



Protecção
de **dados**
e vida privada

■



VIDA PRIVADA E TRATAMENTO DE DADOS DE CARÁCTER PESSOAL



ÍNDICE

A Protecção de Dados – O que é ?	6 _
Os 10 Mandamentos da Protecção de Dados Pessoais	10 _
Os seus direitos enquanto cidadão	18 _
Quando e Como fazer valer os seus direitos ?	22 _
A Comissão Nacional para a Protecção de Dados : o mediador do justo equilíbrio	26 _
Glossário dos conceitos mais utilizados ao nível da protecção de dados	28 _



A PROTECÇÃO DE DADOS – O QUE É ?



Na sociedade de informação em que hoje vivemos, existem vários organismos e instituições que colecionam cada vez mais informações sobre as pessoas.

Com efeito, cada um de nós disponibiliza, voluntária ou involuntariamente, um conjunto de dados pessoais a um grande número de organismos, como por exemplo :

- _ Administração Comunal ou Governamental (carta de condução, autorização ou subsídio) ;
- _ Finanças (declaração fiscal) ;
- _ Médicos e farmácias (consultas e receitas médicas) ;
- _ Segurança Social (reembolso das despesas de saúde) ;

- _ Instituições Bancárias (pedido de empréstimo, balanço de utilização do cartão de crédito) ;
- _ Supermercados (cartões de fidelidade, jogos, concursos) ;
- _ Operadores telefónicos de redes móveis e fixas (comunicações telefónicas) ;
- _ Clubes desportivos, associações culturais ou de tempos livres (cartão de membro) ;
- _ Ou simplesmente aquando de uma navegação na Internet ou de uma tarde de compras num centro comercial, devido ao registo de imagens pelos sistemas de vigilância.

Sendo assim, a circulação dos nossos dados pessoais multiplica-se e propaga-se a cada vez mais e diferentes locais.

Devido à modernização dos meios informáticos, a utilização desses dados tornou-se mais livre e multiforme, tanto ao nível do Estado, administrações, empresas e outros profissionais, como ao nível de clubes e associações.

A criação de perfis pessoais que revelam os nossos hábitos de vida e de consumo tornou-se uma prática corrente (sondagens, cartões cliente, Internet, ...).

Quer seja na recolha ou no registo de dados, passando pela sua utilização até à transmissão a terceiros, os riscos ligados à acumulação e à utilização dos dados pessoais, tornam-se cada vez mais reais.

No entanto, a perda do domínio sobre os seus dados, assim como as intrusões injustificadas na sua vida privada, não são uma fatalidade, muito pelo contrário. A lei de 2 de Agosto de 2002, que traduz uma directiva europeia ¹ sobre a protecção de dados, atribui-lhe direitos. Esta visa proteger a vida privada de pessoas físicas (e até os interesses de pessoas morais) no que toca ao tratamento dos seus dados pessoais por terceiros.

As administrações, empresas e outros profissionais, associações e qualquer outro organismo que recolhe, regista, utiliza e transmite dados pessoais, não podem fazê-lo sem restrições. Devem contactar a pessoa implicada e informar-lhe sobre qual o objectivo a atingir, com o que a lei designa de "tratamento de dados de carácter pessoal". Este tratamento deve-se limitar ao que é necessário e relativo aos objectivos fixos inicialmente. Cada utilização de dados deve, portanto, realizar-se respeitando regras rígidas, cujo controlo é assegurado pela Comissão Nacional para a Protecção de Dados ². Para que haja transparência no tratamento de dados, qualquer ficheiro que contenha informações relativas a pessoas, deve ser declarado à autoridade de controlo ou autorizado por esta (tendo em conta o tipo de dados ou de tratamento) antes de poder ser explorado.

A legislação sobre a protecção de dados pessoais não se limita aos ficheiros informáticos, mas inclui todo o tipo de suportes (ficheiros em papel, registos áudio e vídeo).

A protecção da vida privada é um direito fundamental, assim como a inviolabilidade do domi-

¹ (Directiva 95/46/CE de 24 de Outubro de 1995)

² www.cnpd.lu

cílio, o segredo da correspondência ou ainda a liberdade de opinião e de expressão.

Os mesmos princípios também se aplicam a todos os 25 Estados membros da União Europeia e para além destes (Suiça, Noruega, Liechtenstein, Islândia, etc.).





