

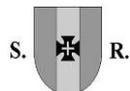


Gabinete do Encarregado-Geral
de **Proteção de Dados**

POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS PARA A ADMINISTRAÇÃO PÚBLICA DA REGIÃO AUTÓNOMA DA MADEIRA

Documento Ref.	RGPD-DOC-05-2
Versão:	1.0
Data:	Junho de 2022
Autor:	SRF-GEGPD
Proprietário:	Governo Regional da Madeira (GRM)





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

Revisões - Histórico

Versão	Data	Autor da Revisão	Sumário das Alterações

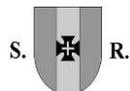
Distribuição

Nome	Função

Aprovação

Nome	Cargo	Assinatura	Data
Martin Freitas	Encarregado-Geral de Proteção de dados		





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

Índice

POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS PARA A ADMINISTRAÇÃO PÚBLICA DA REGIÃO AUTÓNOMA DA MADEIRA.....	1
1. SUMÁRIO EXECUTIVO	4
2. ENQUADRAMENTO RELATIVO AO TRATAMENTO DE DADOS PESSOAIS	5
3. POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS	6
3.1 Regulamento Geral sobre a Proteção de Dados	6
3.2 Definições	6
3.3 Identificação dos intervenientes no processo de tratamento de dados pessoais	7
3.4 Princípios relativos ao tratamento de dados pessoais	7
3.5 Direito dos titulares de Dados Pessoais	8
3.4 Licidade do tratamento	10
3.5 Segurança no tratamento e dos dados pessoais	13
3.6 Contratos que envolvam o tratamento de dados pessoais	14
3.7 Transferências Internacionais de Dados Pessoais	14
3.8 Encarregado da Proteção de Dados	14
3.9 Notificação de Violação de Dados (<i>Data Breach</i>)	15
4. MODELO DE GOVERNAÇÃO E DE APLICAÇÃO DA PRESENTE POLÍTICA	16
5. METODOLOGIA PARA A CONFORMIDADE COM O RGPD	17





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

1. SUMÁRIO EXECUTIVO

A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental.

A Política Geral de Proteção de Dados (doravante, PGPD) tem o intuito de assegurar, na Administração Pública Regional (APR), um nível coerente e elevado de proteção dos dados pessoais das pessoas singulares, direito esse que deve ser ponderado e equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.

Deste modo, a PGPD determina e uniformiza o modo como os diferentes serviços públicos regionais e respetivos trabalhadores abordam as obrigações do Regulamento Geral sobre a Proteção de Dados Pessoais (RGPD)¹, encaminhando as suas atividades de tratamento de dados pessoais rumo à conformidade.

Em traços gerais, a presente política aborda o enquadramento legislativo a ter em consideração, as definições e a terminologia do RGPD, os princípios relativos ao tratamento de dados pessoais, os direitos dos titulares de dados pessoais, a licitude que justifique o seu tratamento, a segurança no tratamento dos dados pessoais, as responsabilidades dos diversos intervenientes em causa; o papel do Encarregado da Proteção de Dados e as os procedimentos RGPD entre os quais as notificações em caso de violação de dados. Adicionalmente, são apresentadas medidas imprescindíveis para assegurar a progressiva conformidade com o RGPD, garantindo a sua demonstração por parte dos devidos intervenientes.

De modo concludente, apresenta o modelo de governação do Governo Regional da Madeira e os mecanismos procedimentais indispensáveis para a sua implementação.

Tal Política seguirá complementada por políticas específicas em matéria de dados pessoais (designadamente, políticas de segurança da informação, a política de cookies, entre outras), e por outras políticas a serem desenvolvidas pela entidade com a tutela da área da informática.

O controlo, auditoria e fiscalização das políticas de proteção de dados será da entidade competente para orientação e fiscalização da aplicação geral do Regulamento Geral sobre a Proteção de Dados (RGPD) e da Lei n.º 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do RGPD, a qual é assegurada pelo serviço indicado no anexo I, com competências de Encarregado Proteção de Dados (EPD).

¹ Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (RGPD).





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

2. ENQUADRAMENTO RELATIVO AO TRATAMENTO DE DADOS PESSOAIS

A Administração Pública Regional no exercício da sua atividade procede ao tratamento de uma série de dados pessoais de diversos tipos de titulares dos dados, **incluindo, nomeadamente:**

- Trabalhador / Funcionário
- Utente / Cliente
- Cidadão
- Colaborador / Parceiro / Fornecedor / Prestador de serviço / Investidor
- Aluno / Formando
- Docente / Formador
- Encarregado de Educação
- Representante Legal
- Investigador / Historiador
- Candidato
- Subscritor
- Turista / Visitante (físico e/ou online)
- Agente (Desportivo; Cultural; Segurança, ...)
- Emigrante / Imigrante
- Voluntário
- ex-Trabalhador
- Outros (em consonância com o catálogo de categorização de titulares de dados atualizado).

