matosinhos

CM Matosinhos

24/05/2018
OrdemServ/2018/9

**ORDEM DE SERVIÇO**

*A Todos/as os Trabalhadores/as da*
*Câmara Municipal de Matosinhos*

No próximo dia 25 de maio produz efeitos o novo Regulamento Geral de Proteção de Dados, regulamento europeu que visa dar maior proteção aos dados pessoais dos/as cidadãos/ cidadãs europeus/ europeias. Esta data emblemática deve ser vista por todos como um ponto de partida, e não de chegada, rumo a uma nova forma das instituições, organismos públicos, e empresas, se relacionarem com a informação.

O regulamento é rigoroso para as organizações, desde logo porque as obriga a um conjunto de exigências relacionadas com o tratamento da informação pessoal, incluindo algumas adaptações informáticas, em matéria de arquitetura de segurança das redes e sistemas de informação relativos a dados pessoais, a realizar nos próximos meses, como aliás foi objeto de recomendação por parte do Conselho de Ministros, no quadro da Resolução do Conselho de Ministros n.º 41/2018, publicada em Diário da República no dia 28 de Março (Diário da República n.º 62/2018, Série I).

A Câmara Municipal de Matosinhos, ciente da responsabilidade que tem na gestão dos dados dos seus/suas colaboradores/as, fornecedores e munícipes, tem em execução, apoiada por um parceiro externo, um procedimento de levantamento dos processos internos que tratam dados pessoais, para garantir o cumprimento do Regulamento. Este procedimento está a permitir identificar processos que poderão ter de ser alterados com base nas novas regras. Está ainda a ser levada a cabo uma avaliação da Segurança da nossa infraestrutura informática para garantir que os dados nos nossos sistemas estão guardados com segurança, como o Regulamento obriga.

Sem prejuízo das medidas técnicas e organizativas que estão a ser desenhadas e executadas pelos serviços competentes, a aplicação do RGPD implica um compromisso por parte de todos/as.

A Câmara Municipal de Matosinhos irá, assim, desenvolver ações de formação e sensibilização junto dos seus/suas colaboradores/as, de maneira a envolver e informar, todos/as e cada um/a, das atenções devidas que deverão ter quando acedem a dados pessoais.

matosinhos

A Câmara Municipal de Matosinhos reforça o seu compromisso com a comunidade e com os/as cidadãos/ cidadãs, dando nota que irá continuar a tratar os dados pessoais dos/as seus/suas munícipes e colaboradores/as com a diligência, sobriedade e cuidado que se impõem às organizações motivadas apenas pelo respeito pelo interesse público.

Em anexo a esta ordem de serviço, chama-se a atenção para alguns conceitos inerentes à implementação do RGPD e orientações que os serviços deverão continuar a procurar cumprir no exercício das suas atribuições e competências.

Divulgue-se e publicite-se nos termos da lei.

A Presidente da Câmara

Dr.ª Luísa Salgueiro

**ANEXO**

**CONCEITOS**

***DADOS PESSOAIS***

É toda a informação relativa a uma pessoa singular que a identifica ou permite a sua identificação, direta ou indireta.
Existem várias categorias de dados pessoais.

- Descritivos e de identificação (ex. nome e NIF)
- Saúde (ex. análises clínicas)
- Financeiros (ex. saldos de crédito)
- Vida (ex. estado civil)
- Educação (ex. títulos académicos)
- Emprego (ex. profissão)
- Criminal (ex. registo criminal)

matosinhos

Há ainda a categoria de dados pessoais sensíveis que são todo os dados que revelam a origem racial ou étnica, opções políticas, convicções religiosas, filiação sindical, bem como dados de saúde, genéticos, ou relativos à orientação sexual. Devido à sua sensibilidade, estes dados são alvo de proteções adicionais.

***QUEM É TITULAR DOS DADOS PESSOAIS?***

Todas as pessoas singulares identificadas pelos dados pessoais. São exemplos de titulares de dados:

•Cliente
•Cliente potencial
•Ex-Cliente
•Beneficiário efetivo
•Representante Legal
•Avalista/fiador
•Procurador
•Colaborador
•Ex-Colaborador
•Familiar do colaborador

O regulamento não é aplicável a pessoas coletivas.

***O QUE É O TRATAMENTO DE DADOS PESSOAIS?***

O tratamento de dados pessoais consiste numa operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não. São considerados como tratamento a recolha, o registo, a consulta, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a utilização, a divulgação, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição de dados pessoais.