OS 10 MANDAMENTOS DA PROTECÇÃO DE DADOS PESSOAIS



A entidade que manusear os dados relativos a outras pessoas deve respeitar os seguintes princípios :

1. PRINCÍPIO DA LEGITIMIDADE

O tratamento de dados pessoais só é possível se existir uma razão suficientemente legítima que o justifique. A entidade que desejar manusear os dados de alguém, deve solicitar a autorização prévia da pessoa implicada. Por outro lado, o tratamento de dados também é permitido se for indispensável para a execução de um contrato; respeitar uma obrigação de serviço público

ou legal; ou ainda para proteger a sua própria vida. Por fim, o tratamento pode ser legitimado se existir um interesse justificado, mas com a condição de que este não afecte muito a sua vida privada.

Este princípio constitui o primeiro teste para detectar se o tratamento é lícito, e responde à questão de **quando** é que os seus dados podem ser solicitados e utilizados por terceiros. Os princípios que se seguem descrevem as regras que estes últimos devem respeitar aquando da utilização dos dados, respondendo à questão de **como** tratá-los.

2. PRINCÍPIO DA FINALIDADE

A utilização dos seus dados pessoais (incluindo sons e imagens) deve-se limitar a uma finalidade explícita e previamente determinada.

A recolha, registo e utilização dos seus dados pessoais são estritamente limitados ao necessário para atingir os objectivos previamente definidos pela administração, empresa, associação, profissional ou independente.

A entidade inicial não deve transmitir os dados a outros organismos ou pessoas, a não ser que estes os utilizem no contexto da concretização dos mesmos objectivos e de um modo compatível.

EXEMPLO

No seguimento de um acidente de trabalho, o patrão contacta o médico para obter informações sobre o estado de saúde do seu empregado. Pensando não estar a fazer nada de errado em tranquilizá-lo, a assistente do médico fornece-lhe informações sobre o diagnóstico estabelecido.

Ao fazê-lo, ela transpõe a finalidade para a qual o gabinete médico detém essas informações, ou seja, garantir os seus serviços de saúde.

3. PRINCÍPIOS DA NECESSIDADE E DA PROPORCIONALIDADE

O Princípio da Proporcionalidade implica que o tratamento se limite aos dados directamente relacionados com a finalidade inicial. Estes dados devem, não só ser úteis, mas também necessários para quem os processar e devem-se resumir ao objectivo a atingir.

EXEMPLO

Aquando da reserva telefónica de uma mesa, o gerente do restaurante pede-lhe o número do seu cartão de crédito.

Esta informação é considerada excessiva relativamente à finalidade a atingir, que consiste na planificação das mesas disponíveis.

4. PRINCÍPIO DA EXACTIDÃO DE DADOS

Tendo em conta que informações falsas ou incompletas podem prejudicar a pessoa à qual se referem, devem ser efectuados todos os esforços para que os dados tratados estejam correctos e actuais. Caso contrário, estes deverão ser rectificados ou apagados.

A lei também o protege contra qualquer decisão negativa, automaticamente tomada por um sistema informático, sem que você possa fazer valer o seu ponto de vista.

EXEMPLO

Você solicita um empréstimo pessoal, junto do seu Banco, para a compra de mobiliário. Depois da introdução do seu dossier, via Internet, você recebe imediatamente uma resposta negativa do Banco, que lhe recusa a atribuição do empréstimo solicitado. Aqui verifica-se que não houve a intervenção de um conselheiro do Banco e que o pedido foi calculado através de um sistema informático que o avalia com base em estatísticas e cálculos pré-estabelecidos.

Você tem o direito de exigir que o seu dossier seja reexaminado, encontrando-se com o seu conselheiro bancário, que deverá recebê-lo a fim de ouvir os seus argumentos.

Aquando do encontro, você pode fazer valer, de um modo plausível, que por exemplo, a sua situação financeira melhorou devido à atribuição de uma herança. Poderá mesmo acontecer que certos números tidos em conta estejam errados ou ainda que houve uma confusão com algum homónimo endividado.



5. PRINCÍPIO DA LEALDADE

A recolha, registo, utilização e transmissão dos seus dados pessoais, devem ser realizados de boa fé e nunca sem o seu conhecimento.

Caso contrário, os dados devem ser imediatamente apagados ou tornados anónimos. A sua utilização posterior, com outros objectivos que não os previstos inicialmente, é um princípio interdito.