Por proceder ao tratamento destas categorias de titulares de dados, a Administração Pública Regional está sujeita à legislação que determina de que modo este tratamento pode ser efetuado e as medidas de segurança e de salvaguarda que devem ser tomadas para a proteção destes dados pessoais.

A presente política teve em consideração a legislação mais relevante em matéria de proteção de dados e descreve as etapas que os departamentos da Administração Pública Regional devem adotar para garantir a sua conformidade com a legislação em vigor.

Por conseguinte, esta Política aplica-se a todas as pessoas, procedimentos e processos que fazem parte da Administração Pública Regional, incluindo, os dirigentes, os trabalhadores, os fornecedores/ prestadores de serviços e quaisquer outros terceiros que, direta ou indiretamente interajam e/ou acedam aos sistemas de informação do Governo Regional da Madeira (GRM).

A adoção dos valores e princípios expressos nesta política não é uma opção: deve ser seguida por todos os trabalhadores e serviços da Administração Pública Regional, sem exceção.





3. POLÍTICA GERAL DE PROTEÇÃO DE DADOS PESSOAIS

3.1 Regulamento Geral sobre a Proteção de Dados

O Regulamento Geral sobre a Proteção de Dados (RGPD) é uma das legislações mais relevantes e que veio regular o modo como as entidades devem proceder ao tratamento de dados pessoais. A Administração Pública Regional pretende garantir a sua conformidade, de uma forma clara, transparente e demonstrável, com 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 e com a Lei n.º 58/2019 (doravante Lei Nacional de Execução), de 8 de agosto, que assegura a execução, na ordem jurídica nacional do referido regulamento e com toda a legislação relevante em matéria de privacidade e proteção de dados.

3.2 Definições

O RGPD contempla 26 definições de conceitos relevantes em matéria de proteção de dados pessoais, das quais destacamos as que consideramos mais importantes para esta Política, a saber:

‘Dados Pessoais’: informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

‘Categorias especiais de dados pessoais’: dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

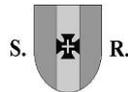
‘Tratamento’: operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

‘Pseudonimização’: o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;

‘Responsável pelo tratamento’: a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

‘Subcontratante’: uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

dados pessoais por conta do responsável pelo tratamento destes;

'Destinatário': uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento;

'Terceiro': a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;

3.3 Identificação dos intervenientes no processo de tratamento de dados pessoais

Previamente a qualquer procedimento a desenvolver, tendo em vista a conformidade com o RGPD, afigura-se imprescindível identificar os diversos intervenientes e em que papel as entidades da Administração Pública Regional realizam as atividades de tratamento de dados pessoais:

- Responsável pelo tratamento;
- Responsável conjunto;
- Subcontratante;
- Terceiro.

Para o efeito de avaliação do papel em que cada entidade da Administração Pública Regional intervém em cada operação de tratamento de dados pessoais, desenvolveu-se um procedimento específico para enquadrar as responsabilidades dos diferentes intervenientes.

3.4 Princípios relativos ao tratamento de dados pessoais

Em compromisso permanente com a salvaguarda dos dados pessoais sob o tratamento das entidades administrativas, a Administração Pública Regional (APR) estabelece como primordial o cumprimento dos princípios gerais enunciados pelo Regulamento, designadamente:

- a) Na relação com os titulares de dados, a APR assegura que as operações de tratamento de dados decorram com respeito pelas bases de licitude para a sua prossecução; que o tratamento atenda a uma relação de equilíbrio em consonância com a posição e maturidade do titular; e que as informações manifestadas permitam o fácil acesso e compreensão (**Princípio da licitude, lealdade e transparência**);
- b) A APR estabelece quais os dados pessoais a serem recolhidos para finalidades determinadas, explícitas e legítimas, não podendo os mesmos ser tratados posteriormente de uma forma incompatível com as finalidades originárias (**Princípio da limitação das finalidades**);





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

- c) São objeto de tratamento apenas os dados pessoais estritamente pertinentes, adequados e limitados ao necessário relativamente às finalidades traçadas (**Princípio da minimização dos dados**);
- d) A APR assegura que os dados pessoais sejam corrigidos e atualizados sempre que necessário, garantido a adoção de medidas que garantam o exercício da retificação e apagamento de dados inexatos (**Princípio da exatidão**);
- e) Os dados pessoais são submetidos a uma conservação prudente, de forma que possibilite a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados, sem demérito da sua conservação em arquivo de interesse público, para fins estatísticas, históricos ou de investigação científica (**Princípio da conservação**);
- f) Será imperativa a adoção de medidas técnicas e organizacionais que garantam a segurança dos dados pessoais, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação (**Princípio da integridade e confidencialidade**).
- g) O responsável pelo tratamento é responsável pelo cumprimento do RGPD e tem de poder comprová-lo. (**responsabilidade**).

