

RGPD | Regulamento Geral de Proteção de Dados

Perguntas Frequentes

- 1) **A empresa de contabilidade que contratei recebe por *email* a documentação empresarial que contem dados dos meus colaboradores. O que devo fazer para garantir a privacidade dos dados?**

Deve garantir as condições adequadas de segurança no envio da informação (existem diversas possibilidades, como a encriptação de dados) e informar os seus colaboradores deste envio, referindo a sua finalidade. É também importante sensibilizar internamente para as boas práticas internas na utilização do correio eletrónico. Deve ainda assegurar, através de contrato, que o subcontratante cumpre também os requisitos do RGPD.

- 2) **Tenho de designar um Encarregado de Proteção de Dados na minha empresa?**

A nomeação de um Encarregado de Proteção de Dados (*Data Protection Officer*) só é obrigatória nos organismos públicos e nas empresas que lidam com dados pessoais considerados sensíveis ou em grande escala.

- 3) **O que devo fazer se detetar uma falha de segurança na proteção dos dados pessoais de clientes da empresa?**

Se a falha de segurança implicar um risco para os titulares dos dados, deve reportar a ocorrência num prazo de **72 horas** à Autoridade Nacional de Controlo e, se da análise do risco se verificar que o mesmo é elevado, deverá informar o(s) cliente(s) de que a informação que contem os dados pessoais foi violada. Este reporte deverá conter informação relativa ao tipo e amplitude da falha ocorrida bem como medidas

adotadas na sua resolução. E desde logo criar e implementar procedimentos que excluam situações futuras idênticas.

4) **Sou gerente de uma microempresa e não trato dados pessoais de forma regular, como devo proceder?**

O RGPD é aplicável a todas as empresas que façam tratamento de dados pessoais, independentemente da sua dimensão ou setor de atividade. No entanto, atendendo à situação particular das micro, pequenas e médias empresas, o Regulamento prevê uma derrogação para as organizações com menos de 250 trabalhadores, mas apenas relativamente à obrigação de conservação do registo das atividades de tratamento de dados.

5) **No âmbito do recrutamento de novos colaboradores, recolho informação alargada de possíveis candidatos, o que devo fazer com essa informação após conclusão do processo?**

Essa informação deverá ser mantida apenas pelo prazo necessário para o cumprimento da finalidade para que foram recolhidos os dados. Se houver interesse de manter a informação dos dados, deverá comunicar ao titular essa intenção e recolher o seu consentimento, indicado os motivos e o prazo associados para a conservação dos dados.

6) **Regularmente envio a *newsletter* da empresa para a base de contactos que detenho, para divulgação dos meus produtos e serviços. Necessito de solicitar consentimento?**

Sim. É necessário solicitar consentimento respeitando os termos definidos no regulamento.

7) Basta atualizar as políticas de privacidade para estarmos em conformidade?

Não. É necessário que as políticas de privacidade estejam em consonância com o RGPD e garantir que as mesmas estão a ser observadas.

8) Tendo muitos dados pessoais em papel na minha empresa, que medidas devo tomar?

A empresa deve introduzir medidas de proteção em todos os formatos de armazenamento de dados. Deve averiguar onde se encontram, quem acede, a necessidade de conservação, e a sua eliminação caso não tenha licitude para os manter.

9) O *email* profissional é um dado pessoal?

Se esse *email* apresentar elementos que possa identificar uma pessoa singular então representa um dado pessoal e deve ser protegido com os mecanismos adequados.

10) Tenho os dados pessoais da minha empresa alojados no *data center* de uma empresa externa. Como posso proteger estes dados?

A empresa deve exigir no contrato de serviço de alojamento as necessárias medidas de segurança dos dados de forma a proteger os direitos dos titulares dos dados.

11) Como posso obter a certificação para exercer as funções de EPD (Encarregado de Proteção de Dados, em inglês *Data Protection Officer*)? O IPAC vai acreditar os EPD?

O RGPD não exige a certificação dos EPD para exercer essas funções (artigo 37.º, n.º). Esclarecemos também que o IPAC não acredita EPD.

