RGPD POUR L'EMPLOYEUR

Dans La Boucherie Belge n°4 du 8 avril 2018 un article général en ce qui concerne le Règlement Général sur la Protection des Données a été publié.
Ci-dessous vous trouverez des informations concernant vos obligations en tant qu'employeur.

En tant qu'employeur, vous traitez certaines données personnelles de vos collaborateurs (nom, adresse, photo, profil en ligne, données salariales, numéro du registre national, données login de l'ordinateur, etc ...).
Par '**traitement de données**', on entend e.a.: stocker, rassembler, collecter, établir, mettre à jour, modifier, utiliser, consulter, envoyer, transmettre, diffuser, effacer, avec l'intention de les reprendre dans un fichier (informatique ou manuel (p.ex. fiches, fardes, boîtes, ...)
Par '**données personnelles**', on entend les données permettant d'identifier une personne.

Exemples: administration des salaires et du personnel, conservation d'un dossier du personnel, tenue d'une base de données de postulants/travailleurs/intérimaires, systèmes d'enregistrement des présences (badges, pointeuses), surveillance par caméras, système track&trace dans les véhicules d'entreprise, album photos des travailleurs sur intranet, données sur la situation familiale d'un travailleur, photos d'une fête du personnel, données login des systèmes informatiques, données des gsm des travailleurs à usage privé, mots de passe pour les e-mails, systèmes de géolocalisation...

INFORMEZ VOTRE PERSONNEL

Il est obligatoire de communiquer les données suivantes à votre personnel:

- ¬ qui est responsabledu traitement des données personnelles (c'est l'employeur);
- ¬ quels sont les objectifs de ce traitement (pourquoi les données sont traitées);
- ¬ qui traite les données (qui peut traiter les données communiquées par l'employeur, p.ex. secrétariat social, assureur accidents de travail, service externe de prévention et de protection au travail, médecin-contrôle, etc.);
- ¬ quelles données sont traitées;
- ¬ d'où ces données proviennent (du travailleur lui-même ou d'autres sources);
- ¬ la base juridique pertinente pour traiter les données personnelles (dans beaucoup de cas, une base légale);
- ¬ le droit de retirer son autorisation (seulement si vous n'avez pas de base légale);
- ¬ le délai de stockage de ces données (leur durée de conservation);
- ¬ le droit de transmettre ces données;
- ¬ qui le travailleur peut contacter au sujet du traitement de ses données;
- ¬ le droit de regard, de correction, d'effacement, de limitation, d'objection;
- ¬ le droit d'introduire une réclamation auprès de l'Autorité de Protection des Données (APD, qui succède à la Commission de la Protection de la Vie Privée 'Privacycommission');
- ¬ les données concernant un 'Privacy officer', agent de protection de la vie privée (s'il y en a un) (voir plus loin);
- ¬ si les données seront envoyées hors de l'UE et, sic'est le cas, quels sont ses droits;
- ¬ si les données personnelles sont centralisées sur un serveur du bureau principal à l'étranger.

Vous devez **informer** le travailleur des données ci-dessus de manière **proactive**.
Vous devez **communiquer** ces informations au travailleur de manière écrite et transparente.
La manière la plus facile de remplir ce devoir de communication est de faire insérer une '**privacy policy'** (politique de confidentialité) dans votre règlement de travail (via la procédure de modification du règlement de travail).

DOCUMENTEZ LA BASE JURIDIQUE DU TRAITEMENT

Via la signature de la politique de confidentialité, vous obtenez de votre travailleur l'autorisation de traiter ses données personnelles. Cette autorisation constitue alors la base juridique vous permettant de traiter les données.
Si un travailleur refuse de donner son autorisation, vous avez quand même le droit dans certains cas de traiter les données de ce travailleur, à savoir si vous pouvez démontrer un intérêt justifié ou une base légale. Ce qui importe en tout cas, c'est que vous documentiez et motiviez la 'base juridique' pour laquelle vous estimez pouvoir faire appel à une base juridique déterminée. Vous devez alors reprendre celle-ci dans le registre des données (voir ci-dessous) et la communiquer aux travailleurs via votre obligation d'information (voir ci-dessus).

CONSTITUEZ UN REGISTRE DES ACTIVITÉS DE TRAITEMENT DES DONNÉES

Vous devez conserver un registre interne des activités de traitement des données et le tenir à jour périodiquement. Ce registre peut être tenu par écrit mais aussi de manière informatique au sein de votre entreprise. Ce n'est pas un document public et il reste interne.
Vous devez ydécrire tous les processus où vous traitez des données personnelles et communiquer, par processus, les éléments suivants:

- ¬ qui est responsable du traitement des données personnelles;
- ¬ quelles données sont traitées;
- ¬ de quelle personne des données sont traitées;
- ¬ la raison du traitement des données;
- ¬ qui reçoit les données (p.ex. le secrétariat social dans le cadre de l'administration des salaires);
- ¬ le délai de conservation des données;
- ¬ les mesures de sécurisation (p.ex. les informations sont-elles cryptées? les bases de données ne sont-elles accessibles qu'avec un mot de passe? quelles sont les personnes dans l'organisation qui ont un mot de passe? quels sont les moyens de détecter, de signaler et d'enquêter sur des fuites de données?)

Vous ne devez mentionner dans le registre **que les traitements réguliers et fréquents** de données personnelles (exception: si vous employez plus de 250 travailleurs). Vous devez de temps en temps actualiser le registre, chaque fois que des modifications surviennent.

