

AUTORIZAÇÃO N.º ⁴¹⁰⁶ /2014

1. O Pedido

ESEGUR – SOLUÇÕES DE BACKOFFICE, SA, com o NIF 502784822, vem notificar à Comissão Nacional de Protecção de Dados (CNPD), um tratamento de dados pessoais com a finalidade de gestão de recursos humanos.

Do pedido de autorização verifica-se que:

- a) Os dados pessoais objeto de tratamento são: nome, sexo, estado civil, agregado familiar, nacionalidade, naturalidade, data de nascimento, documento de identificação (BI, CC ou outro), residência fiscal, e-mail, contacto telefónico, morada, competências linguísticas, competências académicas, competências sociais, fotografia, percurso profissional (empresa, local, departamento funções, nível, remuneração e outros dados de compensação, situação contratual, data de admissão, promoções, formações, experiência profissional passada, situação militar, elementos do agregado familiar com grau de deficiência igual ou superior a 60%, NIF e NIB; dados para gestão de processos e registo de sanções disciplinares; dados referentes a benefícios atribuídos aos colaboradores relacionados com a prestação de serviços por terceiros (veículos automóveis, telefones, e outros benefícios conexos).
- b) A recolha dos dados é feita por via direta, presencialmente, por telefone, por impresso e através da internet, e por via indireta na medida em que alguns dados podem ser preenchidos pelos recursos humanos, designadamente os dados de identificação que resultam da celebração ou da execução do contrato e por consulta a bases de dados da DGCI e do Banco de Portugal;
- c) A requerente elenca as entidades subcontratantes encarregadas do processamento da informação: Companhias de Seguros (Alliance Portugal, SA), corretores de seguros (Gestão Activa – Consultores de Seguros, Lda.), Agências de Viagens (para marcação de viagens e alojamento de



- trabalhadores – Top Atlântico, SA), Operadores de telecomunicações (TMN), Manutenção informática (Capgemini Portugal, SA), gestão de servidores (Oblog – Consulting, SA), advogados (para prestação de serviços jurídicos), Grupo ESEGUR (para gestão centralizada de recursos humanos).
- d) Não se verificam interconexões nem fluxos internacionais de dados para países terceiros;
 - e) Pretende-se a conservação dos dados por períodos variáveis, contemplando um período máximo de dez anos após a cessação do vínculo laboral;
 - f) O exercício do direito de acesso é feito por forma presencial ou por forma escrita, por telefone ou por email,
 - g) São indicadas medidas de segurança física e de segurança lógica;

2. Análise

Constitui fundamento de legitimidade para o tratamento a execução do contrato, nos termos da alínea a) do artigo 6.º da Lei 67/98 de 26 de outubro (LPD).

A informação tratada é recolhida de forma lícita (cf. Artigo 5º, nº1, alínea a) da LPD), para finalidades determinadas, explícitas e legítimas (cf. alínea b)) e os dados a tratar consideram-se adequados, pertinentes e não excessivos (cf. alínea c)).

Nota-se que entre o responsável e as subcontratadas para o processamento da informação deve ser celebrado o contrato previsto no n.º 3 do artigo 14.º da Lei n.º 67/98 de 26 de outubro (LPD), aí se estabelecendo, designadamente, que as subcontratadas atuam apenas mediante instruções do responsável e que lhes incumbe o cumprimento das obrigações previstas no n.º 1 do mesmo artigo.

Importa referir que dos dados tratados parece decorrer que o responsável inclui na presente notificação os dados pessoais de eventuais candidatos com a finalidade de recrutamento. Ora, sendo esta finalidade autónoma, sujeita a diferente fundamento de legitimidade, sendo recolhidos outros dados e tendo condições de tratamento distintas, está a mesma sujeita ao cumprimento do artigo 27.º da LPD.



Quanto à comunicação de dados prevista a empresas de manutenção dos sistemas informáticos de suporte à base de dados e a entidade prestadoras de serviços no âmbito da gestão de recursos humanos deverão ser transmitidos os dados estritamente necessários à prossecução das finalidades descritas

Relativamente aos prazos máximos de conservação de dados, atento o disposto na alínea e) do n.º 1 do artigo 5.º da LPD, devem os dados pessoais ser conservados apenas durante o período necessário para a prossecução das finalidades da recolha e do tratamento posterior, pelo que se entende que a conservação por dez anos após a cessação do vínculo laboral é excessiva.