EXEMPLO

O seu supermercado propõe-lhe um cartão de fidelidade para que possa beneficiar de descontos especiais ou de promoções de fim de ano. Futuramente, ao passar pela caixa, o conteúdo do seu carrinho de compras será registado e servirá para estabelecer um padrão de consumo cuja evolução será regularmente observada.

Caso esta situação ocorra sem o seu conhecimento, não tendo sido informado no momento da subscrição, o princípio da lealdade está a ser violado.

6. PRINCÍPIO DA SEGURANÇA E DA CONFIDENCIALIDADE

Os seus dados pessoais devem ser tratados de modo confidencial e armazenados em locais e suportes seguros.

Caso este princípio não seja respeitado, é a entidade que tem em curso o tratamento de dados, quem deverá assumir a responsabilidade. Esta obrigação também se aplica ao comportamento dos seus colaboradores e deve ser tida em conta nos contratos realizados com agentes externos (nomeadamente os prestadores de serviços) e na escolha dos equipamentos técnicos (no contexto da segurança informática).

EXEMPLO

Você tenciona mudar de rede de telemóvel. Após o estudo do seu dossier, o delegado comercial da sociedade que você escolheu, recusa-o como novo cliente. Este indivíduo, antigo agente comercial do seu anterior operador de telemóvel, reporta-se a um litígio que você tem com essa empresa, relativamente ao montante de uma factura.

Ao permitir que os seus agentes comerciais obtenham informações provenientes do departamento de contabilidade, o anterior operador negligenciou a garantia

de que as informações pessoais, relativas aos seus clientes, sejam acessíveis apenas aos empregados que realmente necessitem destas para o cumprimento do seu trabalho.

Será que o pessoal foi suficientemente precavido para as tentações de utilização abusiva dos dados relativos à clientela? Como será que o agente comercial pôde trazer um ficheiro de um cliente da sua antiga para a sua nova empresa? Será que houve um roubo de ficheiro?

Em todo o caso, as medidas de segurança e organização interna da empresa foram insuficientes para garantir a confidencialidade dos dados de carácter pessoal. A responsabilidade pode ser atribuída ao Director, que falhou com as suas obrigações legais, assim como à indelicadeza do funcionário.

7. PRINCÍPIO DA TRANSPARÊNCIA

A lei garante-lhe a informação necessária relativa aos tratamentos a que os seus dados são sujeitos e assegura-lhe a possibilidade de um controlo pessoal. Quem desejar manusear os seus dados pessoais deverá adverti-lo no momento da recolha e em caso de transmissão a terceiros.

Você tem o direito de pedir informações quanto aos dados pessoais registados e quanto à sua utilização, assim como solicitar a destruição de informações cujo tratamento não estará conforme a lei.

O registo de todas as bases de dados junto da Comissão Nacional para a Protecção de Dados, contribui para que exista transparência. Este registo público de tratamento de dados pessoais pode ser consultado na sua página de Internet ³.

EXEMPLO

Visto que você está constantemente cansado, o seu médico prescreve-lhe uma análise de sangue, a fim de determinar as causas do seu cansaço. A recolha de sangue é realizada por um laboratório externo que transmite os resultados dessa análise ao seu médico. Verifica-se, no entanto, que foi realizada uma despistagem ao vírus da Sida, sem o seu conhecimento.

Isto constitui uma transgressão aos princípios da transparência e da lealdade.

³ www.cnpd.lu Disponibilização on-line prevista para fim de 2004.

8. ALGUNS DADOS PARTICULARMENTE SENSÍVEIS SÃO SUBMETIDOS A UMA PROTECÇÃO MAIS REFORÇADA

O tratamento de informações a seu respeito, que demonstrem as suas opiniões e convicções ou que estejam relacionadas com o seu estado de saúde ou a sua vida sexual, bem como os seus dados genéticos, é interdito, exceptuando alguns casos enumerados de modo limitativo pela lei.

Sendo assim, a Comissão Nacional para a Protecção de Dados deverá autorizar expressamente o tratamento deste tipo de dados.

EXEMPLO

Numa entrevista de trabalho, o Director de Recursos Humanos da empresa à qual se está a candidatar, coloca-lhe questões sobre a sua opinião relativamente ao financiamento de reformas e sobre os respectivos pontos de vista dos partidos políticos. Paralelamente, ele demonstra-lhe ter em consideração os empregados sindicalizados.

