O **Regulamento Geral sobre a Proteção de Dados,** Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho da União Europeia, de 27 de Abril de 2016, diretamente aplicável a partir de 25 de Maio de 2018, 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, reforçando a proteção jurídica dos direitos dos titulares dos dados e criando novas obrigações e responsabilidades para todas as entidades públicas e privadas. Neste sentido, o Governo Regional dos Açores tem vindo a desenvolver políticas organizativas, técnicas e de segurança no que concerne o tratamento de dados pessoais na Administração Pública Regional, que garantam a conformidade com o Regulamento Geral sobre a Proteção de Dados.

1. Conceitos gerais

Dados pessoais: toda a informação relativa à identificação ou que possa levar à identificação do seu titular de forma direta ou indireta.

Responsável pelo Tratamento dos Dados Pessoais: pessoa singular ou coletiva, autoridade pública, entidade, instituição ou outro organismo que determina as finalidades e os meios de tratamento de dados pessoais e aplica as medidas técnicas e organizativas adequadas para assegurar e comprovar que o tratamento é realizado em conformidade com o regulamento.

Tratamento de Dados Pessoais: entendem-se por operações tratamento de dados pessoais a recolha, registo, consulta, utilização, modificação, análise, transferência, conservação, apagamento ou destruição dos mesmos.

Princípios relativos ao tratamento de dados pessoais:

i. Licitude, lealdade e transparência: os dados pessoais são objeto de tratamento lícito, leal e transparente em relação ao titular dos dados.

ii. Limitação de finalidade: os dados pessoais recolhidos para finalidades determinadas, explícitas e legítimas.

iii. Minimização de dados: os dados pessoais recolhidos são adequados e pertinentes e limitados ao que é necessário relativamente à finalidade do tratamento.

iv. Exatidão: os dados pessoais devem ser exatos e atualizados sempre que necessário.

v. Limite da conservação: os dados pessoais serão conservados apenas durante o tempo necessário para as finalidades a que foram recolhidos.

vi. Integridade e confidencialidade: os dados pessoais serão tratados de forma que garanta a sua segurança e proteção, incluindo proteção contra o seu tratamento não autorizado ou ilícito.

vii. Responsabilidade: o responsável pelo tratamento dos dados pessoais tem a obrigação de garantir os princípios colocados e deve poder comprovar esta garantia.

Direitos dos titulares de dados: os titulares dos dados têm o direito à informação (finalidades, responsável do tratamento, prazo de conservação, etc.), o direito ao acesso, à retificação, ao esquecimento, à portabilidade dos dados, a limitar ou opor-se ao tratamento dos seus dados pessoais, a apresentar reclamação junto à autoridade de controlo e a recorrer a ação judicial.

2. Procedimento interno de resposta ao Exercício dos Direitos: a partir de 25 de maio, será disponibilizada uma minuta de requerimento que deverá ser presencialmente preenchida pelo requerente (titular dos dados), devendo verificar-se a identidade do titular dos dados mediante a apresentação do documento de identificação (B.I. / Cartão de Cidadão) e enviar a cópia digitalizada do requerimento preenchido para rgpd@azores.gov.pt para que lhe seja dado seguimento pelo respetivo responsável.

Em seguida, deve ser entregue ao requerente uma cópia digitalizada do requerimento preenchido e destruído o original.

3. Boas Práticas Comportamentais: Todos os colaboradores devem garantir a confidencialidade e a segurança do tratamento dos dados pessoais no decorrer das suas atividades profissionais, de modo a prevenir-se, igualmente, contra acessos ou divulgações não autorizados, consulta, alteração, cópia ou eliminação dos dados pessoais de forma indevida ou ilícita. Cada colaborador é individualmente responsável por respeitar as políticas de privacidade e segurança preconizadas, devendo adotar as seguintes medidas, entre outras, no que concerne as operações de tratamento de dados pessoais em suporte físico e digital:

- Garantir o sigilo profissional relativamente a informação interna ou dos utentes, clientes ou outros, atuando com discrição em relação aos dados e informações recolhidas, respeitando o princípio da confidencialidade;
- Não revelar a pessoas não autorizadas ou a terceiros informação não só sobre os dados pessoais que trata, mas também qualquer informação relativa aos procedimentos de tratamentos de dados e às tecnologias de informação
- Realizar o acesso e as operações de tratamento de dados pessoais apenas para os fins autorizados. A recolha, acesso, divulgação ou outra operação de tratamento não autorizada é punível por lei.
- Organizar a estação de trabalho de modo a que não hajam impressos com dados pessoais, chaves de arquivos físicos ou senhas de acesso a sistemas informáticos que possam ser alvo de acesso indevido por terceiros;
- Todos os colaboradores têm um username e password únicos e estes não podem ser partilhados com qualquer outro colaborador;
- Tomar as precauções necessárias para evitar o acesso de terceiros, sendo que a segurança das credenciais de acesso ao sistema e dados pessoais é também da responsabilidade do utilizador;
- Proceder à alteração das credenciais de acesso e passwords com regularidade, ou quando a alteração lhes for exigido e/ou quando se suspeite do comprometimento das mesmas;
- Tomar precauções ao executar de início de sessão no sistema, em aplicações ou bases de dados (certificando-se, p.ex., de que não há pessoas próximas que consigam visualizar os caracteres que estão a ser digitados);
- Nas situações em que é necessário deixar a estação de trabalho, ativar manualmente o bloqueio do ecrã e no final do dia, encerrar a sessão de trabalho;
- Não é permitida a tentativa de acesso ou o acesso não autorizado a aplicações informáticas cujo acesso não tenha sido previamente atribuído ao colaborador (ou unidade orgânica); e é interdito a qualquer colaborador proporcionar o acesso a terceiros a qualquer informação ou software;
- Não ignorar os alertas de segurança do sistema, modificar qualquer programa ou aceder às áreas para as quais não tenham sido especificamente autorizados;
- Não instalar softwares ou executar aplicações de origem desconhecida, evitando códigos maliciosos (por exemplo, vírus, trojan, worms ou scripts não autorizados);
- A configuração de hardware e software do sistema não deve ser alterada sem autorização prévia;
- Nenhum colaborador pode fazer, ou executar por qualquer forma, direta ou indireta, cópias de bases de dados, documentação, arquivos físicos, software, ou outros relacionados com dados pessoais e o seu tratamento que não reportem diretamente ao exercício da sua atividade profissional;
- Em caso da utilização de dispositivos removíveis de armazenamento (ex: PEN´s), devem ser tomadas as medidas necessárias para impedir que os suportes de dados possam ser lidos, copiados ou alterados por pessoas não autorizadas;
- No caso dos suportes de dados em papel, a impressão e/ou cópias de documentos contendo dados pessoais devem ser limitadas ao estritamente necessário e todos os utilizadores devem garantir que nenhuma impressão e/ou cópia fica esquecida na impressora/fotocopiadora;

- Garantir a integridade dos dados, salvaguardado a respetiva confidencialidade, comunicando de imediato ao responsável hierárquico qualquer situação ou erro que viole a integridade da utilização e da introdução de dados, com vista à imediata correção dos erros detetados;
- Proceder ao reporte imediato ao superior hierárquico de qualquer comportamento suspeito do sistema ou violação da segurança do sistema, incluindo pessoal, hardware, software, comunicações, documentos ou segurança física.