La CSL vous informe

COMPRENDRE LA NOUVELLE LÉGISLATION EN MATIÈRE DE **PROTECTION DES DONNÉES PERSONNELLES**

DIE NEUEN RECHTSVORSCHRIFTEN FÜR DEN **SCHUTZ PERSONENBEZOGENER DATEN**

2018

CHAMBRE DES SALARIES
LUXEMBOURG

COMPRENDRE LA NOUVELLE LÉGISLATION EN MATIÈRE DE **PROTECTION DES DONNÉES PERSONNELLES**

Aperçu des règles de base en matière de protection des données personnelles tenant compte des nouveautés introduites par le Règlement européen (UE) 2016/679

Qui est concerné et qui est protégé ?
Que faire pour être conforme à la loi ?
Quels sont les droits des personnes protégées ?

Préface

Dans le cadre de la vie active et professionnelle, nombreuses sont les situations où des données personnelles de clients, patients, salariés, administrés etc, sont utilisées, traitées, enregistrées, stockées par des tiers et cela pour diverses raisons et finalités.

Que ce soit la collecte ou l'enregistrement des données, leur exploitation ou leur transmission à des tiers, il existe toujours un risque d'atteinte aux droits et libertés de la personne concernée, notamment en cas d'utilisation abusive de ses données personnelles.

Le règlement européen (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, a posé un nouveau cadre légal pour protéger les personnes physiques contre une utilisation abusive de leurs données personnelles.

La présente brochure a pour finalité de fournir au lecteur un aperçu des principes de base en matière de protection des données afin de lui permettre de saisir la philosophie de cette législation.

Pour approfondir la problématique et apprendre à gérer au quotidien la protection des données personnelles, la Chambre des salariés (CSL) propose des formations spécifiquement axées sur ce thème.

Je vous souhaite une bonne lecture.

Jean-Claude Reding

Président de la CSL
Präsident der Arbeitnehmerkammer

Sommaire

I. Les explications préalables

Le contexte

Dès que nous participons à la vie en société, il est fort probable que nos données personnelles se mettent à circuler.

Nous livrons en effet tous, consciemment ou inconsciemment, des données personnelles à une multitude d'organismes, tel par exemple :

- à un commerçant lorsque nous acceptons de livrer des informations personnelles (nom et adresse, numéro de téléphone, courriel, âge, date de naissance etc.) afin d'obtenir la carte de fidélité de son magasin ;
- à l'administration communale, lors de l'inscription de notre enfant dans une structure d'accueil communale (coordonnées de l'enfant, coordonnées des parents, numéro de téléphone privé et professionnel, lieu de travail des parents etc.) ;
- à notre employeur qui aura besoin de disposer non seulement de notre nom et adresse, mais aussi de notre numéro de sécurité sociale et de notre numéro de compte bancaire ;
- à l'administration fiscale lors de la remise de la déclaration d'impôt ;
- à notre médecin traitant nous communiquerons même (et forcément) des informations relatives à notre état de santé ;
- à notre banquier qui, lorsque nous lui demandons de nous accorder un prêt bancaire, nous demandera en sus des informations dont il dispose déjà sur nous, les coordonnées de notre employeur etc.

Dans le cadre de la vie active/professionnelle, nombreuses sont ainsi les situations où des données personnelles de clients, patients, salariés, administrés etc., sont utilisées, traitées, enregistrées, stockées par des tiers et cela pour diverses raisons et finalités.

Que ce soit la collecte ou l'enregistrement des données, leur exploitation ou leur transmission à des tiers, il existe en permanence un risque d'atteinte à ses droits pour la personne concernée. Aussi peut-être ne désire-t-elle simplement pas que ses données personnelles soient enregistrées ou encore continuées à des tiers.

I. Les explications préalables

Pourquoi est-il nécessaire de protéger les données à caractère personnel ?

En vertu de l'article 11(3) de notre Constitution « *L'État garantit la protection de la vie privée, sauf les exceptions fixées par la loi.* »

La notion de vie privée

Le droit à la vie privée se définit comme le droit pour une personne d'être libre de mener sa propre existence avec le minimum d'ingérences extérieures, ce droit comportant la **protection contre toute atteinte portée au droit au nom, à l'image, à la voix, à l'intimité, à l'honneur et à la réputation, à l'oubli ou à sa propre biographie**.

La jurisprudence de la Cour européenne des droits de l'homme n'a pas limité le droit au respect de la vie privée au seul domicile privé : « *le respect de la vie privée doit aussi englober dans une certaine mesure le droit de l'individu de nouer et de développer des relations avec ses semblables. Il n'y a* ***aucune raison de principe d'en exclure les activités professionnelles ou commerciales***. » (Arrêt du 23 novembre 1992, Niemietz c/ Allemagne, A251/B)

Chaque personne physique a donc le droit au respect de sa vie privée et l'État est le garant de ce principe, sauf les entorses que la loi autorise.

Les exemples cités ci-avant montrent que dans de nombreuses situations, il est indispensable que des données personnelles de personnes physiques circulent afin que la société puisse fonctionner.

Il s'agit donc de trouver un équilibre entre la nécessité de garantir le principe du respect à la vie privée et le besoin de faire circuler, d'utiliser et de gérer les données personnelles des citoyens.

Ceci est l'objectif poursuivi par la législation relative à la protection des données personnelles.

