Protection de la vie privée au travail et données personnelles

Brochure à l'usage des militants

Introduction

La protection des données et de la vie privée, un thème syndical?

C'est un thème qui revêt une importance croissante dans le monde du travail: la protection des données et de la vie privée. Le processus de digitalisation de la société dans son ensemble, qui n'épargne pas les entreprises et les organisations, impacte la vie privée et les données personnelles de chacun d'entre nous. L'essor de l'intelligence artificielle, qui est de plus en plus utilisée sur les lieux de travail, a également un impact considérable sur cette question, étant donné qu'elle a besoin de collecter des quantités massives de données pour fonctionner. Nous nous intéressons dans cette brochure à l'impact de la législation sur la protection des données sur le monde du travail. Dans un premier temps, nous ferons le point sur la législation puis nous verrons comment elle s'applique dans les relations de travail, entre l'employeur et les travailleurs. Il s'agira de voir quelles données peuvent être traitées et à quelles conditions, et de voir quelles limites légales entourent le contrôle et la surveillance des travailleurs.
Enfin, nous verrons comment cette législation impacte (ou pas) le travail syndical et les missions des représentants syndicaux.

Pour toute information complémentaire, nous vous invitons à consulter le site internet de référence pour toutes les questions ayant trait au respect de la vie privée et à la protection des données, dans un cadre professionnel. Il s'agit du site de l'Autorité de protection des données, organe de contrôle indépendant chargé de veiller au respect des principes fondamentaux de la protection des données à caractère personnel. Cet organe remplace la Commission pour la protection de la vie privée: **www.autoriteprotectiondonnees.be.**

Il est également possible de leur adresser une question en particulier, sur un cas précis qui se poserait dans le cadre de votre travail:
www.autoriteprotectiondonnees.be/citoyen/agir/demander-une-information.

Enfin, vous pouvez également consulter le site internet de la CSC, où vous trouverez des réponses aux questions les plus fréquemment posées:
www.lacsc.be/vie-privee/

Table des matières

I. Législation règlementant la protection des données 6

1. La protection de la vie privée sous l'angle des données personnelles 7
2. Qu'entend-on par «donnée personnelle»? 7
3. RGPD: principes généraux 8
4. Les droits des personnes concernées 10
5. Obligations pour les responsables de traitement 11
6. Traitement de données sensibles 13

II. Protection de la vie privée au travail 14

1. Conditions au traitement des données des travailleurs et obligations des employeurs 15
   - 1.1 Traitement des données des travailleurs 15
   - 1.2 Traitement de données relatives à la santé 17
   - 1.3 Obligations pour les employeurs 17
   - 1.4 Comment faire valoir mes droits? 18
2. Contrôle et surveillance des travailleurs: principes de base 20
   - 2.1 Surveillance par caméra au travail: CCT n°68 21
   - 2.2 Contrôle des communications électroniques en réseau: CCT n°81 22
   - 2.3 Le contrôle des travailleurs en cas de suspicion de vol: CCT n°89 24
   - 2.4 La géolocalisation 25
   - 2.5 Le recrutement et la sélection de travailleurs: CCT n°38 27

III. Protection des données et travail syndical 28

1. Données personnelles et affiliation 29
2. Utilisation des données personnelles par les représentants syndicaux 29
3. Impact du RGPD sur la concertation sociale 30
4. Contrôle du respect du RGPD par l'employeur 33

I. Législation règlementant la protection des données

1. La protection de la vie privée sous l'angle des données personnelles

En Belgique, il existe déjà une règlementation autour de la protection de la vie privée depuis 1992. Suite à plusieurs évolutions, on parle désormais de données personnelles lorsqu'il s'agit de la question de la vie privée. Il s'agit maintenant d'une réalité plus palpable, ce qui permet de légiférer plus concrètement autour des informations spécifiques que sont les données personnelles.

La législation de base règlementant la protection des données est désormais surtout européenne. C'est le «**RGPD**», le *Règlement Général sur la Protection des Données* (en anglais, GDPR pour *General Data Protection Regulation*), entré en vigueur en 2018, qui s'applique à tous les citoyens des États membres de l'Union européenne et à toutes les organisations, publiques et privées, établies sur le territoire de l'Union européenne qui traitent des données personnelles.

La loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel a mis la législation belge de la protection des données en conformité avec le RGPD et a mis en œuvre certaines clauses ouvertes contenues dans le RGPD.

2. Qu'entend-on par «donnée personnelle»? (art. 4.1 RGPD)

Une donnée personnelle, c'est toute information qui se rapporte à une personne physique qui peut être identifiée, directement ou indirectement.

Voici quelques exemples de données personnelles: nom, prénom, date de naissance, adresse, numéro de registre national, données de localisation (coordonnées GPS), identifiant en ligne, éléments spécifiques propres à son identité physique, physiologique (taille, poids, etc.), économique ou sociale (salaire, le fait d'être marié, d'avoir des enfants, etc.).

On distingue deux catégories de données: les données dites **ordinaires**, et les données **sensibles** (dites *catégories particulières de données à caractère personnel*, art. 9 RGPD). Nous y reviendrons plus loin.

3. RGPD: principes généraux (art. 5-6 RGPD)

Le RGPD protège les données personnelles de tous les citoyens européens, en limitant les conditions selon lesquelles ces données peuvent être traitées.

On entend par «traitement» toute opération ou ensemble d'opérations (automatisées ou non) appliquées à des données ou des ensembles de données à caractère personnel. L'organisation ou personne qui effectue ce traitement va être le ou la Responsable de traitement.

Les gouvernements, les syndicats et les entreprises[1] vont ainsi être considérés comme des «responsables de traitement», c'est-à-dire des organisations qui sont amenées à traiter des données personnelles.

Exemples d'opérations de traitement: la collecte, l'enregistrement, la conservation, la modification, l'extraction, la consultation, l'utilisation, la transmission, la diffusion ou toute autre forme de mise à disposition, l'effacement ou la destruction d'une donnée personnelle.

Six principes de base doivent être respectés pour que des données personnelles puissent être traitées:

1. En premier lieu, le **traitement doit être licite**, loyal et transparent. Pour qu'un traitement soit licite (= autorisé), il faut que celui-ci se justifie par l'une de ces six raisons (au moins):
   - **La personne concernée a donné son consentement:** la personne doit donner son accord de manière explicite et claire pour que des données à caractère personnel la concernant fassent l'objet d'un traitement, pour une ou plusieurs finalités spécifiques. Dans les articles 4 et 7 du RGPD, il est précisé que le consentement doit être à la fois libre, spécifique, éclairé et univoque. Cela signifie que le consentement ne peut pas par exemple être lié à la conclusion d'un contrat (libre), qu'il doit être demandé pour une ou plusieurs finalités spécifiques, que les personnes auront dû être informées suffisamment (éclairé), et que le consentement doit résulter d'un acte positif clair[2] (univoque). Ce consentement peut être retiré à tout moment.

