MC&A
SOCIEDADE DE ADVOGADOS, RL

news

TABLE OF CONTENTS



LEGAL ALERT April 2017


**contactos/contacts:**

Pedro Gonçalves Paes

pgp@legalmca.com



www.legalmca.com

PORTUGAL

# Regulamento Europeu n.º 2016/679

Volvido que está quase 1 ano após a publicação (27 de Abril de 2016) do Regulamento Europeu n.º 2016/679, relativo à protecção do tratamento e circulação de dados pessoais, e este será aplicável às empresas portuguesas a partir de 25 de Maio de 2018.

Este Regulamento revogará a actual legislação relativa à protecção e circulação de dados, implementada pela Directiva 95/46/CE e pela Lei nº 67/98, acarretando mudanças significativas para os comportamentos a adoptar pelas empresas que realizem o tratamento de dados pessoais.

As principais medidas a tomar pelas empresas para preparar a aplicação do Regulamento Europeu de Protecção de Dados são as seguintes:

**1. Informações a fornecer aos titulares dos dados;**
O Regulamento obriga a prestar mais informações aos titulares dos dados do que a legislação em vigor. Neste sentido, todos os impressos, políticas de privacidade e textos em que se prestem informações aos titulares dos dados, devem ser reformulados. As reformulações a realizar deverão ter em conta que o Regulamento impõe que a prestação de informações seja realizada de forma concisa, inteligível e de fácil acesso.

**2. Categorias especiais de dados;**
Tal como acontece na legislação em vigor, apenas em casos previamente autorizados podem tratar-se dados considerados sensíveis. Contudo, a utilização de sistemas biométricos para controlar a assiduidade ou o acesso a locais restritos (v.g. de trabalhadores) terá que ter em conta a necessidade de autorização prévia por parte da Comissão Nacional de Proteção de Dados - CNPD.

**3. Obrigações relativas ao registo do tratamento de dados;**
Perante a nova legislação, as empresas ficam obrigadas a registar (documentar) por escrito e em formato electrónico, de forma detalhada, todas as operações de tratamento de dados. Esta medida é particularmente importante na preparação para a aplicação do Regulamento, dado permitir efectuar um levantamento das actividades internas da empresa em matéria de protecção de dados.

**4. Subcontratação;**
O Regulamento impõe a obrigação de subcontratar apenas com

Av. da Liberdade, 262-4 Esq.
1250-149 LISBOA

T 351 21 356 9930
F 351 21 356 9939

ANGOLA
R. Rainha Ginga, 187
Ed. Rainha Ginga, Piso Int.
LUANDA

T 244 222 338 358

MOZAMBIQUE
Av. Marginal, 4159
MAPUTO

T 258 829 035 529

*(in association)*



entidades que apresentem garantias de cumprimento da legislação relativa à protecção de dados, estipulando ainda o conteúdo obrigatório dos contratos. Neste sentido, todos os contratos de subcontratação em que uma empresa seja subcontratante ou subcontratada, devem ser revistos, passando a incluir o objecto e duração do tratamento de dados bem como o tipo de dados pessoais e de titulares.

**5. Segurança do tratamento de dados;**
Deverão adoptar-se medidas técnicas e organizativas adequadas e necessárias para assegurar e comprovar que o tratamento de dados é conforme ao Regulamento. Estas medidas deverão ter em conta o nível de segurança adequado a garantir a confidencialidade e integridade dos dados, a prevenir a destruição ou perda e alterações acidentais ou ilícitas, bem como a divulgação e acessos não consentidos de dados. O Regulamento prevê medidas técnicas e organizativas de segurança desejáveis a pseudonimização, cifragem e minimização de acesso a dados pessoais.

**6. Notificação de violações de dados pessoais;**
As violações de dados pessoais que consubstanciem riscos para os direitos dos titulares dos dados devem ser notificadas à CNPD, sem demora injustificada, no prazo de 72 horas após conhecimento da violação. Não obstante, todas as violações, ainda que não consubstanciem riscos, deverão ser registadas e documentadas.

Neste sentido, deverão adoptar-se procedimentos internos (e ao nível da subcontratação) que regulem os casos de violações de dados pessoais, promovendo medidas de detecção, identificação e investigação das violações, bem como medidas que mitiguem os riscos da sua ocorrência.
Em casos de subcontratação, o subcontratado deverá notificar o subcontratante de qualquer violação de dados, após o seu conhecimento, sem demoras injustificadas. Prevê-se, ainda, a obrigação de notificar o titular dos dados da violação, para os casos em que da violação de dados possa resultar um elevado risco para os direitos dos titulares dos dados.

**7. Direitos dos titulares dos dados;**
O Regulamento amplia os direitos dos titulares dos dados, criando novos direitos, de entre os quais se destacam o direito à limitação, ao apagamento e à portabilidade do tratamento dos dados. Os pedidos a realizar ao abrigo dos direitos mencionados devem obter resposta por parte empresa no prazo máximo de 1 mês.

Por conseguinte, é necessário rever os procedimentos internos de garantia do exercício destes direitos, tendo especial atenção ao prazo máximo de resposta, de forma a incluir os procedimentos relativos aos direitos criados pelo Regulamento.

**8. Consentimento dos titulares dos dados;**
O Regulamento impõe às empresas o dever de conseguir demonstrar, em qualquer altura, que o titular dos dados deu o seu consentimento para um determinado tratamento de dados.

Tal dever implica que as empresas avaliem se o consentimento é ou não obtido de forma livre e inequívoca.

Por outro lado, consagrando um direito a retirar o consentimento, o Regulamento impõe que as empresas adoptem procedimentos eficazes que permitam que o consentimento seja tão fácil de retirar como de obter.