Normalmente recolher informações desta natureza (dados sensíveis) é interdito pela lei.

9. A VIGILÂNCIA DE PESSOAS IDENTIFICÁVEIS É ESTRITAMENTE DELIMITADA PELA LEI

Uma autorização da Comissão Nacional para a Protecção de Dados é necessária antes de recorrer a meios técnicos para vigiar pessoas, nomeadamente através de câmaras de vídeo, informaticamente, etc. O tratamento de dados pessoais recolhidos desta forma, só é possível em situações bem concretas e pré-definidas pela lei. Isto inclui a vigilância em locais públicos, nos meios de transporte, em centros comerciais, bem como no seu local de trabalho. Neste último caso, a vigilância só será possível se você, o Comité Misto, a Delegação do Pessoal ou a Inspecção do Trabalho tenham sido previamente advertidos.

EXEMPLO

As suas conversas telefónicas são registadas pela empresa onde você trabalha, sem que tenha sido antecipadamente avisado.

Esta situação vai de encontro ao Princípio da Transparência. Assim sendo, o patrão deve dispôr de uma autorização emitida pela Comissão Nacional para a Protecção de Dados, à qual pertence, a fim de confirmar a legitimidade e a proporcionalidade desta prática.

10. A UTILIZAÇÃO DOS SEUS DADOS PARA FINS PUBLICITÁRIOS OU COMERCIAIS DEVE SER SUBMETIDA À SUA AUTORIZAÇÃO EXPRESSA

Você pode, a qualquer momento, proibir a utilização dos seus dados pessoais para fins comerciais. O Marketing directo, realizado através dos meios de comunicação modernos (sms, e-mail, etc.) é proibido, caso não haja o consentimento da pessoa em questão.

EXEMPLO

A sua caixa de correio é invadida por correio publicitário personalizado.

Você pode solicitar às lojas e sociedades comerciais a anulação do envio deste tipo de correio.

O que se passou foi que um comerciante obteve o seu endereço, através do seu clube desportivo, que lhe transmitira as coordenadas pessoais de todos os membros do clube, do qual é patrocinador. O clube desportivo não deveria ter comunicado o seu ficheiro de membros, uma vez que esses dados deveriam servir exclusivamente à gestão do clube e à organização das suas actividades.

Ao alterar a finalidade, a utilização dos dados pessoais torna-se ilícita, sendo punida por lei.

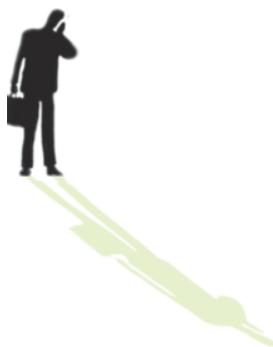




OS SEUS DIREITOS ENQUANTO CIDADÃO



A lei sobre a protecção de dados de carácter pessoal tende a assegurar uma transparência ao nível do seu tratamento e encoraja uma certa autodeterminação de cada cidadão. Esta atribui-lhe direitos permitindo-lhe verificar você mesmo o que advém dos seus dados pessoais.



1. DIREITO À INFORMAÇÃO

Você deve ser esclarecido no momento da recolha dos dados, ou o mais tardar na altura do seu registo. As finalidades para as quais os seus dados serão utilizados devem ser disponibilizadas pela entidade que os recolhe e trata. O mesmo acontece, caso esta tencionar transmiti-los a terceiros.

2. DIREITO DE ACESSO ÀS SUAS INFORMAÇÕES PESSOAIS

Você tem o direito de aceder aos seus dados pessoais e obter uma cópia destes, bem como solicitar a rectificação de informações erradas ou inadequadas, e até mesmo a sua eliminação.

3. DIREITO DE OPOSIÇÃO AO TRATAMENTO DE DADOS PESSOAIS

Você tem o direito de se opôr ao tratamento dos seus dados de carácter pessoal, por motivos legítimos, tendo em conta um contexto específico.

A qualquer momento, poderá proibir, sem dar qualquer justificação, a utilização dos seus dados, para fins prospectivos ou ainda por razões comerciais ou movimentos de orientação ideológica (partidos políticos, sindicatos, igrejas e movimentos religiosos, etc.)

