



Protection
des **données**
et **vie privée**





VIE PRIVÉE ET TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL



SOMMAIRE

La protection des données – de quoi s'agit-il ?	6 _
Les 10 commandements de la protection des données personnelles	10 _
Vos droits de citoyen	18 _
Quand et comment faire valoir ses droits ?	22 _
La Commission nationale pour la protection des données : l'arbitre du juste équilibre	26 _
Glossaire des termes les plus courants en matière de protection des données	28 _



LA PROTECTION DES DONNÉES – DE QUOI S'AGIT-IL ?



Dans la société de l'information d'aujourd'hui, de nombreux organismes et institutions collectent de plus en plus d'informations sur les personnes.

En effet, chacun de nous livre, volontairement ou non, des données personnelles à une multitude d'organismes, par exemple :

- _ à l'administration communale ou gouvernementale (permis, autorisation ou subside) ;
- _ au fisc (déclaration fiscale) ;
- _ aux médecins et à la pharmacie (consultations et ordonnances) ;
- _ à la caisse de maladie (remboursement des dépenses de santé) ;
- _ aux banques (demande de prêt, décompte de l'utilisation de la carte de crédit) ;

- _ aux supermarchés (cartes de fidélité, jeux-concours) ;
- _ à l'opérateur de GSM et aux P&T (communications téléphoniques) ;
- _ aux clubs sportifs, associations culturelles ou de loisirs (carte de membre) ;
- _ ou tout simplement à l'occasion d'une navigation sur Internet ou d'un après-midi de shopping en raison de l'enregistrement d'images par des systèmes de surveillance.

Ainsi, la circulation de nos données personnelles se multiplie et se propage à des endroits de plus en plus nombreux.

Grâce aux moyens informatiques modernes, l'exploitation de ces données est devenue de plus en plus aisée et multiforme et ceci aussi bien au niveau de l'État et des administrations, des entreprises et autres professionnels, qu'au niveau des clubs et associations.

L'établissement de profils personnels révélant nos habitudes de vie et de consommation devient pratique courante (sondages, cartes client, Internet...).

Que ce soit la collecte ou l'enregistrement des données, en passant par leur exploitation jusqu'à la transmission de ces données à des tiers ; à chaque instant, les risques pour les concernés sont réels, liés à l'accumulation et l'utilisation de ses données personnelles.

Or la perte de votre maîtrise sur les données qui vous concernent ainsi que les intrusions injustifiées dans votre vie privée ne sont pas une fatalité, bien au contraire. La loi du 2 août 2002, qui transpose une directive européenne sur la protection des données¹, vous accorde des droits. Elle vise à protéger la vie privée des personnes physiques (et même les intérêts des personnes morales) à l'égard du traitement de leurs données personnelles par des tiers.

Les administrations, les entreprises et autres professionnels, les associations et tout autre organisme qui collectent, enregistrent, utilisent et transmettent des données personnelles ne peuvent pas le faire sans restrictions. Ils doivent en avvertir 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 se limiter à ce qui est nécessaire et proportionné aux buts initialement fixés. Chaque utilisation des données doit donc se faire dans le respect de règles strictes, dont le contrôle est assuré par la Commission nationale pour la protection des données². Dans un souci de transparence, tout fichier contenant des informations relatives à des personnes doit aussi être respectivement déclaré à l'autorité de contrôle ou autorisé par elle (selon le type de données ou de traitement) avant de pouvoir être exploité.

La législation sur la protection des données personnelles ne se limite d'ailleurs pas aux fichiers informatiques, mais concerne tout type de support (fichiers papier, enregistrements audio et vidéo).

La protection de la vie privée constitue un droit fondamental, tout comme l'inviolabilité du

¹ (Directive 95/46/CE du 24 octobre 1995)

² www.cnpd.lu

domicile, le secret de la correspondance, ou encore la liberté d'opinion et d'expression.

Les mêmes principes s'appliquent d'ailleurs dans tous les 25 États membres de l'Union européenne et au-delà (Suisse, Norvège, Liechtenstein, Islande, etc.).





