



## **POLÍTICA DE PRIVACIDADE**

### **ÂMBITO**

Esta política aplica-se a todos os colaboradores e sócios da Ribeiro, Rigueira, Marques, Roseiro & Associados, SROC, Lda. (RRMR). Os colaboradores sujeitos a esta política incluem aqueles que tenham celebrado com a RRMR um contrato de trabalho dependente ou de prestação de serviços, bem como entidades subcontratadas, parceiros e consultores externos regulares (que doravante serão simplesmente designados por colaboradores).

O termo privacidade está associado a um conjunto complexo de requisitos legais que se aplicam aos dados pessoais, o qual vai para além da segurança de dados e da confidencialidade. Por exemplo, inclui requisitos sobre a transparência do uso de dados e sobre a sua conservação.

O cumprimento desta política é obrigatório e, por conseguinte, todos os colaboradores e os sócios têm a responsabilidade individual de garantir a sua conformidade com a mesma e, se necessário, devem solicitar esclarecimentos aos sócios e à pessoa que na RRMR foi nomeada para ser responsável pela implementação do Regulamento Geral de Proteção de Dados (RGPD) – designada por Encarregado de Proteção de Dados (EPD).

Compete aos sócios da RRMR definir os mecanismos apropriados para alcançar a conformidade com esta política, sendo igualmente responsáveis pela sua implementação operacional, com o apoio do EPD.

A violação desta política por qualquer colaborador ou sócio pode resultar na abertura de um procedimento disciplinar, sem prejuízo da aplicação de disposições aplicáveis de carácter civil e criminal. As normas sobre procedimento disciplinar estão descritas no capítulo dos Recursos Humanos do Manual de Controlo de Qualidade (MCQ).

Esta política baseia-se nos princípios estabelecidos no RGPD.

### **PRINCÍPIOS DE PROTEÇÃO DE DADOS**

No âmbito da nossa atividade, podemos eventualmente efetuar tratamentos de dados pessoais: seja quando recebemos dados pessoais no decurso das nossas oportunidades de negócio, dos nossos compromissos com clientes ou de uma série de outras atividades relacionadas e de suporte. Os dados podem ser recebidos diretamente de um Titular de Dados (por exemplo, pessoalmente, via correio, e-mail, telefone ou de outras fontes), nomeadamente dos nossos clientes, parceiros, subcontratados, prestadores de serviços de suporte.

Em qualquer contexto desta política, os colaboradores e sócios devem apenas solicitar dados pessoais de um Titular de Dados que sejam relevantes e necessários para cumprir determinada finalidade, no âmbito de algum trabalho que tenha sido adjudicado à RRMR.

No caso de existirem situações que impliquem a obtenção de dados pessoais, a RRMR compromete-se a cumprir com os princípios de proteção de dados pessoais definidos pelo RGPD, concretamente:

- **Licitude, lealdade e transparência:** significa que devemos ter uma razão legítima por força da qual tratamos dados pessoais, por exemplo, consentimento do Titular dos Dados ou cumprimento de alguma obrigação legal a que estamos sujeitos. Também significa que devemos informar, de forma inequívoca, o Titular dos Dados sobre o tratamento;
- **Limitação das finalidades:** devemos apenas solicitar dados pessoais para finalidades determinadas, explícitas e legítimas e não os tratar para além da finalidade para a qual foram solicitados;
- **Minimização dos dados:** os dados pessoais objeto de tratamento devem ser adequados, pertinentes e limitados ao necessário;
- **Exatidão:** temos a obrigação de garantir que os dados pessoais são exatos e atualizá-los, sempre que necessário;
- **Limitação da conservação:** não devemos reter dados pessoais por um período superior ao necessário para as finalidades para as quais são tratados, embora possamos reter alguns para fins históricos e estatísticos;
- **Integridade e confidencialidade:** devemos ter em vigor controlos de segurança adequados para proteção dos dados contra o tratamento não autorizado e ilegal, perda, destruição ou danificação, incluindo medidas técnicas e organizacionais, tais como processos definidos, formação e consciencialização;
- **Transferência legal fora do Espaço Económico Europeu (EEE):** apenas transferimos dados pessoais para fora do EEE, nomeadamente para Angola (enquanto unidade de negócios da RRMR), desde que existam salvaguardas adequadas, tal como a existência de base contratual;
- **Direitos do Titular de Dados:** os Titulares dos Dados têm vários direitos que devemos respeitar (por exemplo, o direito a aceder a uma cópia dos dados que arquivamos).

