COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Registo n.º 70/2013

O Infarmed – Autoridade Nacional do Medicamento e Produtos de Saúde, IP notificou a Comissão Nacional de Protecção de Dados (CNPD) um tratamento de dados pessoais com a finalidade de disponibilização da plataforma "Transparência e Publicidade".

O Decreto-Lei n.º 20/2013, de 14 de fevereiro, no artigo 159.º, sob a epígrafe Transparência e Publicidade, vem criar obrigações para as entidades abrangidas pelo referido diploma, que concedam ou recebem subsídios, patrocínios, subvenções ou qualquer outro valor, em dinheiro ou espécie, designadamente a obrigação de declarar tais recebimentos.

O n.º 6 do referido artigo aplica-se a pessoas singulares.

Para cumprimento desta obrigação o Infarmed disponibilizou a plataforma no endereço http://placotrans.infarmed.pt.

Os sujeitos passivos da obrigação de declaração dos valores recebidos devem registar-se no endereço acima mencionado, sendo-lhe solicitados os seguintes dados: Tipo de entidade (ARS, armazenista, associação profissional, associação/grupo de doentes, distribuidores por grosso, fabricante, farmácia, hospital, local de venda MNSRM, outros coletivos, profissionais de saúde, representante local, sociedade médica, titular AIM e outros), Número de Identificação Fiscal (NIF), Nome completo, endereço eletrónico, pessoa de contacto, telefone de contacto, tipo de morada (trabalho, residência), endereço postal, país, distrito e concelho.

Após submissão eletrónica do registo, no e-mail fornecido, é recebido um link de ativação e, subsequentemente, as credenciais de acesso (Nome de utilizador e password).

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Com as credenciais de acesso, após autenticação, é disponibilizado o formulário para declaração dos recebimentos. Neste, aparece, por defeito, a identificação da entidade recetora (nome, NIF, endereço postal e e-mail), existindo campos para a caraterização da aceitação e identificação da entidade contribuinte.

Foi declarado não existir comunicação de dados, nem interconexões, nem fluxos transfronteiriços.

Os do titular dos dados, designadamente de acesso e retificação podem ser exercidos por escrito para a morada do responsável, na Av. do Brasil, n.º 53 1749-004 Lisboa.

No que respeita a medidas de segurança, o responsável declara não existirem medidas de segurança física ou lógica.

O prazo máximo de conservação da informação declarado foi de cinco anos.

O fundamento de legitimidade para o tratamento de dados (recolha, conservação e disponibilização) é o cumprimenta da obrigação legal previsto na alínea b) do artigo 6.º da LPD, por referência ao n.º 6 do artigo 159.º do Decreto-Lei n.º 20/2013, de 14 de fevereiro.

Os dados recolhidos são adequados, necessários e não excessivos, com exceção do NIF, porquanto aquele número, nos termos do artigo 2.º do Decreto-lei n.º 14/2013, de 28 de janeiro, é *destinado exclusivamente ao tratamento de informação de índole fiscal.* Assim, este dado não pode ser objeto de tratamento.

Quanto às credenciais de acesso estabelecidas (NIF e palavra-passe), sendo a palavra–passe criada pelo responsável, sem possibilidade de alteração pelo utilizador, levanta muitas reservas, tanto mais que o atributo de utilizador é do conhecimento de terceiros.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

De facto o NIF está disponível em inúmeros locais e é de fácil acesso, designadamente na Internet.

Quanto à palavra passe atribuída, sendo alfanumérica com apenas cinco caracteres, não cumpre os requisitos básicos de robustez exigidos.

Nos termos em que está implementado, utilizando como username um dado de acesso praticamente público, através de um ataque por "*brute force*", com facilidade permitiria aceder indevidamente à página com as credenciais de um utilizador e, naturalmente, efetuar declarações em seu nome.

Acresce que foi declarado não existirem seguranças lógicas.

Não existindo verificação da identidade do registando, qualquer pessoa pode atribuir a outro o recebimento de quantias que poderão ter por objetivo denegrir a sua imagem, tanto mais que a informação está disponibilizada em rede aberta e, consequentemente, está acessível a todo o tempo por qualquer pessoa, em qualquer lugar.

O responsável deve, por isso, corrigir a situação em colaboração com as Ordens Profissionais, para a criação de condições para a autenticação por mecanismos fortes de identificação do profissional de saúde.

A CNPD tem vindo a alertar para o facto dos sistemas de informação que contenham dados pessoais deverem ser acompanhados, desde a sua conceção, dos indispensáveis estudos de impacto técnico, de modo a atingirem plenamente as suas finalidades sem resultarem em violações dos direitos fundamentais dos cidadãos (*Privacy by design*).

É fundamental que o responsável faça a análise de riscos do projeto, para poder responder às potenciais ameaças à segurança, física e lógica.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Importa, também, que crie mecanismos de auditoria, por forma a garantir a rastreabilidade dos acessos.

Os *logs*, para terem validade legal devem estar assinados digitalmente.

O Infarmed deve identificar um conjunto de situações consideradas anómalas de forma a poder desenvolver um sistema de alarmes, que permita identificar utilizações indevidas do sistema.

Face ao exposto, regista-se, com as condições supra indicadas, de acordo com o n.º 1 do artigo 27º e o n.º 1 do artigo 30º ambos da LPD, o tratamento, nos seguintes termos:

**Responsável** - Infarmed – Autoridade Nacional do Medicamento e Produtos de Saúde, IP;

**Categoria de dados pessoais tratados** – Tipo de entidade, Nome completo, endereço eletrónico, pessoa de contacto, telefone de contacto, tipo de morada (trabalho, residência), endereço postal, país, distrito e concelho, tipo de bem, quantia e nome da entidade contribuinte;

**Finalidade** – disponibilização da plataforma "Transparência e Publicidade";

**Forma de exercício do direito de acesso e retificação** – escrito para a morada do responsável, na Av. Do Brasil, n.º 53 1749-004 Lisboa;

**Interconexões** – Não há;

**Comunicação de dados pessoais** – Não há;

**Fluxo transfronteiriço de dados pessoais** – Não há;

**Prazo máximo de conservação dos dados** – Cinco anos.

Aos titulares dos dados deve ser garantido o direito de informação previsto no artigo 10º da LPD, incluindo o n.º 4 por haver recolha de dados em rede aberta.

A CNPD alerta o Infarmed relativamente à obrigação que sobre ele recai de adotar as medidas de segurança adequadas ao risco que o tratamento de dados pessoais

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

apresenta, estando obrigado a cumprir o artigo 14.º da LPD.

Até à alteração dos procedimentos nos termos previstos no presente instrumento de legalização, deve o Infarmed, IP abster-se de disponibilizar a informação na Internet.

Lisboa, 12 de abril de 2013
A Secretária da CNPD

Isabel Cristina Cruz