Primavera

Tudo o que precisa saber sobre o RGPD

Lista de perguntas e respostas essenciais sobre o Regulamento Geral de Proteção de Dados (RGPD)

Índice

Regulamento Geral de Proteção de Dados

Como assegurar a proteção dos dados pessoais na era digital

Atualmente existem organizações que comercializam ou trocam os dados de pessoas singulares de forma indiscriminada. Somos constantemente contactados por empresas às quais nunca fornecemos os nossos dados, e esse contacto repete-se vezes sem conta, sempre sobre o mesmo assunto.

Subscrevemos um serviço ou efetuamos uma simples pesquisa na internet e os websites que consultamos passam a apresentar-nos publicidade orientada. Ainda mais grave, na maioria das vezes, as empresas/entidades gerem os dados sem sabermos como, nem para que finalidade, e por tempo ilimitado.

É precisamente para combater este uso excessivo, e muitas vezes indevido de dados pessoais, que surge o RGPD.

O Regulamento Geral de Proteção de Dados (RGPD) ou General Data Protection Regulation (GDPR) é um Regulamento Europeu (EU 2016/679) que pretende reforçar e uniformizar as medidas de proteção dos dados pessoais de todos os cidadãos da União Europeia, devolvendo aos indivíduos o controlo da sua informação pessoal.

A necessidade de rever a atual legislação, Diretiva 95/46/EC, de 1995 e aplicável até maio de 2018, prende-se com as profundas alterações que a tecnologia, nomeadamente o surgimento da internet, trouxe à forma de tratamentos dos dados por parte das empresas, assistindo-se a uma massificação do uso das redes sociais, o online banking, soluções SaaS, Cloud, Internet das Coisas e outras tecnologias que proliferam nesta era digital.

O RGPD não se aplica a pessoas, mas sim a empresas. Ao longo deste guia iremos dar-lhe conta de tudo o que precisa saber para garantir que a sua empresa cumpre a legislação e, enquanto cidadão, quais os direitos que lhe assistem.

O que é o Regulamento Geral de Proteção de Dados (RGPD)?

O RGPD refere-se ao Regulamento 2016/679, de 27 de abril de 2016, e é um diploma que estabelece as regras referentes à proteção, tratamento e livre circulação de dados pessoais das pessoas singulares em todos os países membros da União Europeia. Este regulamento revoga a Diretiva 95/46/CE e a Lei n.º 67/98, (conhecida como Lei de Proteção de dados), que transpôs esta Diretiva para o ordenamento jurídico português.

Quais os objetivos do RGPD?

O RGPD veio reforçar a Proteção de Dados prevista no art.º 8.º da Carta dos Direitos Fundamentais da União Europeia.

Pode dizer-se que o RGPD surgiu com três objetivos principais:

1. Atualizar a legislação relativa à proteção de dados pessoais, alinhando-a com a nova era digital proporcionada pela contínua evolução tecnológica.

2. Harmonizar a legislação existente nesta matéria nos diversos Estados-Membros da União Europeia, dando um passo significativo no sentido da criação do mercado único digital.

3. Reforçar os direitos dos cidadãos, protegendo-os dos riscos e ameaças relativos à utilização indevida dos seus dados pessoais.

A partir de quando se aplicará o RGPD?

O RGPD tem aplicação direta a partir de **25 de maio de 2018**. O regulamento foi aprovado em 27 de abril de 2016, após quase cinco anos de negociações e cerca de 4 000 adendas, sendo aplicado diretamente, isto é, sem necessidade de qualquer transposição para a ordem jurídica interna. Até ao dia 25 de maio de 2018, em Portugal, continuará a ser aplicável a Lei de Proteção- lei n.º 67/98, de 26 de outubro.

A quem se aplica?

O novo Regulamento aplica-se essencialmente aos responsáveis pelo tratamento dos dados pessoais, ou seja:

1. Às organizaçõs estabelecidas em território da União Europeia, independentemente de o tratamento dos dados pessoais decorrer dentro ou fora da União.

2. A todas as organizações que tratem dados pessoais de cidadãos residentes no território da União Europeia, mesmo que estabelecidas fora do território da União.

Neste contexto, o RGPD aplica-se nas seguintes situações:

Neste contexto, o RGPD aplica-se nas seguintes situações:

Oferta de bens ou serviços a titulares dos dados (independentemente de existir pagamento ou não).