## LICITUDE E LEALDADE NO TRATAMENTO

Na eventualidade de recolhermos dados pessoais é necessário ter uma base legal para o inerente tratamento. De acordo com o RGPD, devemos identificar, pelo menos um, dos seguintes motivos para tratamento de dados pessoais:

- **Consentimento:** O Titular dos Dados deu o consentimento para que os mesmos sejam tratados para uma ou mais finalidades específicas;
- **Contratual:** O tratamento é necessário para a execução de um contrato do qual o Titular dos Dados faz parte ou para diligências pré-contratuais;



- **Legal:** O tratamento é necessário para cumprir com uma obrigação legal, à qual o responsável pelo tratamento está sujeito;
- **Interesses vitais:** O tratamento é necessário para proteger os interesses vitais do Titular dos Dados;
- **Interesse público:** O tratamento é necessário para o desempenho de uma tarefa realizada no interesse público;
- **Interesses legítimos:** O tratamento é necessário para os interesses legítimos do responsável pelo tratamento, exceto quando prevalecerem interesses ou direitos e liberdades fundamentais do Titular dos Dados.

O RGPD exige que se forneça aos Titulares dos Dados informações sobre o tratamento, a fim de garantir um tratamento equitativo e transparente.

#### **TRATAMENTO APENAS PARA FINALIDADES ESPECÍFICAS**

Na eventualidade de recolhermos e tratarmos dados pessoais, devemos garantir que apenas os utilizamos para as finalidades específicas que foram comunicadas ao respetivo Titular.

A RRMR não deve tratar dados pessoais para fins adicionais, que não tenham sido comunicados ao Titular dos Dados.

#### **TRATAMENTO ADEQUADO, PERTINENTE E LIMITADO**

Sempre que recolhermos e tratarmos dados pessoais devemos seguir o princípio da minimização dos dados, ou seja, devemos recolher apenas os dados pessoais mínimos, necessários para realizar uma tarefa específica.

Adicionalmente, devemos garantir que temos uma quantidade adequada de dados pessoais para realizar uma tarefa específica de maneira adequada. Por exemplo, recolher os dados necessários apenas para identificar uma pessoa.

O princípio minimizar os dados mantidos e tratados também se aplica a qualquer partilha ou outras atividades de tratamento. Ou seja, na eventualidade de partilharmos dados interna ou externamente ou se os usarmos em testes, devemos assegurar, em cada caso, que só partilhamos e/ou utilizamos a quantidade mínima.

#### **EXATIDÃO DOS DADOS PESSOAIS**

É obrigação dos sócios e colaboradores da RRMR assegurar que os dados pessoais são mantidos exatos e atualizados. Assim, devemos garantir a implementação de processos adequados para manter os dados exatos, sempre que necessário (por exemplo, dos colaboradores ou de clientes atuais e potenciais).



## **CONSERVAÇÃO DE DADOS PESSOAIS**

Os dados pessoais não devem ser conservados por mais tempo do que o necessário. Isto significa que devemos definir e aplicar períodos de conservação máximos dos dados pessoais que tratarmos e implementar processos para os eliminar no seu termo.

Concretamente, os períodos de conservação que podem ser aplicados são os seguintes:

- pelo tempo que for necessário para a atividade ou serviços relevantes;
- qualquer período de conservação exigido por Lei;
- o fim do período em que os litígios ou investigações possam surgir em relação aos serviços; ou
- pelo período mínimo previsto no contrato.

## **DIREITOS DOS TITULARES DE DADOS**

O RGPD exige que informemos as pessoas sobre os dados pessoais que recolhemos, as finalidades e meios para os quais são objeto de tratamento. Tal informação é dada sob a forma de um “Aviso de Privacidade”.

