BARROCAS
ADVOGADOS

NOTA INFORMATIVA

sobre o

Regulamento Geral para a Proteção de Dados Pessoais (RGPD)

(Regulamento (UE) nº 2016/679)

(1)

Aplicação: O RGPD, aprovado pelo Parlamento Europeu e pelo Conselho, datado de 27 de abril de 2016, aplicar-se-á em cada estado membro sem necessidade de transposição, substituindo a Diretiva (UE) nº 95/46 e as demais normas de direito interno de cada estado membro que tenham sido publicadas para transpor aquela Diretiva. Esta última, bem como as normas internas de cada estado membro que a transpuseram, terminam a sua vigência logo que o RGPD entre em vigor.

O RGPD prevê, em limitados aspetos, a possibilidade de ser publicada legislação interna em cada estado membro que constitua um complemento regulatório.

(2)

RGPD entrada em vigor: O RGPD entrará em vigor em 25 de maio de 2018.

(3)

Em que consistem os dados pessoais?:

Os dados pessoais das pessoas singulares protegidos podem ser da mais diversa natureza e incluem, entre outras, informações:

- biográficas
- sobre a residência e a naturalidade
- antropomórficas
- filiação

- composição do agregado familiar
- dados relativos à saúde
- dados bancários e, em geral, os relativos à situação patrimonial e económica, pretérita e atual do cidadão titular dos dados pessoais
- particularidades da vida pessoal
- posição na sociedade civil e comportamento social
- conteúdo dos registos não públicos ou de acesso restrito de ordem pessoal, cível, criminal, predial ou de propriedade em geral
- documentos de identificação, número de cartão de crédito
- outras relativas à privacidade ou à vida social do cidadão.

(4)

Propósito: Os dados pessoais das pessoas singulares são considerados um direito fundamental destas, conforme consta do preâmbulo do RGPD e se encontra igualmente consagrado no artigo 8º., nº 1., da Carta dos Direitos Fundamentais da União Europeia e no artigo 16º, nº 1., do Tratado sobre o Funcionamento da União Europeia, que estabelecem que todas as pessoas singulares têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.

O RGPD, ainda nos termos do seu preâmbulo, estabelece que visa contribuir para a realização de um espaço de liberdade, segurança e justiça em vista da construção de uma união económica, o progresso económico e social, a consolidação e convergência das economias no âmbito do mercado interno e para o bem estar das pessoas singulares.

(5)

Fundamentos do RGPD: Transcrevemos aqui, para melhor compreensão do propósito do RGPD, os nºs. 5 e 6 do seu preâmbulo:

"A integração económica e social resultante do funcionamento do mercado interno provocou um aumento significativo dos fluxos transfronteiriços de dados pessoais. O intercâmbio de dados entre intervenientes públicos e privados, incluindo as pessoas singulares, as associações e as empresas, intensificou-se na União Europeia. As autoridades nacionais dos Estados-

membros são chamadas, por força do direito da União, a colaborar e a trocar dados pessoais entre si, a fim de poderem desempenhar as suas funções ou executar funções por conta de uma autoridade de outro Estado-Membro."

"A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram, por isso, um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais."

(6)

Empresas e Instituições

Afetadas pelo RGPD:

O RGPD aplica-se aos responsáveis pelo tratamento de dados, eventuais subcontratantes contratados por aqueles e encarregados do tratamento, que se encontrem estabelecidos na União Europeia (UE).

De novidade relativamente ao regime que tem vigorado, o RGPD também se aplica aos responsáveis pelo tratamento de dados, eventuais subcontratantes e encarregados do tratamento ao serviço de empresas e instituições[*] que, embora não estabelecidos no território de algum estado membro da UE, nele realizem tratamento de dados[**] relativos a cidadãos residentes na UE.

[*] Por "instituições" entende-se as pessoas jurídicas coletivas que não sejam sociedades comerciais ou civis, incluindo pessoas coletivas públicas (o estado, os institutos públicos, as autarquias, etc.).

[**] Por "tratamento de dados", na linguagem do RGPD, entende-se as empresas ou entidades públicas ou privadas de natureza diversa das empresas, que recolham e utilizam dados pessoais de qualquer pessoa individual com quem se relacionem (empregados, funcionários, clientes, eventuais futuros clientes e qualquer outra pessoa individual a qualquer outro título), desde que residentes na UE.