12) Os organismos que tenham ou venham a obter acreditação pelo IPAC poderão outorgar certificações no âmbito do RGPD?

O RGPD estipula que os organismos de certificação possam ser acreditados pelo IPAC e, nesse caso, poderão outorgar certificações no âmbito do RGPD (artigo 43.º, n.º 1, alínea b) - de momento não se encontra nenhum acreditado, mas consultando periodicamente o [Diretório de Entidades Acreditadas](#) do IPAC poderá manter-se atualizado nesta matéria.

13) Quais as empresas acreditadas que certificam o cumprimento legal do RGPD?

Os organismos de certificação que venham a ser acreditados serão listados no [Diretório de Entidades Acreditadas](#) do IPAC.

Esclarecemos ainda que a certificação atestará a conformidade do processo de tratamento de dados da empresa com a especificação de certificação usada, pelo que não haverá uma certificação direta da conformidade legal, até porque o RGPD não atribui tal tarefa aos organismos de certificação - contudo, a certificação poderá ser utilizada como um dos elementos para demonstrar o cumprimento do RGPD (artigo 24º, n.º 3; artigo 25º, n.º 3; artigo 28º, n.º 5; artigo 32º, n.º3; artigo 42º, n.º1 e n.º2).

14) Como poderei acreditar junto do IPAC a minha empresa no âmbito do RGPD e quais os procedimentos e custos associados?

Informamos que os candidatos devem cumprir os requisitos da norma NP EN ISO/IEC 17065 (que pode ser adquirida junto do [IPQ](#), bem como os critérios adicionais que a autoridade de controlo possa eventualmente estabelecer (artigo 43.º). Os procedimentos de acreditação do IPAC estão [publicamente disponíveis](#) - deve começar por consultar o Regulamento Geral de Acreditação (DRC001) bem como os documentos conexos por este referenciados, em particular o Procedimento para Acreditação de Organismos de Certificação (DRC006). O Regulamento de Preços corresponde ao documento DRC004 e encontra-se igualmente disponível na mesma secção.

15) Que tipos de certificação estão previstas no âmbito do RGPD?

O RGPD prevê (considerando n.º 100; artigo 42.º, n.º 1) a certificação do processo de controlo e tratamento de dados, podendo incluir ainda a certificação de produtos (ex. *software* ou *hardware*) ou de serviços.

16) É obrigatório certificar a minha empresa no âmbito do RGPD?

Não (artigo 42.º, n.º 3). Contudo, a certificação poderá ser utilizada como um dos elementos para demonstrar o cumprimento do RGPD (artigo 24º, n.º 3; artigo 25º, n.º 3; artigo 28º, n.º 5; artigo 32º, n.º 3; artigo 42º, n.º 1 e n.º 2).

17) Pretendo criar um organismo de certificação no âmbito do RGPD - qual o procedimento de certificação que devo usar?

O RGPD não estabelece qual o procedimento de certificação a usar, pelo que poderá usar qualquer documento que tenha o conteúdo apropriado, quer seja uma norma nacional, europeia ou internacional, quer seja uma especificação que desenvolva ou tenha sido desenvolvida por terceiros, sem prejuízo do diploma de execução nacional poder ter disposições nesse sentido. Deverá cumprir com as disposições previstas nos artigos 42.º e 43.º, bem como as orientações dadas no documento [EA-1/22](#), Anexo 2, *Specific Guidance on validation of certification schemes* -.

18) É obrigatória a acreditação ou certificação da nossa empresa para prestar consultoria no âmbito do RGPD?

O RGPD não exige a certificação ou acreditação dos consultores para prestar esses serviços. De qualquer modo, não é possível ao IPAC proceder à acreditação de consultores, dado estes não efetuarem atividades de avaliação da conformidade.

19) O IPAC pode acreditar a minha empresa para formação na área de proteção de dados? Será a acreditação ou certificação obrigatória?

O RGPD não exige a certificação ou acreditação das empresas de formação para prestar esses serviços. De qualquer modo, não é possível ao IPAC proceder à acreditação de empresas de formação dado estas não efetuarem atividades de avaliação da conformidade. No âmbito do RGPD, o IPAC procede apenas à acreditação de organismos de certificação.