É permitido à autarquia tratar os dados pessoais:

• para execução de um contrato ou diligências pré-contratuais
• para cumprimento de uma obrigação legal
• quando existe interesse legítimo da empresa.

matosinhos

• quando é obtido o consentimento do cliente

***CONSENTIMENTO***

O consentimento do/a titular dos dados é necessário para permitir ações de marketing direto de produtos e serviços não similares aos já contratados e de produtos de entidades terceiras.
O consentimento tem de ser dado de forma inequívoca e por meio de uma declaração comprovável a qualquer momento.
O silêncio, as opções pré-validadas ou a omissão não são consideradas como um ato de consentimento válido.
O consentimento do/a titular dos dados para as ações de marketing direto de produtos e serviços não similares aos/às contratados/às e de produtos de entidades terceiras pode ser dado e retirado quantas vezes o/a titular quiser e a qualquer momento.
O consentimento deve ser tão fácil de dar como de retirar.

***ACESSO***

O/A titular tem o direito de aceder a qualquer momento:

• aos dados pessoais que a empresa detém a seu respeito, tenham estes sido cedidos pelo/a próprio/a ou recolhidos junto de terceiros
• às finalidades do tratamento dos dados
• aos/às destinatários/as dos dados
• aos prazos de conservação, se definidos
• à informação sobre a existência de decisões automatizadas, incluindo a definição de perfis

***PORTABILIDADE***

OA titular tem o direito de solicitar à empresa informação sobre os dados pessoais que lhe digam respeito e que tenha fornecido, e de receber essa informação num formato estruturado, de uso corrente e de leitura automática e ainda o direito de transmitir esses dados a outra entidade.

***ESQUECIMENTO***

matosinhos

Em determinadas situações o/a titular tem o direito de solicitar o apagamento/ esquecimento dos seus dados pessoais. A título de exemplo:

• quando os dados pessoais deixam de ser necessários para as finalidades inicialmente definidas
• quando o consentimento para o tratamento dos dados tenha sido retirado
• caso o/a titular se tenha oposto ao tratamento
• quando os dados tenham sido tratados ilicitamente

***OPOSIÇÃO***

Em determinadas situações o/a titular tem o direito de se opor ao tratamento dos seus dados pessoais. A título de exemplo:

• para efeitos de comercialização direta de produtos da autarquia e de terceiros, incluindo a definição de perfis para o efeito
• nos casos em que os interesses legítimos da autarquia não prevaleçam aos direitos e liberdades fundamentais do/ titular, sempre analisados individualmente

***LIMITAÇÃO***

Em determinadas situações o/a titular tem o direito a solicitar a limitação do tratamento, exemplo:

• enquanto os dados pessoais não se encontrem registados com exatidão, tendo sido solicitada a sua atualização
• o tratamento dos dados pessoais for ilícito
• os dados pessoais já não sejam necessários para as finalidades definidas
• o titular se tiver oposto ao tratamento dos seus dados pessoais e ainda não tiver obtido resposta a esse pedido

***TRANSPARÊNCIA DA INFORMAÇÃO***

Em todos os momentos em que sejam recolhidos dados pessoais, o/ titular deve ser informado:

• sobre as finalidades do tratamento dos dados
• dos contatos do/a Encarregado/a da Proteção de Dados (DPO)
• da identidade do/a responsável pelo tratamento;

matosinhos

• dos/as destinatários/as ou categorias de destinatários/as dos dados pessoais (ex. STS)

***SEGURANÇA DOS DADOS PESSOAIS***

O regulamento obriga a aplicação de medidas técnicas que assegurem um adequado nível de segurança dos dados pessoais. São exemplo dessas medidas:

• pseudonimização e encriptação de dados
• confidencialidade, integridade e resiliência dos sistemas e serviços de tratamento
• capacidade de restabelecer o acesso aos dados pessoais em caso de incidente técnico ou físico
• processos eficazes de avaliação de segurança no tratamento de dados pessoais

O regulamento prevê uma maior autorresponsabilização dos/as responsáveis pelo tratamento de dados na avaliação de riscos, deteção e mitigação de violações de dados e notificação das entidades reguladoras.