Elle a ainsi pour finalité de donner un certain nombre de garanties aux personnes physiques en insérant tout traitement de données dans des conditions légales précises.

La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

Le Luxembourg était assez précurseur en matière de protection des données alors que bien avant la première directive européenne en la matière, il avait voté déjà en 1979 une loi réglementant l'utilisation de données nominatives dans les traitements informatiques.

L'arrivée des nouvelles technologies a fait que les échanges d'informations ne se sont plus arrêtés aux frontières et ceci a mené à la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 traitant de l'harmonisation du niveau de protection au sein de l'Union Européenne et du principe de libre circulation des données.

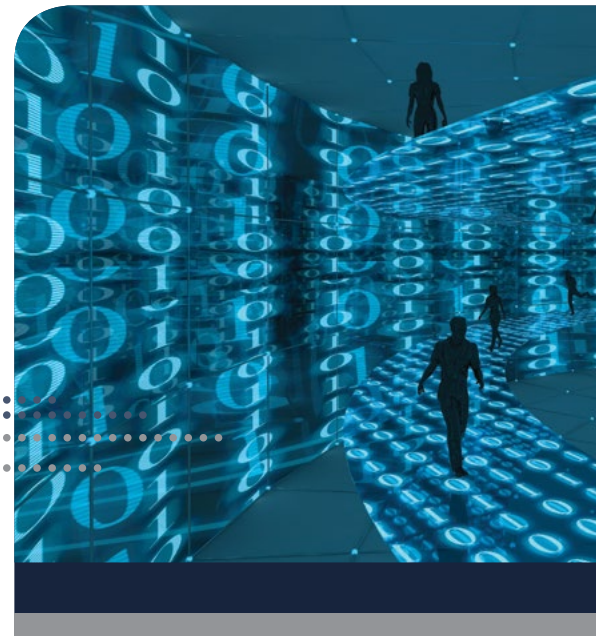
C'est par la loi (modifiée) du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel que le Luxembourg a transposé cette directive en droit luxembourgeois, toujours en recherchant un équilibre entre d'une part, la protection des droits et libertés fondamentaux des personnes concernées (protection de la vie privée) et d'autre part, la libre circulation de ces données.

Depuis lors, toutes les personnes physiques ou morales telles des administrations, des entreprises, des associations et tous autres organismes, qui collectent, enregistrent, utilisent ou transmettent des données personnelles de personnes physiques, c.-à-d. des données qui permettent de les identifier, ne peuvent le faire que dans les conditions posées par la loi modifiée de 2002.

Ces entités doivent en avertir la personne concernée et lui communiquer le but poursuivi de ce que la loi appelle « *le traitement des données à caractère personnel* ».

Ce traitement doit être conforme à la loi et se limiter à ce qui est nécessaire et doit être proportionné aux buts initialement fixés.

Chaque utilisation des données doit donc se faire dans le respect de règles strictes, le contrôle en étant assuré par la Commission nationale pour la protection des données.



À l'origine, la loi de 2002 prévoit que tout fichier contenant des informations relatives à des personnes doit être ou bien déclaré à l'autorité de contrôle ou bien autorisé par elle (selon le type de données ou de traitement) avant de pouvoir être mis en place.

En 2007, la loi a été modifiée dans l'optique de simplifier substantiellement les formalités obligatoires, se traduisant par un allègement du régime d'autorisation préalable et par une simplification importante du régime de notification des traitements.

Précisons encore que la législation sur la protection des données personnelles s'applique aussi bien aux fichiers informatiques qu'aux fichiers papier, enregistrements audio et vidéo etc.

La loi réglemente aussi le traitement de données concernant la sécurité publique, la défense, la recherche, la santé et la poursuite d'infractions pénales ou la sûreté de l'État.

La nouvelle législation en matière de protection des données à laquelle tous les acteurs devront se conformer pour au plus tard le 25 mai 2018

Depuis la première directive européenne de 1995 (ayant donné lieu à la loi nationale de 2002 en matière de protection des données personnelles) la technologique a progressé et continue à évoluer de plus en plus vite.

De nombreux changements sont intervenus depuis et avec cela la nécessité d'adapter le cadre légal afin d'assurer une protection optimale des citoyens quant au traitement de leurs données à caractère personnel et avec cela leur droit au respect de leur vie privée.

Il a donc apparu nécessaire pour le législateur européen de poser d'une part, un cadre de protection des données garantissant une protection forte pour les citoyens tout en tenant compte des nouvelles évolutions technologiques, et, d'autre part, une harmonisation des règles en vigueur dans les différents États membres de l'Union européenne en permettant au marché économique de se développer dans l'ensemble du marché intérieur, dans le respect des droits fondamentaux des personnes physiques.

I. Les explications préalables

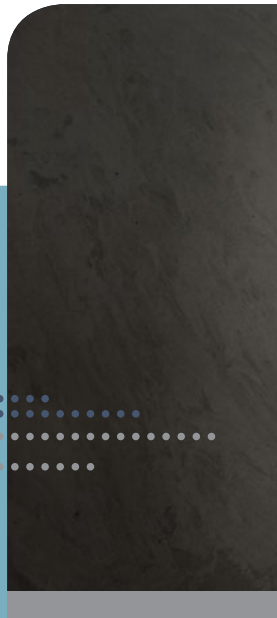
C'est dans cette optique que la Commission européenne a en 2012 initié une réforme du cadre légal existant, dans le but d'adapter les règles aux nouveaux défis, dans un souci de pérennité et de neutralité technologique, en tenant compte de l'évolution technologique et sociétale des deux dernières décennies.

