documento de consulta

APOIO À **GESTÃO DE DADOS PESSOAIS** PARA CLIENTES **ARTSOFT**

Manual de apoio à compreensão do RGPD

Este documento foi produzido com base no Regulamento (UE) do Parlamento Europeu e do Conselho, de 27 de abril de 2016, L119 Jornal Oficial da União Europeia que pode ser consultado nos documentos oficiais que disponibilizamos. Dele constam os principais aspetos que deve ter em consideração para implementar políticas, plano de ações, estratégias e formas de cumprir o RGPD, com integridade, que regem os princípios do regulamento.

Este resumo foi totalmente elaborado pela ARTSOFT para clientes que tenham adquirido a solução Gestor de Dados Pessoais, módulo incorporado no ARTSOFT para o ajudar a gerir os Dados Pessoais. É ainda intransmissível e deve ser guardado em lugar seguro, mas disponível para todos os que tenham contacto direto com dados pessoais, para esclarecimento de dúvidas ou apoio na gestão diária de dados.

Versão 0.1 / 25.05.2018. Atualizações ao documento serão comunicadas sempre que existirem. Mais informações sobre este documento: marketing@artsoft.pt.

REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS PESSOAIS (RGPD)

1. O QUE É?

O Regulamento Geral sobre a Proteção de Dados Pessoais é o novo quadro legal que entrou em vigor no dia 25 de maio de 2018 na União Europeia e que estabelece as regras relativas à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Os Regulamentos da UE têm aplicação direta em todos os Estados-Membros, o que significa que o RGPD prevalece sobre quaisquer leis nacionais.

A aplicação de coimas que pode ir até 4% do volume de negócios global anual ou 20 milhões de Euros (o que for mais elevado), torna o conhecimento do RGPD indispensável.

2. A QUEM SE DESTINA?

Esta legislação aplica-se a todas as organizações estabelecidas em território da União Europeia e àquelas que, estando localizadas fora da UE, tratem dados de titulares aí residentes, desde que comercializem os seus produtos/serviços (a título oneroso ou gratuito) ou monitorizem comportamentos que ocorram dentro da UE.

3. O QUE SÃO DADOS PESSOAIS?

Dados pessoais são toda e qualquer 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:

Nome, números de identificação civil/fiscal/segurança social, morada, endereço eletrónico, número de endereço IP, dados de localização, data de nascimento, altura, peso, idade, composição do agregado familiar, padrão da íris, impressão digital, etc.

DOCUMENTO RESUMO RGPD – NOTAS A RETER

4. SOBRE O TITULAR DOS DADOS (pessoa singular)

Os titulares de dados deverão ter o direito de aceder gratuitamente aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e em intervalos razoáveis, a fim de tomar conhecimento do tratamento e verificar a sua licitude. Por conseguinte, cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível, do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos, quando tiver por base a definição de perfis, das suas consequências.

Quando possível, o responsável pelo tratamento (a empresa) deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. O ARTSOFT criou a plataforma dadospessoais.artsoft.pt para clientes do módulo Gestor de Dados Pessoais poderem disponibilizar esse sistema.

Todos os titulares de dados deverão ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito, ou ainda se o tratamento dos seus dados pessoais não respeitar o disposto no regulamento. (Considerando 65, pág. 12)

5. SOBRE O CONSENTIMENTO

O consentimento do titular deverá ser dado mediante um ato positivo que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente o tratamento dos dados que lhe digam respeito, como, por exemplo, mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral (que fique registada). (Considerando 32, pág. 6)

O consentimento pode ser dado validando uma opção ao visitar um *website* ou mediante declaração que indique claramente que aceita o tratamento dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para cada um desses fins. (Considerando 32, pág. 6)

Em conformidade com a Diretiva 93/13/CEE, uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. (Considerando 42, pág. 8). A ARTSOFT disponibiliza um modelo que poderá usar.

O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. O consentimento deve ser tão fácil de retirar quanto de dar. (Artigo 7, pág. 37)

6. SOBRE TRATAMENTO DOS DADOS

O tratamento de dados é uma 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 dos mesmos.

O tratamento deverá ser considerado lícito caso seja necessário no contexto de um contrato ou da intenção de celebrar um contrato. (Considerando 44, pág. 8)

O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. (Considerando 50, pág. 9)

Em qualquer tratamento é importante que o responsável pelo tratamento (empresa) garanta a devida segurança e confidencialidade, para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas. (Considerando 39, pág. 7)

Tratamento de dados sensíveis

Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica. (Considerando 51, pág. 10)

Tratamento por interesse legítimo

Os interesses legítimos dos responsáveis pelo tratamento podem constituir um fundamento jurídico para o mesmo, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expetativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável

pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento.