A Administração Pública Regional deve cumprir com todos os requisitos legais e atuar em conformidade com estes Princípios, quer seja nos tratamentos de dados pessoais já implementados, quer seja pela introdução de novos métodos e metodologias de tratamento, tais como, novos sistemas de tecnologia e de informação.

3.5 Direito dos titulares de Dados Pessoais

O titular de dados pessoais detém um catálogo de direitos passíveis de serem exercidos nos termos do RGPD, entre os quais:

- Direito à Informação;
- Direito de Acesso;
- Direito de Retificação;
- Direito ao Apagamento dos Dados;
- Direito à Limitação do tratamento;
- Direito à Portabilidade;
- Direito de Oposição;
- Direitos relativos a decisões individuais automatizadas, incluindo definição de perfis;
- Direito à comunicação sobre a ocorrência de violação dos seus dados pessoais (quando aplicável).

Para o exercício destes Direitos afigura-se imprescindível a existência de procedimentos apropriados de modo que, por um lado, os Titulares dos Dados possam solicitar o exercício dos seus direitos e, sendo caso disso, obtê-lo a título gratuito, e por outro, que as entidades da Administração Pública Regional possam tomar as medidas adequadas para dar seguimento aos pedidos dos Titulares dos Dados, dentro dos prazos estipulados no





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

Regulamento Geral sobre a Proteção de Dados. Se o titular dos dados apresentar o pedido por meios eletrónicas, a sua resposta deve ser emanada, sempre que possível, pela mesma via, salvo pedido em contrário do titular.

Prazos de resposta aos pedidos dos titulares dos dados, a contar da data da receção do pedido:

Direitos dos Titulares dos Dados	Prazos
Direito à Informação	Imediato quando os dados são recolhidos junto do titular dos dados ou dentro de um prazo razoável quando forem obtidos a partir de outra fonte.
Direito ao Acesso	Sem demora injustificada, o mais tardar no prazo de um mês*.
Direito à Retificação e notificação	Sem demora injustificada, o mais tardar no prazo de um mês*.
Direito ao Apagamento e notificação	Sem demora injustificada, o mais tardar no prazo de um mês*.
Direito à Limitação do tratamento e notificação	Sem demora injustificada, o mais tardar no prazo de um mês*.
Direito à Portabilidade	Sem demora injustificada, o mais tardar no prazo de um mês*.
Direito de Oposição	Sem demora injustificada, o mais tardar no prazo de um mês* ou no momento da primeira comunicação ao titular dos dados.
Direitos relativos a decisões individuais automatizadas, incluindo definição de perfis	Não especificado. Por analogia com prazos máximos das outras respostas, no prazo de um mês.
Direito à comunicação sobre a ocorrência de violação dos seus dados pessoais (quando aplicável)	Sem demora injustificada (cfr. considerando 86 do RGPD).

Tabela 1 - Definição de prazos de resposta a pedidos dos Titulares de Dados

** Possibilidade de prorrogação até dois meses, quando seja necessário, atendendo à complexidade do pedido e o número de pedidos (a prorrogação do prazo de resposta deverá ser informada ao titular de dados, juntamente com os motivos da demora).*

Quando a Administração Pública Regional considerar que o pedido de exercício do direito do titular dos dados deve ser indeferido, é imperativo, em resposta, expor as razões do indeferimento, entre as quais:

- Impossibilidade de verificar comprovadamente a identidade do requerente;
- Falta de legitimidade ativa para formular o pedido – quando a pessoa não seja a titular dos dados pessoais sobre os quais pretende exercer ou não seja representante do titular;
- Falta de justificação documental de representação para deduzir o pedido – sujeito representante que não apresente documento comprovativo dessa qualidade;
- Falta de concretização do pedido – quando não seja possível compreender sobre quais os dados pessoais pretende o exercício do direito;
- Conflito com direitos e liberdades de terceiros, inclusive a proteção de dados pessoais de terceiros;
- Limitação de direitos por cumprimento de medidas legislativas necessárias e proporcionadas numa sociedade democrática (cfr. Artigo 23.º do RGPD);
- Impraticabilidades específicas de cada direito a exercer.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

Nessa resposta de indeferimento, deve informar o titular da possibilidade de apresentar reclamação a uma autoridade de controlo e intentar ação judicial (cfr. n.º 4 do artigo 12.º do RGPD).