Cette réforme a mené à un « *paquet* » de textes sur la protection des données qui contient :

- le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (abrogeant la directive 95/46/CE), ci-après « **le règlement (UE) 2016/679** », qui **prévoit le régime général en matière de protection des données à caractère personnel**, et
- la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (abrogeant la décision-cadre 2008/977/JAI du Conseil).

Le règlement (UE) 2016/679 prévoit un délai de mise en application de deux ans. Il entrera définitivement en vigueur à partir du 25 mai 2018, date à laquelle il remplacera ainsi définitivement et directement les législations nationales actuellement existantes au sein des 28 États membres.

Le règlement (UE) 2016/679, tenant à harmoniser les règles nationales existantes et à moderniser le cadre légal, a pour but de renforcer la protection des données à caractère personnel dans une société de plus en plus digitale, en redonnant aux citoyens le contrôle des données personnelles qui les concernent, que celles-ci soient collectées et utilisées par les acteurs économiques privés ou par les acteurs du secteur public.



I. Les explications préalables

Étant donné qu'il s'agit d'un règlement européen, il est d'application directe dans tous les États membres, y compris au Luxembourg.

C'est par conséquent dès lors le règlement (UE) 2016/679 qui prévoit la majorité des dispositions de fond désormais applicables en matière de protection des données.

Le projet de loi n° 7184 portant création de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 vient compléter le règlement (UE) 2016/679 en se limitant à compléter le cadre européen par les dispositions nationales qui s'imposent, à savoir l'adaptation de la législation en ce qui concerne la Commission nationale pour la protection des données (CNPD) afin essentiellement d'octroyer à cette commission les nouveaux pouvoirs qui lui seront nécessaires pour qu'elle puisse exercer les missions qui lui reviennent de par le nouveau règlement (UE) 2016/679.

Le règlement (UE) 2016/679 prévoit en effet une responsabilisation accrue de tous les acteurs qui traitent des données personnelles et cela par le biais d'un autocontrôle des entreprises et des moyens de contrôles et de sanctions nettement plus conséquents et dissuasifs au profit des autorités nationales de contrôle en cas de violation constatée aux règles applicables, le but en étant une protection plus efficace des données personnelles.

Le projet de loi n° 7184 vise ainsi à doter la CNPD des moyens nécessaires tout en étendant son champ de compétences aux traitements de données à caractère personnel tombant dans le champ d'application de la future loi transposant la directive (UE) 2016/680 (projet de loi n° 7168) concernant la protection des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale (mais à l'exception des traitements de données à caractère personnel effectués par les juridictions).

I. Les explications préalables

Les missions et les pouvoirs de la CNPD vont être augmentés telle notamment la possibilité d'imposer des amendes administratives très dissuasives, pouvant aller jusqu'à 20 millions d'euros, ou dans le cas d'une entreprise jusqu'à 4% du chiffre d'affaires annuel mondial total. Aussi la CNPD aura-t-elle des pouvoirs réglementaires très étendus en matière de protection des données.

Néanmoins, notons d'emblée que le mécanisme actuel des autorisations préalables concernant les traitements de données à des fins de surveillance sur le lieu de travail semble être supprimé.

Le projet de loi prévoit la suppression de la loi modifiée de 2002 étant donné que les règles en matière de protection des données personnelles résultent désormais essentiellement du règlement (UE) 2016/679.

Le projet de loi n° 7168 est relatif à la protection des données personnelles en matière pénale et de sécurité nationale.

Il complète la transposition du cadre légal européen en portant transposition en droit luxembourgeois de la directive (UE) n° 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

Ce projet, tout comme la directive européenne de base, tend à adapter les règles en matière pénale aux exigences posées par les évolutions technologiques des dernières décennies.

Il fixe les règles relatives à la protection des données applicables aux traitements de données à caractère personnel effectués par les autorités compétentes (notamment la police, l'inspection générale de la police, le service de renseignement, l'administration pénitentiaire, l'armée, la cellule de renseignement financier, le parquet, le juge d'instruction etc.) à des fins de :

- prévention et de détection des infractions pénales ;
- enquêtes et de poursuites en matière d'infractions pénales ;
- exécution de sanctions pénales ;
- protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;
- protection contre les menaces pour la sécurité nationale et sa prévention.

Nous consacrons les informations et explications qui suivent exclusivement au régime général de la législation relative à la protection des données personnelles et non pas aux règles spécifiques applicables en matière pénale.

II. Les règles essentielles de la législation générale en matière de protection des données personnelles

1. Qui est concerné par la législation relative à la protection des données personnelles et qui est protégé par cette législation ?

EST CONCERNÉE : Toute personne physique ou morale qui utilise des données personnelles de personnes physiques

Toute personne physique ou morale qui utilise/traite des données personnelles de personnes physiques est tenue de respecter les règles légales issues de la législation relative à la protection des données personnelles. Cette personne est appelée le responsable du traitement. C'est elle qui décide de traiter/utiliser les données personnelles d'autres personnes et pourquoi elle le fait et comment elle le fait.

Responsable du traitement

C'est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine les finalités et les moyens du traitement des données.