4. DIREITO À INFORMAÇÃO SOBRE OS PROCESSOS DE DECISÃO AUTOMÁTICOS

Relativamente a decisões tomadas com base em processos automatizados (ex. aprovação de um crédito de consumo ou de um contrato de seguro), você tem o direito de ser informado acerca da lógica que comanda este processo. A empresa ou o organismo implicado deve-lhe dar a possibilidade de fazer valer o seu ponto de vista e até contestar a decisão, em último caso.



QUANDO E COMO **FAZER VALER OS SEUS DIREITOS ?**





1. CONSULTA DO REGISTO PÚBLICO

A Comissão Nacional para a Protecção de Dados criou um registo público de tratamento de dados, acessível na Internet ⁴.

Este permite-lhe verificar se existe alguma entidade susceptível de possuir informações relativas à sua pessoa e se o terá declarado junto da Comissão Nacional para a Protecção de Dados. Cada base de dados e tratamento de dados devem, com efeito,

ser notificados e autorizados individualmente. Por exemplo, uma empresa que obtiver a autorização para instalar um sistema de vigilância, não fica dispensada de comunicar que gere um ficheiro cliente.

⁴ www.cnpd.lu

2. RECLAMAÇÃO DIRECTA

Você pode fazer valer os seus direitos de acesso e de rectificação, directamente junto da entidade responsável, quer seja no momento da recolha, utilização ou tratamento dos seus dados pessoais. Você pode, portanto, solicitar que seja advertido sobre a finalidade do tratamento de dados, isto é, quais os objectivos a atingir. A entidade responsável deverá lhe comunicar quais são os seus dados que se encontram armazenados, para que você possa verificar a sua exactidão, pertinência e a necessidade do armazenamento, tendo sempre em conta o objectivo que se pressupõe atingir.

Envie o seu pedido de informação por escrito, de preferência em carta registada, juntando uma cópia do seu bilhete de identidade. As informações sobre o tratamento de dados pessoais devem ser obtidas gratuitamente.

3. A RECLAMAÇÃO JUNTO DA COMISSÃO NACIONAL PARA A PROTECÇÃO DE DADOS

Se a sua reclamação, junto da respectiva entidade, ficar sem resposta, você poderá considerar dirigir-se à Comissão Nacional para a Protecção de Dados.

A Comissão Nacional tem por missão dar seguimento a todas as reclamações provenientes de pessoas lesadas. Esta poderá impedir o tratamento de dados, em caso de desrespeito da lei. Também poderá ordenar a supressão de dados e submeter o caso ao procurador público. Em caso de infracção, poderão ser atribuídas multas.

Aconselhamos vivamente o envio da sua reclamação por escrito, explicando de modo detalhado o problema verificado.

4. APELO AO TRIBUNAL

Se o seguimento dado pela Comissão Nacional para a Protecção de Dados não lhe parecer satisfatório, você terá sempre o direito de submeter o caso a Tribunal. Se assim fôr, deverá contactar um advogado, para ser aconselhado.

Uma acção em tribunal é igualmente indispensável, caso haja uma violação dos seus direitos, ao nível da sua vida privada, que lhe tenha causado danos e/ou prejuízo de interesses.



A COMISSÃO NACIONAL PARA A PROTECÇÃO DE DADOS : O MEDIADOR DO JUSTO EQUILÍBRIO



A legislação em matéria de protecção de dados de carácter pessoal procura o justo equilíbrio entre a sociedade de informação e a protecção da vida privada.

Ao colocar a balança em equilíbrio entre os interesses dos que pretendem, legitimamente, adquirir e utilizar informações relativas a alguém e a expectativa natural dos cidadãos em poder contar com o respeito de um certo anonimato e com a toma de precauções particulares relativamente a certos dados íntimos, a Comissão Nacional para a Protecção de Dados contribui ao estabelecimento de um clima de confiança entre os cidadãos e os actores públicos e privados detentores de dados, quer sejam profissionais do domínio comercial ou não. Este clima de



confiança favorece igualmente o desenvolvimento de actividades económicas, valendo-se das novas tecnologias (e-comércio), a modernização da Administração (e-Governo) e a livre circulação de informação.