De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. (Considerando 97, pág. 9)

7. SOBRE O PRAZO DE CONSERVAÇÃO DOS DADOS

Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. (Considerando 39, pág. 7)

8. SOBRE A TRANSPARÊNCIA DO RESPONSÁVEL PELO TRATAMENTO DE DADOS

O tratamento de dados pessoais deverá ser transparente para as pessoas singulares que os cujos dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento, ou na medida em que os dados pessoais são ou virão a ser tratados. (Considerando 39, pág. 7)

A empresa deve fornecer ao titular dos dados informações a respeito do tratamento a que vai submeter os mesmos, de forma concisa, transparente, inteligível e de fácil acesso. (Art.º 12, Alínea 1, pág. 39)

No que respeita ao pedido de acesso aos dados, ou à portabilidade dos mesmos, a empresa deve fornecer a informação sem demora injustificada **e no prazo máximo de um mês** a contar da data de receção do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. Deve a empresa avisar o titular dos dados, caso necessite de prorrogação. (Art.º 13, Alínea 3, pág. 40)

As informações e quaisquer comunicações e medidas tomadas devem ser fornecidas a título gratuito ao titular dos dados. Estas informações poderão constar numa política de privacidade ou, como nota, num documento a que o titular dos dados tenha acesso, ou ainda enviadas diretamente ao particular. Algumas das informações que deverá facultar: identidade e os contactos da empresa e, se for caso disso, o seu representante, entidades ou destinatários que poderão ter acesso aos dados, prazos de conservação, acesso ao direito de solicitar esquecimento, retificação, ou limitação no tratamento de dados, existência de decisões automatizadas, incluindo a definição de perfis, e violações que

possam decorrer no exercício do tratamento de dados. (Art.º 13, Alínea 5, pág. 40)

Sempre que os dados pessoais forem suscetíveis de ser legitimamente comunicados a outro destinatário, o titular dos dados deverá ser informado aquando da primeira comunicação dos dados pessoais a esse destinatário. Sempre que o responsável pelo tratamento tiver a intenção de tratar os dados pessoais para outro fim que não aquele para o qual tenham sido recolhidos, antes desse tratamento o responsável pelo mesmo deverá fornecer ao titular dos dados informações sobre esse fim e outras informações necessárias. (Considerando 61, pág. 12)

9. SOBRE INFORMAÇÕES A DISPONIBILIZAR QUANDO SOLICITAR DADOS PESSOAIS

Quando os dados pessoais forem recolhidos, a empresa que os solicitar deve facultar, aquando da recolha desses, informações como: (Art.º 13, alínea 1 e 2, pág. 40 e 41)

A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;

Os contactos do encarregado da proteção de dados, se for caso disso;

As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

Os destinatários ou categorias de destinatários dos dados pessoais, se os houver, como, por exemplo, transferência de dados para parceiros;

Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;

A existência do direito de solicitar à empresa o acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;

O direito de apresentar reclamação a uma autoridade de controlo.

10. SOBRE INFORMAÇÕES A DISPONIBILIZAR APÓS OS DADOS RECOLHIDOS

O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: (Art.º 15, Alínea 1, pág. 40)

As finalidades do tratamento dos dados; (a ARTSOFT disponibiliza um modelo)

As categorias dos dados pessoais em questão; (a ARTSOFT disponibiliza um modelo)

Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados;

Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;

A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos mesmos, ou do direito de se opor a esse tratamento;

O direito de apresentar reclamação a uma autoridade de controlo;

Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;

A existência de decisões automatizadas, incluindo a definição de perfis;

O titular dos dados tem o direito de ser informado das garantias adequadas, relativamente à transferência de dados.

11. SOBRE O DIREITO À RETIFICAÇÃO DOS DADOS, À LIMITAÇÃO DO TRATAMENTO, E AO APAGAMENTO DOS DADOS

O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a **retificação dos dados pessoais** inexatos que lhe digam respeito. (Art.º 16, pág. 43)

O titular dos dados tem o direito de obter da empresa **a limitação do tratamento**, se se aplicar uma das seguintes situações:

Contestar a exatidão dos dados pessoais, durante um período que permita à empresa verificar a sua exatidão;

O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial; (Art.º 18, pág. 44)

O titular tem o direito de obter do responsável pelo tratamento o **apagamento dos seus dados pessoais**, sem demora injustificada, e este tem a obrigação de apagar os mesmos, sem demora injustificada. Abaixo alguns motivos que justificam o apagamento imediato: (Art.º 17, pág. 43)

Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;

O titular retira o consentimento em que se baseia o tratamento dos dados e se não existir

outro fundamento jurídico para o referido tratamento;

O titular opõe-se ao tratamento e não existem interesses legítimos prevalecentes que justifiquem o tratamento ou ;

Os dados pessoais foram tratados ilicitamente;

Excetuam-se, no entanto, alguns motivos pelos quais não deverá aceitar o apagamento:

Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;

Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos;

Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

A empresa deve comunicar a cada destinatário a quem tiver entregue os dados pessoais, as retificações ou apagamento. (Art.º 19, pág. 45)

13. SOBRE O DIREITO À PORTABILIDADE

O titular dos dados tem o direito de receber os dados que lhe digam respeito e que tenha fornecido à empresa, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o possa impedir. (Art.º 20, pág. 45)