[1] *Dans cette brochure, nous utilisons le terme «entreprise(s)» pour désigner les sociétés, les institutions (de santé), les organisations...*

[2] *Si quelqu'un ne répond pas à un e-mail qui demande le consentement de la personne, on ne peut donc pas considérer qu'il a donné son consentement, par exemple.*

À noter que dans le cadre d'une relation de travail, la question du consentement est problématique étant donné que les travailleurs se trouvent dans une relation de subordination vis-à-vis de leur employeur. Nous y reviendrons plus loin.

Les autres bases légales présentées ci-dessous permettent de traiter les données personnelles d'une personne sans son consentement.

- **Le traitement est nécessaire à l'exécution d'un contrat:** par exemple le contrat de travail, qui suppose notamment de recueillir des données pour payer un salaire.
- **Le traitement est nécessaire au respect d'une obligation légale** (exemple: quand une entreprise est responsable de traitement, elle est soumise à certaines obligations en matière de bien-être au travail qui supposent le traitement de données personnelles).
- **Le traitement est nécessaire à la protection des intérêts vitaux de la personne concernée** (exemple: contexte médical où la vie de la personne est en jeu).
- **Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique** (exemple: une commune a besoin de récolter des données afin de délivrer une carte de riverain pour le stationnement).
- **Le traitement est nécessaire à la défense d'un intérêt légitime du responsable de traitement,** à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée (exemple: traitement qui vise à assurer la sécurité informatique, ou une prévention de la fraude).

2. Le **traitement doit être réalisé dans un but précis**, dans une finalité déterminée. Les données en question ne pourront en principe pas être utilisées pour une autre finalité que celle qui avait été invoquée au départ. Ces données ne pourront être utilisées pour une autre finalité qu'après avoir vérifié que la nouvelle finalité est compatible avec la finalité initiale.
3. Le **traitement des données doit être minimisé**: cela signifie qu'on utilise uniquement les données dont on a vraiment besoin pour atteindre le but recherché, la finalité recherchée.
4. Les **données traitées doivent être exactes** et, si nécessaire, tenues à jour. Si des données personnelles se révèlent inexactes, elles doivent être effacées ou rectifiées.

5. La **conservation des données doit être limitée.** Celle-ci dépendra de la finalité et de la période (plus ou moins longue) durant laquelle on aura besoin de ces données.
6. Enfin, les **mesures techniques ou organisationnelles appropriées devront être prises** afin de garantir la sécurité des données personnelles.

4. Les droits des personnes concernées (art. 12-22 RGPD)

Le RGPD confère une série de droits aux citoyens par rapport à leurs données:

1. **La transparence:** le responsable de traitement doit informer la personne concernée d'une façon concise, transparente et compréhensible en ce qui concerne le traitement de ses données. Les informations qui doivent être données concernent:
   - les finalités du traitement;
   - la base juridique du traitement;
   - les catégories de destinataires des données;
   - l'identité et les coordonnées du responsable du traitement;
   - l'existence de certains droits pour la personne concernée (voir points 2 à 8).
2. **Le droit d'accès:** les personnes concernées ont le droit de savoir quelles sont les données personnelles qui sont traitées, quelles sont les finalités du traitement, quels sont les destinataires auxquels les données seront communiquées, et quelle est la durée de conservation. La personne concernée a le droit d'obtenir gratuitement une copie de ses données à caractère personnel traitées.
3. **Le droit de rectification:** la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, ou rectifiées si elles sont inexactes.
4. **Le droit à l'effacement** («droit à l'oubli»): la personne concernée a le droit d'obtenir du responsable du traitement l'effacement de données à caractère personnel la concernant sous certaines conditions, par exemple si les données ne sont plus nécessaires, si la personne retire son consentement, s'oppose au traitement, ou si les données ont fait l'objet d'un traitement illicite (voir art. 17 RGPD).

5. **Le droit à la limitation du traitement:** sur demande, une organisation doit arrêter de traiter les données personnelles d'un individu, par exemple si la personne conteste l'exactitude des données à caractère personnel ou si le traitement est illicite (voir art. 18 RGPD).

   Le responsable du traitement notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification ou tout effacement de données à caractère personnel ou toute limitation du traitement.
6. **Le droit à la portabilité des données:** il est possible de récupérer une partie de vos données dans un format lisible par une machine, afin de pouvoir les utiliser à vos propres fins.
7. **Le droit d'opposition:** la personne concernée peut s'opposer à un traitement lorsque ce dernier est fondé sur les intérêts légitimes (du responsable) ou nécessaire à l'exécution d'une mission d'intérêt public. Sauf en cas de marketing direct, elle devra mettre en avant «des raisons tenant à sa situation particulière». Néanmoins, le responsable pourra continuer à réaliser le traitement s'il démontre qu'il existe des motifs légitimes et impérieux qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.
8. La personne concernée a le **droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques** ou «affectant de manière significative» les personnes (sauf exceptions, voir art. 22 RGPD).

   Une décision automatisée est une décision qui a été prise par un algorithme, sans intervention humaine. Par exemple, l'octroi ou le refus d'un crédit peut se fonder exclusivement sur la décision d'un algorithme qui applique automatiquement certains critères à la situation financière du demandeur, sans aucune intervention humaine.

5. Obligations pour les responsables de traitement (art. 24-37 RGPD)

Les personnes ou les organisations qui traitent des données (= les responsables de traitement) doivent respecter une série d'obligations:

- Mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD.

