PROTECTION DES DONNEES DANS L'UNION EUROPEENNE

TABLE DES MATIERES

INTRODUCTION

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance

- Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

L'information relative aux personnes, désignée comme "données à caractère personnel", est recueillie et utilisée dans de nombreux aspects de la vie quotidienne. Par exemple, un individu fournit des données personnelles lorsqu'il/elle sollicite l'inscription à une bibliothèque, s'inscrit à un club de gymnastique, ouvre un compte bancaire etc. Les données nominatives peuvent être recueillies directement auprès de la personne ou extraites d'une base de données existante. Ces données peuvent être utilisées par la suite à d'autres fins et/ou partagées avec des tiers. Les données personnelles peuvent être toute information identifiant une personne, telle qu'un nom, un numéro de téléphone, ou une photographie.

Les progrès de la technologie informatique, tout comme les nouveaux réseaux de télécommunications, permettent aux données personnelles de passer les frontières avec une grande facilité. Par voie de conséquence, les données concernant les citoyens d'un Etat membre sont souvent exploitées dans d'autres Etats membres de l'UE. Les données personnelles étant recueillies et échangées plus fréquemment, une réglementation concernant les transferts de données est nécessaire.

De façon générale, les législations nationales relatives à la protection des données exigent de bonnes pratiques de gestion des données de la part des organes gérant les données, dénommés "responsables de fichiers". Ces derniers ont ainsi l'obligation de gérer les données loyalement et dans des conditions sûres, et d'utiliser les données personnelles à des fins explicites et légitimes. Les législations nationales ont aussi garanti une série de droits aux personnes, tels le droit d'être informées lorsque des données personnelles sont traitées et de s'en voir communiqué la raison, le droit d'accéder aux données et, le cas échéant, le droit de faire modifier ou supprimer les données.

Bien que les législations nationales relatives à la protection des données visent à garantir les mêmes droits, certaines différences existaient. Ces différences pouvaient créer des obstacles potentiels à la libre circulation de l'information et constituer des fardeaux supplémentaires pour les opérateurs économiques et les citoyens. Au nombre de ces entraves, on peut citer l'obligation de s'enregistrer ou d'être autorisé à gérer des données par des autorités de surveillance dans plusieurs Etats membres, la nécessité de se conformer à des normes différentes, et la possibilité d'être interdit de transfert de données vers d'autres Etats membres de l'UE. De surcroît, certains Etats membres ne disposaient pas de législation en matière de protection des données.

Pour toutes ces raisons, il était nécessaire d'agir au niveau européen, et les directives CE s'inscrivent dans cette perspective.

LA LEGISLATION EUROPEENNE EN MATIERE DE PROTECTION DES DONNEES

Afin de lever les obstacles à la libre circulation des données sans diminuer la protection des données personnelles, la directive 95/46/CE (directive protection des données) fut mise au point pour harmoniser les dispositions nationales dans ce domaine.

Il en résulte que les données personnelles de tous les citoyens disposeront d'une protection équivalente dans l'ensemble de l'Union. Les quinze Etats membres de l'UE étaient tenus d'aligner leur législation nationale sur les dispositions de la directive d'ici au 24 octobre 1998.

Une directive est un acte législatif européen dont les Etats membres sont destinataires. Une fois cette législation adoptée au niveau européen, chaque Etat membre doit en assurer la transposition efficace dans son système juridique. La directive prescrit un résultat final. La forme et les méthodes d'application sont laissées à l'appréciation de chaque Etat membre. En principe, une directive prend effet moyennant des mesures nationales d'application (législation nationale). Toutefois, il est possible que même lorsqu'un Etat membre n'a pas encore appliqué une directive, certaines des dispositions de celle-ci puissent avoir un effet direct. Ceci signifie que si une directive confère des droits directs aux personnes, des personnes peuvent arguer de la directive devant un juge sans avoir à attendre la transposition de cette directive dans la législation nationale. De surcroît, si les personnes estiment avoir subi un préjudice du fait que les autorités nationales n'ont pas transposé la directive correctement, elles peuvent être habilitées à engager des poursuites en dommages-intérêts. Ces dommages ne peuvent être obtenus qu'auprès des tribunaux nationaux.

