ABREU & MARQUES
E ASSOCIADOS
SOCIEDADE DE ADVOGADOS, RL

PERSONAL DATA

THE NEW EU REGULATION ON PERSONAL DATA

FUNDAMENTAL ISSUES

The New EU Regulation number 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data shall apply in all member States from May 25, 2018.

This new Regulation addresses several fundamental issues as follows:

I) DATA SUBJECT'S RIGHTS

The Regulation lists the rights of the data subject whose personal data is being processed.

These strengthened rights give individuals more control over their personal data, including through:

- the need for the individual's clear consent to the processing of personal data;
- easier access by the subject to his or her personal data;
- the rights to rectification, to erasure and "to be forgotten";
- the right to object, including to the use of personal data for the purposes of "profiling";
- the right to data portability from one service provider to another.

It also foresees the obligation for controllers (those who are responsible for the processing of data) to provide transparent and easily accessible information to data subjects on the processing of their data.

The Regulation also foresees the conditions applicable to child's consent in relation to information society services.

II) COMPLIANCE

The Regulation details the general obligations of the controllers and of those processing the personal data on their behalf (processors).

These include the obligation to implement appropriate security measures, according to the risk involved in the data processing operations they perform (risk-based approach).

THE NEW EU REGULATION ON PERSONAL DATA
(CONTINUATION)

The Regulation foresees joint controllers as well as new principles and concepts like the data protection by design and by default and such as pseudonymisation in the processing of data.

III) RECORDS OF PROCESSING ACTIVITIES AND BREACHES

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. Save in specific cases, this is not applicable to companies with less than 250 employees.

Controllers are also required, in certain cases - namely when likely enrisking the rights and freedoms of natural persons - to provide notification of personal data breaches to the supervisory authority and, when the referred risk is high, to the data subject.

The processor must notify the controller without undue delay after becoming aware of a personal data breach.

IV) DATA PROTECTION IMPACT ASSESSMENT

The Regulation specifies that where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller shall consult the supervisory authority prior to processing.

V) DATA PROTECTION OFFICER

All public authorities and those companies that perform certain risky data processing operations will also need to appoint a data protection officer.

The controller, and, when applicable, the processor, must ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

The controller and processor shall support the data protection officer in performing the tasks listed in the Regulation by providing resources necessary to carry out those tasks and access to personal data and processing operations, as well as to maintain his or her expert knowledge.

The controller and processor shall also ensure that the data protection officer shall not receive any instructions regarding the exercise of those tasks (principle of independence). Such officer shall in no circumstance be dismissed or penalized by the controller or the processor for performing his tasks.

The data protection officer shall directly report to the highest management level of the controller or the processor.

VI) CODES OF CONDUCT AND CERTIFICATION

The Regulation foresees the creation of codes of conduct intended to contribute to the proper application of the same and the establishment of data protection certification mechanisms and of data protection seals and marks and certification bodies.

VII) MONITORING

The Regulation confirms the existing obligation for member states to establish an independent supervisory authority at the national level.

It also aims to establish mechanisms to create consistency in the application of data protection law across the EU. In particular, in important cross-border cases where several national supervisory authorities are involved, a single supervisory decision is taken.

This principle, known as the one stop shop, means that a company with subsidiaries in several member states will only have to deal with the data protection authority in the member state of its main establishment.

The Regulation includes the setting up of a European Data Protection Board. This board is to comprise representatives of all independent supervisory authorities.

VIII) REMEDIES, LIABILITY AND PENALTIES

The Regulation recognizes the right of data subjects to lodge complaints with a supervisory authority, as well as their right to judicial remedy, compensation and liability.

To ensure proximity for individuals in the decisions that affect them, data subjects will have the right to have a decision of their data protection authority reviewed by their national court. This is irrespective of the member state in which the data controller concerned is established.

The Regulation provides for very severe sanctions against controllers or processors who violate data protection rules. Data controllers can face fines of up to €20 million or 4% of their global annual turnover. These administrative sanctions will be imposed by the national data protection authorities.

THE NEW EU REGULATION ON PERSONAL DATA
(CONTINUATION)

IX) TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES

The Regulation also covers the transfer of personal data to third countries and international organizations.

To this end, Regulation puts the Commission in charge of assessing the level of protection given by a territory or processing sector in a third country. Where the Commission has not taken an adequacy decision on a territory or sector, transfer of personal data may still take place in particular cases or when there are appropriate safeguards (standard data protection clauses, binding corporate rules, contractual clauses).

July 5, 2016

Maria João Graça / Senior Associate Lawyer
maria.graca@amsa.pt

Abreu & Marques e Associados, Sociedade de Advogados, RL
Rua Filipe Folque, 2 - 4.º andar, 1069-121 Lisboa - Portugal
Tel: +(351) 213307100 – Fax: +(351) 213147491
E-mail: amsa@amsa.pt – Website: www.amsa.pt

In Angola:
Rua da Missão, nº 125 - R/C, Luanda
Tel: +(244) 222 331 187 – E-mail: angola@amsa.pt