3.4 Licitude do tratamento

Consoante as bases de licitude contempladas pelo RGPD, que legitimam o tratamento de dados pessoais (artigo 6.º do RGPD) e o tratamento de categoriais especiais de dados (artigo 9.º do RGPD), é intenção da Administração Pública Regional identificar os fundamentos legais apropriados a cada tipo de tratamento de dados pessoais, bem como, documentar todos os tipos de tratamento, de acordo com o Regulamento Geral sobre a Proteção de Dados.

Os fundamentos de licitude do tratamento do artigo 6.º são:

- **Base Contratual - Para execução de um contrato ou diligências pré-contratuais:** Quando os dados pessoais recolhidos e tratados forem necessários para o cumprimento de um contrato com o titular de dados ou para diligências pré-contratuais a pedido do titular.
- **Obrigação Jurídica - Para cumprimento de uma obrigação jurídica:** Sempre que os dados pessoais são recolhidos e alvo de tratamento para cumprir uma obrigação jurídica a que o responsável pelo tratamento está sujeito (releva suportar com a respetiva base legal).
- **Interesses Vitais - Para defesa dos interesses vitais:** Caso em que os dados pessoais são necessários para proteger os interesses vitais do titular de dados ou de outra pessoa singular. A Administração Pública Regional manterá provas documentadas razoáveis para estes casos, sempre que este seja o fundamento legal para o tratamento de dados pessoais.
- **Interesse Público:** Quando o tratamento de dados pessoais seja necessário:
 - Ao exercício de funções de interesse público, como tal definidas pelo direito da EU ou por normas a que o responsável pelo tratamento está sujeito;
 - Ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento.

A avaliação de interesse público ou de dever será sempre documentada e disponibilizada como prova, quando necessário.

- **Consentimento:** em casos muito específicos em que não seja aplicável outros motivos de licitude, a Administração Pública Regional poderá solicitar o consentimento explícito para tratamento de dados pessoais, determinando sempre quais as finalidades específicas.

Quando estejam em causa dados pessoais de menores, deve ser obtido o consentimento dos titulares das responsabilidades parentais, excecionando-se apenas as situações de oferta de serviços da sociedade da informação em que o consentimento das crianças é lícito se elas tiverem pelo menos 13 anos.

Devem ser ainda fornecidas informações sobre a utilização dos dados aos respetivos titulares, no momento da sua recolha, bem como, dos seus direitos em relação aos dados e o direito de retirar o seu consentimento a qualquer momento. Estas informações são prestadas de modo inteligível e de fácil acesso e numa





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

linguagem clara e simples.

Sempre que os dados pessoais não sejam obtidos diretamente junto do Titular, estas informações devem ser prestadas ao titular dos dados, com a maior brevidade possível, nunca excedendo o prazo de um mês. Devem ainda ser fornecidas informações acerca da identidade e contactos do responsável pelo tratamento e os contactos do encarregado da proteção de dados.

Em resumo, o consentimento é válido quando o titular de dados consinta o tratamento dos seus dados pessoais para uma ou mais finalidades específicas, de forma:

- Específica, informada e inequívoca - com possibilidade de manifestar o consentimento de forma separada, consoante as finalidades;
 - Válida - sendo o titular informado sobre o seu objeto e consequências, de modo inteligível, de fácil acesso e numa linguagem clara e simples;
 - Livre - quando titular exerça uma verdadeira escolha e não existir risco de fraude, intimidação, coação ou consequências negativas importantes caso seja recusado o tratamento (sem relação de desequilíbrio);
 - Mediante declaração ou ato positivo inequívoco;
 - Comprovável - responsável capacitado para demonstrar o consentimento manifestado; e
 - Suscetível de ser retirado em qualquer momento (retirada não compromete a licitude do tratamento efetuado até esse ato).
- **Para a prossecução de interesses legítimos:** sempre que o tratamento de dados pessoais for do interesse legítimo da Administração Pública Regional e, após análise, se entender que não afeta os direitos e liberdades do titular de dados de maneira significativa. A análise deve ser documentada e disponibilizada sempre que solicitada pelo titular de dados alvo dessa apreciação (Avaliação de Interesse Legítimo).

Da Avaliação de Interesse Legítimo, deve constar os seguintes elementos:

- Análise dos interesses legítimos do responsável ou de terceiros;
- Ponderação dos direitos e liberdades fundamentais dos titulares que possam vir a ser lesados; e
- Análise das expectativas razoáveis dos titulares dos dados, garantindo que estes possam razoavelmente prever esse tratamento adicional.