Par exemple le médecin qui traite les données de ses patients, l'employeur qui traite les données de ses salariés, l'école qui traite les données de ses élèves, le propriétaire d'un magasin qui tient son fichier clients etc.

EST CONCERNÉE ET PROTÉGÉE : Toute personne physique dont les données personnelles sont utilisées

Dès que des données personnelles (nom, prénom, âge, numéro de téléphone, courriel, adresse, image de la personne, sa voix etc.) permettant d'identifier des personnes physiques, sont traitées (c.-à-d. utilisées, stockées, gérées etc.) par une autre personne physique ou morale (appelée le responsable du traitement), le cadre légal protecteur s'applique.

Attention : Seules les personnes physiques sont protégées par la législation relative à la protection des données personnelles à l'exclusion des personnes morales.

Donnée à caractère personnel

Il s'agit de toute information se rapportant à une personne physique et permettant de l'identifier.

Tels par exemple son nom, son adresse, son numéro de téléphone, son numéro d'identifiant, sa donnée de localisation, sa capture d'image, sa donnée physique, culturelle, sociale, économique etc.

II. Les règles essentielles de la législation générale en matière de protection des données personnelles

La législation relative à la protection des données personnelles détermine aussi ce que l'on entend exactement par un traitement de données.

Traitement de données

Il s'agit de toute opération effectuée ou non à l'aide de procédés automatisés et appliqués à des données.

Tels par exemple la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation etc. peu importe le support utilisé.

Mais attention : Sont exclus du champ d'application de la législation relative à la protection des données personnelles, les traitements mis en œuvre dans le cadre des activités personnelles/domestiques d'une personne physique.

Exemple :
Je n'ai pas besoin de prêter attention à la législation relative à la protection des données personnelles lorsque j'enregistre les coordonnées de mes amis et connaissances dans mon agenda privé.

Précisons encore que la législation relative à la protection des données personnelles s'applique à tout traitement de données effectué sur le territoire de l'Union européenne, peu importe où se situe le responsable du traitement et la ou les personnes physiques dont les données sont traitées.

Elle s'applique en outre à tout traitement de données relatives à des personnes physiques se trouvant sur le territoire de l'Union européenne et lié à une offre de biens/servies ou au suivi de leur comportement, peu importe où se situe le responsable du traitement et peu importe où les données sont traitées.

2. Quelles sont les conditions de licéité d'un traitement de données personnelles ?

Les règles de base

Chaque responsable d'un traitement doit s'assurer de :

- traiter les données de manière **licite, loyale et transparente** ;
- **limiter les finalités** : les données ne peuvent être traitées que pour une ou plusieurs finalités déterminées, explicites et légitimes ;
- utiliser des **données adéquates, pertinentes et non excessives** au regard des finalités déterminées ;
- garantir l'**exactitude des données** et, si nécessaire, les mettre à jour ;
- **limiter la durée de conservation** des données ;
- garantir une **sécurité appropriée des données** (contre le traitement non autorisé ou illicite, contre la perte, la destruction ou les dégâts d'origine accidentelle notamment).

Le responsable du traitement doit à tout moment pouvoir prouver que toutes ces obligations sont respectées.

Les 6 bases légales possibles

Un traitement mis en œuvre n'est licite que s'il correspond à un des six cas d'ouverture posés par la législation relative à la protection des données personnelles.

Chaque traitement mis en œuvre doit donc trouver son fondement dans un des 6 cas qui suivent :

CAS 1
Accord de la personne concernée

Si la personne concernée a donné son accord au traitement, alors cela a pour effet de rendre le traitement légitime.

Exemple : Monsieur X accepte de fournir ses coordonnées dans un commerce pour recevoir la carte client du magasin

Exception : Lors d'un traitement mis en œuvre par un employeur à des fins de surveillance sur le lieu de travail (voir explications p.26 et p.28) le consentement du salarié ne permettra pas de légitimer un traitement mis en œuvre dans des conditions illégales.

Notons que le responsable du traitement doit pouvoir prouver le consentement et si le consentement est donné dans une déclaration écrite qui comprend également d'autres questions, la demande de consentement doit être présentée sous une forme qui la distingue clairement des autres questions, et elle doit être formulée en des termes clairs et simples.

La personne concernée a en outre le droit de retirer son consentement à tout moment.

CAS 2
Exécution d'un contrat

Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.

Exemple : Si Madame Y ne donne pas son adresse privée au commerçant auquel elle a acheté une armoire, celle-ci ne pourra pas lui être livrée et installée à son domicile. Il est donc nécessaire à l'exécution du contrat qu'elle livre cette information.

CAS 3
Obligation légale

Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.

Exemple : La loi impose au banquier de vérifier l'identité exacte de son client ; il est donc légitime pour lui de prendre une copie du document d'identité de son client.

CAS 4
Sauvegarde des intérêts vitaux

Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.

Exemple : Le médecin est tenu de prendre note des allergies de ses patients afin de ne pas leur prescrire des médicaments qu'ils ne supporteraient pas.

CAS 5
Mission d'intérêt public/relevant de l'exercice de l'autorité publique

Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Exemple : Dans le cadre de sa mission publique de la récolte de fonds publics, l'administration fiscale est autorisée à enregistrer un certain nombre de données personnelles des citoyens.

CAS 6
Intérêt légitime du responsable du traitement

Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement.