LES 10 COMMANDEMENTS DE LA PROTECTION DES DONNÉES PERSONNELLES



Celui qui traite des données concernant d'autres personnes doit respecter les principes suivants :

1. LE PRINCIPE DE LÉGITIMITÉ

Le traitement de données personnelles n'est possible que s'il existe une raison suffisamment légitime pour le justifier. Celui qui souhaite traiter vos données doit, avant de pouvoir le faire, vous demander votre accord. Alternativement, le traitement de données est aussi permis s'il est indispensable pour pouvoir exécuter un contrat, pour respecter une obligation de service public

ou une obligation légale, ou encore pour protéger votre propre vie. Finalement, le traitement peut être légitimé s'il existe un intérêt justifié à condition que le traitement de vos données n'affecte votre vie privée que de façon minimale.

Ceci constitue le premier test pour savoir si le traitement est licite. Il répond à la question **quand** est-ce que vos données peuvent être demandées et utilisées par un tiers. Les principes suivants décrivent les règles que ce dernier doit respecter lors de l'utilisation de vos données. Ils répondent à la question du **comment** du traitement de vos données.

2. LE PRINCIPE DE FINALITÉ

L'utilisation de vos données personnelles (y compris des images et sons) doit être strictement limitée à une finalité explicitement déterminée au préalable.

La collecte, l'enregistrement et l'utilisation de vos données personnelles sont strictement limités à ce qui est nécessaire pour atteindre des buts expressément fixés d'avance par l'Administration, l'entreprise, l'association, le professionnel ou l'indépendant qui s'y livre.

Ceux-ci ne doivent pas les transmettre à d'autres organismes ou personnes, sauf si ces derniers en ont besoin dans le cadre de la réalisation des mêmes buts et ne les utiliseront que de manière compatible.

EXEMPLE

Suite à un accident de travail, votre employeur souhaite se renseigner sur votre état de santé auprès de votre médecin traitant. Croyant ne rien faire de mal en le rassurant, l'assistante du médecin lui fournit des informations sur le diagnostic établi par le médecin.

Ce faisant, elle transgresse la finalité pour laquelle le cabinet médical détient ces informations, à savoir assurer vos soins de santé.

3. LES PRINCIPES DE NÉCESSITÉ ET DE PROPORTIONNALITÉ

Le principe de proportionnalité implique que le traitement doit se limiter à vos données pour lesquelles il existe un rapport direct avec la finalité initiale du traitement. Ces données doivent non seulement être utiles, mais aussi nécessaires pour celui qui traite vos données. Les données traitées ne doivent pas être excessives par rapport au but poursuivi.

EXEMPLE

Lors de la réservation par téléphone d'une table, le gérant de restaurant vous demande de lui fournir le numéro de votre carte de crédit.

Cette information est à considérer comme excessive par rapport à la finalité poursuivie qui consiste dans la planification des tables disponibles.

4. LE PRINCIPE D'EXACTITUDE DES DONNÉES

Comme des informations inexacts ou incomplètes peuvent nuire à la personne à laquelle elles se rapportent, tous les efforts doivent être faits pour que les données traitées soient correctes et actuelles. Si ce n'est pas le cas, les données personnelles doivent être rectifiées ou bien effacées.

La loi vous protège également contre toute décision négative prise automatiquement par ordinateur, dont vous pourriez faire l'objet sans pouvoir faire valoir votre point de vue personnel.

EXEMPLE

Vous sollicitez un prêt personnel auprès de votre banque pour un achat de mobilier. Après introduction de votre dossier par Internet, vous recevez immédiatement une réponse négative de votre banque qui vous refuse l'octroi du prêt demandé. Il s'avère qu'il n'y a pas eu d'intervention d'un conseiller de banque, mais que la demande a été calculée à l'aide d'un logiciel qui évalue votre demande sur base de statistiques et de ratios préétablis.