Nota: A prossecução das atribuições das entidades públicas, de carácter administrativo, não é abrangida pelo critério dos interesses legítimos – faz-se por intermédio de ato legislativo, nos termos do n.º 2 do artigo 3.º e no n.º 2 do artigo 266.º, ambos da Constituição da República Portuguesa (CRP) e no artigo 3.º (Princípio da Legalidade) do Código do Procedimento Administrativo (CPA).

Relativamente aos fundamentos de licitude do artigo 9.º:

- **Consentimento Explícito:**

De utilização residual, o consentimento deve ser explícito (além de preencher as características aplicáveis nos termos do artigo 6.º). Implica a manifestação expressa por parte do titular dos dados, nomeadamente:





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

- Por declaração escrita e assinada;
- Com preenchimento de formulário eletrónico específico ou envio de uma mensagem de correio eletrónico;
- Por declaração oral (gravada), em casos específicos.

● **Obrigações e exercícios de direitos:**

Se o tratamento for necessário para cumprimento de obrigações e exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação:

- Laboral;
- Segurança social; e
- Proteção social.

● **Interesses Vitais**

Quando o tratamento seja necessário para proteção de interesses vitais do titular de dados ou outra pessoa singular, caso o titular de dados esteja física ou legalmente incapacitado de dar o consentimento.

● **Atividades legítimas em organismos sem fins lucrativos**

Se tratamento decorrer no âmbito de atividades legítimas de uma fundação, associação ou outros organismos sem fins lucrativos, desde que:

- Prossigam fins políticos, filosóficos, religiosos ou sindicais;
- Os dados pessoais digam respeito a membros ou antigos membros ou a pessoas que tenham mantido contactos regulares relacionados com os seus objetivos; e
- Não haja divulgação a terceiros (exceto se fundamentada em consentimento).

● **Tornados públicos pelo titular**

Quando dados pessoais a serem tratados tenham sido manifestamente tornados públicos pelo seu titular.

● **Influência sob um direito num processo judicial**

Quando o tratamento seja necessário à declaração, ao exercício ou à defesa de um direito num processo judicial, ou sempre que os tribunais atuem no exercício das suas funções jurisdicionais.

● **Interesse público importante**

Quando o tratamento seja fundamentado por motivos interesse público importante, com base no direito da União ou de um Estado-Membro.

● **Medicina preventiva ou do trabalho**

Se o tratamento for necessário para medicina preventiva e do trabalho*, nomeadamente:

- Avaliação da capacidade de trabalho do funcionário;
- Diagnóstico médico, prestação de cuidados ou tratamento de saúde ou de ação social; ou
- Gestão de sistemas e serviços de saúde ou de ação social.

*Desde que o profissional esteja sujeito à obrigação de sigilo profissional.

● **Interesse público (no domínio da saúde pública)**

Quando o tratamento seja necessário por motivo de interesse público no domínio da saúde pública, nomeadamente:

- Proteção contra ameaças transfronteiriças graves para a saúde; ou
- Para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde, dos medicamentos ou dispositivos médicos.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

- **Fins arquivísticos, científicos, históricos ou estatísticos**

Quando o tratamento seja necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, desde que:

- Sejam adotadas medidas técnicas e organizacionais de segurança dos dados (v.g. pseudonimização);
- Seja pautado pelo princípio da minimização dos dados; e
- Transite para novos tratamentos que já não permitam a identificação dos titulares dos dados (quando possível).

3.5 Segurança no tratamento e dos dados pessoais

A Administração Pública Regional (APR) na persecução das suas atividades procurará desenvolver e implementar, o quanto possível, um conjunto de procedimentos e tecnologias de segurança adequadas por forma a assegurar um nível de proteção e confidencialidade apropriados ao risco, nomeadamente, à proteção contra qualquer forma de tratamento indevido ou ilegítimo, contra qualquer perda ou destruição de dados acidental ou ilícita, acesso ou divulgação não autorizados.

A Administração Pública Regional, sempre que possível, deve adotar os princípios da Proteção de dados desde a conceção e por defeito (Data Protection by Design and by Default) e deve assegurar que todos os novos projetos, processos e procedimentos que venha a adotar, levarão em consideração, desde o seu planeamento, os meios de tratamento e as medidas que garantam a segurança dos dados pessoais ao longo do seu ciclo vital, inclusive na sua destruição.

Desde a conceção, a Administração Pública Regional desenhará vias procedimentais que possibilitem o titular de dados controlar o tratamento das suas informações pessoais, o que implica uma relação de transparência relativamente às funções e operações de tratamento sobre os seus dados.

