle, sécurité logicielle, formation/habilitation, etc.). L'utilisation de la sous-traitance ne décharge pas le responsable de traitement de cette obligation. Le contrat de sous-traitance doit faire apparaître explicitement les mesures de sécurité et de confidentialité à prendre, et que le responsable du traitement a déterminées comme nécessaires.

1.7 La mise hors service

Lorsqu'un responsable de traitement décide de mettre celui-ci hors service, il en informe le correspondant Informatique et Libertés par courrier. Le traitement est alors retiré du registre de la liste des traitements automatisés.

2. Droit d'accès des personnes concernées

Le correspondant Informatique et Libertés tient le registre de la liste des traitements de données à disposition de toute personne qui en fait la demande, selon les modalités les plus pertinentes (support papier, pages Intranet pour les données du personnel, et pages Internet pour les autres, en particulier). Ce registre présente de façon résumée les traitements et les données auxquels ils s'appliquent. Il ne comporte pas les valeurs des données propres à chaque personne.

L'exercice du droit d'accès aux données elles-mêmes se fait selon les modalités ci-dessous.

2.1 L'information des personnes concernées

Lors de leur collecte, les personnes concernées doivent être avisées des finalités du traitement des données. Cette information doit être fournie quelle que soit la nature du contact (téléphone, courrier postal, courrier électronique, questionnaire, guichet, etc.). Le responsable du traitement détermine le support le plus approprié de cette information. Cette information doit contenir au moins les éléments suivants:

- le fait que le traitement est effectué par ou pour la RATP,
- la finalité principale du traitement,
- les conséquences d'un éventuel refus,
- les modalités d'exercice du droit d'accès.

Pour accéder aux données stockées, les demandes et réclamations doivent être adressées au Correspondant Informatique et Libertés de la RATP. Les coordonnées du Correspondant Informatique et Libertés mentionnées sur les documents de collecte de données ou sur les documents généraux de la RATP sont:

- le numéro de téléphone de la ligne affectée à cet usage (01 58 77 41 83)
- l'adresse de la boîte postale (Correspondant Informatique et Libertés de la RATP - 13 Rue Jules Vallès - LAC JV27 - 75547 Paris)
- l'adresse électronique (cil-ratp@ratp.fr).

2.2 L'exercice du droit d'accès via le correspondant Informatique et Libertés

Le responsable d'un traitement informe le Correspondant Informatique et Libertés de la procédure mise en place dans son entité (lieux et heures d'accès, identité des collaborateurs chargés des accès aux données, coordonnées, ...) en remplissant la zone "Accès aux données" du formulaire de déclaration.

Les demandes d'accès ou les réclamations sont reçues par le Correspondant Informatique et Libertés ou son secrétariat. En cas de doute, celui-ci contacte la personne concernée afin d'obtenir

Ce document est la propriété de la RATP. Il ne peut être reproduit, même partiellement sans son autorisation.

des précisions sur sa demande. Dans le cas général, il contacte les collaborateurs des responsables de traitements en cause, qui lui fournissent les données demandées. Il collationne ces données et les transmet à la personne au maximum 2 mois après sa demande. Il tient un journal de ces demandes et des dates des réponses apportées.

Lorsque les données sont gérées par un sous-traitant, son contrat prévoit explicitement son obligation de fournir au correspondant Informatique et Libertés de la RATP les données à caractère personnel demandées, pour satisfaire à l'exercice du droit d'accès.

Lorsque la personne concernée demande à consulter ses données sur place et que cette possibilité est prévue, le correspondant Informatique et Libertés l'oriente vers le responsable du traitement ou son collaborateur désigné à cet effet. La personne est reçue le plus tôt possible et moins de 2 mois après avoir effectué sa demande. La personne justifie de son identité par tout moyen; elle peut se faire assister du conseil de son choix ou se faire représenter (le mandataire doit alors faire la preuve de son mandat). Le responsable informe le correspondant Informatique et Libertés des suites données.

cas particulier 1: pour la consultation des données liées à leur statut d'agents de la RATP, ceux-ci peuvent continuer à s'adresser à leur responsable hiérarchique ou à leur responsable Ressources Humaines. Le contact du correspondant Informatique et Libertés reste possible comme recours pour les agents n'ayant pas obtenu satisfaction par la voie précédente.

cas particulier 2: pour la consultation des données à caractère médical, la personne concernée peut désigner un médecin auquel ces données seront transmises directement par le personnel médical en charge du traitement. La mise en relation de ces interlocuteurs est alors assurée par le correspondant Informatique et Libertés ou son secrétariat.

2.3 L'opposition, la rectification, la suppression

Hormis les cas énumérés au 1.6.1, toute personne peut s'opposer à ce que les données à caractère personnel la concernant soient collectées et/ou traitées. Elle doit alors être avisée par le responsable du traitement ou son représentant des conséquences de ce refus, le cas échéant.

A l'occasion de l'exercice du droit d'accès, toute personne peut exiger de la RATP que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, ou périmées.