Vous avez alors le droit d'exiger que votre dossier soit réexaminé, et ce sur base d'une entrevue avec votre conseiller de banque qui devra vous recevoir pour écouter votre argumentation.

Lors de cet entretien, vous pouvez faire valoir de façon plausible que, par exemple, votre situation financière s'est récemment améliorée grâce à un héritage. Il se pourrait même que certains chiffres pris en compte soient inexacts ou qu'il y ait confusion avec un homonyme surendetté.



5. LE PRINCIPE DE LOYAUTÉ

La collecte, l'enregistrement, l'utilisation et la transmission de vos données personnelles doivent se faire de bonne foi, et non pas à votre insu.

En outre, vos données doivent être effacées ou rendues anonymes le plus rapidement possible. L'utilisation ultérieure de vos données personnelles à des fins autres que celles initialement prévues est en principe interdite.

EXEMPLE

Votre supermarché vous propose une carte de fidélité pour vous faire profiter de remises spéciales lors de vos achats ou d'une ristourne en fin d'année. Lors de vos futurs passages en caisse, le contenu de votre panier d'achat est enregistré et sert à établir un profil de consommation dont l'évolution sera régulièrement observée.

Si cela se fait à votre insu et si vous n'en avez pas été informé au moment d'y souscrire, le principe de loyauté est violé.

6. LE PRINCIPE DE SÉCURITÉ ET DE CONFIDENTIALITÉ

Vos données personnelles doivent être traitées de manière confidentielle et être stockées à des endroits et sur du matériel sûrs.

Celui qui traite vos données engage sa responsabilité en cas de non-respect de ce principe. Cette obligation lui incombe aussi en ce qui concerne le comportement de ses collaborateurs et doit être prise en compte dans les contrats conclus avec les sous-traitants (notamment les prestataires de services) et dans le choix des équipements techniques (dans le cadre de la sécurité informatique).

EXEMPLE

Vous voulez changer de réseau de téléphone mobile GSM. Or, après l'étude de votre dossier, le délégué commercial de la société que vous venez de choisir vous refuse comme nouveau client. Cette personne, anciennement agent commercial auprès de votre précédent opérateur de GSM, se réfère à un litige que vous avez eu avec cette société au sujet du montant d'une facture.

En permettant à ses agents commerciaux de se procurer des informations du département comptable, votre précédent

opérateur de GSM a omis de veiller à ce que les informations personnelles concernant ses clients soient accessibles seulement à ceux de ces employés qui en ont réellement besoin pour leur travail.

Est-ce que le personnel a été par ailleurs suffisamment mis en garde contre les tentations d'utilisation abusive des données relatives à la clientèle ? Comment l'agent commercial a-t-il pu emmener un fichier client de son ancien vers son nouvel employeur ? Y a-t-il eu vol de fichier ?

En tout état de cause, les mesures de sécurité et l'organisation interne de l'entreprise étaient défectueuses pour assurer la confidentialité des données à caractère personnel. La responsabilité pourrait en être attribuée à la direction qui a failli à ses obligations légales, tout comme à l'égard de l'employé indélicat.

7. LE PRINCIPE DE TRANSPARENCE

La loi vous garantit l'information nécessaire relative aux traitements auxquels sont soumises des données vous concernant et vous assure la possibilité d'un contrôle personnel. Celui qui souhaite traiter vos données personnelles devra

vous avertir respectivement dès la collecte des données et en cas de transmission de vos données à des tiers.

Vous avez le droit de demander des renseignements quant aux données personnelles enregistrées et quant à leur utilisation ainsi que de faire effacer des informations dont le traitement ne serait pas conforme à la loi.

L'enregistrement de toutes les bases de données auprès de la Commission nationale pour la protection des données contribue à la transparence. Ce registre public des traitements de données personnelles pourra être consulté sur son site Internet³.

EXEMPLE

Étant donné que vous êtes régulièrement épuisé, votre médecin traitant vous prescrit une analyse de sang afin de déterminer les causes de votre fatigue. La prise de sang est réalisée par un laboratoire externe qui transmet les résultats de cette analyse à votre médecin. Il s'avère qu'un dépistage HIV a été réalisé à votre insu.