La directive protection des données s'applique à "toute opération ou ensemble d'opérations appliquées à des données à caractère personnel", désignées comme "traitement des données". Ces opérations comprennent la collecte des données personnelles, leur conservation, leur diffusion etc. La directive s'applique aux données traitées par des moyens automatisés (par exemple une base de données informatique de clients) ainsi qu'aux données faisant partie ou destinées à faire partie de fichiers non automatisés dans lesquels celles-ci sont accessibles suivant des critères spécifiques. (Par exemple, les fichiers papiers traditionnels, tels qu'un fichier sur cartes dans lequel les données de la clientèle sont rangées par ordre alphabétique).

La directive protection des données ne s'applique pas aux données traitées à des fins strictement personnelles ou pour des activités liées aux ménages (par exemple un agenda personnel électronique ou un fichier ne répertoriant que la famille ou l'entourage). Elle ne s'applique pas non plus à des domaines tels que la sécurité publique, la défense ou le droit pénal, qui ne sont pas du ressort de la CE et demeurent une prérogative nationale. La législation nationale assure généralement la protection des personnes dans ces domaines.

Il existe en outre une directive distincte, la directive 97/66/CE qui traite plus particulièrement de la protection de la vie privée dans le secteur des télécommunications. Cette directive stipule que les Etats membres doivent garantir la confidentialité de la

communication par le biais de réglementations nationales. Ceci signifie que toute écoute, interception, stockage ou autre type d'interception ou de surveillance des communications non autorisés est illégal. Lorsque l'identification de la ligne appelante est offerte, les utilisateurs doivent avoir la possibilité de ne pas souscrire à ce service ou de ne pas voir leur identité dévoilée lorsqu'ils passent un coup de téléphone. À l'inverse, les abonnés à ce service doivent avoir la possibilité de rejeter les appels entrants en provenance de personnes ayant bloqué leur identification de ligne appelante. De surcroît, la directive stipule que lorsque des annuaires de télécommunications imprimés ou électroniques existent, les abonnés ont le droit d'obtenir gratuitement la non-inscription à ces annuaires.

QUI PEUT ÊTRE UNE PERSONNE CONCERNÉE ? NOUS SOMMES TOUS DES PERSONNES CONCERNÉES

CHAQUE FOIS QUE VOUS RÉSERVEZ UN VOL, QUE VOUS VOUS PRÉSENTEZ À UN EMPLOI, QUE VOUS UTILISEZ UNE CARTE DE CRÉDIT, OU QUE VOUS SURFEZ SUR INTERNET, VOUS DÉVOILEZ CERTAINES DONNÉES PERSONNELLES.

DEONTOLOGIE DU MAITRE DE FICHIERS

Qui peut être maître de fichiers ?

Les maîtres de fichiers sont les personnes ou l'organisme "qui déterminent les objectifs et les moyens du traitement", tant dans le secteur public que dans le secteur privé. Un médecin traitant est généralement le détenteur des données traitées sur sa clientèle ; une société est la détentrice des données traitées sur ses clients et salariés ; un club sportif contrôle les données traitées sur ses membres et une bibliothèque publique les données traitées sur ses utilisateurs.

Les maîtres de fichiers sont tenus d'observer plusieurs principes. Ces principes visent non seulement à protéger les personnes concernées, mais constituent également une déclaration de saine pratique commerciale contribuant à un traitement des données fiables et efficaces.

Chaque maître de fichiers doit adhérer aux règles de traitement des données de l'Etat membre où il ou elle est établi(e), même si les données traitées appartiennent à une personne résidant dans un autre Etat. Lorsque le maître de fichiers n'est pas établi dans la Communauté (par exemple une société étrangère, il ou elle doit se conformer aux lois de(s) l'Etat(s) membre(s) si l'équipement de traitement (par exemple un centre informatique) est situé au sein de la Communauté européenne.

LES RÈGLES SONT LES SUIVANTES :

- les données doivent être traitées loyalement et légalement ;
- elles doivent être collectées à des fins explicites et légitimes et utilisées en conséquence ;
- les données doivent être pertinentes et non excessives rapportées à l'usage auquel elles sont destinées ;
- les données doivent être précises, et le cas échéant, tenues à jour ;
- les maîtres de fichiers sont tenus de prévoir des dispositifs raisonnables permettant aux personnes concernées de rectifier, effacer ou verrouiller les données incorrectes les concernant ;
- les données identifiant des personnes ne doivent pas être conservées plus longtemps qu'il n'est nécessaire ;
- la directive stipule que chaque Etat membre doit prévoir une ou plusieurs autorités de surveillance de manière à assurer le suivi de l'application de la directive. Une responsabilité de l'autorité de surveillance consiste à tenir un registre public à jour de façon que le grand public ait accès aux noms de tous les maîtres de fichiers et aux types de traitements que ceux-ci effectuent.