Adicionalmente, levará a cabo a realização de avaliações de impacto sobre a proteção de dados (AIPD) antes de decorrer o tratamento de dados pessoais, quando tal seja legalmente exigido, servindo de mecanismo de identificação de riscos sobre os direitos e liberdades das pessoas e de alinhamento das medidas necessárias à sua mitigação.

As Avaliações de Impacto sobre a Proteção de Dados (AIPD) devem incluir, entre outras componentes:

- Descrição acerca dos dados pessoais que serão processados e quais as respetivas finalidades;
- Avaliação sobre se o tratamento de dados pessoais proposto é necessário e proporcional à(s) sua(s) finalidade(s);
- Avaliação dos riscos sobre os direitos e liberdades dos titulares de dados pessoais;
- Quais as medidas necessárias para mitigar os riscos identificados e demonstrar a conformidade com a legislação.

A utilização de técnicas e tecnologias que permitam a minimização de dados e a pseudonimização serão levadas em consideração, sempre que se mostre adequado e apropriado.

A equipa que elabora a AIPD, em conjugação com o interlocutor, deve ter em consideração o procedimento e os





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

fluxos de comunicação criados e aprovados para o efeito.

Por definição, a Administração Pública Regional desenha os procedimentos por forma a que sejam operacionalizados e selecionados os dados pessoais estritamente necessários para cada finalidade específica do tratamento, por forma a que a quantidade de dados recolhidos, a extensão do tratamento e a sua acessibilidade estejam, por padrão, direcionados para a privacidade da pessoa. Assim, os dados pessoais do titular serão disponibilizados a um número de pessoas realmente relevantes e interessadas no procedimento.

3.6 Contratos que envolvam o tratamento de dados pessoais

A Administração Pública Regional garantirá que todas as relações contratuais que envolvam o tratamento de dados pessoais, estão sujeitas a um contrato escrito, com aditamento de cláusulas de confidencialidade e de tratamento de dados pessoais.

Na fase pré contratual dos procedimentos aquisitivos e nos contatos que venham a ser celebrados devem ser sempre colocadas cláusulas relativas à confidencialidade e a proteção de dados pessoais.

3.7 Transferências Internacionais de Dados Pessoais

A Administração Pública Regional poderá efetuar transferências internacionais de dados pessoais para finalidades determinadas, explícitas e legítimas.

As transferências de dados pessoais para países fora da União Europeia serão prévia e cautelosamente analisadas, por forma a garantir que o nível de proteção providenciado nos países terceiros ou organizações internacionais para os quais os dados sejam transferidos, estejam em equivalência com a proteção de dados pessoais exigida no Regulamento comunitário. Para tal a Administração Pública Regional verifica a existência de decisões de adequação emitidas pela Comissão Europeia, sob pena de aplicar garantias adequadas ou regras aplicáveis ao setor empresarial, com o intuito de criar condições para que os titulares de dados gozem dos mesmos direitos oponíveis.

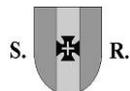
Caso ocorram transferências internacionais de dados, o tratamento deve ser lícito, leal e transparente em relação ao titular dos dados.

3.8 Encarregado da Proteção de Dados

A nomeação de um Encarregado da Proteção de Dados é exigida pelo Regulamento Geral sobre a Proteção de Dados, sempre que a organização seja uma autoridade ou organismo público, ou se a entidade em causa efetuar tratamento de dados pessoais que exija um controlo regular e sistemático dos titulares dos dados em grande escala, ou, ainda, se efetuar tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações.

Face a esta obrigatoriedade, para os organismos públicos o Governo Regional criou a entidade referida no anexo I da presente política, que atua no âmbito das suas atribuições e competências, assegurando de forma interdepartamental e para toda a Administração Pública Regional, o controlo, auditoria e fiscalização da aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD) e da Lei n.º 58/2019, de 8 de agosto, a fim de salvaguardar os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos de dados pessoais.





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

Adicionalmente, procedeu à nomeação do Encarregado Geral de Proteção de Dados (EPD) para as entidades da Administração Pública Regional.

O Encarregado de Proteção de Dados (EPD) desempenha as funções elencadas no artigo 39.º do RGPD e no artigo 11.º da Lei n.º 58/2019, de 8 de agosto, num quadro de independência e autonomia.

Nos termos dos artigos 37.º, 38.º e 39.º do RGPD, e em conformidade com as linhas orientadoras do WP 243 ver.01 do Grupo de Trabalho do Artigo 29.º, o EPD ocupa uma posição de intermediário entre as partes interessadas, assumindo um papel de facilitador no cumprimento das disposições do RGPD. A implementação e comprovação de conformidade incumbe ao Responsável pelo Tratamento e/ou ao Subcontratante.