Ceci constitue une transgression des principes de transparence et de loyauté.

³ www.cnpd.lu Mise en ligne prévue pour fin 2004.

8. CERTAINES DONNÉES PARTICULIÈREMENT SENSIBLES SONT SOUMISES À UNE PROTECTION ENCORE RENFORCÉE

Le traitement d'informations vous concernant qui font apparaître vos opinions et convictions ou qui sont en rapport avec votre état de santé et votre vie sexuelle, y compris vos données génétiques, est interdit, hormis quelques exceptions énumérées de façon limitative par la loi.

De plus, la Commission nationale pour la protection des données devra en principe autoriser expressément le traitement de ce type de données.

EXEMPLE

Lors d'un entretien d'embauche, le directeur des ressources humaines de l'entreprise auprès de laquelle vous postulez vous pose des questions relatives à votre opinion au sujet du financement des retraites et aux points de vue respectifs des partis politiques à ce sujet. Parallèlement, il vous signale qu'il tient un relevé des salariés membres de syndicats.

Or recueillir des informations de cette nature (données sensibles) est normalement interdit par la loi.

9. LA SURVEILLANCE (AUDIO, VIDÉO, DONNÉES) DE PERSONNES IDENTIFIABLES EST STRICTEMENT LIMITÉE PAR LA LOI

Une autorisation de la Commission nationale pour la protection des données est nécessaire avant de recourir à des moyens techniques pour surveiller des personnes, notamment par caméra vidéo, traçage informatique, etc. Le traitement de vos données personnelles ainsi recueillies n'est possible que dans des cas de figure bien précis, énumérés par la loi. Ceci inclut la surveillance dans les lieux publics, les moyens de transport et les centres commerciaux ainsi que sur votre lieu de travail. Dans ce dernier cas, elle ne pourra se faire que si vous-même, respectivement le comité mixte, la délégation du personnel ou l'Inspection du travail et des mines avez été informés au préalable.

EXEMPLE

Vos conversations téléphoniques sont enregistrées par votre entreprise sans que vous en ayez été averti auparavant.

Ceci est contraire au principe de transparence. Par ailleurs, l'employeur doit disposer de l'autorisation de la Commission

... nationale pour la protection des données à qui il appartient de vérifier la légitimité et la proportionnalité d'une telle pratique.

10. L'UTILISATION DE VOS DONNÉES À DES FINS DE PUBLICITÉ OU DE DÉMARCHAGE COMMERCIAL EST SOUMISE À VOTRE AUTORISATION EXPRESSE

Vous pouvez à tout moment interdire l'utilisation de vos données personnelles à des fins commerciales. Le marketing direct à l'aide des moyens de communication modernes (SMS, e-mail, etc.) est en principe interdit si vous n'y avez pas marqué votre accord.

EXEMPLE

Vous êtes assailli de courrier publicitaire personnalisé.

Vous pouvez demander aux magasins et sociétés commerciales d'arrêter l'envoi de ces courriers.

Il s'avère que le commerçant a reçu votre adresse par votre club sportif qui lui a transmis les coordonnées personnelles de tous les membres du club dont il est le sponsor. Le



club sportif n'aurait pas dû communiquer son fichier de membres alors que les données qui y figurent devaient servir exclusivement à la gestion du club et à l'organisation de ses activités.

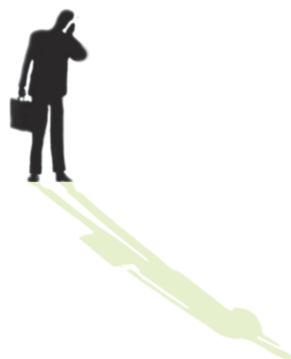
Le détournement de finalité constitue une utilisation illicite de données personnelles qui est punie par la loi.



