Recomendação n.º 1/2019

Regulamento Geral sobre a Proteção de Dados (RGPD)

A presente Recomendação alude às medidas que os colaboradores devem adotar, designadamente:

i) Realizar o acesso e as operações de tratamento de dados pessoais apenas para os fins a que estão autorizados.

A recolha, acesso, divulgação ou outra operação de tratamento não autorizada é punível por lei.

i) Garantir o sigilo profissional relativamente às atividades profissionais e à informação interna, incluindo de colaboradores, utentes, clientes, prestadores de serviços ou outros indivíduos particulares, atuando com discrição em relação aos dados e informações tratadas, respeitando os princípios da confidencialidade e privacidade.

ii) Assegurar a confidencialidade e a segurança do tratamento dos dados pessoais no decorrer das suas atividades profissionais, de modo a prevenir o tratamento não autorizado ou ilícito, incluindo acesso ou divulgação não autorizados, consulta, alteração, cópia, danificação ou eliminação dos dados pessoais de forma indevida ou ilícita.

CONTROLO DE ACESSOS FÍSICOS ÀS INSTALAÇÕES

a. As instalações devem possuir um sistema de controlo de acessos que permita o registo de entradas e saídas e a segregação de espaços com diferentes níveis de acesso.

b. Aquando do acesso de visitantes deve ser efetuado o registo na Portaria (entrada principal), bem como a confirmação da visita/reunião com o respetivo destinatário interno.

c. Devem existir zonas neutras de acesso, tais como salas de espera e de reuniões de trabalho com equipas externas.

d. As salas de arquivo físico de processos devem ser alvo de controlo através de um sistema eletrónico que permita o registo dos acessos, bem como as salas de servidores e bastidores de comunicações.

e. Não devem ser transmitidas informações sobre os colaboradores, limitando-se apenas à respetiva disponibilidade. No caso de indisponibilidade, deve ser solicitado que se deixe recado e não deverá ser prestada nenhuma informação sobre a localização do colaborador ou a sua ausência do edifício.

ENVOLVIDOS

CONSELHO EXECUTIVO

PESSOAL DOCENTE

PESSOAL NÃO DOCENTE

PORTARIA

SERVIÇOS ADMINISTRATIVOS

SEGURANÇA FÍSICA DOS PROCESSOS
GESTÃO E ARQUIVO DE PROCESSOS FÍSICOS

a. Devem ser definidos o fluxo e os intervenientes autorizados nos processos que envolvam tratamento de dados pessoais, de modo a garantir que o acesso ao arquivo físico apenas é realizado por pessoas autorizadas.

b. Todos os processos, dossiers, capas e documentos contendo dados pessoais devem ser arquivados em armários fechados com chave, quer seja em salas de arquivo, quer seja em gabinetes de pessoal.

c. Todos os processos são guardados num local seguro, que assegure a sua integridade, confidencialidade, fiabilidade e autenticidade, garantido ao nível da segurança a prova de invulnerabilidades, perda, furto e destruição.

d. Deve ser adotada uma política de secretária limpa, sendo que o posto de trabalho deve estar organizado de modo a que não haja impressos ou suportes digitais móveis (ex. pen), com dados pessoais, chaves de arquivos físicos ou senhas de acesso a sistemas informáticos que possam ser alvo de acesso indevido por terceiros.

e. Cada trabalhador é responsável pelos documentos/processos que lhe são confiados, pelo que não os podem deixar em cima da secretária sem qualquer vigilância, ou em outro local onde não consiga garantir o sigilo.

f. Não podem ser utilizadas fotocópias que contenham dados pessoais como folhas de rascunho ou para outras finalidades, pois pode ocorrer a sua dispersão e o acesso ser facilitado a terceiros.

ENVOLVIDOS

CONSELHO EXECUTIVO

PESSOAL DOCENTE

PESSOAL NÃO DOCENTE

SERVIÇOS ADMINISTRATIVOS

IMPRESSÃO DE DOCUMENTOS

a. As impressões e/ou cópias de documentos contendo dados pessoais devem ser limitadas ao estritamente necessário.

b. A reprodução dos documentos deve ser efetuada com recurso a um sistema de impressão segura (ex. máquinas fotocopiadoras com autenticação do utilizador).

c. Todos os utilizadores devem garantir que nenhuma impressão e/ou cópia fica esquecida na impressora/fotocopiadora.

d. Devem ser destruídos, sempre que possível triturados, os documentos contendo dados pessoais que não sejam necessários arquivar, incluindo as fotocópias, utilizadas apenas como instrumento de trabalho que contenham dados pessoais.

ENVOLVIDOS

CONSELHO EXECUTIVO

PESSOAL DOCENTE

PESSOAL NÃO DOCENTE

SERVIÇOS ADMINISTRATIVOS

DISTRIBUIÇÃO FÍSICA E TRANSPORTE DE PROCESSOS E DOCUMENTOS

a. A transmissão, transferência e transporte de documentos contendo dados pessoais, quer entre diferentes serviços dentro de um mesmo edifício quer entre diferentes instalações, quando realizada em suporte físico, deve ser devidamente protegida (em envelope apropriado para o efeito e identificado como confidencial, se possível com uma caraterização específica) de modo a impedir o acesso não autorizado ao seu conteúdo.

b. A informação que contenha dados pessoais, em suporte papel, é remetida por protocolo ou por correio registado ou por correio registado com aviso de receção, estas são as três formas de garantir a segurança dos dados.

c. Na distribuição e transporte realizada por colaboradores internos, os envelopes que contenham documentos com dados pessoais devem estar permanentemente sob o controlo da pessoa que os transporta.

d. Deve ser evitada a circulação desnecessária dos processos e documentos que contenham dados pessoais.