Controlo do comportamento desses titulares se o mesmo decorrer dentro da União Europeia.

O responsável esteja estabelecido fora da União Europeia, mas num local onde é aplicável o direito de um dos Estados-Membros por força do Direito Internacional Público.

Dados Pessoais

O que são dados pessoais?

Constituem dados pessoais informação relativa a uma pessoa singular identificada ou identificável a partir desses dados. Considera-se identificada a pessoa que é diferenciada de todas as outras e identificável aquela que, embora não tendo ainda sido identificada, pode vir a sê-lo.

Exemplos de dados pessoais:

__Nome, morada, endereço eletrónico, número de IP, dados de localização
__Data de nascimento
__Número de identificação civil
__Número de identificação fiscal
__Número de identificação da Segurança Social
__Altura, peso e idade
__Composição do agregado familiar
__Padrão da íris e impressão digital
__Elementos de identidade física, fisiológica, genética, mental, económica, cultural ou social
__Perfis de Redes Sociais e informação recolhida por cookies
__Informação bancária
__Informação fiscal
__(...)

O que são categorias especiais de dados pessoais?

Existem alguns dados pessoais que estão enquadrados em categoriais especiais por revelarem informação do foro íntimo e alusiva à vida privada dos cidadãos.

Exemplos de dados pessoais especiais:

__Origem racial/étnica
__Opiniões políticas
__Convicções religiosas ou filosóficas
__Filiação sindical
__Dados relativos à saúde, vida sexual, orientação sexual ou vida privada
__Dados de crédito e solvabilidade
__Condenações penais e infrações

Os dados pessoais não são apenas aqueles que permitem denominar um titular, basta que o distingam ou permitam distinguir de outras pessoas (de forma isolada ou em conjunto com outros dados) para serem considerados dados pessoais.

O que são dados pessoais diretos e dados pessoais indiretos?

Os dados pessoais podem ser divididos em diretos e indiretos.

Dados pessoais diretos:
Aqueles que permitem, por si só, identificar de forma imediata o titular.

Exemplos: *nome ou fotografia.*

Dados pessoais indiretos:
Aqueles que apenas permitem identificar uma pessoa se forem complementados com outro(s) dado(s) ou informações(s) sobre o titular.

Exemplo: *N.º do Cartão de Cidadão - por si só este dado não permite identificar o sujeito, mas se for consultado o Registo Civil, já é possível obter essa identificação.*

O que distingue o tratamento de dados pessoais do tratamento de dados pessoais especiais?

A principal diferença reside no facto de o tratamento de dados pessoais especiais ser proibido, com exceção dos casos em que está permitido o seu tratamento (previstas no art.º 9.º, n.º 2 do Regulamento).

Tratamento de dados

Em que consiste o tratamento de dados?

Considera-se tratamento de dados pessoais qualquer operação realizada sobre os dados pessoais, efetuada com ou sem meios automatizados.

Alguns exemplos de situações em que existe tratamento de dados pessoais:

_Recolha de dados pessoais

_Registo de dados pessoais

_Organização de dados pessoais

_Estruturação de dados pessoais

_Conservação de dados pessoais

_Adaptação de dados pessoais

_Alteração de dados pessoais

_Recuperação de dados pessoais

Segurança e Privacidade dos Dados

Quais os princípios orientadores da segurança e privacidade de dados?

Existem quatro princípios básicos que devem orientar a recolha e tratamento de dados pessoais, nomeadamente:

1

Confidencialidade

Os dados pessoais devem estar protegidos do acesso ou exposição não autorizados.

2

Integridade

Os dados pessoais devem conservar todas as caraterísticas que foram definidas pelo seu titular, desde o momento em que foram fornecidos, até à sua eliminação.

3

Disponibilidade

O acesso aos dados pessoais só deverá estar disponível mediante validações de perfis, permissões e condições previamente estabelecidas.

4

Conformidade legal e normativa

A recolha e tratamento de dados pessoais deve respeitar as regras estabelecidas pelo RGPD e restante legislação conexa.

Direitos dos Titulares

Que direitos têm os titulares dos dados?