(7)

Caráter Transfronteiriço do Tratamento de Dados:

Do exposto no número anterior, resulta a possibilidade de empresas ou instituições não sediadas no território de algum estado membro da UE deverem observar o disposto no RGPD. Isso pode resultar:

- quer pelo facto de essas empresas ou instituições tratarem dados de pessoas singulares residentes no território de um estado membro da EU, com o fim de lhes oferecer bens ou serviços,
- quer pelo facto de, por algum outro motivo, monitorizarem o comportamento e, consequentemente, tratarem dados pessoais, no território de um estado membro da EU, de pessoas singulares nele residentes.

Em síntese, muito embora o RGPD se aplique a todas as empresas e instituições que procedam ao tratamento de dados pessoais, as disposições relativas à necessidade de instituir um EPD só terão aplicação relativamente ao tratamento de dados em grande escala ou ao tratamento de dados sensíveis (ou, nas palavras do art. 9.º do RGPD, "categorias especiais de dados pessoais", que incluem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, dados genéticos, dados biométricos, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa).

Por outro lado, no que às sanções diz respeito, os limites máximos das coimas fixadas pelo RGPD de até 20 milhões de euros ou até 4% do volume de negócios anual a nível mundial, muito embora sejam, em abstrato, aplicáveis, sê-lo-ão, previsivelmente, apenas às violações mais graves de direitos dos titulares, sendo certo que esta é uma matéria que, com toda a certeza, será objeto de concretização através da legislação de cada estado membro.

(8)

Nomeação obrigatória de um representante na UE:

As empresas ou instituições não sediadas no território de um estado membro da UE, na situação descrita no número anterior, devem nomear um representante residente no território de um estado membro que atuará como ponto de contacto para os efeitos do RGPD.

O representante está obrigado à sua presença física no território da UE.

Em resumo, o RGPD aplica-se a empresas ou instituições sedeadas ou não no território da EU que, nas condições descritas, efetuem o tratamento de dados de residentes no território da UE, entendendo-se como tal o conjunto dos territórios pertencentes aos estados membros da UE.

(9)

Novos Instrumentos de Controlo dos Dados Pessoais:

Nos termos do RGPD, os cidadãos residentes na UE usufruem, adicionalmente a outros direitos que já provinham da legislação anterior, também do **direito ao esquecimento**, isto é, à eliminação compulsiva dos dados pessoais em poder das empresas ou instituições a quem tenha sido reconhecido o direito ao seu tratamento sempre que (i) os dados pessoais em questão tenham deixado de ser necessários ou (ii) tenha sido retirada a autorização ao tratamento concedida pelo titular dos dados quando aquela autorização tenha sido necessária ou, ainda, (iii) quando os dados pessoais tenham sido obtidos ilicitamente.

A este propósito, convém lembrar que o acórdão do Tribunal de Justiça da União Europeia, de 13 de maio de 2014, proferido no caso Google, entendeu que qualquer interessado pode exigir que sejam bloqueadas as fontes de que resultem informações obsoletas, incompletas, falsas ou irrelevantes e não sejam de interesse público.

Embora este acórdão tenha sido proferido no âmbito de legislação que será revogada ou alterada pelo RGPD, a doutrina que dele resulta continuará a servir de referência para a interpretação e aplicação do RGPD.

Um outro direito criado por este Regulamento denomina-se **direito à portabilidade**, que consiste no direito de um interessado titular de dados pessoais que tenham sido proporcionados a uma empresa ou instituição poder pedir a estas que efetuem a sua transmissão direta a outra empresa ou instituição igualmente responsável pelo tratamento de dados, sempre que:

- o seu tratamento tenha sido baseado no consentimento dado pelo titular dos dados a quem estes respeitem; e
- e quer o tratamento quer a sua transmissão sejam processados por meios automatizados.