Exemple : Il peut être légitime pour un commerçant d'effectuer un traitement de données personnelles à des fins de prospection. Attention : la personne physique concernée a toujours le droit de s'y opposer.

3. Existe-t-il des données que l'on n'a pas le droit de traiter ?

Oui. La législation relative à la protection des données personnelles interdit de traiter des données ayant trait :

- à l'origine raciale ou ethnique ;
- aux opinions politiques ;
- aux convictions religieuses ou philosophiques ;
- à l'appartenance syndicale ;
- aux données génétiques ;
- aux données biométriques ;
- aux données concernant la santé, la vie sexuelle ou l'orientation sexuelle.

Notons que la législation relative à la protection des données personnelles fixe de nombreuses exceptions à ce principe, tel par exemple en matière de santé, la permission pour les professionnels de la santé de traiter les données liées à l'état de santé du patient.

Ou encore les cas dans lesquels le traitement d'une donnée sensible est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres du responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où le traitement est autorisé en vertu d'une disposition légale européenne, nationale ou d'une convention collective de travail prévoyant des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée.

Ou encore lorsque la personne concernée a donné son consentement explicite au traitement d'une ou de plusieurs données (dont en principe le traitement est interdit) pour une ou plusieurs finalités spécifiques, sauf lorsque la loi prévoit que l'interdiction de traiter la ou les données interdites, ne peut être levée par le consentement de la personne concernée. (voir « exception » p.20)

4. Est-ce qu'il existe des traitements de données spécialement réglementés ?

Certains traitements de données sont spécialement réglementés, notamment les traitements effectués dans le cadre de la liberté d'expression, les traitements et accès du public aux documents officiels, les traitements à des fins de recherche scientifique ou historique ou statistiques et les traitements de données dans le cadre des relations de travail.

Traitement de données personnelles dans le cadre des relations de travail

Sur le plan européen

Suivant l'article 88 du règlement EU 2016/679 « *Les États membres peuvent prévoir, par la loi ou au moyen de conventions collectives, 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****, aux fins, notamment,* ***du recrutement, de l'exécution du contrat de travail, y compris le respect des obligations fixées par la loi ou par des conventions collectives, de la gestion, de la planification et de l'organisation du travail, de l'égalité et de la diversité sur le lieu de travail, de la santé et de la sécurité au travail, de la protection des biens appartenant à l'employeur ou au client, aux fins de l'exercice et de la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ainsi qu'aux fins de la résiliation de la relation de travail****.*

Ces règles comprennent des mesures appropriées et spécifiques pour protéger la dignité humaine, les intérêts légitimes et les droits fondamentaux des personnes concernées, en accordant une ***attention particulière à la transparence du traitement, au transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe et aux systèmes de contrôle sur le lieu de travail.*** »

Le texte européen permet ainsi au législateur national de réglementer particulièrement la question de la protection des données sur le lieu du travail.

Sur le plan national

Le législateur luxembourgeois a prévu dans son article L.261-1 du Code du travail national qu'un traitement de données à des fins de surveillance touchant des salariés ne peut être mis en œuvre par l'employeur que s'il est nécessaire :

1. Pour les **besoins de sécurité et de santé des travailleurs**.

   Exemple : Surveillance d'une station-service par caméra : protéger les salariés contre les agressions, risque d'explosion etc.

2. Pour les **besoins de protection des biens de l'entreprise**.

   Exemple : Protection de la salle des coffres-forts d'une banque par caméra

3. Pour le **contrôle du processus de production portant uniquement sur les machines**.

   Exemple : Surveillance d'une chaîne d'assemblage automatique de produits

4. Pour le **contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte du salarié**.

5. Dans le cadre d'une **organisation de travail selon l'horaire mobile**.

En ce qui concerne les points n° 1, 4 et 5 le comité mixte d'entreprise lorsqu'il existe, et dès les prochaines élections sociales, la délégation du personnel dans les entreprises d'au moins 150 salariés, a un pouvoir de décision quant à l'instauration d'un tel traitement aux fins de surveillance des salariés.

Notons que le consentement de la personne concernée ne rend pas légitime un traitement mis en œuvre par l'employeur à des fins de surveillance et qui serait non conforme à la loi.

Avant de mettre en œuvre un traitement de données personnelles à des fins de surveillance, l'employeur doit au préalable informer aussi bien les salariés concernés, ainsi que le comité mixte d'entreprise ou, à défaut, la délégation du personnel[2] ou, à défaut encore, l'Inspection du travail et des mines.

2 Dès les prochaines élections sociales : la délégation du personnel sera dans tous les cas informée, et à défaut ce sera l'ITM.

Traitement de données personnelles dans le cadre des relations de travail

suite...

Si le traitement est effectué en violation de l'article L.261-1 du Code du travail, alors l'employeur s'expose à une peine d'emprisonnement de 8 jours à 1 an et à une amende de 251 à 125.000 euros ou d'une de ces peines seulement.

Notons encore qu'une juridiction saisie d'une violation légale pourrait prononcer la cessation d'un traitement contraire à la loi sous peine d'astreinte.

À ce jour les traitements de données mis en œuvre par un employeur à des fins de surveillance sur le lieu de travail, doivent être au préalable autorisés par la Commission nationale pour la protection des données (CNPD).