Os contactos do Encarregado de Proteção de Dados para as entidades da Administração Pública Regional são os constantes do Anexo I.

3.9 Notificação de Violação de Dados (*Data Breach*)

A Administração Pública Regional deve considerar as medidas técnicas e organizacionais a serem tomadas para informar as partes afetadas em situações de violações de dados pessoais.

De acordo com o Regulamento Geral sobre a Proteção de Dados, quando a Administração Pública Regional, enquanto entidade responsável pelo tratamento, tiver conhecimento de uma violação de dados pessoais, deve notificá-la à Autoridade de Controlo, sem demora injustificada e, sempre que possível, no **prazo de 72 horas**, após ter tido conhecimento da ocorrência.

A Autoridade de Controlo designada no ordenamento jurídico português é a Comissão Nacional de Proteção de Dados (CNPD), pelo que poderá ser contactada através dos meios constantes do anexo I da presente política.

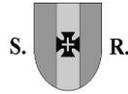
As entidades administrativas regionais devem registar as violações de dados pessoais por forma a demonstrar que a CNPD foi prontamente comunicada quando exigível e, ainda, registar incidentes de segurança mesmo que não desencadeiem a efetiva violação de dados.

Paralelamente à obrigatoriedade de notificar a Autoridade de Controlo, poderá ocorrer circunstâncias em que seja, igualmente, obrigatória a comunicação ao titular de dados pessoais (se reunidos os requisitos legais e nas condições descritas no artigo 34.º do RGPD).

Previamente a qualquer comunicação à CNPD, recomenda-se que seja dado conhecimento ao Encarregado de Proteção de Dados de qualquer ocorrência de violação de dados pessoais, através dos contactos constante do anexo I da presente política, para análise e recomendação das medidas a serem tomadas e as notificações a serem realizadas.

A entidade responsável pelo tratamento deve ter em consideração o procedimento de resposta a violações de dados pessoais, que inclui um plano de ação e de implementação rápida.

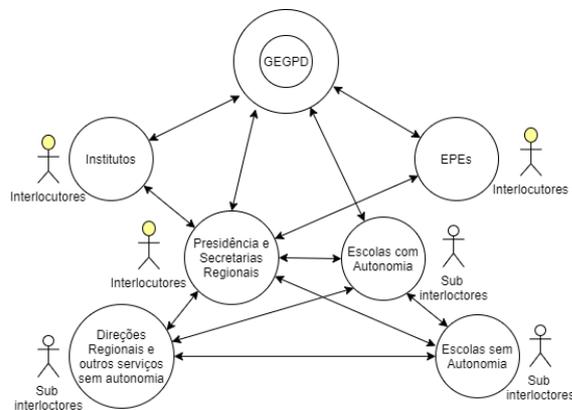




REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

4. MODELO DE GOVERNAÇÃO E DE APLICAÇÃO DA PRESENTE POLÍTICA

O modelo de governação definido para a aplicação da presente política é um modelo híbrido em rede / árvore constituído pelos interlocutores das principais entidades / departamentos (Presidência, Secretarias, Institutos e EPEs) do Governo Regional e por sub interlocutores em cada uma das entidades responsáveis pelo tratamento de dados (Direções Regionais, estabelecimentos de ensino e serviços equivalentes que participam na definição das finalidades e os meios de tratamento).



Neste processo de transformação, os interlocutores e os sub interlocutores são agentes primordiais na implementação das ações necessárias para assegurar a conformidade com o RGPD, na criação de uma cultura de privacidade nas suas organizações e na gestão do processo de mudança a que as diversas entidades da Administração Pública Regional estarão sujeitas.

Como não existe proteção de dados pessoais sem segurança da informação, a entidade que tutela a área informática no Governo Regional e as unidades orgânicas responsáveis pela área de informática, no caso dos serviços da administração indireta e sector empresarial, são também essenciais na aplicação da presente política de proteção de dados e na criação de condições e outras políticas de segurança da informação, que se relacionam diretamente com a presente política e que contemplem, nomeadamente, algumas das seguintes componentes: a política de uso aceitável; comunicações eletrónicas, controlo de acessos; utilização de dispositivos móveis (BYOD); teletrabalho; segurança física; antivírus e *anti-malware*; política de cookies, segurança nos sistemas e na rede; armazenamento de dados; planos de salvaguarda e recuperação de dados; planos de continuidade de negócio, computação na nuvem; criptografia, sistemas de Inteligência Artificial (AI), entre outras.

A gestão da conformidade, o controle, autoria e fiscalização na aplicação da presente política será assegurada pelo serviço indicado no anexo I, com competências de Encarregado Proteção de Dados (EPD).