- Lorsqu'il est fait appel à des sous-traitants, collaborer uniquement avec ceux qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Le traitement de données par un sous-traitant est obligatoirement régi par un contrat ou un acte juridique devant notamment reprendre certains éléments prévus à l'art. 28 du RGPD.
- Faciliter l'exercice des droits conférés à la personne concernée.
- Tenir un registre de toutes les activités de traitement comprenant le nom et les coordonnées du/des responsable(s) de traitement, les finalités du traitement, une description des catégories de personnes concernées et des catégories de données personnelles, les catégories de destinataires auxquels les données ont été ou seront communiquées, les délais prévus pour l'effacement des différentes catégories de données, et une description générale des mesures de sécurité.
- Coopérer avec l'autorité de contrôle dans l'exécution de ses missions.
- Mettre en œuvre des procédures de sécurisation efficaces. Cela suppose de prendre des mesures au niveau informatique notamment pour éviter les fuites, d'anonymiser ou de chiffrer des données, ou aussi par précaution de limiter les personnes qui ont accès à ces données personnelles.
- Informer l'Autorité de protection des données en cas d'une violation des données susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Cette information doit se faire dans les meilleurs délais et, si possible, dans les 72 heures après en avoir pris connaissance. De plus, si cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement doit la communiquer à la personne concernée dans les meilleurs délais.
- Réaliser une analyse d'impact dès lors que le traitement des données présente un risque élevé pour les droits et libertés des personnes.
- Désigner un délégué à la protection des données (DPO) lorsque certaines conditions sont remplies (voir art. 37 RGPD).

6. Traitement de données sensibles (art. 9 RGPD)

Le RGPD mentionne une catégorie spécifique de données: les **données sensibles.** Selon le RGPD, il s'agit des **données à caractère personnel qui révèlent l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, biométriques, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle.**

Le traitement de ces données est en principe interdit, mais des exceptions sont prévues. Ainsi, le traitement de ces données sera permis si la personne a donné son consentement (explicite), ou, en l'absence de son consentement, si ce traitement est par exemple nécessaire pour respecter une obligation légale (que ce soit une loi ou une convention collective, en matière de droit du travail notamment), ou s'il est nécessaire aux fins de la médecine du travail par exemple.

II. Protection des données et de la vie privée au travail

1. Conditions au traitement des données des travailleurs et obligations des employeurs

Le RGPD s'ajoute aux dispositions en vigueur régissant la relation de travail et renforce les obligations de l'employeur. Bien que le RGPD vise à harmoniser la réglementation en matière de protection des données au sein de l'UE, il prévoit une exception pour le domaine des relations de travail. Il est ainsi possible de prévoir des règles spécifiques relatives au traitement des données à caractère personnel des travailleurs, tant au niveau sectoriel qu'au niveau de l'entreprise, par le biais de conventions collectives de travail par exemple (art. 88 RGPD).

1.1 Traitement des données des travailleurs

Au travail, des données personnelles de tous les travailleurs sont traitées à plusieurs moments. La plupart du temps, ce sera à l'une de ces trois conditions:

1. Les **travailleurs ont donné leur consentement** (individuellement). Attardons-nous sur la particularité de cette base légale dans le cadre de la relation de travail. Étant dans un lien de subordination, il a été considéré que le travailleur peut difficilement donner librement son consentement. Or, c'est une condition pour considérer que le consentement est valable. Il est donc très hasardeux pour un employeur de justifier un traitement spécifique de données personnelles de ses travailleurs sur la seule base de leur consentement. Il conviendra pour l'employeur de pouvoir se reposer sur une autre base légale.
2. Le **traitement est nécessaire à l'exécution d'un contrat** (le contrat de travail).
3. Le **traitement est nécessaire au respect d'une obligation légale.** C'est le cas lorsqu'une loi, un décret, ou une convention collective de travail (CCT) oblige à ce que pour la respecter, on doive traiter des données personnelles.

Dans une entreprise, une donnée personnelle va être soit une donnée nominative, c'est-à-dire une information qui n'est pas anonyme mais qui se rapporte directement à un travailleur; soit une donnée non-nominative sur base de laquelle on pourrait identifier indirectement un travailleur.

Bases légales possibles pour traiter les données personnelles des travailleurs sans leur consentement

- Exécution d'un contrat (de travail)

  Exemple: données nécessaires au paiement du salaire, prestations, situation de handicap…

  - composition du ménage, numéro de compte, adresse…
- Respect d'une obligation légale

  Exemple: traitement de données destinées à un organisme de sécurité sociale lors de l'embauche (déclaration Dimona).
- Poursuite de l'intérêt légitime de l'employeur, à savoir bien souvent le bon fonctionnement de l'entreprise

  Exemple: traitement de données personnelles dans le but de sécuriser les accès aux bâtiments.

Si l'une de ces bases juridiques est respectée, on n'a donc pas besoin du consentement des travailleurs, mais on doit toujours respecter ce devoir de transparence. L'employeur doit informer les travailleurs au sujet du type de données qui seront récoltées.

Pour traiter des données dans d'autres cas, le consentement des travailleurs sera nécessaire.

Exemple: la diffusion de photos de travailleurs sur l'intranet ou le site internet de l'entreprise. On ne peut pas invoquer l'exécution du contrat, une obligation légale ou le bon fonctionnement de l'entreprise. Le consentement de chaque personne est donc nécessaire.

Un exemple de traitement interdit: l'affiliation syndicale

L'appartenance à un syndicat est une donnée sensible, cela veut dire qu'un employeur n'a en aucun cas le droit de vous demander si vous êtes affilié à un syndicat. C'est contraire au RGPD.

Aucune loi ne prévoit qu'un employeur puisse demander si on est membre d'un syndicat, il n'y a aucune raison, et aucun intérêt, à lui répondre.

1.2 Traitement de données relatives à la santé

Le RGPD interdit en principe le traitement de données relatives à la santé, qui sont dites «sensibles». **Un employeur n'a donc pas accès aux données médicales.** Et ce, ni lors du recrutement, ni dans le cadre de la relation de travail.

Un employeur ne peut pas interroger un candidat travailleur sur son état de santé. En effet, la discrimination sur la base de l'état de santé actuel ou futur est interdite. Le futur travailleur n'est dès lors pas obligé de répondre à des questions relatives à son état de santé. Si c'est à l'employeur qu'il incombe l'obligation de prendre toutes les mesures nécessaires à la santé et au bien-être de ses travailleurs sur le lieu de travail, c'est toutefois au médecin du travail qu'il appartient de soumettre les (futurs) travailleurs à un examen de santé et de décider s'ils sont (toujours) aptes à l'exercice de leur profession. Mais le médecin doit se limiter à informer l'employeur si un travailleur est ou non apte au travail, sans jamais lui communiquer d'informations relatives à une éventuelle maladie ou affection.

