THE EUROPEAN GENERAL DATA PROTECTION REGULATION

TOP SEVEN ACTIONS COMPANIES NEED TO TAKE

MACEDO VITORINO & ASSOCIADOS
Sociedade de Advogados, RL

FOREWORD

The General Data Protection Regulation ("GDPR") promises to be the most significant global development in data protection laws across all European Union ("EU") Member States since Directive 95/46/EC ("Data Protection Directive"), which was implemented in Portugal by Law 67/98, of 26 October 1998.

The GDPR will be directly applicable in all EU Member States from 25 May 2018. The new regulation will have a global scope, as businesses based outside the EU that offer goods or services to individuals in the EU may be required to comply with the GDPR.

The risk of fines up to 4% of annual worldwide turnover or €20 million is surely a strong incentive for companies to comply with the GDPR.

The new regulation is expected to be homogenously applied throughout the EU. Notwithstanding, Portuguese law will apply in cases it may impose more detailed conditions, such as those relating to the processing of sensitive data, particularly genetic data, biometric data or data concerning health. Portuguese law may also contain specific rules regarding the processing of employees' personal data, especially for the purposes of recruitment, performance and termination of the employment contract, which will apply together with the GDPR.

The combined application of the GDPR and the Portuguese law will be particularly relevant where companies collect and process data from Portuguese individuals and/or the Portuguese supervisory authority acts as lead authority due to the fact the main establishment or the single establishment of the controller or processor is located in Portugal.

Individuals, who are resident in Portugal, will have the right to lodge complaints with the Portuguese supervisory authority. For proceedings against a data controller or processor, the plaintiff will have the right to bring the action before the Portuguese courts if the data controller or processor's business or the individuals' residence is located in Portugal.

Although the core data protection rules remain broadly the same, there are important changes with impact on day-to-day business and for which companies should be aware of and prepare in advance.

As companies prepare for the entry into force of the GDPR, we propose a seven steps plan detailing the main aspects of the GDPR that companies need to take. This should be also used as an opportunity to improve the way the companies deal with personal data within their organization. The countdown to 2018 has started.

STEP 1. Map your data.

Make a personal data asset register to identify what personal data is held, where it came from, if you share personal information, who with, how and why.

Broadly speaking, a "personal data asset" is a set of personal data defined and managed as a single unit, for instance, a database of customers' contacts, employees' health data, etc.. Bear in mind that national laws, such as Portuguese law, may be more detailed on the definition of special categories of data (sensitive data).

The key is to initially map all your individual pieces of information and subsequently group them into recognizable and manageable portions and with similar risks concerning privacy and storage, considering:

- The type of data items being processed, including sensitive data;
- The purpose of the data processing;
- The duration of the data processing activity;
- The geographical scope of the processing activity.

Be sure you cover all personal data involving your business. To do this, consider auditing your data collection systems.

This is not necessarily a high-cost task, as it is likely that you have already resources within your organization that you may use to assist you with this.

You may ask each department and each country subsidiary where you are present to detail:

- The types of personal data, in particular if sensitive data is being used;
- How long they need to keep each data type;
- The purposes of the data;
- Where data is stored, etc..

You may also use documentation of previous data audits, technical register and management tools, software asset lists, etc.. This will allow you to know of any personal data you hold and how you should manage and protect it within your organization.

STEP 2. Review your privacy policy, procedures and documentation.

Confirm if existing consents remain valid and whether, in some cases, you may rely on other conditions.

Individuals' consent is one of the means that may justify personal data processing, but there could be other legitimate basis (e.g. the performance of a contract to which the individual is party or to take steps, at the individual's request, before entering into a contract).

Consent must be freely given, specific, informed and a clear affirmative action of the individual (written or oral statement). In case of sensitive data processing or personal data transferring outside the EU, the consent needs to be explicit. Silence, pre-ticked boxes or inactivity of the individual are not valid.