VOS DROITS DE CITOYEN



La loi sur la protection des données à caractère personnel tend à assurer une transparence en matière de traitement de vos données personnelles et encourage une certaine autodétermination de chaque citoyen. Elle vous confère des droits permettant de vérifier vous-même ce qu'il advient de vos données personnelles.



1. LE DROIT À L'INFORMATION

Vous devez être informé au moment même de la collecte des informations, au plus tard lors de l'enregistrement. Les finalités pour lesquelles vos données sont utilisées doivent être portées à votre connaissance par l'Administration, l'entreprise, le professionnel ou l'association qui collecte et traite les données personnelles. Il en est de même si celui qui traite vos données personnelles envisage de les transmettre à des tiers.

2. LE DROIT D'ACCÈS À VOS INFORMATIONS PERSONNELLES

Vous avez le droit d'accéder à vos données personnelles et d'obtenir une copie de celles-ci. Vous pouvez réclamer que des informations inexactes ou inadéquates soient rectifiées, voire supprimées.

3. LE DROIT DE VOUS OPPOSER AU TRAITEMENT DE VOS DONNÉES PERSONNELLES

Vous avez le droit de vous opposer au traitement de vos données à caractère personnel pour des motifs légitimes tenant à votre situation particulière.

En tout état de cause, vous pouvez vous opposer, sans devoir fournir aucune justification, à l'utilisation de vos données à des fins de prospection et notamment pour des raisons commerciales ou de démarchage à orientation idéologique (partis politiques, syndicats, églises et groupements religieux, etc.).

4. LE DROIT D'INFORMATION SUR DES PROCESSUS DE DÉCISION AUTOMATISÉS

Pour des décisions qui sont prises sur base de processus automatisés (p.ex. approbation d'une demande de crédit de consommation ou d'un contrat d'assurance), vous avez le droit d'être informé sur la logique qui commande ce processus automatisé. L'entreprise ou l'organisme concerné doit vous accorder la possibilité de faire valoir votre point de vue et de contester, le cas échéant, la décision.



QUAND ET COMMENT **FAIRE VALOIR SES DROITS ?**





1. LA CONSULTATION DU REGISTRE PUBLIC

La Commission nationale pour la protection des données a établi un registre public des traitements de données qui est accessible sur Internet ⁴.

Ce registre public des traitements de données vous permet de vérifier si telle ou telle Administration, entreprise, association, professionnel ou indépendant est susceptible de détenir des informations concernant votre personne et s'il/si elle a déclaré

ce traitement auprès de la Commission nationale pour la protection des données. Chaque base de données et chaque traitement de données doivent en effet respectivement lui être notifiés et autorisés séparément. Celui qui a obtenu l'autorisation d'installer un système de surveillance n'est par exemple pas dispensé pour autant de notifier qu'il gère un fichier clientèle.

⁴ www.cnpd.lu

2. LA RÉCLAMATION DIRECTE

Vous pouvez faire valoir vos droits d'accès et de rectification à tout moment directement auprès de l'Administration, l'entreprise, l'association, le professionnel ou l'indépendant dès la collecte, l'enregistrement, l'utilisation ou le traitement de vos données personnelles. Vous pouvez donc demander à être renseigné sur la finalité du traitement, c'est-à-dire les buts poursuivis. Celui qui traite vos données doit vous informer sur les données précises stockées vous concernant afin que vous puissiez en vérifier l'exactitude, la pertinence et la nécessité du stockage, compte tenu de la finalité poursuivie par celui qui traite vos données.

Adressez votre demande de renseignements par écrit, de préférence par courrier recommandé, en y joignant une copie de votre carte d'identité. Le renseignement sur le traitement de données personnelles doit être obtenu gratuitement.

3. LA PLAINTÉ AUPRÈS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Si votre réclamation adressée directement à l'Administration, l'entreprise, l'association, le professionnel ou l'indépendant est restée sans suite, vous pouvez envisager de vous adresser à la Commission nationale pour la protection des données.