No uso da competência prevista na alínea f) do n.º 1 do artigo 23.º da LPD fixa-se o prazo em um ano após o fim da relação contratual, sem prejuízo de tal prazo se estender pelo tempo de duração de eventual processo judicial e até ao limite de seis meses após o trânsito em julgado da respetiva sentença. Admite-se ainda a conservação do processo individual do trabalhador para fim de registo histórico.

Quanto aos registos relativos a processos e sanções disciplinares, e tendo a Requerente universo de colaboradores ao seu serviço, estamos perante uma finalidade determinada, explícita e legítima.

Os dados a colher, tendo em atenção a finalidade pretendida, apresentam-se como adequados, pertinentes e não excessivos. Cumpre avaliar do fundamento de legitimidade que permita à requerente realizar o presente tratamento.

A CNPD tem entendido, dada a formulação genérica do artigo 8.º, n.º 2, da Lei nº 67/98, de 26 de outubro, que o tratamento de dados sobre gestão de sanções disciplinares (vg. «decisões que apliquem penas») terá que ser objeto de autorização - artº 28.º, n.º 1 - al. a) da Lei 67/98, de 26 de outubro.

A Requerente tem legitimidade para o tratamento de sanções disciplinares, na medida em que – nos termos do artº 332º do CTrabalho – a entidade patronal está obrigada a

manter atualizado o registo das sanções disciplinares. Este tratamento é, assim, necessário ao cumprimento de finalidades legalmente estabelecidas (cfr. artº 8.º/n.º 2 da citada Lei), as quais se configuram como legítimas e não existe, por regra, uma prevalência dos direitos dos titulares dos dados. Efetivamente, tal como resulta do citado normativo do CTrabalho, um dos objetivos do registo das sanções disciplinares é precisamente assegurar o controlo, pelas entidades competentes, da aplicação de sanções disciplinares abusivas.

Consigna-se, no entanto, que o acesso à informação sobre sanções disciplinares deve ser restrito apenas às pessoas com necessidade de aceder a esta informação, devendo o sistema estar dotado de níveis diferenciados de acesso que garantam que outras pessoas não autorizadas não acessem.

3. Conclusão

Assim, nos termos das disposições conjugadas do artigo 6.º, n.º 2 do artigo 8.º, n.º 1 do artigo 27.º, alínea a) do n.º 1 do artigo 28.º e artigo 30.º da Lei de Protecção de Dados, autoriza-se o tratamento de dados supra referido nos seguintes termos:

Responsável: ESEGUR – SOLUÇÕES DE BACKOFFICE, SA.

Categoria de dados tratados: nome, sexo, estado civil, agregado familiar, nacionalidade, naturalidade, data de nascimento, documento de identificação (BI, CC ou outro), residência fiscal, e-mail, contacto telefónico, morada, competências linguísticas, competências académicas, competências sociais, fotografia, percurso profissional (empresa, local, departamento funções, nível, remuneração e outros dados de compensação, situação contratual, data de admissão, promoções, formações, experiência profissional passada, situação militar, elementos do agregado familiar com grau de deficiência igual ou superior a 60%, NIF e NIB; dados para gestão de processos e registo de sanções disciplinares; dados referentes a benefícios atribuídos aos colaboradores relacionados com a prestação de serviços por terceiros (veículos automóveis, telefones, e outros benefícios conexos).

Finalidade: gestão de recursos humanos;



Comunicação de dados: a entidade subcontratantes, prestadoras de serviços e no âmbito da gestão de recursos humanos, devendo apenas ser transmitidos os dados estritamente necessários à prossecução das finalidades descritas.

Forma do exercício do direito de acesso e retificação: por forma presencial, por escrito, por telefone para os contactos do Recursos Humanos ou para o endereço eletrónico indicado

Interconexões: não se verificam.

Transferências de dados para países terceiros: não se verificam

Tempo de conservação de dados: um ano após o fim da relação contratual, sem prejuízo de tal prazo se estender pelo tempo de duração de eventual processo judicial e até ao limite de seis meses após o trânsito em julgado da respetiva sentença;

Aos titulares dos dados deve ser garantido o direito de informação previsto no artigo 10.º da LPD.

Lisboa, 29 de abril de 2014

A handwritten signature in black ink, appearing to read 'Filipa Calvão', is written over a horizontal line.

Filipa Calvão (Presidente)