GLOSSAIRE

Données à caractère personnel :
Informations relatives à des personnes identifiées ou identifiables. Les personnes dont les données sont identifiées sont dénommées *personnes concernées*

Données sensibles :
Toutes données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Traitement de données à caractère personnel :
Toute opération effectuée sur les données à caractère personnel, à l'aide d'un procédé automatisé ou non, telles que la collecte, l'enregistrement, la conservation, l'adaptation, la consultation, l'utilisation et la destruction.

Responsable de traitement :
Entité juridique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données personnelles.

Destinataire(s) des données :
Toute entité qui reçoit ou accède aux données personnelles traitées, en dehors du responsable de traitement et du sous-traitant (et leurs employés et/ou préposés), est un *destinataire* des données.

Finalités du traitement :
Objectif principal pour lequel les données sont traitées. Les *finalités* doivent être distinguées des *sous-finalités* d'un traitement qui sont des raisons annexes justifiant le traitement afin d'atteinte l'objectif principal constituant la *finalité* du traitement.

Durée de conservation :
Durée maximale pour laquelle les données personnelles sont conservées par le responsable de traitement et ses éventuels sous-traitants.

DPO *Délégué à la Protection des Données*
(*Data Protection Officer* en anglais) :
Personne chargée de s'assurer de la mise en œuvre et du suivi de la conformité de l'ensemble des traitements de ladite entité avec la législation sur la protection des données personnelles

CHECKLIST

- ☑ Identifier des activités utilisant des données personnelles
- ☑ Choisir les données nécessaires et les trier par finalité
- ☑ Informer les personnes de l'usage de leurs données et de leurs droits
- ☑ Sécuriser les données recueillies

Quand J'ai tout checké, je peux solliciter Eittel Missika

CONTACT DPO

03 22 71 51 35
Fréderic Berdal
dpo@keolis.com
KEOLIS AMIENS

Au cœur de la conformité

RGPD

KEOLIS AMIENS
ametis
AMIENS MÉTROPOLE

CAS CONCRETS

Mme A. DRH, crée un fichier pour enregistrer les dossiers de candidature chez AMETIS. Elle enregistrera ainsi des informations sur de potentiels candidats afin d'apprécier leur capacité à occuper l'emploi proposé et mesurer leurs aptitudes professionnelles.

Pour cela, elle collecte tous les documents fournis par le candidat (CV, diplômes, portfolios, lettres de recommandation). Elle se rend compte que le candidat lui a adressé sa pièce d'identité . N'ayant pas besoin de cela pour recruter un candidat, elle décida de supprimer la pièce de son système et informa par mail le candidat que cet élément n'est pas nécessaire à cette étape de la procédure et des droits dont il dispose.

Pour Mme A. seul le directeur du service concerné par l'emploi ouvert aura accès aux informations du candidat et uniquement pendant la durée du recrutement.

Enfin, elle se rapprocha du DPO pour qu'ils déterminent ensemble la durée de conservation des informations sur les candidats.

M. X. en charge de la relation clientèle d'AMETIS dispose d'une base de données clients, constituée des années auparavant, servant à adresser quotidiennement à ces derniers des informations sur les offres et services d'AMETIS et ses partenaires.

A cet effet, il souhaiterait poursuivre l'utilisation de cette base alors qu'il ne dispose plus de la preuve du consentement des clients et abonnés présents sur cette liste .

Heureusement, M. X. consulte M. Y., DPO d'AMETIS () pour qu'il valide sa démarche. Ce dernier s'y oppose. Alors M. X. adopte une autre approche : il contacte l'ensemble des clients figurant dans cette base afin de redemander leur consentement .

Désormais, le fichier ne contient que les informations des clients ayant répondu favorablement et donné leurs consentements. Le service communication et le servie informatique seront les seuls à accéder à la base de données nouvellement constituée et les informations contenues dans cette base seront conservées tant que la personne concernée ne désinscrit pas.

M. V. a la charge de la gestion du fichier des infractions constatés sur le réseau AMETIS.

A cette fin, il est amené à conserver les données des contrevenants en vue de détecter une répétition de fraude au transport appelée le délit d'habitude.

Dès lors, il aimerait conserver les données des contrevenants pendant une durée de 5 ans de manière à « emmerder » aussi longtemps que possible les usagers de bus non titulaires de titre de transports .

A la suite d'un entretien avec M. Y., DPO d'AMETIS, M. V. a changé d'avis et désormais, il conservera les données des contrevenants pendant 12 mois maximum . En outre, seuls les agents habilités et les contrôleurs assermentés consulteront ce fichier d'infraction via des code d'accès et des mots de passe individuels régulièrement mis à jour afin de protéger la vie privée des personnes inscrites sur le fichier.

LA RGPD EN 9 POINTS

8. J'adopte une bonne hygiène numérique pour garantir la sécurité de toutes les données collectées

• Est-ce que mon mot de passe est suffisamment fort ? *****

• Est-ce que j'effectue des sauvegardes régulières des informations que je manipule ?

• Est-ce que je range mes documents sensibles dans un coffre-fort ou une armoire sécurisée dont je suis le seul à connaître la combinaison ou à en avoir la clé ?

1. J'identifie mes activités utilisant des données personnelles.

• Est-ce que je manipule des données personnelles ?

2. Je détermine la finalité de chaque fichier de mon activité et je me tiens à celle-ci.

• Pourquoi ai-je besoin des données personnelles ?

• À quoi me serviront les données personnelles collectées ?

• Recueillir et prouver le consentement éclairé des individus

3. J'identifie, pour chaque fichier, qui peut avoir besoin de ces informations

• Qui est-ce qui accèdera au sein de l'entreprise à mes données ? (Collègues par ex.)

• Qui est-ce qui accèdera hors de l'entreprise à mes données ? (Partenaires par ex.) /!\ Je ne dois pas divulguer des données à des tiers non autorisés.

4. J'identifie, pour chaque fichier combien de temps je dois garder chaque type d'informations (et je ne les conserve pas au-delà).

• Combien de temps dois-je conserver les données collectées ?

• Ai-je des obligations légales de conserver les données pendant un certain temps ?

• Dois-je conserver certaines données en vue de me protéger contre un éventuel contentieux ? Lesquelles ?

• Est-il pertinent de conserver toutes les données aussi longtemps ?

5. Documenter les mesures et les procédures de protection

6. Sécuriser les données contre les risques de perte de vol ou de Divulgation

7. J'informe toujours les personnes au moment de la collecte et je respecte leurs droits.

• Quelles informations dois-je fournir aux personnes concernées ?

• Ai-je permis aux personnes d'exercer leurs droits ?

KEOLIS AMIENS