A reaproximação, num plano comunitário, das legislações nacionais ao nível da protecção de dados, tornou-se indispensável para ultrapassar os obstáculos à livre circulação de dados no seio do mercado único. A Directiva Europeia visa assim o estabelecimento, em toda a Europa, de um mesmo nível de protecção dos direitos e liberdades dos indivíduos, no que se refere ao tratamento dos seus dados pessoais. Daí ter ajudado a ultrapassar todos os obstáculos, ao nível dos fluxos fronteiriços de dados pessoais,

no seio da União Europeia, impondo sempre condições restritas que limitam a circulação em países que não asseguram uma protecção adequada.

No Luxemburgo, a Comissão Nacional para a Protecção de Dados é uma autoridade de controlo independente e competente nesta área, tanto no sector público como no privado.

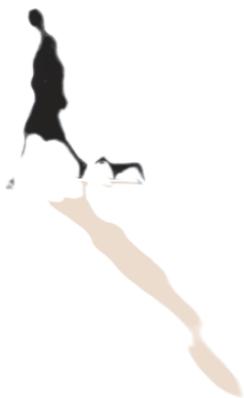
Endereço para contacto :



**Comissão Nacional
para a Protecção de Dados**

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

GLOSSÁRIO DOS CONCEITOS MAIS UTILIZADOS AO NÍVEL DA PROTECÇÃO DE DADOS





1. DADO DE CARÁCTER PESSOAL

Toda a informação, de qualquer natureza, e independentemente do seu suporte (incluindo o som e a imagem) relativa a uma pessoa identificada ou susceptível de o ser. Uma pessoa física (cidadão) ou moral (sobretudo as empresas) é considerada identificável, se esta realmente poder ser identificada, directa ou indirectamente, sobretudo por referência a um número de identificação ou a um ou mais elementos específicos, próprios da sua identidade física, fisiológica, genética, psicológica, cultural, social ou económica.

2. TRATAMENTO DE DADOS DE CARÁCTER PESSOAL

Qualquer operação ou conjunto de operações, realizadas ou não através de processos informatizados, aplicados a dados. Trata-se da recolha, registo, organização, conservação, adaptação ou modificação, extracção, consulta, utilização, comunicação por transmissão, difusão ou qualquer outra forma de divulgação de dados, aproximação ou interconexão, bem como do encerramento, desaparecimento ou destruição de dados.

3. FICHEIRO DE DADOS DE CARÁCTER PESSOAL

É todo o conjunto estruturado de dados, acessíveis segundo critérios determinados, podendo ser centralizado, descentralizado e distribuído de forma funcional ou geográfica.

4. RESPONSÁVEL DO TRATAMENTO

É a pessoa física ou moral, autoridade pública, serviço ou qualquer outro organismo que (sozinho ou juntamente com outros) determina as finalidades e os modos de tratamento dos dados de carácter pessoal.

5. INTERCONEXÃO

Toda a forma de tratamento que consiste na correlação entre dados tratados de acordo com uma finalidade e outros tratados segundo as mesmas finalidades ou ainda que tenham sido relacionados por um ou mais responsáveis do tratamento.

6. FINALIDADE

É o objectivo definido antes da execução do tratamento, que está na base da selecção das operações a realizar para o atingir e na determinação dos dados submetidos a essas operações. Não será coerente englobar, numa certa finalidade, um conjunto de objectivos supérfluos ou muito numerosos. A determinação da finalidade, ou finalidades relacionadas, do tratamento é um elemento essencial para avaliar a sua legitimidade.

7. CONSENTIMENTO DA PESSOA ENVOLVIDA

Toda a manifestação de vontade expressa, inequívoca, livre, específica e consciente, através da qual a pessoa implicada ou o seu representante legal, judiciário ou estatutário, aceita que os dados de carácter pessoal sejam objecto de tratamento.

EDITOR SIP **EM COLABORAÇÃO COM A** CNPD **DATA** 12|2005 **LAYOUT** MV-CONCEPT.LU **IMPRESSÃO** TIPOGRAFIA FR.FABER





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

*Para mais
informações sobre a
protecção de dados :*



COMISSÃO NACIONAL
PARA A PROTECÇÃO
DE DADOS

33, BD ROOSEVELT L-2450 LUXEMBOURG

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

WWW.GOUVERNEMENT.LU

ENDEREÇO POSTAL : L-4100 ESCH-SUR-ALZETTE

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

INFO@CNPD.LU / WWW.CNPD.LU