La Commission nationale a notamment pour mission de traiter toute réclamation émanant des personnes concernées. Elle peut interdire un traitement de données en cas de non-respect de la loi. Elle peut aussi ordonner la suppression de données et saisir le procureur d'État. Des peines pourront être prononcées en cas d'infraction.

Il est vivement recommandé de soumettre votre réclamation par écrit en expliquant de façon détaillée le problème constaté.

4. LA SAISINE DU TRIBUNAL

Si les suites données par la Commission nationale pour la protection des données ne vous paraissent pas satisfaisantes, vous êtes toujours en droit de saisir le tribunal. Dans pareil cas, il sera sans doute nécessaire de contacter un avocat qui pourra vous conseiller.

Une action en justice est également indispensable si vous voulez réclamer des dommages et intérêts en cas de violation de vos droits en matière de vie privée.

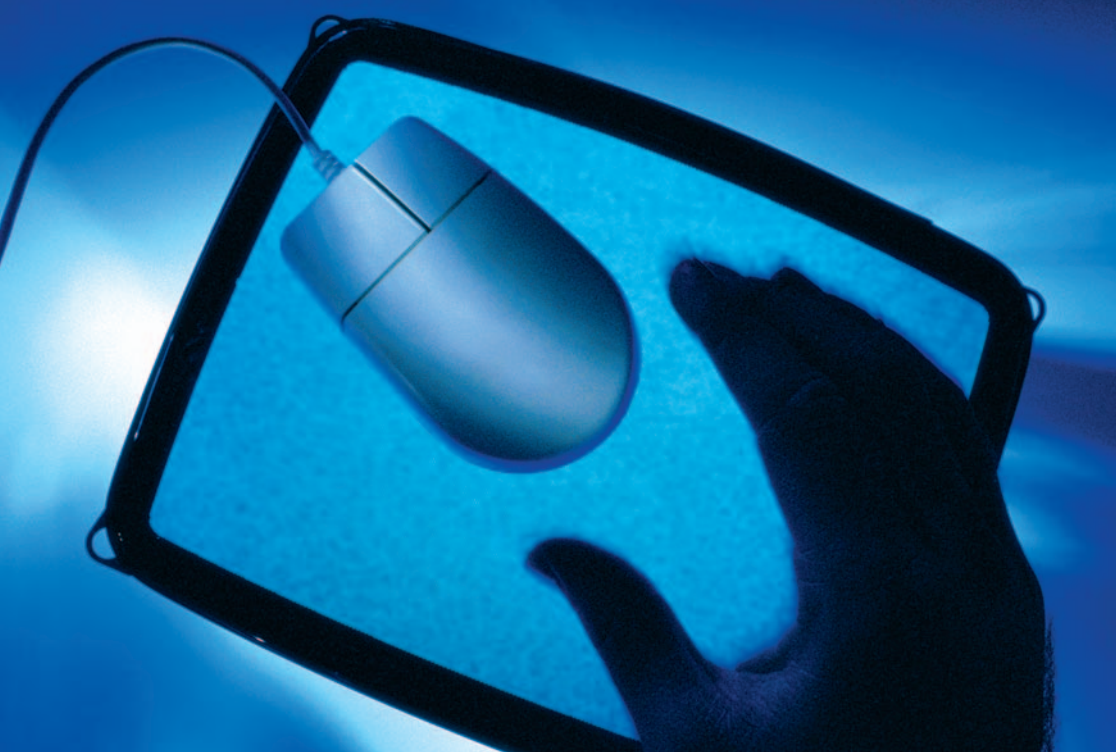


LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES : L'ARBITRE DU JUSTE ÉQUILIBRE



La législation en matière de protection des données à caractère personnel recherche le juste équilibre entre la société de l'information et la protection de la vie privée.