***PRINCÍPIOS DE TRATAMENTO***

Os dados pessoais têm de ser objeto de um tratamento lícito, leal e transparente.
Os dados devem ser recolhidos para as finalidades inicialmente determinadas e não devem ser utilizados posteriormente para outros fins não compatíveis.
Os dados recolhidos e tratados devem ser adequados e limitados ao que é necessário.
Os dados devem ser exatos, atualizados e conservados apenas durante o período necessário à finalidade do tratamento.
Os dados devem ser tratados de forma segura.

***AVALIAÇÃO DO IMPACTO SOBRE A PROTEÇÃO DE DADOS (DPIA)***

O regulamento prevê medidas preventivas de proteção de dados para as operações de tratamento de dados pessoais.
Esta avaliação é da responsabilidade da autarquia e no caso de existirem riscos elevados deverão ser adotadas medidas de mitigação.
Antes da recolha ou de um novo tratamento de dados pessoais devem ser realizadas avaliações de impacto.

matosinhos

***RESPONSABILIDADE***

A autarquia é responsável pelo tratamento, determinando as finalidades e os meios utilizados no tratamento de dados pessoais. Mas é também responsável por assegurar o cumprimento do regulamento por parte dos seus subcontratantes. Um subcontratante é uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta da empresa.

***ENCARREGADO/A DE DADOS***

O regulamento prevê a nomeação de um/a Encarregado/a de Proteção de Dados (DPO).

O DPO tem como principais funções:

• consciencializar e formar os/as colaboradores/as

• ser o ponto de contacto com os/as titulares dos dados nos temas de privacidade

• cooperar com as entidades de supervisão

• controlar e monitorizar os riscos das operações de tratamento de dados pessoais

• assegurar o registo atualizado das operações de tratamento de dados pessoais

***VIOLAÇÃO DE DADOS PESSOAIS***

Uma violação de dados pessoais é uma violação da segurança, com origem interna ou externa, que coloca em risco a integridade, a privacidade e a segurança dos dados pessoais e dos/as seus/as titulares. As violações de dados pessoais podem ser acidentais ou ilícitas e podem resultar no acesso, divulgação ou alterações não autorizadas, ou na destruição e perda de dados pessoais.

***NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS***

No caso de ocorrer uma violação de dados pessoais, comunique-a de imediato ao/à Encarregado/a de Proteção de Dados para que sejam iniciadas as medidas de avaliação, controlo e mitigação dos possíveis impactos. O/A Encarregado/a de Proteção de Dados deve comunicar as violações de dados, sem demora injustificada ao titular dos dados, e à CNPD (Comissão Nacional de Proteção de Dados) no prazo máximo de 72 horas desde a tomada de conhecimento da situação.

matosinhos

## ORIENTAÇÕES

- Os serviços deverão proteger todos os dados que detêm, quer ao nível físico (suporte de papel) quer ao nível digital.
- Os/as funcionários/as de cada serviço deverão acautelar os processos pelos quais são responsáveis, de modo a que eventuais dados pessoais não sejam transmitidos a quem não detém legitimidade.

- Deverão adotar uma politica de "secretária limpa", ou seja, no fim do expediente evite deixar processos em cima da sua secretária.

- Os/as funcionários/as deverão de compreender as regras que cada serviço adote na proteção dos seus dados e respeitá-las, bem como todo o resguardo que os/as colegas de trabalho tenham de efetuar no âmbito da proteção dos dados.
- Sempre que se ausentar bloqueie o seu computador.
- Não transmita a sua palavra passe a ninguém.
- Não transmita informações para além do necessário ao exercício da sua função ou esclarecimento do público.
- Não envie e-mails que contenham dados pessoais com conhecimento a quem não tem responsabilidade ou não careça dos mesmos para a sua atividade.
- Os/as dirigentes dos serviços deverão dar permissões de acessos aos/às seus/suas trabalhadores/as, somente no que é necessário para o exercício da função de cada um/a.
- Deverão continuar a ser cumpridas, de forma muito rigorosa, todos os deveres e princípios que são impostos/as aos /às trabalhadores/as em funções públicas, designadamente o dever de sigilo, entre outros.
- Qualquer dúvida que os/as trabalhadores/as da autarquia tenham sobre este assunto, deverão coloca-las ao/à respetivo/a superior hierárquico/a.

Alerta-se todos/as os/as trabalhadores/as que as presentes orientações são meramente exemplificativas das diferentes boas práticas que deverão de adotar no âmbito das suas atribuições e competências. Os conceitos acima referidos não invalidam a análise do respetivo Regulamento Geral de Proteção de Dados.