This will require you to take a proactive approach in your daily data management. If you rely on individuals' consent for processing their data, you should be able to prove that the consent has been given by the individual. This requirement could be particularly challenging to confirm in some cases.

Review your contracts with data processors. If you have considered yourself as a data processor to avoid being directly linked to data protection rules, consider reviewing your position.

The GDPR will apply directly to data processors, which will be subject to more detailed obligations and may be liable for compensation claims.

If you act as data controller (i.e. if you determine the purpose and means of processing), update your relevant master agreement to incorporate the new data processor wording and obligations required by the GDPR and check if you need to update the current contracts with data processors.

If you act as data processor (i.e. if you act under a data controller's instructions), consider the implications of becoming directly subject to the GDPR, including what liability you could bear, what liabilities should properly be passed to your customers and third parties and if your current terms need to be changed.

Ensure that you are able to prove you are compliant with the GDPR.

The GDPR requires you to create and maintain a record with your data processing activities if:

- You employ more than 250 persons;
- The data processing is likely to result in a risk to the individuals' rights;
- The data processing is not occasional; or
- If the processing includes sensitive data or data relating to criminal convictions and offences.

The records must be in writing and include detailed information on data processing activities, including your details and of the Data Protection Officer; the data processing purposes; types of data; data recipients; international data transfers; security measures.

You must cooperate with and provide your records to the national supervisory authority, if necessary. For this purpose, you should review national legislation governing national supervisory authorities, their powers and procedures.

Adapt your product development procedures to include a privacy impact assessment.

A privacy impact assessment is required if data processing operations are likely to result in a high risk to individuals.

Although there are a few guidelines on the concept of "high risk", processing could be considered high risk if it prevents individuals from exercising a right or using a service or a contract, or since it is carried out systematically on a large scale.

Review the decisions and papers published by the national supervisory authorities of the countries where you collect data to determine which activities can be considered of "high risk". Decisions of the Portuguese supervisory authority are published at its website: www.cnpd.pt.

A data protection impact assessment aims to assess the origin, nature, accuracy and severity of those risks and implement security measures to mitigate them, such as encryption, and ensure an appropriate level of security.

In case you cannot mitigate such high risks by implementing appropriate measures considering the technology now available and the costs of implementation, you should consult your supervisory authority prior to carrying out a personal data processing.

STEP 3. Consider the new rights of individuals.

Be sure you comply and/or can comply with individuals' "right to data portability".

The "right to data portability" improves the existing individuals' right to access their personal data upon an access request. This right will entitle the individual to ask for and receive his/her personal data, which he/she has provided to you (as data controller), in a structured, commonly used and machine-readable format.

The individual will be also entitled to transmit his/her data to another data controller for free and without hindrance from the data controller to whom the data was provided.

You may eventually need to implement technical tools, for instance a direct download opportunity to be used by individuals or to make available an application programming interface (API).

Individuals may also intend to use of a data store or a trusted third party, to hold and store the data and grant permission to controllers to access and process the data.

Be sure you comply and/or can comply with individuals' "right to be forgotten".

The "right to be forgotten" (or the "right to erasure") means that individuals are entitled to require the deletion or removal of their personal data and the refraining from further dissemination of such data, including data items available or processed by online means.

This right will be subject to certain exceptions, e.g. for compliance with a legal obligation or the performance of a task carried out in the public interest; for reasons of public interest in public health; for historical, statistical or research purposes.

Bear in mind that the GDPR requires you to comply with a one-month deadline following an individual's request.

You should consider changing or updating your procedures, including how you would provide data electronically and in a commonly used format or delete personal data upon the individuals' request.

STEP 4. Be sure that your personnel are fully aware of the implications of the GDPR and have training on the new data protection rules.

As a first step you need to asses if a Data Protection Officer ("DPO") is required and where this role would fit within your organization.

You may need:

- To create a job specification for the DPO's role; and/or
- To appoint a single DPO for the whole of your business; or
- To make individual appointments for each legal entity and/or jurisdiction.