O Grupo de Trabalho previsto no artigo 29 do RGPD[***] publicou as orientações finais a ter em conta na execução do direito à portabilidade, nos seguintes termos:

- no tratamento de dados deve ser dada importância às preocupações e aos valores tradicionais relativos à sua proteção, designadamente os que respeitam aos direitos pessoais sensíveis na ordem jurídica, económica e, bem assim, em relação ao meio utilizado na sua divulgação, evitando-se a concessão de preferência a conceitos e métodos não tradicionais e estereotipados que se revelam incompatíveis com a vulnerabilidade dos dados pessoais;
- alargamento da obrigatoriedade da observância do regime da portabilidade de dados aos responsáveis pelo tratamento de dados existentes em cada empresa ou instituição e, não apenas, como até

[***] Este Grupo de Trabalho emitirá, periodicamente, diretivas interpretativas do RGPD e sobre o modo como está a ser aplicado.

agora, aos administradores, gerentes ou diretores da gestão das empresas ou instituições;

- a legislação sobre a portabilidade dos dados em setores específicos tem aplicação preferente relativamente às normas sobre a matéria contidas no RGPD. A este propósito, deve recordar-se que o RGPD é um regulamento geral sobre a proteção de dados, facto que não exclui, assim, a existência de regulamentos específicos aplicáveis a certas áreas económicas ou institucionais que mereçam da parte do legislador comunitário um tratamento particular;
- os dados que estão sujeitos ao direito à portabilidade são aqueles que tenham sido fornecidos de modo ativo e consciente pelo titular dos dados, bem como os recolhidos pela entidade que os trata, a partir da utilização de um serviço ou em virtude de um ato de aquisição ou mera utilização de um produto.

  Não inclui, assim, os dados facultados pelo seu titular, enquanto possam significar distorção da concorrência no mercado.

(10)

Princípio da Responsabilidade Civil:

As empresas ou instituições detentoras de dados pessoais devem adotar medidas que assegurem o cumprimento de princípios, direitos e garantias que o RGPD estabelece ou visa proteger.

Rejeita, por isso, por completo o procedimento de empresas ou instituições detentoras de dados pessoais no sentido de apenas atuarem em caso de infração do RGPD e demais legislação aplicável à proteção de dados pessoais, uma vez que um procedimento retardado dessa natureza pode causar prejuízos de difícil reparação ou de difícil compensação.

Estabelecem-se, a propósito, uma série de medidas em vista da proteção do que se deixa dito, tais como:

- concessão da proteção de dados desde o momento do seu desenho ou configuração;
- proteção de dados por defeito;

- estabelecimento de medidas de segurança;
- manutenção de um registo de tratamentos de dados;
- realização de ações de avaliação de impactos sobre a proteção de dados
- nomeação de um encarregado de proteção de dados (EPD);
- obrigatoriedade de notificação, às autoridades competentes da proteção de dados, das violações ocorridas e a sua segurança futura;
- obrigatoriedade da notificação às autoridades competentes sobre a proteção de dados das violações à sua segurança;
- realização de ações de avaliação de impactos sobre a proteção de dados
- promoção de códigos de conduta e meios de certificação.

(11)

EPD – (Encarregado de Proteção de Dados):

a) **Quando é necessária a sua existência**?

Sem prejuízo de eventuais orientações a serem publicadas no âmbito nacional de cada estado membro, é necessária a sua existência:

- sempre que o tratamento de dados seja efetuado por uma autoridade pública;
- sempre que o tratamento de dados seja efetuado em grande escala ou requeira uma atenção particular ou, ainda, se trate de tratamento de dados sensíveis.

b) **Deve, ainda, ser tido em conta o seguinte**:

- um grupo empresarial pode ter apenas um EPD responsável por todo o grupo;
- o EPD deve ter conhecimentos especializados em direito e no domínio da proteção de dados;
- os dados resultantes da atividade do EPD devem ser publicados e comunicados à autoridade de controlo.

c) **O órgão de gestão da empresa ou instituição deve assegurar a participação do EPD** em todas as questões que tenham por objeto a proteção de dados.

Do mesmo modo, o órgão de gestão da empresa ou instituição deve apoiar o EPD no desempenho das suas funções, garantindo que ele não receba instruções de qualquer natureza durante o desempenho das suas funções.

Acresce, que os titulares dos dados, no exercício dos seus direitos, poderão contactar o EPD sobre quaisquer questões relativas aos dados pertinentes.