Lorsqu'un travailleur est malade, l'employeur doit être informé de l'absence pour raison médicale mais il n'a pas à en connaitre la raison exacte, il n'a pas accès aux informations du médecin traitant ou du médecin conseil. La remise d'un certificat médical pour une absence de plus d'une journée est obligatoire si le règlement de travail de l'entreprise ou une CCT le prévoit. Dans les autres cas, l'employeur doit chaque fois en faire la demande. L'article 31 de la loi de 1978 sur les contrats de travail reprend les différentes mentions qui doivent figurer sur un certificat médical, notamment la durée de l'incapacité de travail. Par contre, le diagnostic n'est jamais mentionné vu qu'il s'agit d'une donnée couverte par le secret médical. La partie du certificat médical qui est réservée au service de contrôle mentionne le diagnostic, et cela est conforme au RGPD qui prévoit une exception à l'interdiction de traiter ce type de données en raison d'une obligation légale en matière de droit du travail (pour plus d'infos, voir titre 4 du livre I^{er} du code du bien-être au travail).

1.3 Obligations pour les employeurs

Le RGPD oblige l'employeur, en tant que responsable de traitement, à communiquer au travailleur les informations suivantes:

- la durée pendant laquelle les données personnelles seront conservées ou, lorsque ce n'est pas possible, les critères utilisés pour

déterminer cette durée (en principe, le délai de conservation des documents sociaux est de 5 ans à dater de la fin du contrat de travail);

- lorsque le traitement est fondé sur le consentement du travailleur, le droit de retirer ledit consentement à tout moment;
- le droit d'introduire une plainte auprès de l'Autorité de protection des données.

La communication de ces informations n'est soumise à aucune exigence de formalisme spécifique mais Il est préférable que cette information soit inscrite dans le règlement de travail afin que cela soit établi de manière paritaire, avec la contribution des représentants syndicaux dans les organes de concertation sociale.

En tant que responsable de traitement, **l'employeur doit** en outre **tenir un registre comportant les données traitées.** En vertu du RGPD, toutes les entreprises occupant plus de 250 travailleurs sont obligées de tenir un tel registre. Pour les plus petites entreprises, cette obligation est valable si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées, n'est pas occasionnel ou porte sur des données sensibles. En pratique, ce sera donc le cas dans quasiment toutes les entreprises. D'ailleurs, selon l'Autorité de protection des données, la gestion du personnel constitue un traitement non occasionnel. L'APD recommande à toutes les entreprises de tenir un registre de données, et ce même si cette obligation ne leur est pas applicable.

L'employeur devra **notifier toute violation des données personnelles à l'APD et au(x) travailleur(s) concerné(s)** et il devra permettre de rectifier ou d'effacer des données.

Enfin, l'employeur a l'obligation de **minimiser les données traitées**, c'est-à-dire qu'il ne peut traiter que les données *«adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées».*

Le non-respect de ces obligations peut couter jusqu'à 20.000.000 euros ou 4% du chiffre d'affaires mondial annuel de l'entreprise.

1.4 Comment faire valoir mes droits? (art. 12 RGPD)

Tous les droits que le RGPD donne aux citoyens européens doivent valoir aussi pour les travailleurs (droit à l'information, droit à l'accès, droit à l'oubli, à la rectification...). Comme détaillé précédemment, c'est le responsable du traitement, à savoir dans ce cas, l'employeur, qui doit faciliter l'exercice de ces droits par les travailleurs vis-à-vis de leurs données personnelles.

Suite à une **demande d'un travailleur fondée sur l'exercice d'un de ces droits, le responsable de traitement devra informer la personne concernée de la suite donnée à sa demande** «sans retard excessif et, en tout état de cause, dans un délai d'un mois à compter de la réception de la demande». Ce délai pourra être prolongé de deux mois s'il s'agit d'une demande complexe ou si plusieurs demandes ont été effectuées. La demande pourra être soit acceptée, soit refusée.

Si le responsable du traitement ne donne pas suite à la demande, il doit en informer la personne concernée sans tarder et au plus tard dans un délai d'un mois, en indiquant les raisons de ce refus. Le responsable de traitement doit de plus informer la personne de la possibilité d'introduire une réclamation auprès de l'Autorité de protection des données et d'introduire un recours en justice.

Si vous constatez que votre employeur traite des données personnelles vous concernant d'une manière qui ne vous semble pas correcte, la première voie serait donc de vous adresser à l'employeur, selon la procédure décrite ci-dessus. Si cela ne mène à rien, il est également possible de s'adresser à l'Autorité de protection des données (APD) ou de faire un recours en justice.

Mais qu'en est-il du rôle du syndicat dans ce cadre?

Selon la loi belge qui transpose le RGPD, une organisation syndicale ne peut pas représenter un travailleur vis-à-vis de l'APD. Il n'est donc pas possible de se faire représenter officiellement par la CSC auprès de cette autorité de contrôle. Mais si un problème se pose au niveau des données traitées par l'employeur, il s'agit d'un litige entre le travailleur et l'employeur. Et en cas de litige individuel, tout travailleur a le droit d'être assisté par son délégué syndical, qui interviendra vis-à-vis de l'employeur afin de défendre ses droits. Dans l'esprit de la loi, la délégation syndicale est donc l'interlocuteur vis-à-vis de l'employeur, mais pas vis-à-vis de l'APD, même s'il s'agit d'une problématique liée au traitement de données personnelles.

Par ailleurs, selon l'art. 12 de la CCT n°5, la délégation syndicale a le droit d'être reçue par le chef d'entreprise à l'occasion de tout litige ou différend de caractère collectif survenant dans l'entreprise. Si une politique de traitement des données s'avère problématique, le différend est collectif, et la DS est donc

compétente. Ce serait par exemple le cas si tous les travailleurs d'une entreprise se trouvent dans l'obligation de signer un document autorisant l'employeur à récolter des données personnelles qu'il n'a pas le droit de traiter.

En résumé, ce n'est pas parce qu'il s'agit d'une matière spécifique, à savoir la protection des données, que le droit du travail est forcément impacté. Les délégations syndicales gardent leurs compétences: si les droits d'un travailleur sont menacés, la DS est compétente.

2. Contrôle et surveillance des travailleurs: principes de base

Nous nous concentrons ici sur le contrôle des travailleurs et l'ingérence qui peut s'exercer vis-à-vis de leur vie privée. Plusieurs conventions collectives de travail traitent de cas précis de surveillance des travailleurs.