O RGPD vem precisamente reforçar os direitos dos titulares sobre os seus dados, permitindo-lhes ter conhecimento sobre que dados seus estão a circular, quem os conhece e para que fins serão utilizados. O Regulamento estabelece um conjunto de direitos como:

1. Direito à transparência

Os titulares dos dados têm o direito de saber que tratamentos são efetuados sobre os seus dados.

Por exemplo, no caso de estarem a ser recolhidas imagens e som (ou poderem vir a sê-lo) deverá existir informação visível que informe os titulares sobre a realização das gravações.

2. Direito à informação

Os titulares têm o direito de solicitar ao responsável pelo tratamento dos dados, informações sobre o tipo de tratamento a que os seus dados estão a ser sujeitos. As informações devem ser prestadas por escrito. Se o titular assim o solicitar, a informação poderá ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.

Por exemplo, no momento da recolha dos dados, o titular deve ser informado sobre o tratamento de que os mesmos serão alvo.

3.Direito de acesso

Os titulares têm o direito de saber se os seus dados são ou não objeto de tratamento por parte de uma organização. Caso sejam alvo de tratamento, o titular tem o direito a aceder aos seus dados pessoais e às seguintes informações:

__Finalidade do tratamento;

__Categorias dos dados pessoais em questão;

__Destinatários ou categorias de destinatários a quem os dados são, foram ou serão divulgados;

__Prazo previsto de conservação de dados, ou se tal não for possível, os critérios para fixar esse prazo;

__Garantias de conhecimento e tratamento adequado sempre que os dados forem transferidos para um país terceiro ou uma organização internacional;

__Acesso a uma cópia dos dados pessoais em fase de tratamento. Se o pedido for apresentado por meios eletrónicos, a informação deverá ser fornecida num formato eletrónico de uso corrente.

4. Direito de retificação

Direito de solicitar a retificação de dados incorretos e preenchimento de dados incompletos. Cada retificação efetuada pelo responsável pelo tratamento implica a comunicação dessa alteração às entidades a quem os dados tenham sido transmitidos, salvo se essa comunicação se revelar impossível ou implicar um esforço desproporcionado.

O direito ao apagamento tem de ser conciliado com as obrigações jurídicas que o responsável pelo tratamento de dados deve assegurar relativamente às entidades oficiais, que nesse caso se sobrepõem. Por exemplo, o dever de manutenção de faturas emitidas.

5. Direito ao apagamento

Os titulares dos dados têm o direito de solicitar o apagamento dos mesmos, o que deverá decorrer sem demora injustificada. O apagamento dos dados é ainda obrigatório nas seguintes situações:

__Quando os dados deixam de ser necessários para a finalidade que motivou a sua recolha ou tratamento;

__Quando o titular retira o consentimento para o tratamento (desde que não exista outro fundamento para esse tratamento);

__Quando o titular se opõe ao tratamento e não existem interesses legítimos prevalecentes que justifiquem esse tratamento;

__Quando os dados foram tratados ilicitamente;

__Para dar cumprimento a uma obrigação jurídica decorrente do direito da União Europeia ou de um Estado-Membro a que o responsável esteja sujeito;

__Quando os dados foram recolhidos no contexto da oferta de serviços da sociedade da informação.

6. Direito à limitação do tratamento

O titular pode opor-se ao apagamento dos seus dados pessoais e solicitar a limitação do seu tratamento (inserção de uma marca nos dados pessoais conservados para limitar o seu tratamento no futuro).

Neste contexto, o titular tem direito a que o responsável faça a limitação do tratamento num dos seguintes casos:

6.1 Durante o período em que o responsável de proteção de dados valida a exatidão dos mesmos, após contestação de incorreção por parte do titular.

6.2 Quando existe tratamento ilícito e o titular se opõe ao apagamento, pode solicitar a limitação da utilização.

6.3 Quando o responsável já não precisa dos dados para tratamento, mas os mesmos são requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

6.4 No caso do titular se opor ao tratamento nos termos do 21.º, n.º 1 até se verificar que os motivos legítimos do responsável se sobrepõem aos do titular.

6.5 Quando o titular se opõe ao tratamento de dados que lhe digam respeito para efeitos de comercialização.

O responsável pelo tratamento tem de comunicar a cada destinatário, a quem os dados tenham sido transmitidos, qualquer limitação de tratamento que tenha feito, salvo se essa comunicação se revelar impossível ou implicar um esforço desproporcionado.

