REGIÃO AUTÓNOMA DOS AÇORES

SECRETARIA REGIONAL DOS TRANSPORTES E OBRAS PÚBLICAS

DIREÇÃO REGIONAL DAS OBRAS PÚBLICAS E COMUNICAÇÕES

Recomendação nº 1/2019 do Grupo de Trabalho para o RGPD do Governo Regional dos Açores

Considerando o Regulamento Geral sobre a Proteção de Dados (RGPD), Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, diretamente aplicável desde 25 de maio de 2018, que revoga a Diretiva 95/46/CE e define o novo regime jurídico de proteção de pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

Considerando que o referido Regulamento veio reforçar a proteção jurídica dos direitos dos titulares dos dados, criando novas obrigações e responsabilidades para todas as entidades no que concerne à proteção de dados, privacidade e segurança da informação, preconizando a implementação de medidas organizacionais e técnicas que garantam a salvaguarda das propriedades da informação, designadamente, a confidencialidade, integridade, disponibilidade e autenticidade, bem como a segurança da informação e do seu tratamento, de modo a prevenir acessos não autorizados, divulgação não autorizada, modificação, remoção ou eliminação de forma indevida ou ilícita.

Considerando que, neste sentido, o Governo Regional dos Açores tem vindo a desenvolver políticas organizativas, técnicas e de segurança no que concerne ao tratamento de dados pessoais nos organismos e serviços da Administração Pública Regional, incluindo o setor público empresarial.

Considerando as competências do Grupo de Trabalho responsável pela coordenação e orientação da implementação do RGPD nos departamentos do Governo Regional dos Açores, conforme Orientação 1/2018 do XII Governo Regional dos Açores, de 21 de fevereiro.

Neste âmbito, 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.

ii) 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.

iii) 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.

1. RESPONSABILIZAÇÃO E COMPROMISSO

a. De modo a assegurar a adoção das medidas propostas neste documento, é necessária uma responsabilização clara, firme e eficaz a este objetivo e ao seu cumprimento, que envolva diretamente o topo da hierarquia.

b. A implementação das medidas propostas depende do compromisso e da assunção de responsabilidades de cada elemento envolvido na cadeia de operações que envolvam o tratamento de dados pessoais. É necessário estabelecer mecanismos que permitam aferir e monitorizar de forma contínua o cumprimento e eventual ajuste das medidas adotadas.

c. Os recursos envolvidos na adoção das medidas propostas devem ser proactivos na identificação de situações ou processos envolvendo operações de tratamento de dados pessoais que possam não estar conformes, bem como em sugerir medidas no âmbito da sua atividade que promovam o saneamento das situações identificadas.

2. 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.

3. SEGURANÇA FÍSICA DOS PROCESSOS

3.1. 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.

3.2. 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.

3.3. 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.

4. CONTROLO DE ACESSO À REDE INFORMÁTICA

a. As redes Wi-Fi disponibilizadas nas instalações que possibilitem ligação à RAGRA devem usar encriptação forte e autenticação centralizada e individual.

b. As credenciais únicas de acesso aos sistemas (*username* e *password*) não podem ser partilhadas, nem definidas de forma facilmente identificável.

c. Cada utilizador deve tomar as precauções necessárias para evitar o acesso de terceiros aos sistemas.

d. Não podem ser utilizadas as mesmas credenciais de acesso do GRA em *sites* ou serviços externos.

e. Para garantir a segurança das credenciais de acesso, deve proceder-se à alteração das mesmas com regularidade (90 dias), ou quando a alteração for exigida e/ou quando se suspeite do comprometimento das mesmas.

f. A password deve ter no mínimo 9 caracteres e ser complexa. A sua composição deverá exigir a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas, letras maiúsculas, números e caracteres especiais.

g. Devem ser tomadas precauções no início de sessão dos sistemas em aplicações ou bases de dados (certificando-se, por exemplo, de que não há pessoas próximas que consigam visualizar as credenciais utilizadas).

h. Nas situações em que é necessário abandonar a estação de trabalho, deve ser ativado manualmente o bloqueio do ecrã e, no final do dia, encerrada a sessão de trabalho.

i. De modo a evitar situações de "esquecimento", o bloqueio automático do ecrã da estação de trabalho deve ser ativado, preferencialmente, após 5 minutos de inatividade, podendo ser desbloqueado apenas com credenciais de acesso.

j. O acesso remoto às aplicações do GRA não deve ser efetuado a partir de equipamentos e/ou redes de acesso público.

k. O colaborador não pode tentar aceder a aplicações informáticas e outros recursos cujas permissões não lhe tenham sido previamente atribuídas.

l. Relativamente a pessoas não autorizadas, é proibido proporcionar o acesso ou revelar informação não só sobre os dados pessoais tratados, mas também relativa aos procedimentos de tratamentos de dados e às tecnologias de informação.

m. Não devem ser ignorados os alertas de segurança do sistema.

n. Não podem ser instalados *softwares* ou executadas aplicações de origem desconhecida, com o objetivo de se evitarem códigos maliciosos (ex. vírus, *trojan*, *worms* ou scripts não autorizados).

o. Os utilizadores não devem ter privilégios de administração do posto de trabalho.

p. Não podem ser efetuadas configurações de *hardware* e/ou *software* do sistema sem autorização prévia.

q. Os colaboradores que utilizem equipamentos portáteis são responsáveis por salvaguardar o acesso de terceiros aos mesmos e devem notificar de imediato os serviços de informática em caso de perda ou roubo.

r. Os colaboradores que utilizem equipamentos portáteis devem evitar que os mesmos se conectem a redes Wi-Fi não seguras (abertas).

s. Sempre que possível, devem ser implementados sistemas de encriptação nos equipamentos portáteis do GRA.

t. A transmissão e transferência de dados em suporte digital móvel, quer entre diferentes serviços dentro de um mesmo edifício quer entre diferentes instalações, deve ser efetuada em dispositivos eletrónicos de armazenamento (ex. CD, USB Flash Drives, Hard Disks, SSD) com cifragem e autenticação. Os dados pessoais devem estar permanentemente sob o controlo da pessoa que os transporta.

u. Gestão do ciclo de vida do utilizador:

   i) o departamento responsável pelo processo individual do colaborador deve despoletar o pedido de criação de acesso informático para novos utilizadores;

   ii) se ocorrer mudança de serviço ou funções de um colaborador, o departamento responsável pelo processo individual do colaborador deve solicitar a alteração dos acessos e credenciais desse colaborador aos serviços de informática, se aplicável;

   iii) aquando da cessão de funções do colaborador, o departamento responsável pelo processo individual do colaborador deve solicitar a remoção dos acessos, eliminação das credenciais e indicar qual o tratamento

que deve ser dado à informação existente aos serviços de informática. É, igualmente, da sua responsabilidade solicitar ao colaborador a devolução dos equipamentos que lhe estavam afetos, se aplicável.

5. CONTROLO DE ACESSO APLICACIONAL

5.1. 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.

5.2. 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.

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.

5.3. 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.

6. 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. nº do processo, nº 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.

7. 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.

Ponta Delgada, 22 de julho de 2019

O DIRETOR REGIONAL

FREDERICO FURTADO SOUSA