Le RGPD reprend trois principes dont l'employeur doit tenir compte quand il exerce une surveillance sur le lieu de travail, et quand il traite les données personnelles des travailleurs, afin de minimiser l'ingérence dans la vie privée des travailleurs:

- **La finalité:** la finalité poursuivie par l'exercice du contrôle doit être légitime. Ces finalités légitimes peuvent être déterminées dans une loi ou dans une des CCT traitant d'un aspect particulier de la surveillance des travailleurs.
- **La proportionnalité:** le contrôle doit être limité et proportionnel par rapport à l'objectif visé. Les données traitées doivent se limiter à ce qui est nécessaire pour atteindre la finalité de la surveillance. Concrètement, quand on collecte des données, celles-ci doivent rester le plus globales possible et être éventuellement anonymisées. L'individualisation des données, permettant l'identification d'un travailleur en particulier, ne sera en principe pas permise.
- **La transparence:** les travailleurs doivent être informés que leurs données font l'objet d'un traitement et à quelles fins. Cette information doit intervenir au moment où les données sont collectées, c'est à dire au moment de la conclusion du contrat de travail.

Suite à l'entrée en vigueur du RGPD, les dispositions prévues dans le Règlement s'ajoutent à celles déjà prévues dans les CCT règlementant la surveillance des travailleurs. Nous les passons en revue ci-dessous.

2.1 Surveillance par caméra au travail: CCT n°68

La CCT n°68 traite de la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail dans le secteur privé. Les conditions d'admissibilité et d'installation de la surveillance par caméras sur le lieu de travail y sont décrites, et découlent des trois principes évoqués ci-dessus.

La surveillance par caméras sur le lieu de travail n'est autorisée que lorsque l'une des finalités suivantes est poursuivie:

- la sécurité et la santé;
- la protection des biens de l'entreprise;
- le contrôle du processus de production (qui peut porter tant sur les machines que sur les travailleurs).

Pour les deux premières finalités, la surveillance peut être mise en place de manière permanente. Pour la troisième, si elle porte sur les machines, elle peut être autorisée de manière permanente, mais si elle porte sur les travailleurs, elle ne peut être que temporaire.

Cela signifie que la surveillance par caméras permanente du travailleur n'est pas autorisée et que la surveillance par caméras permanente des machines n'est autorisée que dans la mesure où le but n'est pas de viser le travailleur.

L'employeur doit définir clairement et de manière explicite la finalité de la surveillance par caméras.

Préalablement et lors de la mise en œuvre de la surveillance par caméras, l'employeur doit informer le conseil d'entreprise sur tous les aspects de la surveillance par caméras. À défaut de CE, cette information est fournie au Comité pour la prévention et la protection au travail (CPPT) ou, à défaut d'un tel comité, à la DS ou, à défaut, aux travailleurs.

L'information à fournir porte au moins sur les aspects suivants de la surveillance par caméras:

- la finalité poursuivie;
- le fait que des images soient ou non conservées;

- leur nombre et emplacement(s);
- la ou les périodes de fonctionnement concernées.

Le CE ou, à défaut, le CPPT doit en outre évaluer régulièrement les systèmes de surveillance utilisés et faire des propositions en vue de les revoir en fonction des développements technologiques.

2.2 Contrôle des communications électroniques en réseau: CCT n°81

Dans le secteur privé, en vertu de la loi sur les contrats de travail reconnaissant l'autorité de **l'employeur**, celui-ci **peut contrôler l'usage fait par les travailleurs des moyens de communication à leur disposition**, prendre connaissance de leurs données de communication, et traiter ces données à caractère personnel.

Les conditions de ces traitements sont définies dans la CCT n°81, qui n'autorise le contrôle global des données de communication électroniques en réseau que si les trois principes du RGPD susnommés sont respectés. Pratiquement, cela signifie que **le contrôle doit avoir un but spécifique**, que **l'employeur ne peut pas vérifier systématiquement tout, et que le travailleur doit savoir que l'employeur peut effectuer des contrôles.** Cela n'implique pas que le travailleur doit donner son consentement, mais seulement qu'il doit être informé à l'avance qu'un contrôle est possible.

Le contrôle de données de communication électroniques en réseau n'est autorisé que lorsque l'une ou plusieurs des finalités suivantes est ou sont poursuivies (cela doit être défini explicitement):

- la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui;
- la protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels sont attachés un caractère de confidentialité ainsi que la lutte contre les pratiques contraires;
- la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts afférents, ainsi que la protection physique des installations de l'entreprise;
- le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.

Avant d'installer un système de contrôle, **l'employeur est tenu d'informer le CE, ou, à défaut, le CPPT, ou à défaut, la DS, ou à défaut, les**

travailleurs de tous les aspects de ce contrôle. Ces informations doivent porter sur la politique de contrôle et les prérogatives de l'employeur, la ou les finalités poursuivies, dire si oui ou non les données sont conservées (et si oui où et combien de temps), et préciser si le contrôle est permanent ou non.

Lors de l'installation du système de contrôle, **l'employeur doit aussi informer les travailleurs individuels de tous les aspects du contrôle.** Ces informations doivent se rapporter aux informations collectives, présentées ci-dessus, ainsi qu'aux aspects suivants:

- l'utilisation des outils mis à la disposition du travailleur pour l'exécution de son travail, y compris les restrictions relatives à l'utilisation dans le cadre de la fonction;
- les droits, devoirs et obligations des travailleurs ainsi que les interdictions éventuelles en ce qui concerne l'utilisation des moyens de communication électroniques en réseau de l'entreprise;
- les sanctions prévues dans le règlement de travail en cas de non-respect des règles.

L'employeur peut choisir comment informer les travailleurs: par un affichage, dans le règlement de travail ou le contrat de travail, ou via des instructions lors de l'utilisation (messages à l'allumage du poste de travail et/ou lors de l'activation de certains programmes).

Ces informations ne doivent pas obligatoirement être reprises dans le règlement de travail, mais il est conseillé de reprendre dans celui-ci des règles claires relatives au contrôle électronique sur le lieu de travail, en respectant la concertation sociale.

Dans un premier temps, il est permis de collecter des données globales, mais l'identification des travailleurs n'est pas autorisée.

Concrètement, une recommandation de L'Autorité de protection des données (anciennement Commission de la Protection de la Vie Privée) nous dit qu'en ce qui concerne internet, l'employeur peut collecter des données concernant la durée de la connexion par poste de travail, mais ne peut pas individualiser les sites visités. Et en ce qui concerne la messagerie électronique, l'employeur peut collecter des données concernant le nombre de messages envoyés par poste de travail ainsi que leur volume, mais ne peut pas identifier le travailleur qui les a envoyés.