O EPD deve manter em segredo e sob confidencialidade os dados sob sua proteção.

O EPD não está impedido de exercer outras funções.

d) **As funções do EPD incluem**:

- a prestação de informação e o assessoramento na matéria da proteção de dados ao órgão de gestão da empresa ou da instituição;
- a supervisão do cumprimento das normas de proteção de dados, assim como das políticas do órgão de gestão da empresa ou instituição nos assuntos de proteção de dados;
- a distribuição de funções e responsabilidades ao pessoal sob a sua direção, bem como a sua formação técnica;
- a realização de auditorias aos serviços sob sua direção;
- a prestação de assessoramento às ações de Avaliação de Impacto;
- a cooperação com as autoridades de controlo da proteção de dados e, bem assim, a atuação como elemento de contacto.

(12)

<u>Avaliação de Impacto</u>:

a) Antes de ser efetuada qualquer ação de tratamento de dados que possa conduzir a uma situação de risco para os direitos dos interessados é

necessário realizar uma Avaliação de Impacto que tenha em conta o seguinte:

- que se trate de uma avaliação constante no tempo e completa sobre os aspetos pessoais dos titulares dos dados, incluindo a elaboração de perfis;
- que sejam tidas em conta, no caso de um tratamento em grande escala, categorizações especiais de dados;
- que seja tida em conta, quando aplicável, uma observação regular, a grande escala, de uma zona de interesse publico.

b) Efetuada a Avaliação de Impacto, deve concluir-se se o tratamento de dados em questão pode conduzir ou não à criação de uma situação de alto risco que, consequentemente, requeira uma consulta prévia à autoridade de controlo.

c) O Grupo de Trabalho previsto no artigo 29 do RGPD definirá as situações de alto risco:
- sempre que seja efetuada uma avaliação sistemática e extensiva de dados relativos a pessoas individuais;
- sempre que se processem, a grande escala, dados de caráter sensível segundo os critérios do RGPD;
- sempre que se monitorize uma área de acesso público, a grande escala, de um modo sistematizado.

(13)

Formas de Obtenção do Consentimento do Titular dos Dados Pessoais:

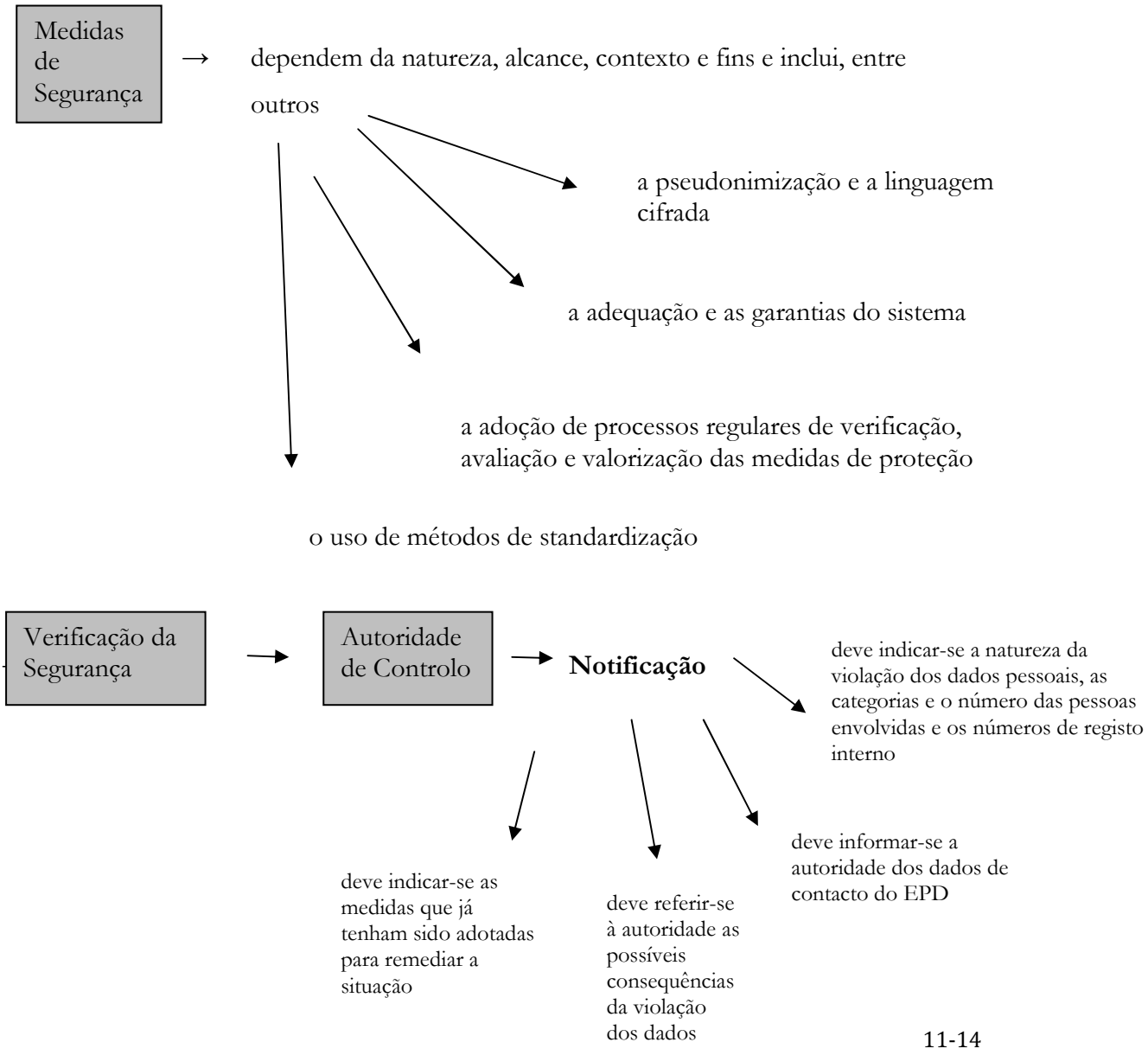
- de um modo geral, o consentimento do titular dos dados pessoais deve ser prestado de modo livre, informado, específico, explícito e inequívoco.