Avec la nouvelle législation nationale, le système de l'autorisation préalable devrait disparaître pour être remplacé par un système de contrôle a posteriori.

Précisons qu'à ce jour ce sont les autorisations préalables de la CNPD qui fournissent un certain nombre de garanties aussi biens aux salariés concernés par un mécanisme de surveillance mis en place, qu'à leur employeur. Ces autorisations précisent les conditions et modalités concrètes de la mise en place du dispositif de surveillance autorisé.

Ainsi par exemple un employeur voulant mettre en place un dispositif de vidéosurveillance doit-il à ce jour obtenir l'aval préalable de la CNPD. Ce qui implique que la CNPD vérifie si les finalités du traitement de données par vidéo caméra répondent à une ou plusieurs des conditions de légitimité admises (sécurité et santé des salariés, protection des biens de l'entreprise ou contrôle du processus de production portant uniquement sur les machines). Ensuite elle analyse au cas par cas en détail la nécessité et la proportionnalité pour chaque « zone » surveillée.

Par exemple, l'installation d'une caméra de surveillance dans un bureau où travaille en permanence un salarié est considérée comme disproportionnée ou excessive, les droits et libertés fondamentaux des salariés prévalant sur les intérêts poursuivis par l'employeur.

De même, l'installation de caméras vidéo dans la cuisine d'un restaurant sera considérée comme disproportionnée et/ou excessive, considérant que tous les salariés employés à la cuisine se trouveront quasiment en permanence sous ces caméras.

C'est pourquoi la CNPD jusqu'à ce jour, dans ses décisions, exclut certaines zones et/ou assortit ses autorisations de conditions et exigences :

- **interdiction d'une surveillance permanente et continue, sauf exceptions rares ;**
- **interdiction d'enregistrer le son associé aux images ;**
- **interdiction de surveiller les prestations et les comportements des salariés ;**
- **interdiction de filmer les endroits réservés aux salariés pour un usage privé ;**
- **champ de vision limité des caméras filmant les accès intérieurs, extérieurs ou les alentours d'un bâtiment ou d'un site ;**
- **durée de conservation des images limitée etc.**

À défaut du maintien de ce mécanisme d'autorisation préalable, la CNPD devrait à l'avenir user de son pouvoir règlementaire[3] pour émettre des lignes de conduites et insérer ainsi les surveillances pratiquées sur le lieu de travail dans des conditions strictes.

3 Voir explications p.44

5. Quels sont les droits de la personne concernée par un traitement de données ?

Toute personne concernée par un traitement de données dispose d'un certain nombre de droits. Ces droits sont largement augmentés avec le règlement (UE) 2016/679.

Il s'agit du droit à l'information, du droit d'accès, du droit de rectification, du droit à l'effacement des données, du droit à la limitation du traitement, du droit à la portabilité des données, du droit d'opposition, du droit de s'opposer au profilage et au traitement automatisé de sa demande, du droit à la réclamation et du droit à réparation.

Droit à l'information

Données recueillies directement auprès de la personne

La personne concernée a le droit d'être informée au moment où les données la concernant sont collectées auprès d'elle-même sur les éléments suivants :

- l'identité et les coordonnées du responsable du traitement ;
- le cas échéant, les coordonnées du délégué à la protection des données (voir explications p.40) ;
- la finalité du traitement et sa base légale ;
- si le traitement est basé sur l'intérêt légitime du responsable du traitement, son intérêt légitime est à spécifier ;
- le ou les destinataires des données ;
- la durée de conservation des données, sinon les critères employés pour la déterminer ;
- l'existence de ses autres droits (droit d'accès, à la rectification, à l'effacement, à la limitation des données etc.) ;
- le caractère réglementaire, contractuel ou obligatoire ou non de la fourniture des données et les conséquences d'un éventuel refus ;
- l'existence d'une prise de décision automatisée ou d'un profilage ;
- le cas échéant l'utilisation des données à une autre fin.

Données non collectées auprès de la personne concernée

Si les données ne sont pas recueillies directement auprès de la personne concernée :

- la source des données doit être indiquée avec la précision si la source est accessible au public ou pas, et
- le responsable du traitement doit fournir les informations énumérées ci-avant[4] :

4 Données recueillies directement auprès de la personne.

- dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, ou
- si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication avec ladite personne, ou
- s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

Notons en outre que toute personne a toujours le droit d'être informée sur demande dans un délai d'un mois, ainsi que d'être informée de toute violation de ses données.

Droit d'accès

La personne concernée a le droit d'accéder aux données traitées avec les informations relevant du droit à l'information et d'obtenir une copie gratuite des données. Précisons qu'en cas de demande de copies supplémentaires, le responsable du traitement pourra demander le paiement de frais raisonnables pour toute copie supplémentaire.

Droit de rectification

Il s'agit du droit de demander la rectification de données inexactes dans les meilleurs délais, ainsi que du droit d'obtenir que des données incomplètes soient complétées.

Droit à l'effacement des données dans les meilleurs délais

Ce droit joue dès que les données ne sont plus nécessaires pour la finalité visée, lorsque le traitement est basé sur le consentement et que le consentement est retiré, dans le cas de l'exercice justifié du droit d'opposition, lorsque le traitement de données est illicite, lorsque l'effacement est nécessaire pour garantir le respect d'une obligation légale, lorsque les données sont collectées dans le cadre de services proposés à des enfants/jeunes de moins de 16 ans.