- En principe, tous les maîtres de fichiers doivent aviser les autorités de surveillance lorsqu'ils traitent des données. Les Etats membres peuvent prévoir une simplification ou une exemption de notification pour des types spécifiques de traitement n'impliquant pas de risques particuliers. Les procédures d'exception et de simplification peuvent également être autorisées, lorsqu'en conformité avec la législation nationale, un responsable indépendant en charge de la protection des données a été désigné par le maître de fichiers. Les Etats membres peuvent exiger une vérification préalable, à conduire par l'autorité de surveillance, avant que ne soient entreprises des opérations de traitement impliquant des risques particuliers. Il appartient aux Etats membres de déterminer quels types d'opérations de traitement impliquent des risques particuliers.

Quand les données personnelles peuvent-elles être traitées ?

Les données personnelles ne peuvent être traitées (à savoir recueillies et exploitées) que si :

* la personne concernée a sans ambiguïté marqué son accord, à savoir a librement et spécifiquement consenti après avoir été dûment informée ;

* le traitement des données est nécessaire à l'exécution d'un contrat ou pour souscrire un contrat sollicité par la personne concernée, à savoir, traitement des données à des fins de facturation ou traitement des données relatives à un candidat à un emploi ou à l'octroi d'un prêt ;

* le traitement est exigé par la loi ;

* le traitement des données est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée. Un exemple est celui d'un accident d'automobile à la suite duquel la personne concernée se trouve dans un état d'inconscience : des auxiliaires médicaux d'urgence sont autorisés à communiquer les résultats de tests sanguins, si ceux-ci sont jugés essentiels pour sauver la vie de la personne ;

* le traitement est nécessaire pour effectuer des missions d'intérêt public ou des missions effectuées par des instances officielles (telles que le gouvernement, les administrations fiscales, la police etc.) ;

* enfin, les données peuvent être traitées à chaque fois que le maître de fichiers ou un tiers a un intérêt légitime à le faire. Cependant, cet intérêt ne peut outrepasser l'intérêt de protection ou les droits et libertés fondamentaux de la personne concernée, et notamment de son droit à la vie privée. Cette disposition établit la nécessité de trouver dans la pratique un équilibre raisonnable entre l'intérêt commercial des maîtres de fichiers et la vie privée des personnes concernées. Cet équilibre est d'abord évalué par les maîtres de fichiers sous le contrôle des autorités en charge de la protection des données bien que la décision finale appartienne le cas échéant aux tribunaux ;

Données sensibles

Des règles draconiennes s'appliquent au traitement des données sensibles : il s'agit des données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux croyances religieuses ou philosophiques, à l'appartenance syndicale, à la santé ou aux préférences sexuelles. En principe, les données de ce type ne peuvent être traitées. Des dérogations sont tolérées dans des circonstances très spécifiques. Ces circonstances incluent le traitement des données si la personne concernée a donné son consentement explicite, les traitements exigées par la législation sur l'emploi, des cas dans lesquels la personne peut être dans l'impossibilité de donner son consentement (par exemple test sanguin sur la victime d'un accident de la route), du traitement de données ayant été publiquement annoncées ou du traitement de données effectuées sur leurs membres par des syndicats, partis politiques ou congrégations. Les Etats membres peuvent prévoir des exceptions supplémentaires dans certains cas, à savoir pour la protection d'intérêts publics jugés vitaux.

La directive s'applique-t-elle au transfert de données sur Internet ?

Il serait relativement illogique et dépourvu de justification juridique d'exempter de la directive sur la protection des données un moyen de transfert aussi important qu'Internet. Force est de convenir au contraire que le simple volume et la nature protéiforme des données personnelles transmises par Internet dans le monde entier, y compris à destination de pays ne disposant pas de protection adéquate, requièrent une attention particulière. La directive protection des données est donc technologiquement neutre: ses dispositions s'appliquent quels que soient les moyens techniques utilisés pour traiter les données personnelles. Par exemple, la directive s'applique à la collecte invisible de données personnelles sur Internet (par ex. les "cookies" utilisés pour repérer les habitudes de consultation de chacun). A l'inverse, si les données personnelles sont recueillies de façon "visible", on pourrait faire valoir l'argument suivant lequel un individu transférant ses propres données a donné son accord à un tel transfert, à condition que celui-ci soit convenablement informé des risques impliqués.