por "inequívoco" entende-se uma declaração expressa ou uma ação positiva que exprima o acordo do titular dos dados;

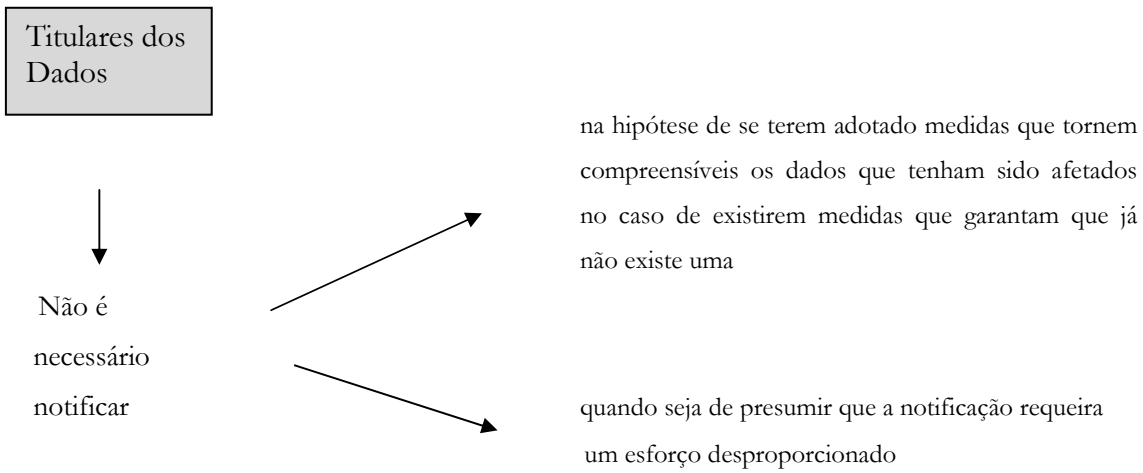
- as empresas devem examinar a forma como se obtém e regista o consentimento, já que as práticas que se baseiam no mero consentimento tácito deixam de ser aceites;
- exige-se o consentimento expresso para certos casos, como é o caso do tratamento de dados sensíveis;
- o consentimento deve ser verificável, de modo que se possa demonstrar que o titular dos dados concedeu um consentimento válido.