Dans un premier temps, sur la base des informations se trouvant sur le serveur, des listes de données globales peuvent être constituées, qui ne permettent pas d'identifier un travailleur individuellement. Si, sur la base de ces listes générales, des anomalies sont soupçonnées, on communique au travailleur l'existence d'une éventuelle irrégularité et on l'avertit d'une probable individualisation des données de communication électroniques si une nouvelle irrégularité de même nature est constatée dans le futur. Ce n'est qu'alors que l'on peut procéder à l'identification du ou des travailleurs individuels sur la base des autres données collectées et qui se trouvent sur le serveur. Lorsqu'un travailleur individuel est tenu pour responsable d'une (nouvelle) irrégularité, il doit être invité à un entretien pour lui permettre de s'expliquer sur l'utilisation des moyens de communication électroniques.

2.3 Le contrôle des travailleurs en cas de suspicion de vol: CCT n°89

Pour prévenir les vols dans son entreprise, **l'employeur peut organiser des fouilles, mais uniquement à la sortie de l'entreprise.** Selon la CCT n°89, de tels contrôles ne sont autorisés que s'ils visent à prévenir ou à constater le vol de biens dans l'entreprise ou sur le lieu de travail. Ils ne peuvent en tous cas pas avoir pour but de mesurer les prestations des travailleurs.

Les contrôles de sortie systématiques ne sont possibles que s'ils ont lieu par le biais de systèmes de détection électroniques et/ou techniques. Les contrôles de sortie effectués par des personnes peuvent exclusivement être effectués par des agents de gardiennage, et pas par l'employeur.

Ces contrôles peuvent uniquement être effectués:

- par voie d'échantillonnage en vue de prévenir les vols et, dans ce cas, la possibilité de contrôle doit exister pour tous les travailleurs concernés sans distinction;
- s'il existe des motifs valables de croire que le travailleur a volé des biens, sur la base du comportement de l'intéressé, d'indices matériels ou des circonstances.

Préalablement et lors de la mise en œuvre d'un système de contrôles de sortie, **l'employeur doit informer le CE sur le système employé.** À défaut de CE, cette information est fournie au CPPT ou, à défaut, à la délégation syndicale ou, à défaut, aux travailleurs.

Cette information porte sur:

- le périmètre de l'entreprise ou du lieu de travail;
- les risques de vol dans l'entreprise ou sur le lieu de travail;
- les mesures afin de prévenir ces risques ou d'y remédier; et
- les méthodes de contrôle.

2.4 La géolocalisation

Il n'existe à ce jour **aucune législation réglant une problématique de plus en plus fréquemment rencontrée dans les entreprises: la «géolocalisation».** L'Autorité de protection des données a toutefois émis un avis à ce sujet (Avis n°12/2005 du 7 septembre 2005). L'Autorité y a déclaré que la surveillance de travailleurs par l'utilisation d'un système de monitoring associé au système de navigation GPS sur les véhicules de service est uniquement autorisée moyennant le respect des principes de finalité, de proportionnalité, et de transparence.

Avant d'installer un système de géolocalisation sur leur flotte de véhicules, les entreprises devraient établir une «geopolicy», reprenant les principes et modalités d'un tel contrôle. Ces règles devront être prises en concertation avec les représentants des travailleurs au sein des organes de concertation de l'entreprise. La politique de géolocalisation devra notamment préciser les finalités du contrôle et la fréquence du contrôle de manière précise et explicite et être annexée au règlement du travail.

Un tel système doit notamment avoir une «finalité légitime» pour être acceptable, à savoir:

- renforcer la sécurité des employés durant les déplacements professionnels;
- la protection des véhicules de l'entreprise et des marchandises transportées;
- optimiser les temps de transport.

Le contrôle des prestations des travailleurs peut aussi être considéré comme une finalité légitime, mais ce ne peut être l'unique objet de la mise en place de la géolocalisation automobile. Un contrôle permanent, avec lecture systématique des données enregistrées par le système de localisation, doit en principe être considéré comme disproportionné. Enfin, il est interdit de récolter ces informations en dehors des heures de travail, lorsque l'employé utilise un véhicule professionnel à des fins privées après son service (pour rentrer à son domicile, par exemple). Ce faisant, le travailleur doit avoir la possibilité de désactiver le suivi lorsqu'il ne travaille pas.

Selon le RGPD, le traitement de données personnelles ne peut, en principe, être effectué que moyennant le consentement de la personne concernée, ou lorsque ce traitement est nécessaire à l'exécution du contrat dont la personne est signataire. Cependant, il existe une troisième exception à l'interdiction de traitement: l'intérêt légitime de l'entreprise.

L'employeur est tenu de communiquer préalablement les informations suivantes:

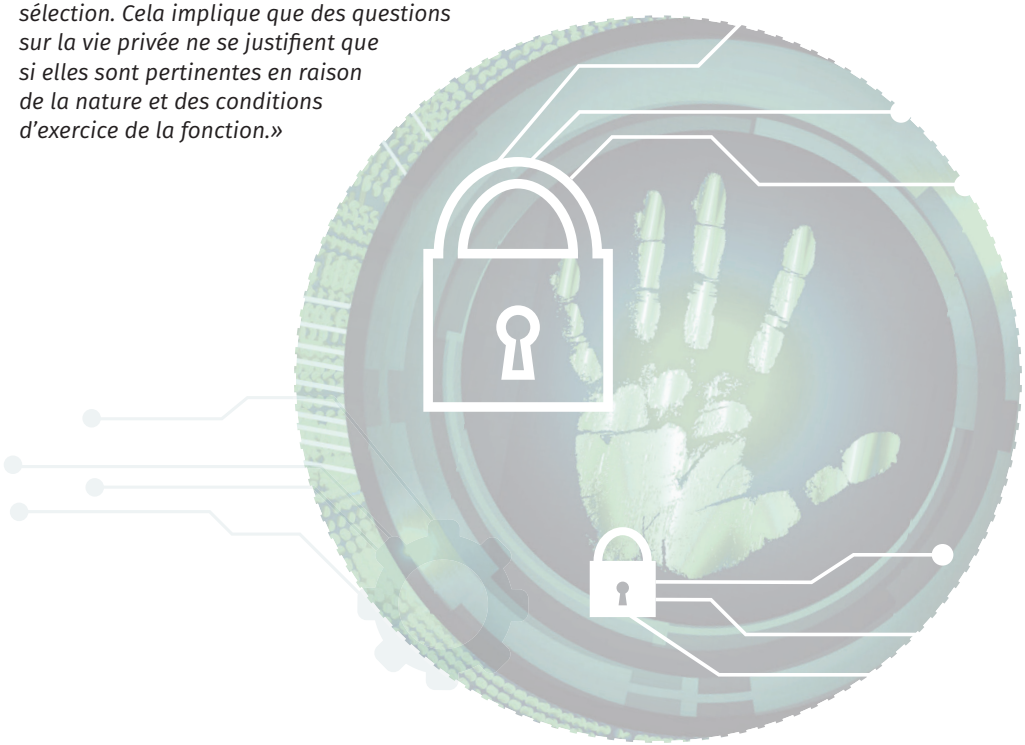
- la base légale pour le traitement des données (la plupart du temps ce sera l'intérêt légitime de l'entreprise);
- qui fait l'objet du contrôle;
- les objectifs poursuivis par le système de géolocalisation;
- la nature des abus qui peuvent mener à un contrôle;
- la durée du contrôle;
- les données traitées;
- si les données sont envoyées en dehors de l'Union européenne;
- quels sont les droits du travailleur, notamment le droit de consulter les données, le droit d'introduire une réclamation auprès de l'Autorité de protection des données, le droit de limiter le traitement des données... ;
- la procédure qui sera suivie après le contrôle.