Q. Une personne reçoit en permanence des messages électroniques non sollicités. Comment faire pour l'éviter, dans la mesure où ces messages émanent de nombreuses sources?

R. La personne dispose du droit de s'opposer au traitement de ses données à des fins de marketing direct. En outre, la personne peut exiger de son fournisseur de services Internet qu'il installe des filtres à courrier ou bien il peut contacter une des associations se vouant à la prévention du "junk mail" (CAUCE, Privacy International, etc). D'autres services existent pour aider à se prémunir du "junk e-mail" tels que www.spamfree.org . Si le problème persiste, la personne peut écrire à son autorité de surveillance nationale.

VOS DROITS EN TANT QUE PERSONNE CONCERNEE

Vous disposez du droit d'être informé de tout traitement des données lorsque vous êtes la personne concernée.

Les maîtres de fichiers sont tenus de vous informer à chaque fois qu'ils recueillent des données personnelles vous concernant, à moins que vous ne l'ayez été au préalable. Vous disposez du droit d'être informé des éléments suivants : l'identité du maître de fichiers, l'objectif du traitement (parfois, les catégories de données doivent être expliquées), les destinataires des données et les droits spécifiques dont ceux-ci disposent en tant que personnes concernées. Vous avez le droit de recevoir cette information, que les données aient été obtenues directement ou indirectement auprès de tiers. Une dérogation peut être accordée dans ce dernier cas si livrer cette information s'avère impossible ou extrêmement difficile.

Vous disposez du droit d'accès aux données vous concernant.

Vous êtes autorisé à prendre contact avec tout maître de fichiers pour déterminer s'il traite ou non des données personnelles vous concernant, pour recevoir un exemplaire de ces données sous une forme intelligible ainsi que toute information disponible concernant leurs sources. Si les données personnelles sont inexactes, ou si celles-ci ont été traitées de façon frauduleuse, vous avez le droit de solliciter la correction ou l'effacement des données. Dans ces cas, la personne concernée peut également exiger du maître de fichiers qu'il notifie les tiers auxquels avaient été précédemment communiquées les données incorrectes, à moins que cela ne s'avère impossible. Une redevance raisonnable peut être prélevée dans certains cas pour assurer l'accès.

Vous devez également avoir accès à la logique présidant aux décisions automatisées.

Des décisions affectant de façon significative la personne concernée, telles que la décision d'octroyer un prêt ou de délivrer une police d'assurance, peuvent être prises sur la seule base du traitement automatisé des données. Le maître de fichiers doit donc adopter des sauvegardes adéquates, pouvant consister à fournir à la personne concernée l'occasion de discuter du motif de la collecte des données ou de contester les décisions basées sur des données erronées.

Exceptions et limitations

Le droit à la vie privée peut parfois entrer en conflit avec la liberté d'expression, et en particulier la liberté de la presse et des médias. Il appartient donc aux Etats membres d'établir des exceptions dans leur législation en matière de protection des données de façon à trouver un équilibre entre ces droits différents mais tout aussi fondamentaux.

La législation nationale peut autoriser d'autres exceptions aux dispositions de la directive. (Il peut s'agir de l'obligation d'informer la personne concernée ; de la publicité à donner aux opérations de traitement des données ; de l'obligation de respecter les principes de base d'une bonne pratique de gestion des données.) Ces exceptions sont autorisées si celles-ci sont nécessaires notamment pour des motifs de sécurité nationale, de défense, de recherches criminelles, d'application du droit pénal, ou encore pour protéger les

personnes concernées ou les droits et la liberté de tiers. En outre, une dérogation au droit d'accéder aux données peut être accordée dans le cas des données traitées à des fins scientifiques ou statistiques.

QUE POUVEZ-VOUS FAIRE SI VOS DROITS SONT ENFREINTS?

Si vous craignez que vos droits n'aient été enfreints, votre première démarche doit consister à contacter la personne qui paraît être à la source de la violation afin de connaître l'identité du maître de fichiers.