(14)

Segurança dos Dados Pessoais:

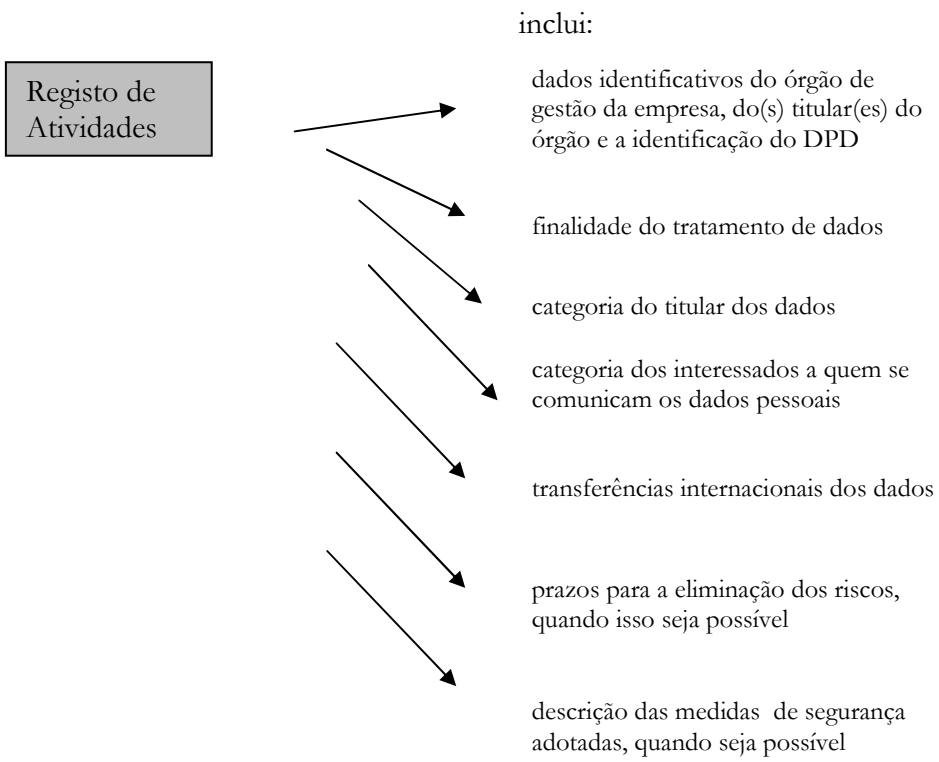


A notificação deve ser efetuada no prazo máximo de 72 h. ou para além deste prazo se se indicarem motivos justificativos da dilação daquele prazo.



(15)

<u>Registo de Atividades</u> *



* Não se aplica a empresas que tenham menos de 250 empregados, salvo quando a situação específica do tratamento de dados envolva riscos que não sejam meramente ocasionais ou abranja certas categorias especiais de dados.

(16)

<u>O Sistema de Janela Única</u>

- Prevê-se a constituição de uma autoridade de proteção de dados que possa estabelecer uma interlocução com autoridades congéneres nos diferentes estados membros da UE.
- As autoridades europeias de proteção de dados devem analisar, em cada caso, o caráter transfronteiriço do tratamento de dados, dando lugar a um procedimento de cooperação interestadual.
- Quando existam discrepâncias insolúveis, pode levar-se o caso ao Comité Europeu de Proteção de Dados, que resolverá a controvérsia mediante a tomada de decisões vinculativas.
- Os particulares poderão efetuar as suas reclamações ou denunciar à sua autoridade nacional, que informará os interessados sobre o resultado final.
- Este sistema não afetará as empresas que exerçam a sua atividade apenas dentro de um estado membro e sejam efetuados tratamentos de dados que respeitem apenas a titulares de dados residentes nesse mesmo estado.

Ver, igualmente, o anexo "Resumo do Regulamento Geral da Proteção de Dados Pessoais"

BARROCAS
ADVOGADOS

Barrocas Advogados
Amoreiras, Torre 2, 15º piso
1070-102 Lisboa
Telf: (351) 21 384 33 00
Manuel P. Barrocas
mpb@barrocas.pt
João Silva Pereira
jsp@barrocas.pt