Notons que des exceptions existent quant à l'exercice de ce droit et cela notamment dans les cas suivants :

- exercice du droit à la liberté d'expression/d'information ;
- nécessité de garantir le respect d'une obligation légale ;
- intérêt public dans le cadre de la santé publique ;
- archivage dans l'intérêt public, recherche scientifique ou historique, statistiques ;
- défense de droits en justice.

Droit d'opposition

Lorsque le traitement a lieu dans le cadre de l'exercice d'une mission publique ou que le traitement est basé sur l'intérêt légitime du responsable du traitement, la personne concernée a le droit de s'opposer pour des raisons tenant à sa situation particulière au traitement, sauf si l'intérêt public prime.

En outre, toute personne a le droit de s'opposer à un traitement de ses données à des fins de prospection, y compris au profilage lié à une telle prospection.

Droit à la limitation du traitement

Ce droit peut être exercé pendant la vérification des données suite à une mise en doute de l'exactitude des données ou lorsque le traitement est illicite et la personne concernée s'oppose à l'effacement, mais demande la limitation ou encore lorsque le responsable du traitement n'a plus besoin des données, mais que la personne concernée en a besoin pour la défense de ses droits en justice ou encore lorsque la personne concernée s'oppose au traitement et le traitement est alors limité pendant le temps nécessaire pour vérifier si des motifs légitimes du responsable du traitement prévalent.

Droit à la portabilité

Lorsque le traitement est fondé sur le consentement de la personne concernée ou lorsque le traitement est effectué à l'aide de procédés informatisés, la personne concernée a le droit de demander que les données soient d'office transférées par le responsable du traitement à un autre responsable du traitement.

Profilage et traitement automatisé de données

Toute personne a le droit de s'opposer à une décision basée sur un traitement automatisé, y compris le profilage, lorsqu'il produit des effets juridiques ou affecte la personne significativement de manière similaire. Sauf si le traitement est nécessaire à la conclusion/exécution d'un contrat ou fondé sur le consentement explicite de la personne ou lorsque le traitement est autorisé par le droit européen ou national du responsable du traitement.

Attention aux données sensibles : elles ne peuvent faire l'objet d'un tel traitement que si la personne concernée a donné son consentement explicite ou dans l'intérêt public et que des mesures appropriées de protection des droits et libertés ont été prises.

Droit à la réclamation

Chaque personne physique peut introduire une réclamation auprès de la CNPD pour violation de ses droits sur base de la législation relative à la protection des données personnelles. La CNPD informe le plaignant de l'état d'avancement et de l'issue de la réclamation.

Droit à la réparation

Le responsable du traitement doit réparer le préjudice subi par la personne concernée, sauf à prouver qu'il n'est pas responsable.

Droit de recours

La loi prévoit aussi un droit de recours contre un responsable du traitement, voir même contre les décisions de la CNPD, ainsi que le droit de se faire représenter par un organisme/association sans but lucratif d'intérêt public et actif dans le domaine de la protection des droits et libertés des personnes en matière de protection des données personnelles.

6. Quelles sont les obligations à respecter par tout responsable de traitement ?

La législation relative à la protection des données personnelles met un nombre important d'obligations à charge du responsable du traitement lesquelles peuvent être résumées comme suit :

- respecter toutes les règles légales posées par la législation relative à la protection des données personnelles à tout moment ;
- savoir démontrer et documenter à tout moment sa conformité à la législation relative à la protection des données personnelles par des mesures techniques et organisationnelles appropriées ;
- assurer la sécurité des données traitées : Le responsable du traitement doit s'assurer de n'utiliser que des moyens garantissant la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes de traitement. Il doit disposer des moyens pour rétablir la disponibilité/accès aux données en cas d'incident. Il doit aussi disposer d'une procédure pour tester, analyser et évaluer régulièrement l'efficacité des mesures de sécurité en fonction du degré de risques de chaque traitement ;

- assurer au maximum la protection des données dès la conception et la protection des données par défaut :
  - > le responsable du traitement doit dans la mesure du possible appliquer, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation ;
  - > il doit garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées ; cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité ;
  - > les mesures mises en place doivent garantir que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.
- choisir (le cas échéant/s'il y a lieu) un sous-traitant qui présente des garanties suffisantes et baser son accord avec le sous-traitant sur un contrat écrit contenant des clauses de confidentialité ;
- tenir le cas échéant un registre des activités de traitement (voir explications p.40) ;
- notifier à la CNPD toute violation des données traitées dans les meilleurs délais et au plus tard dans les 72 heures ;
- informer la personne physique concernée de toute violation de données s'il y a un risque élevé d'atteinte aux droits et libertés ;
- effectuer une analyse d'impact s'il y a un risque élevé pour les droits et libertés des personnes physiques (voir explications p.42 et p.44) ;
- désigner le cas échéant un délégué à la protection des données (voir point 8 p.40 et p.42).

Le non-respect de ces règles expose le responsable du traitement à une amende administrative jusqu'à 20 millions d'euros ou jusqu'à 4% de son chiffre d'affaires annuel mondial.

7. Qui doit mettre en place un registre des traitements de données personnelles et que doit contenir ce registre ?

Toute entreprise ou organisation comptant 250 salariés au moins, ou comptant moins de 250 salariés, et effectuant un traitement susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions, doit mettre en place un registre de tous ses traitements de données personnelles.