Vous trouverez un modèle de registre en cliquant sur le lien https://www.privacycommission.be/fr/modèle-de-registre-des-activités-de-traitement

PROTEGEZ LES DONNEES PERSONNELLES

Vous devez traiter les données de manière aussi sécurisée que possible (p.ex. paranonymisation, pseudonymisation ou encryptage).

Vous devez aussi prendre les précautions nécessaires contre les fuites de données (= empêcher que les données de votre personnel tombent entre de mauvaises mains). Il est important que vous **formiez** et que vous **sensibilisiez** votre **personnel**, de manière à ce que tout le monde au sein de l'entreprise sache comment utiliser correctement des données personnelles.

Exemples de fuites de données: piratage et cybercriminalité, mais aussi fuites fortuites (e-mail envoyé par accident au mauvais destinataire, vol d'un laptop de l'entreprise, notes oubliées dans le train, perte d'une clé USB, etc...).

Vous devez tenir à jour un document interne, un **registre des fuites de données** (description de la fuite, quand elle s'est produite, ce qui est arrivé aux données, quelle personne/groupe de personnes est concerné(e) par la fuite, de combien de personnes et de quelle sorte de données il s'agit, conséquences de la fuite, mesures préventives prises, etc...).

S'il s'agit d'une fuite de données comportant probablement un risque pour les droits et les libertés de personnes physiques, vous devez la signaler à l'APD. Les fuites de données constituant un risque élevé pour l'intéressé, doivent être signalées à l'intéressé lui-même.

LES PARTIES EXTERNES

Quand vous faites appel à des tiers pour traiter les données de votre personnel, vous devez vous assurer qu'ils sont en ordre avec le GDPR.

(p.ex.: secrétariat social, assureur des accidents de travail, prestataires de services informatiques externes, bureau d'intérim, service externe de prévention et de protection au travail, fonds de pension, société de chèque-repas, bureau de sélection et de recrutement, service d'archivage pour e-filing, fournisseur de services cloud pour le stockage de données, firme de surveillance, ...).

Vous devez **conclure** avec ce tiers 'traiteur de données' **un contrat** vous **garantissant** que le tiers respecte la législation sur le GDPR.

Identifiez bien les divers fournisseurs qui traitent les données personnelles de votre entreprise et concluez un contrat avec chacun d'entre eux, pour être certain qu'ils respectent les règles en matière de GDPR et que les données de votre personnel soient bien sécurisées avec eux.

SUGGESTIONS ET CONSEILS CONCRETS

1. Commencez par faire le point de la situation au sein de votre entreprise: Quelles données personnelles traitez-vous actuellement concernant votre personnel? D'où proviennent ces données? Avec qui les partagez-vous? Qui y a accès? Listez ces informations.

2. Sur base de cette liste, regardez – par catégorie de données que vous traitez – si vous avez une base juridique ou l'autorisation du travailleur pour traiter ces données (base légale).

3. Informez les travailleurs de votre entreprise des activités de traitement. Donnez-leur les explications nécessaires à ce sujet et procurez-leur une information écrite en adaptant votre règlement de travail (et éventuellement d'autres documents).

4. Faites un tour d'horizon des risques de perte, de vol ou d'accès non-autorisé et de leursconséquences éventuelles. Sensibilisez votre personnel et formez-le à une manière correcte d'utiliser les données personnelles de collègues, de clients, etc... En cas de besoin, prenez des mesures pour sécuriser les données: nouveaux arrangements, adaptations techniques ou dans l'organisation (limiter l'accès aux données, introduire des procédures de sécurité, des dispositions pour l'utilisation de son propre PC ou laptop, ...).

5. Dressez une liste des organisations et des tiers à qui vous transmettez les données personnelles de vos collaborateurs (p.ex. secrétariats sociaux, assureurs, services externes de prévention et de protection au travail, ...) et veillez à conclure avec chacun d'entre eux un contrat comportant un minimum d'accords et de mentions obligatoires en matière de GDPR.

6. Etablissez le registre des activités de traitement des données et mettez-le à jour à chaque modification: ce registre offre un aperçu du traitement des données, avec chaque fois les objectifs par procédure de traitement.

7. Etablissez un registre des fuites de données et décrivez-y les mesures préventives que vous prenez.

8. Vous êtes confronté à une fuite de données? Signalez-la à l'intéressé(e) et éventuellement à l'APD. Mentionnez la fuite dans le registre des données et décrivez-y les actions que vousentreprenez pour prévenir/limiter les dégâts.

SANCTIONS

A partir du 25 mai 2018, tout employeur qui n'est pas en ordre avec la législation sur le RGPD, risque une amende.

AUTRE LÉGISLATION BELGE

En Belgique, il existe déjà une législation protégeant les travailleurs contre le traitement de leurs données personnelles:

- Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel;
- C.C.T. 68 – surveillance par cameras;
- C.C.T. 81 – contrôle des données de communication électroniques en réseau (utilisation e-mail, internet, etc.);
- C.C.T. 89 – prévention des vols et contrôle des sorties.

Attention: si vous avez pris toutes les mesures pour être conforme au RGPD en tant qu'employeur, mais que vous avez encore des caméras dans l'entreprise, que vous souhaitez exercer un contrôle sur l'utilisation de l'e-mail et d'internet par les travailleurs de votre entreprise, etc..., vous devrez également respecter les obligations supplémentaires contenues dans les CCT nationales susmentionnées.

Source : NSZ