Selon l'APD, certaines utilisations de systèmes de géolocalisation devraient en tous cas être interdites, par exemple si ce contrôle a pour but de contrôler le respect des limitations de vitesse ou de contrôler un travailleur en permanence. En particulier, il ne peut pas être utilisé:

- Dans le véhicule d'un employé qui disposerait d'une liberté dans l'organisation de ses déplacements.
- Pour suivre les déplacements des représentants du personnel dans le cadre de leur mandat.
- Pour collecter la localisation en dehors du temps de travail (trajet domicile-lieu de travail, temps de pause, etc.), y compris pour lutter contre le vol ou vérifier le respect des conditions d'utilisation du véhicule.
- Pour calculer le temps de travail des employés alors qu'un autre dispositif existe déjà.

2.5 Le recrutement et la sélection de travailleurs: CCT n°38

Enfin, mentionnons la convention collective de travail n°38 dont l'article 11 traite du respect de la vie privée des candidats à un poste ouvert dans une entreprise. On peut ainsi y lire que *«la vie privée des candidats doit être respectée lors de la procédure de sélection. Cela implique que des questions sur la vie privée ne se justifient que si elles sont pertinentes en raison de la nature et des conditions d'exercice de la fonction.»*



III. Protection des données et de la vie privée, et travail syndical

1. Données personnelles et affiliation syndicale

L'affiliation syndicale est une catégorie particulière de données personnelles: c'est une donnée sensible. Le traitement de ce type de donnée est donc interdit, sauf s'il est effectué par «*tout organisme à but non lucratif et poursuivant une finalité (...) syndicale dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, à condition que le traitement se rapporte exclusivement aux membres (ou anciens) membres de l'organisme (...) et que les données ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées*» (art. 9 RGPD). En aucun cas l'entreprise et/ou l'employeur ne peuvent s'enquérir de l'affiliation syndicale.

La CSC est responsable de traitement des données personnelles de ses affiliés, et à ce titre, doit donc respecter toutes les obligations qui incombent à un responsable de traitement (voir ci-dessus), ainsi que les principes de légalité, légitimité, proportionnalité et de transparence. Tout cela est précisé sur notre site web et dans notre folder «*Comment la CSC traite vos données personnelles*».

2. Utilisation des données personnelles par les représentants syndicaux dans les entreprises

La CSC est donc la responsable de traitement des données de ses affiliés. Mais en tant que représentant syndical, vous êtes sans doute régulièrement confronté à des situations où des données personnelles sont en jeu, ne fut-ce que pour communiquer avec vos collègues concernant une actualité dans votre entreprise. Quelles seraient les règles à suivre?

Communications aux affiliés

L'envoi d'informations syndicales ou de propagande à nos affiliés ne pose pas de problème car il repose sur l'intérêt légitime de la CSC.

Sauf indication contraire, vous pouvez leur envoyer des e-mails concernant des messages syndicaux. Attention, un affilié peut indiquer qu'il ne souhaite plus recevoir d'e-mails de notre part.

Il pourrait donc être intéressant de constituer des listes de destinataires qui acceptent ou non de recevoir des communications de notre part.

Conseil: il est important de penser à utiliser l'option CCI lorsque vous envoyez un e-mail à plusieurs personnes. Les adresses e-mail de vos destinataires ne seront ainsi pas visibles.

Communications aux non-affiliés

Si vous souhaitez communiquer des informations syndicales à vos collègues non affiliés, la prudence est de mise. Ils doivent toujours pouvoir indiquer qu'ils ne souhaitent plus recevoir d'informations syndicales. À nouveau, une solution pratique doit être mise en place afin de respecter cette volonté des travailleurs.

Enfin, un autre élément important est que les informations devront toujours passer par les représentants syndicaux dans l'entreprise, et ne pas venir de l'organisation syndicale elle-même.

En vertu de la CCT 5, «la délégation syndicale pourra [...] procéder oralement ou par écrit à toutes communications utiles au personnel». On ne pourra donc jamais reprocher à un délégué d'avoir envoyé des e-mails, portant sur des informations syndicales, à l'ensemble du personnel.

Par contre, l'employeur n'a pas l'obligation légale de transmettre la liste nominative du personnel à la DS, mais si la DS devait utiliser une telle liste (éventuellement reconstituée par ses soins, par exemple via le carnet d'adresses d'Outlook) pour communiquer par e-mail vers le personnel, l'employeur ou le DPO ne pourrait pas lui en faire le reproche.

3. Impact du RGPD sur la concertation sociale

Si vous êtes délégué syndical ou si vous siégez dans un organe de concertation sociale, vous avez peut-être déjà été confronté à une situation où des informations ne vous sont désormais plus communiquées par l'employeur, «en vertu du RGPD». Si le RGPD présente une protection importante pour toutes et tous vis-à-vis de nos données personnelles, son utilisation ne doit pas être détournée pour contourner les organes de concertation sociale!

Pour être clairs: **le RGPD n'a pas d'impact sur les données communiquées aux représentants syndicaux dans les organes de concertation.** La plupart des données communiquées sont en effet «non-nominatives», c'est-à-dire des données qui ont été anonymisées ou collectivisées, empêchant que les personnes concernées puissent être identifiées. Il ne s'agit donc simplement pas de données à caractère personnel, car on ne peut pas identifier une personne grâce à ses données. Les obligations du RGPD ne s'appliquent donc pas.