ENVOLVIDOS

CONSELHO EXECUTIVO

PESSOAL DOCENTE

PESSOAL NÃO DOCENTE

SERVIÇOS ADMINISTRATIVOS

CONTROLO DE ACESSO APLICACIONAL
Sistema de Gestão de Correspondência

a. Devem ser definidas e parametrizadas políticas de acesso e procedimentais relativas à utilização da aplicação SGC que garantam a salvaguarda do acesso e do tratamento da informação e, em particular, o tratamento de dados pessoais.

b. Documentos referentes a processos de recursos humanos que contenham dados pessoais (concursos, requerimentos, documentos de identificação, CV, atestados médicos, licenças, férias, justificação de faltas, horas extraordinárias, ações disciplinares, contencioso, entre outros) devem ser tramitados em papel ou por correio eletrónico, Caso sejam enviados por correio eletrónico, devem ser integrados no processo físico e o correio eletrónico eliminado.

ENVOLVIDOS

CONSELHO EXECUTIVO

SERVIÇOS ADMINISTRATIVOS

UTILIZAÇÃO DO CORREIO ELETRÓNICO

a. Não utilizar o correio eletrónico profissional para tratar de assuntos particulares, nem de forma contrária às orientações e mecanismos de segurança do organismo.

b. O envio de correio eletrónico de âmbito geral (ex. newsletters, convocatórias, informações de carácter geral) para múltiplos endereços de correio eletrónico deve ser efetuado utilizando o campo BCC por forma a não expor todos os destinatários.

c. Sempre que possível, a tramitação por correio eletrónico de processos que envolvam dados pessoais deve ser evitada. Nos casos em que seja necessário, o correio eletrónico deve ser dirigido a um único destinatário, que após processamento do seu conteúdo deve eliminá-lo.

d. Não podem ser abertos anexos de correio eletrónico executáveis nem devem ser exploradas hiperligações ou anexos desconhecidos.

e. Correio eletrónico que redirecione para sites externos ao GRA, solicitando autenticação com credenciais do GRA, deve ser reencaminhado para os serviços de informática.

ENVOLVIDOS

CONSELHO EXECUTIVO

PESSOAL DOCENTE

SERVIÇOS ADMINISTRATIVOS

UTILIZAÇÃO DO CORREIO ELETRÓNICO

f. O correio eletrónico potencialmente malicioso deve ser reencaminhado para os serviços de informática.

g. Sempre que haja acesso remoto ao correio eletrónico do GRA, o utilizador deve verificar que terminou com sucesso a sessão remota.

h. O acesso pelo organismo responsável pela gestão do domínio é autorizado em situações excecionais e justificadas para despistes técnicos ou cumprimento de obrigações legais.

i. O acesso à caixa de correio eletrónico é realizado na presença do colaborador.

j. O acesso à caixa de correio eletrónico, com fundamento em ausência, apenas deve ocorrer por razões imperiosas e tem de ser claramente explicitado, e previamente comunicado ao trabalhador, sendo realizado na presença de um representante da comissão de trabalhadores ou de outra estrutura representativa ou de alguém indicado pelo trabalhador.

ENVOLVIDOS

CONSELHO EXECUTIVO

PESSOAL DOCENTE

SERVIÇOS ADMINISTRATIVOS

DISPONIBILIZAÇÃO PÚBLICA EM PORTAIS E PÁGINAS ONLINE

a. A disponibilização pública, nomeadamente em portais e páginas online, de informação, conteúdos ou documentos contendo dados pessoais que possibilitam a identificação dos titulares (incluindo fotografias) deve ser realizada em respeito para com o disposto no RGPD e demais legislação aplicável.

b. A referida disponibilização pública deve ter fundamento jurídico, ser devidamente justificada, evidenciando a licitude do tratamento e se necessário salvaguardar a obtenção de eventuais autorizações.

ENVOLVIDOS

CONSELHO EXECUTIVO

PESSOAL DOCENTE

SERVIÇOS ADMINISTRATIVOS

ATENDIMENTO TELEFÓNICO

a. No caso de atendimento telefónico sobre processos instruídos por cidadãos, não devem ser transmitidos dados ou informações de carácter pessoal sem que haja validação da identidade do titular (ex. n.º do processo, n.º cartão de cidadão).

b. Não devem ser transmitidas informações sobre os colaboradores, limitando-se apenas à respetiva disponibilidade. No caso de indisponibilidade, deve ser solicitado que se deixe recado e não deverá ser prestada nenhuma informação sobre a localização do colaborador ou a sua ausência do edifício.

c. Todos os registos, em suporte de papel, dos contatos telefónicos recebidos pela pelo serviço de atendimento telefónico têm de ser triturados após a conclusão da finalidade da recolha.

ENVOLVIDOS

CONSELHO EXECUTIVO

SERVIÇOS ADMINISTRATIVOS

TELEFONISTA

VIOLAÇÃO DAS MEDIDAS DE PROTEÇÃO DE DADOS PESSOAIS

a. Deve ser garantida a integridade e a confidencialidade dos dados pessoais, devendo ser comunicando de imediato ao superior hierárquico qualquer situação ou erro que as viole, com vista à sua imediata correção.

b. Deve ser imediatamente reportado ao superior hierárquico qualquer comportamento suspeito ou violação de segurança, incluindo pessoal, hardware, software e aplicações, comunicações, documentos ou segurança física.

c. Caso se verifiquem fugas de informação ou quebras de segurança de dados pessoais, estas devem ser reportadas de imediato ao superior hierárquico, o qual deve solicitar o envolvimento direto do EPD.

ENVOLVIDOS

TODOS
OS FUNCIONÁRIOS