Em todas estas situações, os dados podem ser conservados, mas o seu tratamento só poderá decorrer mediante consentimento do titular, para efeitos de declaração, para exercício ou defesa de um direito em processo judicial, para defesa de outra pessoa singular ou coletiva ou por motivos de interesse público da União Europeia ou do Estado-Membro.

7.Direito de oposição

O titular poderá opor-se à utilização dos seus dados para efeitos de comercialização direta.

8.Direito à notificação

Os titulares dos dados devem ser notificados ou ser-lhes dado conhecimento nos casos em que os seus dados pessoais estejam a ser recolhidos ou tratados.

Por exemplo:
Os colaboradores das empresas têm o direito de ser informados sobre as situações em que existe algum tipo de monitorização de equipamentos de trabalho ou geolocalização. No caso de viaturas, quando não se sabe quem conduz, deve ser colocado um dístico na viatura a informar que é efetuada a geolocalização da mesma. Se existir algum tipo de monitorização dos equipamentos/instrumentos de trabalho usados pelo funcionário, o mesmo tem de ser informado/notificado disso.

9. Direito à não sujeição a decisões automatizadas

O titular dos dados tem o direito de solicitar intervenção humana em processos habitualmente automáticos.

Por exemplo:
Nos casos em que existem mecanismos de profiling, o titular pode exigir que haja uma intervenção humana nesse processo automatizado, para que a decisão não seja tomada de forma exclusivamente automática. Porém, se tiver dado o seu consentimento explícito nesse sentido, esse tratamento automatizado já será possível.

10. Direito à portabilidade

O titular dos dados pode solicitar que os mesmos sejam transferidos para outra empresa/entidade (à semelhança do que acontece com as operadoras de telecomunicações). Pode querer transferir os seus dados clínicos, créditos de formação ou outros. Nestes casos, deve ser usado um formato de uso corrente.

2

Incidentes de Violação de Dados

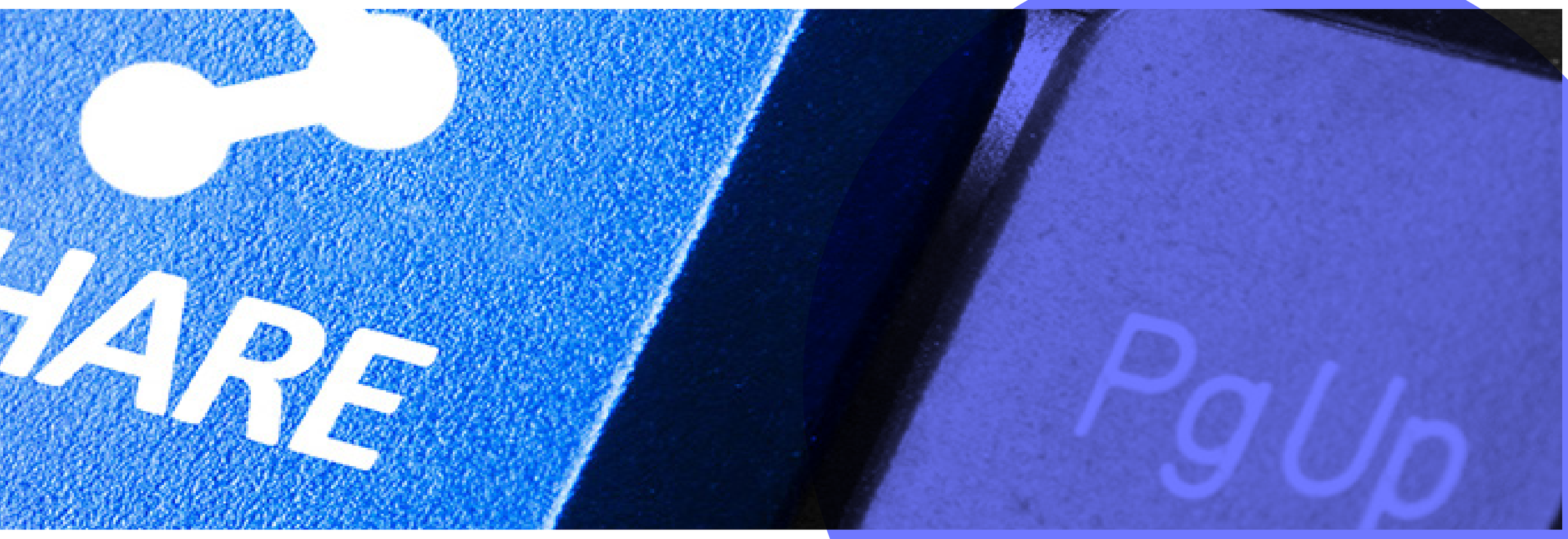
O que são incidentes de violação de dados pessoais?