Par exemple, la CCT n°9 nous dit que: «*Le chef d'entreprise doit fournir au CE les informations qui permettent de se faire une idée exacte sur la structure de l'emploi dans l'entreprise, sur son évolution et sur les prévisions d'emploi*». Ces informations sont non-nominatives. On parle d'«effectifs», on ne cite donc pas de noms mais bien des chiffres. Ce ne sont donc pas des données personnelles. Une entreprise ne peut pas utiliser le RGPD comme argument pour ne pas fournir ce type de données.

En ce qui concerne des données nominatives, par contre, il s'agit bien là de données personnelles. Le consentement des personnes concernées s'avère nécessaire, sauf si le traitement de ces données est une obligation légale. Par exemple, en ce qui concerne l'accueil des nouveaux travailleurs. **L'employeur doit communiquer leurs noms aux représentants syndicaux pour qu'ils organisent leur accueil** (CCT n°22). Le responsable de traitement est l'employeur, qui réunit ces données pour les fournir aux représentants syndicaux. Ce sera à lui de respecter la vie privée de ses travailleurs lors de ce traitement.

De même, **la délégation syndicale, dans le cadre de ses missions syndicales, est responsable du contrôle du respect de la législation sociale par l'employeur** (CCT n°5). Dans ce cadre, elle a, par exemple, **le mandat légal pour contrôler le respect des règles relatives aux heures sup-**

plémentaires (loi sur le travail). À cette fin, l'employeur doit fournir les informations nécessaires sur les personnes qui ont presté des heures supplémentaires et à quel moment. Or, bien souvent, l'employeur considère qu'il s'agit de données personnelles et refuse de les divulguer. Pourtant, **les membres de la délégation syndicale ont un devoir de discrétion à l'égard de ces informations.** Mais il est clair que, de cette manière, l'employeur empêche le contrôle de l'application de législation par la délégation syndicale.

Un argument important à garder en tête au cas où un employeur refuse de donner des informations alors qu'il doit le faire (parce que c'est prévu par la loi ou par une convention collective de travail), c'est l'article 88 du RGPD.

Cet article dit que «*des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des employés dans le cadre des relations de travail peuvent être prévues par les États membres*» (art. 88 RGPD). Il peut s'agir de lois nationales, CCT nationales, sectorielles ou d'entreprise. Le RGPD reconnait par cet article la valeur légale de toute cette législation, comme base légale permettant de traiter des données personnelles. Cela signifie que toute loi ou CCT qui permet ou qui oblige à ce que des données soient traitées doit être respectée, malgré le RGPD. Dans cet article, le RGPD confirme en fait que toutes les lois nationales peuvent être des exceptions à l'interdiction de traitement des données personnelles. Car on l'a vu, l'une des conditions pour traiter des données est le respect d'une obligation légale.

Donc, si sur base d'une disposition légale, l'entreprise est obligée de fournir certaines informations aux organes de concertation, elle ne peut pas se réfugier derrière le RGPD, et elle doit le respecter et donner l'information. Inversement, si une loi belge va plus loin que le RGPD au niveau de la protection des données, elle doit aussi être respectée.

En résumé, le règlement européen ne modifie pas fondamentalement le droit à l'information des membres des différents organes de concertation sociale. Toutes les CCT nationales, sectorielles et d'entreprise restent d'application. Les bases légales permettant l'information-consultation et encadrant les compétences des membres du CE, du CPPT et de la DS restent d'application et les informations reçues habituellement devront continuer à être fournies.

Il pourrait donc être imaginable de faire signer aux représentants des travailleurs des clauses de confidentialité qui assurent que les représentants des travailleurs n'utilisent ces données que dans le cadre de leur mandat.

Cas particulier : élections sociales.

En vertu de la loi du 4/12/2007 relative aux élections sociales, une série de données personnelles sont traitées par les représentants syndicaux, telles que la liste des personnes exerçant des fonctions de direction et de cadre, la liste des candidats, la composition des bureaux électoraux et les listes de témoins.

Les listes électorales, constituées par l'employeur, sont approuvées au sein du Conseil d'entreprise ou du CPPT et sont ensuite mises à disposition auprès de tous les travailleurs, ce qui vise à assurer la transparence et le contrôle collectif tout au long du processus électoral au sein de l'entreprise, et à permettre à chaque travailleur d'introduire une réclamation en cas d'erreur.

Mais attention: Il ne faut pas confondre la liste électorale avec la liste des membres du personnel. La législation relative aux élections sociales n'oblige qu'à envoyer la première et non la seconde. En principe, l'employeur ne doit donc fournir au CE et/ou au CPPT que les données nécessaires à l'établissement de ces listes électorales.

4. Contrôle du respect du RGPD par l'employeur

En tant que représentant syndical, un élément nouveau dans votre travail syndical sera de **s'assurer que l'employeur respecte les obligations prévues par le RGPD,** et qu'il ne traite pas n'importe quelle donnée n'importe comment. Il faut d'abord s'assurer que l'employeur est transparent: l'employeur a l'obligation d'informer les travailleurs au sujet des données traitées. Afin de respecter ce devoir de transparence, il est possible que l'employeur établisse une politique de traitement des données. L'élaboration d'une CCT d'entreprise est également une possibilité, ce qui est préférable d'un point de vue syndical afin que les représentants syndicaux soient associés lors de sa conclusion.

Pour voir si l'employeur respecte les droits des travailleurs et ses nouvelles obligations en tant qu'employeur et responsable de traitement, il peut enfin **être utile de s'assurer que le règlement de travail soit à jour,** si le RGPD implique des modifications du règlement de travail.

Voici une liste de questions qu'il peut être utile de (se) poser en tant que représentant des travailleurs:

- Quelles données personnelles l'employeur souhaite-t-il traiter?
- S'agit-il de données personnelles sensibles?
- Existe-t-il une base juridique (finalité) pour le traitement?
- Les principes de base du traitement sont-ils respectés? (minimisation notamment).
- L'employeur a-t-il pris les mesures de sécurité appropriées (techniques/organisationnelles)?
- Les personnes concernées (les travailleurs) connaissent-elles leurs droits?
- Ces droits sont-ils correctement respectés (garantis)?

ER: Dominique Leyon · Chaussée de Haecht 579 · 1030 Bruxelles · www.lacsc.be · D/2023/0780/1

facebook.com/lacsc

twitter.com/la_csc

www.youtube.com/cscvideo

instagram.com/lacsc