Si vous n'obtenez pas alors de résultat satisfaisant, vous pouvez contacter votre administration nationale de protection des données. D'après la directive, chaque Etat membre doit disposer d'une ou plusieurs autorités publiques pour assurer la bonne application de la législation en matière de protection des données. Cette autorité, souvent désignée sous l'appellation d'autorité de surveillance, est compétente pour entendre les plaintes introduites par toute personne ou entreprise. L'autorité de surveillance doit étudier la plainte et peut interdire temporairement le traitement. Si l'autorité de surveillance estime qu'il y a eu infraction à la législation en matière de protection des données, l'autorité de surveillance peut ordonner, entre autres choses, l'effacement ou la destruction des données et/ou interdire tout traitement ultérieur.

Q. Un fournisseur de télécommunications a livré à une autre société des informations concernant votre compte client (téléphone ou courrier électronique). En conséquence, vous recevez des appels ou des messages électroniques non sollicités. Que pouvez-vous faire?

R. Si les données personnelles ont été collectées à des fins de facturation uniquement et si vous n'avez pas donné votre accord en vue d'un transfert ultérieur de vos données, vous êtes habilité à faire opposition au transfert de vos données à des tiers. La première démarche doit consister à écrire à votre prestataire de services, en exposant clairement votre plainte. Si vous ne recevez pas de réponse satisfaisante, vous devez alors contacter l'autorité nationale de surveillance.

Q. Un prêt vous est refusé en raison d'inexactitudes dans le fichier d'une banque. Vous introduisez une demande d'accès auprès de votre banque pour connaître les informations qui étaient enregistrées dans l'ordinateur de la banque concernant vos antécédents en matière de crédit. La banque refuse toutefois de répondre à votre demande d'accès. Vous adressez plusieurs appels téléphoniques à la banque concernant cette demande mais en vain. Quelle doit être votre démarche suivante?

R. La directive stipule que vous disposez du droit d'accéder "sans délai excessif" à toute donnée personnelle vous concernant. Si les données sont inexactes, vous avez le droit de les rectifier. Par conséquent, si vous ne recevez pas de réponse de la banque dans un délai raisonnable, vous pouvez adresser votre plainte directement à l'autorité nationale de surveillance. D'après la directive, l'autorité nationale de surveillance doit étudier la plainte et informer le plaignant du résultat.

Pour contacter l'autorité de surveillance il vous faut (de préférence par écrit) décrire le problème et présenter suffisamment d'informations pour permettre de le bien cerner. Dans certains Etats membres, l'autorité de surveillance dispose de formulaires types que vous pouvez remplir pour adresser une plainte. Dans le cas où cette formule existe, vous devez employer ces formulaires car ils permettront d'accélérer le traitement de votre dossier et vous recevrez une réponse plus rapidement. Dans certains Etats membres, les

plaintes peuvent être adressées par courrier électronique. Dans d'autres, ceci n'est pas encore possible.

Si vous n'obtenez pas de résultat satisfaisant, vous devrez peut-être aller devant les tribunaux. Dans ce cas, vous serez bien avisé de solliciter un conseil juridique. Aller devant les tribunaux peut également être nécessaire si vous avez subi des préjudices en raison de la violation de vos droits. Vous pouvez avoir droit à des dommages-intérêts.

Q. Votre employeur a communiqué votre dossier médical à votre banque sans solliciter votre autorisation. Le dossier médical comportait des informations dont le contenu peut expliquer pourquoi votre banque refuse de vous accorder un crédit hypothécaire. Avez-vous droit à des dommages-intérêts?

R. Vous avez droit à un dédommagement si vous avez subi un préjudice résultant de la communication illicite de vos données personnelles. Ceci peut être le cas si vos données médicales ont été communiquées sans votre accord.

Toute personne ou entreprise peut introduire une plainte devant la Commission en cas de présomption d'infraction au droit communautaire commise par un Etat membre.

La Commission européenne a pour responsabilité de faire en sorte que le droit communautaire soit appliqué dans de bonnes conditions dans les Etats membres. Le cas échéant, la Commission rappelle aux Etats membres leurs responsabilités pour ce qui est d'appliquer le droit communautaire dans les délais et pour en assurer une mise en vigueur correcte. Dans certains cas, si un Etat membre échoue à remplir ces obligations, la Commission peut se voir dans l'obligation d'entamer une action devant la Cour de justice européenne, qui détermine s'il y a eu ou non infraction au droit communautaire.