### **i. Direito de acesso**

- O Titular dos Dados tem o direito de pedir para ver os dados pessoais que temos a seu respeito, a finalidade do tratamento e a natureza de dados em causa;
- Devemos notificar o Titular dos Dados sobre quais os destinatários com quem vamos partilhar os seus dados, especialmente se o destinatário estiver noutro país ou se pertencer a uma organização internacional;
- Sempre que possível, definiremos o prazo de conservação dos dados para atender aos objetivos comerciais;
- Devemos comunicar ao Titular dos Dados a existência do direito de se opor ao tratamento e do seu direito de retificação e eliminação;
- Devemos comunicar ao Titular dos Dados a existência do seu direito de reclamação a uma Autoridade de Controlo;
- Quando os dados são recolhidos de alguém que não seja o próprio Titular dos Dados, devemos comunicar ao próprio a fonte desses dados;
- Devemos garantir que temos processos em vigor para identificar e responder às questões de acesso por parte do Titular dos Dados, sem demora injustificada, e no prazo máximo de um mês.



## **ii. Direito de retificação**

- Os Titulares dos Dados têm o direito à retificação dos dados incorretos, cabendo à RRMR, concretamente ao EPD, todos os esforços para o fazer de imediato.

## **iii. Direito de eliminação**

- O Titular dos Dados tem o direito de obter do responsável pelo tratamento, a eliminação dos seus dados (direito a ser esquecido). Cabe à RRMR fazer o possível para apagar de imediato os dados mantidos, exceto quando houver uma exigência legal para a sua conservação. Se receber uma solicitação de um Titular de Dados, devem primeiro contactar o ERP, antes de apagar quaisquer dados.

## **iv. Direitos das crianças**

- Todos as pessoas, incluindo as crianças, estão protegidos pelo RGPD. Para crianças menores de 13 anos não devemos processar os seus dados pessoais com base no seu consentimento, salvo autorização pelos respetivos titulares das responsabilidades parentais.

## **v. Divulgação**

- Por vezes, mas muito raramente, podemos enviar aos nossos clientes e parceiros de negócio material de divulgação para informá-los sobre os nossos serviços, eventos futuros ou outras atividades do seu interesse. Nessa eventualidade, devemos indicar o direito a retirar o consentimento a qualquer altura se os clientes ou parceiros desejarem não voltar a ser contactados nesses termos;
- Devemos, também, assegurar que estão implementados processos que garantam que todas as preferências de participação sejam registadas e respeitadas.

## **SEGURANÇA DOS DADOS RETIDOS**

A RRMR manterá a segurança dos dados protegendo a confidencialidade, integridade e disponibilidade dos dados pessoais, concretamente:

- Confidencialidade significa que apenas pessoas autorizadas podem aceder aos dados;
- Integridade significa que os dados pessoais devem ser exatos e adequados para as finalidades inerentes ao tratamento;
- Disponibilidade significa que os utilizadores autorizados devem poder aceder aos dados se precisarem para as finalidades autorizadas.



## **DIVULGAÇÃO DE DADOS**

Todos os colaboradores e os sócios devem evitar qualquer divulgação inapropriada de dados pessoais e cumprir com os deveres gerais da RRMR em relação à confidencialidade.

Geralmente, os dados pessoais só podem ser divulgados:

- Aos colaboradores na estrita medida em que estes possam desempenhar adequadamente as suas funções;
- Nos casos em que a não divulgação dos dados poderá prejudicar a prevenção ou deteção de crimes, a dedução de acusação contra infratores, ou a avaliação ou cobrança de qualquer imposto ou taxa. Para evitar processos criminais, a RRMR deve, em cada caso, avaliar se os motivos são, ou não, adequados para divulgar os dados, sob esta categoria. Todas as divulgações devem ser justificadas e estar devidamente documentadas;
- Os dados pessoais podem ser divulgados para fins legais, apenas nos seguintes casos: (i) seja exigido por Lei, estatuto ou por ordem do Tribunal; (ii) com a finalidade de obter assessoria jurídica; (iii) no âmbito ou para efeitos de um processo judicial ou quando necessário para defesa de um direito legal; ou (iv) para salvaguarda da segurança nacional.