Toute personne a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur. Elle peut notifier cette opposition soit à l'occasion de la collecte des données, soit à l'occasion de l'exercice du droit d'accès.

cas particulier: pour ce qui concerne les données liées à leur statut d'agents de la RATP, ceux-ci peuvent continuer à s'adresser à leur responsable hiérarchique ou à leur responsable Ressources Humaines. Le contact du correspondant Informatique et Libertés reste possible comme recours pour les agents n'ayant pas obtenu satisfaction par la voie précédente.

3. Contrôles

3.1 Contrôles par la CNIL

Les membres de la CNIL, ainsi que ses agents habilités, ont accès de 6 heures à 21 heures, pour l'exercice de leurs missions, aux installations ou établissements servant à la mise en oeuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel.

Ils peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie ; ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles ; ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

Ils peuvent, à la demande du président de la CNIL, être assistés par des experts.

Lorsque la CNIL effectue un contrôle sur place, elle informe au plus tard au début du contrôle le responsable des lieux de l'objet des vérifications qu'elle compte entreprendre, ainsi que de l'identité et de la qualité des personnes chargées du contrôle. Lorsque le responsable du traitement n'est pas présent sur les lieux du contrôle, ces informations sont portées à sa connaissance dans les huit jours suivant le contrôle. Dans le cadre de leurs vérifications, les personnes chargées du contrôle présentent en réponse à toute demande leur ordre de mission et, le cas échéant, leur habilitation à procéder aux contrôles.

La CNIL peut procéder à des vérifications à la demande d'une autorité exerçant des compétences analogues aux siennes dans un autre Etat membre de l'Union Européenne.

Les missions de contrôle sur place de la CNIL font l'objet d'un procès-verbal. L'inventaire des pièces et documents dont les personnes chargées du contrôle ont pris copie est annexé au procès-verbal. Le procès-verbal est signé par les personnes chargées du contrôle qui y ont procédé et par le responsable des lieux ou par toute personne désignée par celui-ci. Le procès-verbal est notifié au responsable des lieux et au responsable des traitements.

Lorsque les opérations de vérification nécessitent l'accès à des données médicales individuelles, le préfet désigne, à la demande du président de la CNIL, un médecin inspecteur de santé publique ou un médecin inspecteur du travail chargé de requérir la communication de ces données; le président de la CNIL peut également désigner un médecin inscrit sur une liste d'experts judiciaires.

Le médecin présente en réponse à toute demande son ordre de mission.

Le médecin consigne dans un rapport les vérifications qu'il a faites sans faire état, en aucune manière, des données médicales individuelles auxquelles il a eu accès. Le rapport est remis au président de la CNIL qui en adresse une copie au professionnel de santé responsable du traitement.

3.2 Contrôles par le correspondant Informatique et Libertés

Le Correspondant Informatique et Libertés peut effectuer ou faire effectuer des contrôles et audits sur les traitements mis en place, soit de façon inopinée, soit selon un programme annuel. Pour ce faire, il peut se faire assister des départements GIS, JUR, ou SIT, ou faire appel à un expert extérieur à la RATP, ou confier l'opération à l'Inspecteur Général.

Il dispose des mêmes droits d'accès aux documents que ceux prévus à l'Article 4-4 de l'IG 432C, limités aux unités de l'EPIC RATP. Il en transmet ensuite les conclusions aux responsables des traitements concernés, ainsi qu'au Président - Directeur général, via le membre du Comité exécutif approprié.

Lorsque les opérations de vérification nécessitent l'accès à des données médicales individuelles, le correspondant Informatique et Libertés sollicite un médecin expert un médecin inspecteur du travail pour effectuer les contrôles. Le médecin consigne dans un rapport les vérifications qu'il a faites sans faire état, en aucune manière, des données médicales individuelles auxquelles il a eu accès

En cas de non respect des obligations de la loi Informatique et Libertés par le responsable d'un traitement, le correspondant lui signifie ce manquement et lui demande un calendrier de correction. Si ce calendrier n'est pas respecté, le correspondant Informatique et Libertés avise le supérieur hiérarchique du responsable du traitement de ce nouveau manquement et lui demande d'établir un plan de suppression des irrégularités. Si nécessaire, le correspondant Informatique et Libertés informe la CNIL après avoir porté le dossier à la connaissance du Président-directeur général de la RATP.

4. Mise en œuvre locale

Lorsque les dispositions de la présente notice technique sont mises en œuvre par une procédure décrite dans un texte réglementaire de département ou d'unité, une copie de celui-ci est fournie au correspondant Informatique et Libertés.

le responsable de l'administration générale de l'ÉPIC

Alain Le Duc
directeur financier performance économique

5. Annexes

- annexe 1: Fiche descriptive succincte
- annexe 2: Déclaration normale RATP
- annexe 3: Déclaration simplifiée RATP

Ces formulaires sont disponibles sur la page Argos >> Espace Infos & Services >> Informatique et Libertés