Os incidentes de violação de dados pessoais são situações associadas ao acesso, alteração ou eliminação indevida de dados pessoais, quer tal ocorra de forma acidental ou ilícita.

Sempre que são verificados esses incidentes, é necessário que as entidades efetuem uma notificação a terceiros. Por um lado, é obrigatória a notificação à Comissão Nacional de Proteção de Dados (CNPD) sem demora injustificada e sempre que possível até 72 horas após conhecimento da existência do incidente. Ultrapassado esse prazo, é necessário justificar os motivos que levaram ao atraso.

Poderá, ainda, ser necessária a notificação do próprio titular dos dados quando o risco para os direitos e liberdades das pessoas singulares for elevado. No entanto, esta comunicação ao titular poderá ser evitada se, por exemplo, o responsável pelo tratamento tiver ativado medidas de proteção adequadas, tanto técnicas como organizativas, especialmente medidas que tornem os dados afetados pela violação incompreensíveis (por exemplo através da cifragem).

Também existe o dever de o subcontratante notificar o responsável pelo tratamento dos dados, sempre que verifique a ocorrência de um incidente.



Avaliação do Impacto de Privacidade (PIA)

Em que consiste a avaliação de impacto de privacidade?

A Avaliação do Impacto de Privacidade, em inglês PIA (Privacy Impact Assessement), deve decorrer especialmente nos casos em que o tratamento dos dados pessoais é efetuado através do uso de novas tecnologias. Essa avaliação deverá considerar a natureza dos dados, o âmbito, o contexto e a finalidade dos mesmos.

Sempre que o tratamento efetuado apresente suscetibilidade de implicar um elevado risco para os direitos e liberdades dos titulares, o responsável pelo tratamento deverá fazer uma avaliação do impacto das operações previstas na proteção dos dados pessoais, antes de iniciar o tratamento.

A realização de um PIA (Privacy Impact Assessement) é obrigatória nas seguintes situações:

1. Quando é feita uma avaliação de aspetos pessoais com base no tratamento automatizado de dados, incluindo definição de perfis que produzem efeitos jurídicos relativamente à pessoa singular.

2. Quando existe tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais ou infrações.

3. Quando é realizado um controlo sistemático de zonas acessíveis ao público em grande escala.

As Autoridades de Controlo de cada país irão disponibilizar uma lista dos tratamentos sujeitos a avaliação prévia de impacto, identificando também as situações em que essa análise não é obrigatória. Se nada for dito, caberá aos responsáveis pelo tratamento essa decisão.

Aspetos mínimos a considerar na avaliação de impacto de privacidade:

__Descrição das operações de tratamento a que os dados serão sujeitos;

__Finalidade das ações de tratamento;

__Interesses legítimos do responsável de proteção de dados (se aplicável);

__Avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;

__Avaliação dos riscos para os direitos e liberdades dos titulares dos dados;

__Medidas previstas e garantias para fazer face aos riscos;

__Medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais, demonstrando a conformidade com o Regulamento;

__Solicitar parecer ao DPO.

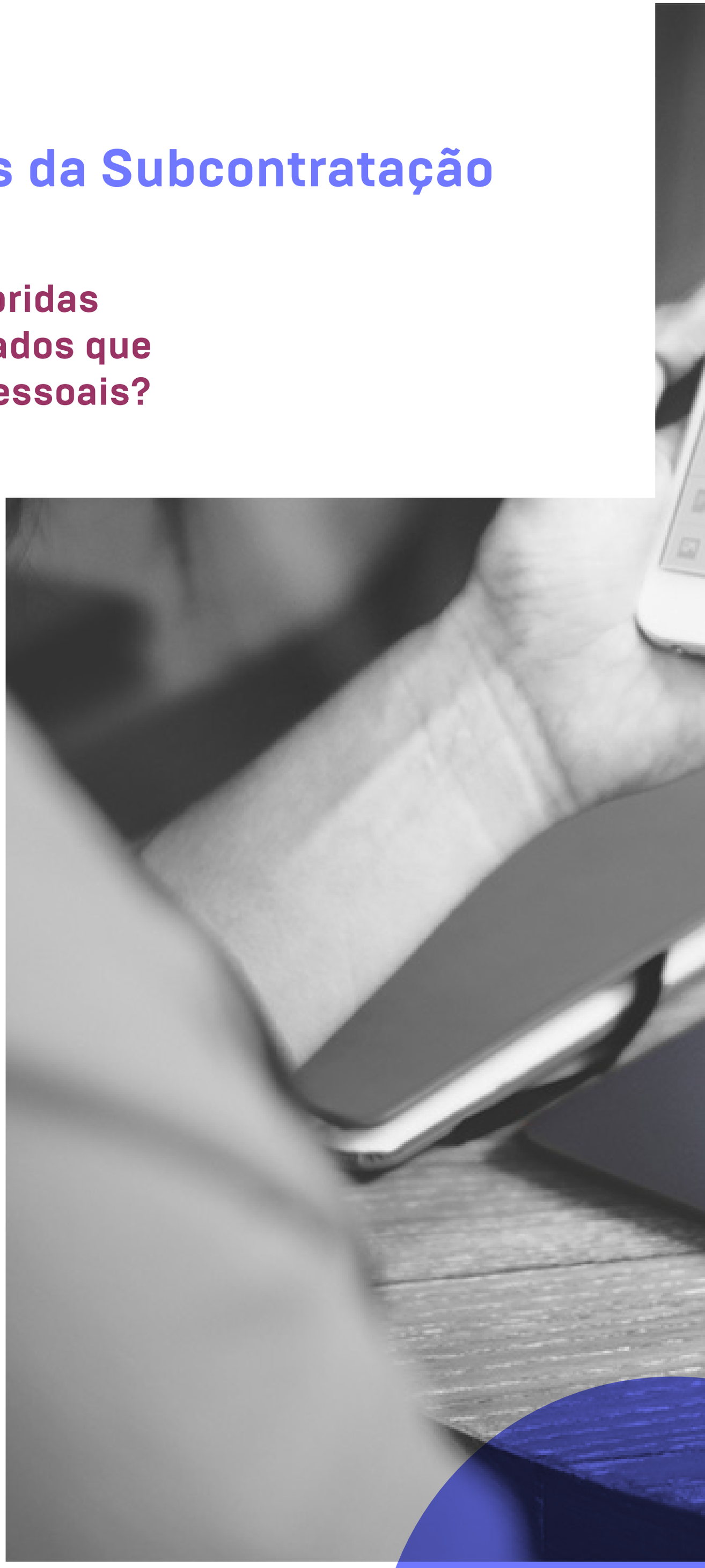
Obrigações Decorrentes da Subcontratação

Que exigências têm de ser cumpridas quando se recorre a subcontratados que efetuam tratamento de dados pessoais?

O recurso a subcontratantes só é possível se estes apresentarem garantias suficientes de execução de medidas técnicas e organizativas adequadas ao RGPD. Por outro lado, o subcontratado não pode contratar outro subcontratante sem autorização prévia específica ou geral do responsável de proteção de dados, sendo que essa autorização terá de ser manifestada por escrito.

No contrato de subcontratação terá de ficar estabelecido o objeto e duração do tratamento, natureza e finalidade, tipo de dados e categorias dos titulares, assim como as obrigações e direitos do responsável. Será ainda necessário acautelar as cláusulas do art.º 28.º, n.º 3.

A relação entre o responsável e o subcontratado pode ser regulada por um contrato individual ou cláusulas-tipo.




Uploading ...
Creative Process.jpg
Management.doc
Digital.jpg
Template.jpg
Project Planning.doc
Recruitment-data.jpg
PRIVACY
Login Problem,
Wrong username or password
MESSENGER
LOGIN

Encarregado de Proteção de Dados

A designação de um Encarregado de Proteção de Dados (DPO) é obrigatória?