Ce registre doit continuellement être tenu à jour et doit contenir les précisions suivantes :

- nom, coordonnées du responsable du traitement, le cas échéant de son représentant et du délégué à la protection des données (voir point 8 ci-après), et le cas échéant de son sous-traitant ;
- la ou les finalités du traitement ;
- la base légale du traitement ;
- les catégories de personnes et de données concernées ;
- les destinataires des données ;
- les délais prévus pour l'effacement si possible, sinon les critères appliqués pour en décider ;
- les personnes ayant accès en interne aux données ;
- les mesures de sécurité techniques et organisationnelles prévues.

8. Quelles sont les règles légales concernant le délégué à la protection des données ?

Qui doit nommer un délégué à la protection des données ?

Dans certains cas le responsable du traitement sera tenu de nommer un délégué à la protection des données, à savoir :

- lorsque le responsable du traitement est une autorité/organisme public, ou
- lorsqu'il traite des données nécessitant un suivi régulier et systématique à grande échelle, ou
- lorsqu'il traite à grande échelle des catégories particulières (celles qui sont en principe interdites d'être traitées) de données.

Quelles sont les missions du délégué à la protection des données ?

Le délégué à la protection des données a les missions suivantes :

- informer et conseiller le responsable du traitement et ses salariés ;

- contrôler le respect de l'application de la législation relative à la protection des données personnelles par le responsable du traitement et ses salariés, notamment en ce qui concerne les règles internes, la répartition des responsabilités, la sensibilisation et la formation du personnel ;
- donner des conseils quant à l'analyse d'impact ;
- coopérer avec l'autorité de contrôle nationale et être son point de contact.

Quels sont les droits et obligations du délégué à la protection des données ?

Le délégué à la protection des données doit :

- être associé par le responsable du traitement à toute question liée à la protection des données ;
- recevoir les ressources nécessaires, y compris les moyens d'entretenir ses compétences en matière de protection des données ;
- recevoir l'accès aux données et aux traitements effectués ;
- exercer sa mission en toute indépendance par rapport au responsable du traitement ;
- rapporter au niveau hiérarchique le plus élevé de la direction du responsable du traitement.

Qui peut être délégué à la protection des données ?

Le délégué à la protection des données peut être un salarié du responsable du traitement dont les tâches ne sont pas en conflit avec ses missions de délégué à la protection des données, ou un indépendant lié par contrat de service au responsable du traitement.

Il doit avoir de bonnes connaissances du droit et des techniques en matière de protection des données.

9. Quand est-ce qu'un responsable de traitement doit-il effectuer une analyse d'impact ?

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement doit demander conseil au délégué à la protection des données, si un tel délégué a été désigné.

L'analyse d'impact relative à la protection des données est, en particulier, requise dans les cas suivants :

- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ; ou
- le traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions ; ou
- la surveillance systématique à grande échelle d'une zone accessible au public.

La CNPD devrait établir et publier une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise.

10. Quel est le rôle de la CNPD, l'autorité nationale de contrôle indépendante ?

La Commission nationale pour la protection des données (CNPD) est chargée de contrôler la conformité de tous les traitements de données par rapport à la législation relative à la protection des données personnelles, y compris en matière pénale et de sécurité nationale sauf en ce qui concerne les traitements émis par les juridictions de l'ordre judiciaire, de l'ordre administratif et du ministère public en matière juridictionnelle (compétence de l'autorité de contrôle judiciaire).

Suite au règlement (UE) 2016/679 la CNPD se voit confier de larges pouvoirs que l'on peut résumer comme suit :

- elle dispose désormais d'un pouvoir réglementaire ;
- elle reçoit les plaintes en matière de protection des données personnelles ;

- elle vérifie la licéité des traitements mis en place ;
- elle fournit sur demande à des personnes physiques des informations sur l'exercice de leurs droits ;
- elle examine et retire le cas échéant les certifications en matière de protection des données ;
- elle mène des investigations/enquêtes avec accès direct aux locaux où sont traités les données, ainsi qu'aux traitements ;
- elle dénonce les infractions aux autorités judicaires ;
- elle met en place des mécanismes pour permettre le signalement confidentiel de violations en matière pénale ;
- elle enjoint au responsable du traitement de communiquer toute violation à la personne physique concernée s'il ne l'a pas fait ;
- elle peut imposer une limitation/interdiction temporaire ou définitive de traitement ;
- elle ordonne la rectification ou l'effacement de données ;
- elle sanctionne par :
  - > des astreintes,
  - > des avertissements,
  - > des verrouillages,
  - > l'effacement ou la destruction des données,
  - > l'interdiction de traitement,
  - > l'insertion de décisions d'interdiction dans les journaux,
  - > une amende administrative jusqu'à 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires annuel mondial du responsable du traitement,
- elle peut agir en justice.

Quiconque entrave la CNPD dans l'exercice de ses missions légales ou met en œuvre un traitement contraire à la loi s'expose à des sanctions pénales (emprisonnement de 8 jours à 1 an et amende de 251 à 125 000 euros).

Notes

CHAMBRE DES SALARIES
LUXEMBOURG

18 rue Auguste Lumière L-1950 Luxembourg
T +352 27 494 200 F +352 27 494 250
csl@csl.lu www.csl.lu