A ambição desta política vai muito para além da simples análise e gestão da conformidade das diversas entidades com o RGPD, pois pretende-se aproveitar a oportunidade para, em parceria, promover a mudança e a modernização da diversas entidades da Administração Pública, com orientações sobre a abordagem a seguir, tendo em consideração os principais referenciais com influência direta no tratamento de dados pessoais, de onde se destaca, a caracterização dos processos de negócio (MEF /CLAV), aplicações e infraestruturas, a definição de medidas





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

corretivas e evolutivas e a aplicação das melhores práticas em termos de arquitetura empresarial.

Este será um processo de mudança progressivo, com a participação de todas as entidades do Governo Regional orientado ao cumprimento e comprovação com as normas de proteção de dados, associado a uma cultura de privacidade de todas as entidades e trabalhadores da Administração Pública Regional, com o patrocínio institucional dos seus dirigentes máximos e com a contribuição permanente dos interlocutores da “Rede de Privacidade e Proteção de Dados (RPPD)”, em estreita colaboração com o serviço indicado no anexo I, com competências de Encarregado Proteção de Dados (EPD).

5. METODOLOGIA PARA A CONFORMIDADE COM O RGPD

A metodologia a ser implementada transversalmente na Administração Pública Regional, teve por base um projeto piloto numa das suas entidades que recolhe e trata dados pessoais sensíveis, tendo em consideração os principais referenciais com influência direta no tratamento de dados pessoais, de onde se destaca, a caracterização dos processos de negócio, consoante a Macro Estrutura Funcional (MEF) e a Classificação e Avaliação da Informação Pública (CLAV).

As principais etapas do modelo de Programa de Privacidade e Proteção de Dados a desenvolver por cada um dos responsáveis pelo tratamento de dados pessoais da Administração Pública Regional, contempla:

- E1. Definição do modelo de governação interno referente à privacidade e à proteção de dados pessoais;
- E2. Análise e conformidade com as legislações aplicáveis;
- E3. Avaliação e mapeamento dos processos de negócio que envolvam dados pessoais;
 - Realização dos questionários iniciais de conformidade com RGPD e respetiva análise;
 - Mapeamento e caracterização dos processos de negócio;
 - Mapeamento e caracterização dos Sistemas de Informação;
 - Registo das Atividades de Tratamento (RATs).
- E4. Avaliação do nível de conformidade, planeamento e implementação de correções, medidas técnicas e organizativas para a proteção de dados pessoais;
- E5. Definição de políticas e avisos de proteção de dados (Direito à Informação e Princípio da Transparência).
- E6. Definição dos procedimentos RGPD e respetiva gestão:
 - Procedimento e modelo de avaliação de impacto sobre a proteção de dados (AIPD);
 - Procedimento e disponibilização de mecanismos para os titulares de dados exercerem os seus direitos em relação aos seus dados pessoais;
 - Procedimento e disponibilização de mecanismos para notificação e gestão de situações de violação de dados pessoais.
- E7. Formação e sensibilização em RGPD para os dirigentes e trabalhadores, principalmente os que tratam de dados pessoais;
- E8. Monitorização e auditoria do desempenho do programa implementado e melhoria contínua.

O sucesso da metodologia para a conformidade com o RGPD e das medidas a desenvolver no âmbito da proteção de dados pessoais depende do empenho de todos os intervenientes neste desafio de mudança!!!





REGIÃO AUTÓNOMA DA MADEIRA
GOVERNO REGIONAL
SECRETARIA REGIONAL DAS FINANÇAS
GABINETE DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS

ANEXO I

CONTACTOS DO ENCARREGADO GERAL DE PROTEÇÃO DE DADOS (EPD) E DA AUTORIDADE DE CONTROLO NACIONAL

Os contactos do **Encarregado de Proteção de Dados (EPD)** para as entidades da Administração Pública Regional são os seguintes:

Gabinete do Encarregado Geral de Proteção de Dados (GEGPD)

Palácio do Governo Regional - Avenida Zarco

9004-527 FUNCHAL

Telefone: (351) 291 145 175

Email: gegpd.geral@madeira.gov.pt e protecaodedados@madeira.gov.pt

A **Autoridade de Controlo** designada no ordenamento jurídico português é a Comissão Nacional de Proteção de Dados (CNPd), que poderá ser contactada através dos seguintes meios:

CNPd - Comissão Nacional de Proteção de Dados

Av. D. Carlos I, 134, 1º

1200-651 Lisboa

T (+351) 213 928 400

F (+351) 213 976 832

Correio eletrónico: geral@cnpd.pt

Formulário de Notificação de Violação de Dados Pessoais: <https://www.cnpd.pt/databreach/>