The appointment of a DPO, where required, will apply to both data controllers and processors, depending on who fulfils the relevant criteria. Even if the controller fulfils the mandatory appointment criteria, the data processor is not necessarily required to appoint a DPO.

It may be useful to appoint a DPO even not legally required, as a DPO should allow you to centralize and focus on data protection issues and help the organization to comply with the GDPR in circumstances where your product development and sales department may not be aware of the importance of protecting individuals' personal data.

The GDPR requires a DPO in three specific cases:

- Where the processing is carried out by a public authority or body (except for courts);
- Where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of individuals on a large scale, such as providing telecommunications services, profiling and scoring customers' credit and insurance premiums; or
- Where the core activities of the controller or the processor consist of processing on a large scale of special categories of data (i.e. genetic data, biometric data, health data) or personal data relating to criminal convictions and offences, as would be the case of processing of patients' health data by a hospital.

This means that large companies collecting other personal data, such as the employees' payroll information or the customer preferences for a given product, would not be required to appoint a DPO, insofar as the collection of such data would not be considered as a core activity.

STEP 5. Adopt internal policies and measures which comply with the privacy "by design" and the privacy "by default" requirements.

"Privacy by design" includes the services and businesses which are based on the processing of personal data or carry out personal data processing to perform their activity and must consider the protection of personal data during the design phase to ensure that data controllers and data processors can comply with their data protection obligations.

These measures may include:

- Minimizing the processing of personal data;
- Pseudonymizing personal data;
- Adopting transparency rules;
- Creating and improving security features; and
- Enabling individual data subjects to monitor their personal data processing.

"Privacy by default" requires the data controller to implement appropriate technical and organizational measures to ensure that, by default, only personal data which are necessary for each specific purpose (including amount of personal data collected, the extent of their processing, their storage and accessibility period), are processed.

"Privacy by default" measures should ensure that, by default, personal data are not made accessible to an indefinite number of persons without the individual data subjects' interference.

The use of an approved certification mechanism could be an option to evidence compliance with the privacy "by design" and the privacy "by default" requirements.

However, the adoption of a certification mechanism may take some time and could prove to be time consuming and expensive. Companies should determine the appropriate measures to implement these requirements on a case by case basis.

STEP 6. Review and update your data security measures.

Review and update your data security measures.

The GDPR states the following security measures:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of the information technology systems;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

These security measures only apply "where appropriate", which means that they are not mandatory in all cases, which gives the company the right to opt for other measures. However, if no adequate measures are adopted, it will be difficult to justify a data breach due to a failure of the security system, increasing the likelihood that the defaulting company will be fined.

Implement technical and organizational measures and a breach notification procedure and improve your current incident management procedure.

In case of a data breach, the GDPR requires the following:

- You must provide a breach notification to the supervisory authority without undue delay and, where feasible, not later than 72 hours after you have become aware of it, unless you could prove that the data breach is unlikely to result in a risk to the individual's rights; and/or
- You must inform the individual without undue delay (in this case, there is no a specific deadline) where the data breach is likely to result in a high risk to the individual's rights and in close cooperation with the supervisory authority.

To ensure this, you should be prepared to: (i) determine whether all appropriate technological protection and organizational measures have been implemented to prevent the breach, (ii) establish immediately that a data breach has occurred and (iii) promptly inform the supervisory authority and the individual, if required.

STEP 7. Review the impact on data transfers outside the EU.

The GDPR preserves and improves the most current rules on this by prohibiting transfers of personal data outside the EEA (unless certain conditions are fulfilled).

The GDPR gives new options to justify international data transfers.

Under the "model contractual clauses", the authorization from the supervisory authority will no longer be required, although it is possible that some supervisory authorities may require to be notified. This option cannot be used by an EU-based processor, as they are not available "processor to processor" model clauses.

Binding corporate rules ("BCRs") are a set of binding obligations, under which a group of companies undertakes to carry out personal data processing in accordance with the GDPR. BCRs will be available to both data controllers and processors.