14. SOBRE O DIREITO À OPOSIÇÃO E ÀS DECISÕES AUTOMATIZADAS

O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito. (Art.º 21, pág. 45)

O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, a não ser que este tenha sido informado e tenha dado o consentimento ou se, por exemplo, o tratamento automatizado for necessário para a celebração ou execução de contrato. (Art.º 21, pág. 45)

15. SOBRE SUBCONTRATANTES (parceiros, etc.)

Qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento, ou de um subcontratante situado na União deverá ser feito em conformidade com o regulamento, independentemente de o tratamento em si ser realizado na União Europeia. (Pág. 4 (22) | Pág. 5 (24))

O subcontratante não pode subcontratar sem que a empresa que detém os dados dê autorização por escrito.

O tratamento em subcontratação tem de ser regulado por contrato ou outro ato normativo ao abrigo do direito da União Europeia, onde constem todas as informações necessárias para cumprir o RGPD.

O subcontratante tem de cumprir o RGPD e disponibilizar à empresa cliente todas as informações que garantam o cumprimento.

O subcontratante deve ter certificação a solicitar a autoridades de controlo. (Art.º 28, pág. 50)

16. SOBRE REGISTOS DAS ATIVIDADES DE TRATAMENTO

Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade. Desse registo devem constar todas as seguintes informações:

O nome e os contactos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados;

As finalidades do tratamento dos dados;

A descrição das categorias de titulares de dados e das categorias de dados pessoais;

As categorias de destinatários a quem os dados pessoais foram ou serão divulgados;

Os prazos previstos para o apagamento das diferentes categorias de dados;

Uma descrição geral das medidas técnicas e organizativas no domínio da segurança;

Nota: As obrigações acima não se aplicam às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados, ou dados pessoais relativos a condenações penais e infrações referido. (Art.º 30, pág. 50)

17. SOBRE SEGURANÇA DOS DADOS PESSOAIS

Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

Cifragem dos dados pessoais e pseudonimização (tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares);

A capacidade de assegurar a confidencialidade, integridade e disponibilidade dos serviços de tratamento;

A criação de um código de conduta ou de um procedimento de certificação que podem ser utilizados como elementos para demonstrar o cumprimento das obrigações estabelecidas no RGPD.

18. SOBRE VIOLAÇÃO DE DADOS E NOTIFICAÇÕES A QUEM DE DIREITO

As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. (Considerando 39, pág. 7)

Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente, sem demora injustificada e, sempre que possível, **até 72 horas** após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.

Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.

A notificação referida deve, pelo menos:

Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;

Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;

Descrever as consequências prováveis da violação de dados pessoais e as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais;

(Art.º 33, pág. 52)

Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos das pessoas singulares, o responsável pelo tratamento deve comunicar também a violação ao titular dos dados sem demora injustificada. No entanto, se o risco não for elevado e a empresa tiver aplicado medidas de proteção, ou se a comunicação exigir um esforço desproporcionado, a comunicação ao titular não é exigida. (Art.º 35, pág. 53)

19. SOBRE O ENCARREGADO DA PROTEÇÃO DE DADOS

O responsável pelo tratamento e o subcontratante devem designar um encarregado da proteção de dados sempre que o tratamento for efetuado por uma autoridade ou um organismo público ou as atividades principais da empresa consistam em operações regulares e sistemáticas dos titulares dos dados em grande escala.

O EPD deve ser designado com base nas suas qualidades profissionais e conhecimentos especializados no domínio do direito. Pode ser um elemento do pessoal da empresa, desde que não tenha interesses legítimos no tratamento ou conflito de interesses (ex.: administrador da empresa ou departamento de marketing/comercial).

Tem como principais funções: informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações no cumprimento do RGDP; controlar a conformidade e cooperar com a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo consulta prévia de, por exemplo, código de conduta. (Art.^{os} 37, 38 e 39, pág. 55)

Nota: Mesmo não sendo obrigatório, pode ser recomendável que alguém na empresa seja nomeado como responsável pelo tratamento dos dados.

20. SOBRE A CERTIFICAÇÃO

Após a empresa garantir que internamente tem assegurado procedimentos que cumpram o RGPD, deve submeter um pedido de certificação à autoridade competente ou outro organismo avaliado para o efeito que comprove a conformidade das operações de tratamento de dados, quando o mesmo estiver disponível.

Este pedido de certificação não é, no entanto, obrigatório. É voluntário e está disponível através de um processo transparente. Para o solicitar, a empresa deve submeter todo o acesso às suas atividades de tratamento.

A certificação é emitida aos responsáveis pelo tratamento e subcontratantes por um período máximo de três anos e pode ser renovada nas mesmas condições, desde que os requisitos aplicáveis continuem a estar reunidos.

Todos os procedimentos de certificação e todos os selos e marcas de proteção de dados aprovados num registo, pelas autoridades competentes, serão disponibilizados ao público por todos os meios adequados. (Art.º 42, pág. 59)