A designação de um Data Protection Officer (DPO), em português “Encarregado de Proteção de Dados” não é obrigatória para todas as entidades.

É obrigatória a designação de um DPO nas seguintes situações:

__Se o tratamento dos dados for efetuado por uma autoridade ou organismo público, exceto tribunais no exercício da sua função jurisdicional.

__Se as atividades principais do responsável ou do subcontratante consistirem em operações de tratamento que exijam um controlo regular e sistemático dos titulares dos dados.

__Se as atividades principais do responsável pelo tratamento ou do subcontratante consistirem em operações de tratamento em grande escala de categorias especiais de dados, nos termos do artigo 9.º e de dados pessoais relacionados com condenações penais e infrações (art.º 10.º).

Num grupo empresarial, pode ser designado um único DPO se o mesmo estiver facilmente acessível para toda a organização, independentemente da localização geográfica. Se assim não for, terá de existir um DPO em cada estabelecimento. O DPO poderá ser alguém interno à organização ou um prestador de serviço em regime de outsourcing.

Coimas e Sanções

Se não forem cumpridas as exigências do RGPD, o que pode acontecer?

As sanções previstas no RGPD são bastante mais gravosas do que as anteriormente existentes.

O limite máximo das coimas varia consoante as obrigações que forem violadas, podendo chegar aos 20 milhões de euros ou até 4% do volume de negócios anual da empresa a nível mundial, de acordo com o exercício financeiro do ano anterior, conforme o valor que for mais elevado.

O apuramento do valor de operações a nível mundial resulta de averiguações sobre a existência ou não de relação de grupo. Esse valor também ficará dependente das obrigações violadas e/ou não cumpridas e da existência de dolo ou negligência, bem como o respetivo grau.

Outras sanções

Para além das coimas, podem ainda ser aplicáveis outras sanções. Com a legislação atualmente em vigor, essas sanções podem passar pela proibição temporária ou definitiva do tratamento, o bloqueio, o apagamento ou destruição total ou parcial dos dados; a publicidade da sentença condenatória ou a advertência ou censura públicas do responsável pelo tratamento.

A violação do RGPD pode resultar em diferentes tipos de sanções:

__Responsabilidade Criminal

__Responsabilidade Administrativa

__Responsabilidade Civil

__Responsabilidade Disciplinar (do ponto de vista dos trabalhadores de uma organização)

__Responsabilidade Social

Estes valores são aplicáveis ao setor privado. Quanto ao setor público, caberá a cada Estado-Membro regular quai as coimas aplicáveis.

is

Proteção de Dados nas Soluções PRIMAVERA

Soluções de gestão PRIMAVERA darão resposta atempada a todas as diretrizes do RGPD

A PRIMAVERA está neste momento a desenvolver mecanismos que assegurem o tratamento integral de todas as diretrizes do Regulamento Geral de Proteção de Dados.

No cumprimento da sua missão de constituir o parceiro tecnológico de eleição das organizações, atempadamente irá disponibilizar novas versões do software que garantam o cumprimento cabal do RGPD.

Informações adicionais

Este documento é da responsabilidade da equipa de juristas da PRIMAVERA e não dispensa nem substitui a leitura integral dos diplomas aplicáveis sobre as matérias abordadas.

As informação contidas neste manual são gerais e abstratas, não devendo servir de base para qualquer tomada de decisão sem assistência profissional qualificada e dirigida ao caso concreto.

Ações de formação

Poderá também inscrever-se nas ações de formação levadas a cabo pelos juristas da PRIMAVERA.

Se precisar de informações adicionais, deixe o seu contacto. Teremos todo o gosto em ajudar!

Os dados serão usados exclusivamente para que possa receber mais informações sobre o RGPD.

Se precisar de mais informações, visite o nosso Website

Evento

RGPD
ESTÁ PREPARADO?

Porto - 6 fevereiro
Lisboa - 8 fevereiro

Increva-se aqui

Primavera

Braga
Edifício PRIMAVERA
Lamaçães
4719-006 Braga

Lisboa
Edifício Arquiparque II
Av. Cáceres Monteiro nº10, 6º
1495-192 Algés
T (+351) 253 309 900
Email comercial@primaverabss.com

www.primaverabss.com

/primaverabss /primaverabss /company/primaverabss