En maintenant la balance en équilibre entre les intérêts de ceux qui souhaitent légitimement obtenir et utiliser des informations vous concernant et votre attente naturelle à pouvoir compter sur le respect d'un certain anonymat et sur la prise de précautions particulières à l'égard de certaines données intimes, elle contribue à établir un climat de confiance entre les citoyens et les acteurs publics et privés détenant ces données, professionnels du domaine commercial ou non. Un tel climat de confiance favorise également le développement des activités écono-



miques faisant appel aux technologies modernes (e-commerce), la modernisation de l'Administration (e-Government) et la libre circulation de l'information.

Le rapprochement, sur un plan communautaire, des législations nationales en matière de protection des données est devenu indispensable pour lever les obstacles à la libre circulation des données au sein du marché unique. La directive européenne vise à établir ainsi à travers toute l'Europe un niveau de protection équivalent des droits et libertés des personnes à l'égard du traitement de leurs données personnelles. C'est pourquoi la directive a aussi pu lever tous les obstacles en matière de flux transfrontaliers de données personnelles au sein de l'Union euro-

péenne, tout en posant des conditions strictes limitant la circulation vers des pays n'assurant pas un niveau de protection adéquat.

Au Luxembourg, la Commission nationale pour la protection des données est l'autorité de contrôle indépendante compétente en cette matière, tant pour le secteur public que privé.

Adresse de contact :



**Commission nationale
pour la protection des données**

68, route de Luxembourg
L-4100 Esch-sur-Alzette
Tél. : 26 10 60-1 / Fax : 26 10 60-29
info@cnpd.lu / www.cnpd.lu

GLOSSAIRE DES TERMES LES PLUS COURANTS EN MATIÈRE DE PROTECTION DES DONNÉES





1. DONNÉE À CARACTÈRE PERSONNEL

Toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable. Une personne physique (le citoyen) ou morale (surtout les entreprises) est réputée identifiable si elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.

2. TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données. Il s'agit de la collecte, de l'enregistrement, de l'organisation, de la conservation, de l'adaptation ou de la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, de la diffusion ou toute autre forme de mise à disposition de données, du rapprochement ou de l'interconnexion ainsi que du verrouillage, de l'effacement ou de la destruction de données.

3. FICHER DE DONNÉES À CARACTÈRE PERSONNEL

Tout ensemble structuré de données accessibles selon des critères déterminés, qu'il soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

4. RESPONSABLE DU TRAITEMENT

La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui (seul ou conjointement avec d'autres) détermine les finalités et les moyens du traitement de données à caractère personnel.

5. INTERCONNEXION

Toute forme de traitement qui consiste en la corrélation de données traitées pour une finalité avec des données traitées pour des finalités identiques ou liées par un ou plusieurs autres responsables du traitement.

6. FINALITÉ

C'est l'objectif choisi avant la mise en œuvre du traitement qui se trouve à la base de la détermination des opérations à effectuer pour l'atteindre ou espérer l'atteindre et de la détermination des données soumises à ces opérations. Il ne peut donc être question d'englober dans une finalité un ensemble d'objectifs flous et trop nombreux. La détermination de la finalité ou des finalités liées du traitement est un élément essentiel pour évaluer la légitimité du traitement.

7. CONSENTEMENT DE LA PERSONNE CONCERNÉE

Toute manifestation de volonté expresse, non-équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou statutaire accepte que les données à caractère personnel fassent l'objet d'un traitement.

EDITEUR SIP EN COLLABORATION AVEC LA CNPD DATE 08 | 2004 LAYOUT MV-CONCEPT.LU IMPRIMERIE ?



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Service Information et Presse

*Pour de plus amples
renseignements
au sujet de la protection
des données :*



COMMISSION NATIONALE
POUR LA PROTECTION
DES DONNÉES

33, BD ROOSEVELT L-2450 LUXEMBOURG

TÉL. : [+352] 478-2181 / FAX : [+352] 46 74 83

WWW.GOUVERNEMENT.LU

ADRESSE POSTALE : L-4100 ESCH-SUR-ALZETTE

TÉL. : [+352] 26 10 60-1 / FAX : [+352] 26 10 60-29

INFO@CNPD.LU / WWW.CNPD.LU