## **INFORMAÇÃO DE COLABORADORES**

### **i. Recolha e Conservação**

- Enquanto entidade empregadora, a RRMR recolhe, trata e conserva dados pessoais de candidatos, trabalhadores, contratados, consultores e parceiros. As pessoas, que na RRMR tratam dados pessoais de colaboradores, devem verificar e documentar qual a base legal inerente ao tratamento que efetuar. Os dados pessoais dos colaboradores só devem ser tratados quando houver um objetivo válido e legítimo para o efeito;
- A recolha de dados pessoais relacionados com os colaboradores ocorre por meio de diversos canais e formatos, nomeadamente, através de formulários de inscrição e eventualmente, dados de outras fontes (por exemplo verificações de empregadores anteriores, registo criminal, cartas de recomendação), etc.;
- A criação e o armazenamento de dados pessoais relacionados com os nossos colaboradores ocorrem por meio de vários canais e formatos, tais como: contratos de trabalho, recibos de remuneração, registos de avaliação, e-mails, registos de doença, etc.

### **ii. Formação e Conscientização**

- Sempre que necessário forneceremos formação personalizada e consciencialização para os colaboradores e sócios, considerada adequada, tendo em conta as funções que desempenham.



## **OBTENÇÃO DE DADOS PESSOAIS PARA A EXECUÇÃO DE FUNÇÕES DE INTERESSE PÚBLICO ENQUANTO REVISORES OFICIAIS DE CONTAS**

Com a entrada em vigor do RGPD na ordem jurídica portuguesa, em 25 de maio de 2018, e em conformidade com os recentes entendimentos da Ordem dos Revisores Oficiais de Contas (OROC) na Circular n.º 47/18, de 30 de abril, cumpre esclarecer o enquadramento dos Serviços de Auditoria e Revisão Legal das Contas que a RRMR, Lda. presta aos seus clientes, no âmbito do RGPD.

Neste contexto, Serviços de Auditoria e Revisão Legal das Contas compreendem o acesso, consulta e verificação de um conjunto de informação, que o ROC, tendo em consideração o seu juízo profissional independente, seleccione como necessário para a realização das suas funções de interesse público e que conservará como prova de auditoria. Eventualmente, este conjunto de informação pode conter informação relativa a dados pessoais.

Porém, o cumprimento dos deveres resultantes do Estatuto da Ordem dos Revisores Oficiais de Contas e das normas de auditoria, de modo particular, a sujeição a sigilo profissional das suas funções de interesse público, acomoda suficientemente os deveres do RGPD, não carecendo de diligências adicionais, nomeadamente, da obtenção do consentimento junto dos titulares dos dados pessoais.

Por conseguinte, no âmbito das funções de interesse público, o tratamento da informação recolhida pelo ROC não configura tratamento de dados pessoais efetuados por conta dos clientes, uma vez que o ROC não é subcontratante do cliente na aceção do artigo 28.º do RGPD. Assim, para os serviços do ROC prevalecem os acordos escritos firmados com os clientes, mediante contrato de prestação de serviços e/ou de carta de compromisso, em conformidade com a Lei, com as normas internacionais de auditoria e cumprindo as orientações da OROC aplicáveis.

Em termos gerais, importa reforçar que, no exercício de funções de interesse público, o ROC não recolhe dados pessoais, nem tem estes por objeto. Por conseguinte, o seu trabalho não é constituído pelo tratamento de dados pessoais e muito menos por dados pessoais sensíveis, os quais são objeto de proteção pelo RGPD.

Em suma, a proteção de dados não é prejudicada pelo exercício das funções de interesse público, por parte do ROC.