Vous n'aurez pas à prouver que vous êtes directement affecté par l'infraction que vous alléguez.
Cependant, les différends entre particuliers ne peuvent être réglés par la Commission dans ce contexte.

Les plaintes sont introduites gratuitement et peuvent être déposées sans l'assistance d'un avocat. Pensez à inclure toute information et documentation pertinentes (par exemple règles nationales applicables) lorsque vous déposez une plainte.

Vous pouvez introduire une plainte auprès de la Commission en écrivant à l'adresse suivante:
Commission des Communautés européennes (à l'attention du Secrétaire général), rue de la loi 200, B-1049 Bruxelles ;
ou en utilisant le formulaire de plainte type disponible sur demande auprès des bureaux de la Commission dans les Etats membres ou sur Internet:
http://europa.eu.int/comm/sg/lexcomm

TRANSFERTS DE DONNEES A DESTINATION DE PAYS NON MEMBRES DE L'UE

En cas de transfert de données vers des pays non membres de l'Union européenne, il peut être nécessaire de prendre des précautions particulières si le niveau de protection des données dans le pays tiers ne correspond pas à celui assuré par le droit européen. En l'absence de telles règles, les niveaux élevés de protection des données institués par la directive seraient rapidement sapés, compte tenu de la facilité avec laquelle les données peuvent être véhiculées dans les réseaux internationaux.

Le principe de la directive veut que les données personnelles ne puissent être transférées dans des pays extérieurs à l'UE, qu'à condition que ceux-ci garantissent un niveau "adéquat" de protection. Une analyse des législations en matière de protection des données et des dialogues avec les plus importants partenaires commerciaux de l'UE est en cours de manière à déterminer quels pays peuvent être considérés comme offrant une protection adéquate.

Lorsque un pays tiers n'assure pas un niveau de protection adéquat, la directive exige le blocage des transferts spécifiques. Les Etats membres doivent informer la Commission de toute mesure de blocage de ce type, ce qui déclenche une procédure communautaire visant à s'assurer que toute décision d'un Etat membre visant à bloquer un transfert spécifique soit étendue à l'UE dans son ensemble ou invalidée.

Que pourraient faire les sociétés appartenant à un pays non membre de l'UE?

Bloquer les transferts de données personnelles est une solution de dernier recours. Il existe d'autres moyens de s'assurer que les données continuent d'être protégées de façon adéquate sans entraîner de désorganisation des flux internationaux de données et des opérations commerciales auxquelles sont associées ces données. Si des entreprises de l'UE ne parviennent pas à déterminer si la législation ou les systèmes d'autoréglementation d'un pays non membre de l'UE assurent une protection adéquate, elles seraient bien avisées d'assurer elles-mêmes cette protection. Celle-ci pourrait être assurée au moyen d'un contrat liant la société envoyant les données et la société destinataire des données et n'appartenant pas à l'UE. L'objet d'un tel contrat serait d’offrir des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes. Si des garanties significatives sont appliquées, il ne devrait pas y avoir de raison pour un Etat membre de bloquer un transfert de données se rapportant à ses citoyens.

ADRESSES ET NUMEROS UTILES

COMMISSAIRES NATIONAUX POUR LA PROTECTION DES DONNEES

Autriche:
Österreischische
Datenschutzkommission
Ballhausplatz, 1
A – 1014 WIEN
Tel: +43/1/531.15.26.79
Fax: +43/1/531.15.26.90
Pas de site web

Belgique:
Commission de la protection de la vie privée
Adresse postale: Ministère de la Justice
Bd. de Waterloo, 115
B – 1000 BRUXELLES
Bureaux: Avenue de la Porte de Hall, 5-8
B – 1060 BRUXELLES
Tel: +32 (0)2/542.72.00
Fax: +32 (0)2/542.72.12
E-mail: privacy@euronet.be
http://www.privacy.fgov.be/

Danemark:
Datatilsynet
Christians Brygge, 28 - 4
DK-1559 KØBENHAVN V
Tel: +45/33.14.38.44
http://www.datatilsynet.dk/
Dt@datatilsynet.dk

Finlande:
Office of the Data Protection Ombudsman
P.O. Box 315
FIN-00181 Helsinki
Tel : +358/9/18251
http://www.tietosuoja.fi/

France:
Commission Nationale de l'Informatique et des Libertés
Rue Saint Guillaume, 21
F – 75340 PARIS CEDEX 7
Tel : +33/1/53.73.22.22
http://www.cnil.fr/