**9. Protecção desde a concepção e por defeito;**
Tanto no momento da definição dos meios de tratamento de dados como no momento do tratamento em si, deverão aplicar-se as medidas técnicas e organizativas mais adequadas à proteção de dados, de forma a assegurar que, por defeito, só sejam tratados os dados pessoais necessários a uma finalidade específica de tratamento de dados.

Esta obrigação aplica-se à quantidade de dados recolhidos, extensão do seu tratamento, prazo de conservação e acessibilidade, assegurando que os dados não são **disponibilizados a um número indeterminado de pessoas.**

**10. Encarregado de protecção de dados;**
O Regulamento prevê ainda a designação de um encarregado de protecção de dados, responsável por prestar aconselhamento, cooperar com a CNPD e controlar a conformidade da actividade da empresa com a legislação relativa à protecção de dados.

Embora a designação deste encarregado seja obrigatória em apenas alguns casos, o Regulamento prevê a possibilidade de qualquer empresa designar um trabalhador para este fim, como forma de garantir a aplicação do regime legal.

## European Regulation nº 2016/679

European Regulation nº 2016/679 providing the processing and flow of personal data was published on 27 April 2016. Almost one year after its publication, it is expected that it shall be implemented by the Portuguese companies as from 25 May 2018.

This Regulation will repeal the existing legislation on the processing and flow of personal data implemented by Directive no. 95/46/EC and Law no. 67/98, and shall entail significant changes in the behaviors to be adopted by the companies carrying out the processing of personal data.
The main steps to be taken by the companies to preparing for the implementation of the European Data Protection Regulation are the following ones:

**1. Information to provide to the data holders;**
This Regulation obliges providing more information to the data holders than the legislation in force. In this respect, all forms, privacy policies and texts must be adjusted. The adjustments to be carried out should take into account the provisions imposed by the Regulation as regards the disclosed information, which should be accurate, intelligible and easily accessible.

**2. Special categories of personal data;**
As it is laid down in the existing legislation, this Regulation also establishes that the sensitive personal data can only be processed in

the situations previously authorised. However, the use of biometric systems to monitor attendance or access to restricted areas (e.g. the workers) should take into account the need for prior authorization by the CNPD - Comissão Nacional de Protecção de Dados (Portuguese Data Protection Authority).

**3. Requirements relating to data processing registration;**
Under the new legislation, the companies are required to document all detailed data processing operations, both in writing and electronic format. This measure is of particular relevance to prepare the implementation of the Regulation, as it will enable the companies to carry out the survey of their in-house activities related to data protection.

**4. Subcontracting;**
The Regulation enforces the obligation to only subcontract to entities providing guarantees of compliance with the data protection legislation and provides for the mandatory contents of the contracts. Therefore, all subcontracting agreements in which any of the parties is either a subcontractor or an outsourcer must be reviewed, in order to include the purpose and the duration of the data processing, as well as the type of personal data and respective holders.

**5. Data protection security;**
Appropriate and necessary technical and organizational measures should be taken to ensure and evidence that data processing complies with the Regulation. These measures shall take into account the adequate level of security to ensure the data confidentiality and integrity and to prevent the destruction or loss and contingent or illegal alterations, as well as the data disclosure and unauthorized access to it. The Regulation also provides the most technical and organizational security tools for the pseudonymization, encryption and minimization of access to personal data.

**6. Personal data breach notification;**
Any personal data breach evidencing eventual risks to the data holder's rights shall be, without undue delay, notified to CNPD, within 72 hours following the date when the breach is known. Notwithstanding, all breaches shall be recorded and documented, even those not evidencing any risks.

In this regard, the companies shall adopt in-house procedures to be also extended to the outsourcing area, to regulate any situations of personal data breaches, thus promoting the adequate measures to detect, identify and investigate the breaches, as well as the measures to minimize the risks of their occurrence.

In subcontracting situations, the outsourcer shall notify the subcontractor of any data breach, after being aware of it, without undue delay. The obligation to notify the data holder about the breach is also provided for in cases where from such breach a significant risk for the rights of the data holders can result.

**7. Data holders rights;**
This Regulation extends the rights of the data holders by providing new rights, namely the right to limit, the right to delete and the right to the portability of data processing. Any requests to be made under these new rights shall be answered by the company no later than one month from the date of the request.

It is therefore necessary to review the in-house procedures aiming to ensure the enforcement of those rights, namely in what concerns the maximum deadline for the response, so that the procedures concerning the new rights provided in this Regulation are included therein.

**8. Data holders' permission;**
The Regulation lays down the obligation for the company to prove, at any time, that the data holder has given its permission for a particular data processing.
Such obligation implies that the company assesses whether or not the permission has been freely and unambiguously given.

On the other hand, the Regulation, while providing the right to withdraw the permission, requires that the companies shall adopt effective procedures to make such permission as easy to withdraw as to obtain.

**9. Protection from design and by default;**
At the time either, data-processing facilities are defined or when the data processing is being handled, the most appropriate technical and organizational measures for data protection should be applied, in order to ensure that, by default, only personal data necessary for a specific data processing purpose are processed.

This requirement applies to the quantity of data collected, the extent of respective data processing and the registration and accessibility deadlines, thus ensuring that the data are not made available to any indeterminate number of persons.

**10. Data protection officer for data protection;**
The Regulation also provides for the appointment of a Data Protection Officer, who will be responsible for providing advice, cooperating with the CNPD and monitoring the compliance of the Company's activity with data protection legislation.

Although the appointment of such responsible is only mandatory in respect to a few cases, the Regulation provides the possibility for any company to appoint a worker for this purpose, in order to guarantee the applicable legislation.