### **ARQUIVOS (COM DADOS PESSOAIS) MANTIDOS COMO SUPORTE AOS RELATÓRIOS EMITIDOS**

Os dados pessoais utilizados pelo ROC no âmbito das funções de interesse público, quer estes sejam consultados, verificados, integrados no trabalho desenvolvido e/ ou conservados para a necessária evidência da prova de auditoria e que sejam necessários para a execução das mesmas e que, por conseguinte, integram as pastas de trabalho, estão legitimados pelo exercício das referidas funções de interesse público, sendo devidamente assegurados todos os cuidados necessários com a conservação e proteção desses dados.

A RRMR tem uma grande preocupação com a confidencialidade dos documentos do cliente. Assim, passado o período de 10 anos, os documentos são destruídos. O mesmo destino deve ser dado aos documentos do cliente a que tenhamos acesso, mas que não sejam necessários para a pasta de auditoria.



A RRMR tem requisitos acrescidos de confidencialidade e segurança para os arquivos dos clientes, onde toda informação em formato digital, está arquivado no servidor e com acesso restrito.

Adicionalmente, para os clientes considerados Entidades de Interesse Público (EIP's) os requisitos de confidencialidade são acrescidos. Assim, os arquivos físicos são guardados à parte, em armários com chave, por forma a restringir o seu acesso apenas às pessoas autorizadas. Quanto aos arquivos informáticos dos clientes EIP's, os mesmos estão guardados na rede, em local separado, em que apenas as pessoas autorizadas têm permissão de acesso.

### **DEVER DE INDEPENDÊNCIA**

Nos termos legais e deontológicos, o ROC exerce as suas funções de interesse público, que lhe estão cometidas, com independência. Para assumir a sua responsabilidade de manter a sua independência, o ROC executa os procedimentos que entender necessários de modo a suportar a opinião, parecer, conclusão que expressa no seu relatório.

Na impossibilidade de executar algum procedimento que entenda necessário, ou de o substituir adequadamente por outro, ou ainda na impossibilidade de aceder a informação necessária para a execução desse(s) procedimento(s), o ROC deve considerar tal facto na emissão da opinião, parecer, conclusão que expressa no seu relatório.

Não compete ao ROC exigir informação ou acesso a dados, mas se lhe for imposta alguma restrição no acesso à informação ou aos dados, compete ao ROC considerar o efeito dessa restrição na emissão do seu relatório.

### **DEVER DE CONFIDENCIALIDADE**

Ainda que o conceito de tratamento de dados pessoais, conforme definido no RGPD, não seja o objeto do trabalho de ROC, é seu dever fazer prova de auditoria e conservá-la. Dito de outra forma, enquanto o relatório emitido pelo ROC é, na generalidade dos casos, público, e em geral não contém dados pessoais, a prova de auditoria que tem de o suportar está sujeita ao segredo profissional.

O ROC está proibido de usar a informação a que acede para qualquer outro fim que não o de evidenciar que os procedimentos que executou suportam as conclusões extraídas e o relatório que emitiu. Assim, não é admitida qualquer outra quebra do dever de segredo que não as expressamente elencadas na Lei. Acresce que o ROC que cesse funções de interesse público numa determinada entidade, permanece vinculado ao dever de segredo profissional.





## **A PROTEÇÃO DE DADOS E A QUALIDADE DO TRABALHO DO REVISOR OFICIAL DE CONTAS**

O objeto do trabalho das funções de interesse público, de acordo com as disposições legais, não é constituído pelo tratamento de dados pessoais. No entanto, no desenvolvimento das suas funções, para a execução de alguns dos procedimentos necessários, o ROC poderá ter de usar informação contendo dados pessoais.

É dever do ROC firmar com a entidade cliente um contrato de prestação de serviços ou registar numa carta de compromisso, ou noutra forma apropriada de acordo escrito, os termos acordados do trabalho, em conformidade com o previsto nas normas internacionais de auditoria, na própria Lei (como é o caso da revisão legal das contas / auditoria), cumprindo as orientações da OROC aplicáveis.

Face ao exposto, é crucial que no acesso à informação necessária à realização do nosso trabalho não haja dependência de consentimentos concretos ou de quaisquer outras salvaguardas, que esses dados possam merecer.

Assim, proteção dos dados pessoais não será prejudicada pelo exercício das nossas funções, atento o disposto na Lei quanto a essas funções.