Allemagne:
Der Bundesbeauftragte für den Datenschutz
Postfach 20 01 12
D – 53131 BONN (Bad Godesberg)
Tel : +49/228/819.95.0
http://www.bfd.bund.de/

Grèce:
Hellenic Data Protection Authority
8 Omirou Street
106 54 Athens, Greece
Tel: +301/33.52.604-5
Fax: + 301/33.52.617
http://www.dpa.gr
contact@dpa.gr

Irlande:
Data Protection Commissioner
Irish Life Centre, Block 4
Talbot Street
DUBLIN 1 – IRL
Tel : +353/1/874.85.44
Pas de site web

Italie:
Garante per la protezione dei dati personali
Largo del Teatro Valle, 6
I – 00186 ROMA
Tel : +39/06/68.18.61
Pas de site web

Luxembourg:
Commission à la Protection des Données Nominatives
Ministère de la Justice
Boulevard Royal , 15
L – 2934 LUXEMBOURG
Tel : +352/478.45.46
Pas de site web

Pays-Bas:
College Bescherming Persoonsgegevens
Prins Clauslaan 20
Postbus 93374
NL - 2509 AJ ´s-GRAVENHAGE
Tel: +31/70/381.13.00
http://www.cbpweb.nl/

Portugal:
Comissão Nacional de Protecção de Dados Pessoais Informatizados
R. de S. Bento, 148 – 3º
P – 1200-821 LISBOA
Tel: (+351) 21.392 84 00
http://www.cnpd.pt

Espagne:
Agencia de Protección de Datos
Paseo de la Castellana, N 41, 5a planta
E - 28046 MADRID
Tel : +34/91/308.40.17
http://www.ag-protecciondatos.es/

Suède:
Datainspektionen
Fleminggatan, 14
9th Floor
Box 8114
S – 104 20 STOCKHOLM
Tel : +46/8/657.61.00
http://www.datainspektionen.se/

Royaume Uni:
Data Protection Commissioner
Water Lane
Wycliffe House
UK - WILMSLOW - CHESHIRE
SK9 5AF
Tel: +44/1625/54.57.45
http://www.dataprotection.gov.uk

Pays AELE

Islande:
Ministry of Justice Data Protection Commission
Arnarhvoll
IS - 150 REYKJAVIK
Tel : +354/560.90.10
Pas de site web

Norvège:
Datatilsynet
The Data Inspectorate
P.B. 8177 Dep
N – 0034 OSLO
Tel : +47/22/42.19.10
http://www.datatilsynet.no/

REPRESENTATIONS DE LA COMMISSION EUROPEENNE EN FRANCE

288, boulevard Saint-Germain
F-75007 PARIS
Tél. : +33 (0)1 40 63 38 00
Fax : +33 (0)1 45 56 94 17 / 18 / 19

2, rue Henri Barbusse
F-13241 MARSEILLE Cedex 01
Tél. : +33 (0)4 91 91 46 00
Fax : +33(0)4 91 90 98 07

POINTS DE CONTACT NATIONAUX POUR LE MARCHE UNIQUE
Pour les citoyens et les entreprises

Centre interministériel de renseignements administratifs (CIRA)
Cité Administrative
Boîte postale 2040
F-59014 LILLE Cedex
Tél. : +33 (0)3 20 49 49 49
Fax : +33(0)3 20 53 23 17

Bureau Union Européenne
Direction des relations économiques extérieures (DREE)
Ministère de l'économie, des finances et de l'industrie
M. Laurent Catenos
Télédoc 534
139, rue de Bercy
F-75572 PARIS Cedex 12
Tél. : +33 (0)1 53 18 82 42
Fax : +33 (0)1 53 18 88 78

DIALOGUE AVEC LES CITOYENS ET LES ENTREPRISES
Europe Direct numéro vert : 0800 90 9700
Internet : http://europa.eu.int/citizens
http://europa.eu.int/business

En composant ce numéro vert ou en consultant les sites Internet, vous pourrez également interroger le « service d'orientation » qui vous aidera à résoudre les pratiques liés à l'exercice de vos droits. Vous obtiendrez une réponse à votre question dans un délai de trois jours ouvrables ainsi que des conseils sur les démarches ultérieures à entreprendre pour prendre contact avec l'organisme le plus apte à vous aider au niveau européen, national ou local.