Codes of conduct or certification is a new justification adopted by the GDPR, which will allow international data transfers to inadequate jurisdictions provided the data importer has signed up to the appropriate codes of conduct or obtained appropriate certification.

"Whitelisted" jurisdictions are countries to which it is allowed to transfer personal data insofar as they have adequate data protection laws, *i.e.* data protection laws that are "essentially equivalent" to the GDPR. The adequacy findings must be reviewed every four years.

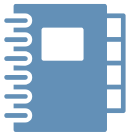
The Privacy Shield, which was adopted on 12 July 2016, replaced the US Safe Harbor scheme, which was repealed by the Court of Justice of the European Union in "Schrems" case.

Minor transfers exemption is allowed, but this will only take place in very limited situations and it will require to provide notification to the supervisory authority and inform the individual.

The individual's consent remains an option to allow a data transfer. However, it may be difficult to rely on the individual's consent, as the consent must be explicit and be given by a clear affirmative action providing a freely given, specific, informed and unambiguous indication of the individual's agreement to the data transfer outside the EEA.

YOUR “TO-DO” LIST

- Map all your data. Ask to each of your departments to detail on a spreadsheet the different types of personal data they use, how long they need to keep each data type and for which purposes.
- Organize a data audit with your HR, commercial, IT and legal teams to understand personal data you hold and how you may manage and protect them.



- Review your privacy policy (the so-called “how we use your information”) and individuals’ consents.
- Review contracts with data processors. If you are a data processor, consider what responsibility you can take and what could be passed to your customers and third parties.
- Review your procedures to confirm whether individuals are able to exercise their privacy rights, including the "right to data portability" and the "right to be forgotten".

- Consider appointing a single DPO or to make individual appointments for each legal entity and/or jurisdiction.
- Train your personnel on compliance matters, internal policies, etc.. Involve your legal team on these actions.

- Review and update your internal policies and technical measures with your IT team to fulfil the privacy “by design” and the privacy “by default” requirements.
- Review your security measures.
- Implement a data breach notification procedure and a procedure for testing the effectiveness of your technical and organizational measures on a periodical basis.

- Review your current international data transfers and understand if they will be justified under the GDPR.
- Consider adopting a key-solution with your legal team to obtain a wide-ranging justification for your international data transfers, e.g. model contractual clauses, binding corporate rules or an intragroup agreement, codes of conduct or certification.

ABOUT US

Our Data Protection Practice

ABOUT US

In today's competitive global market, Macedo Vitorino & Associados can provide a comprehensive commercial and corporate law advice to domestic and foreign clients. We have strong relationships with many of the leading international firms in Europe, the United States and Asia, which enable us to handle effectively any cross border legal matters.

Since the incorporation of the firm we have been involved in several high profile transactions in all of the firm's fields of practice, including banking and finance, capital markets, corporate and M&A, corporate restructurings etc..

We are mentioned by The European Legal 500 in most of its practice areas, including Banking and Finance, Capital Markets, Project Finance, Corporate and M&A, Tax, Telecoms and Litigation.

Our firm is also mentioned by IFLR 1000 in Project Finance, Corporate Finance and Mergers and Acquisitions and by Chambers and Partners in Banking and Finance, Corporate and M&A, TMT, Dispute Resolution and Restructuring and Insolvency.

We advise clients on all aspects of data protection, including:

- Preparing and filing notifications and applications for authorization with the Portuguese Data Protection Authority;
- Data compliance programs;
- Drafting and review privacy policies and notices for cross borders data use;
- Drafting and reviewing contracts and specific clauses relating to data protection matters, including IT contracts, outsourcing and data licensing;
- Dealing with cross border data transfers;
- Reviewing technological solutions, including cloud computing and geolocation;
- Regulatory data compliance in specific sectors, such as banking and finance, health, telecommunications and media, information technology, e-commerce.

If you are a client of Macedo Vitorino & Associados and wish to discuss any of the matters covered in this briefing, please contact:

Claudia Fernandes Martins

Email: cmartins@macedovitorino.com

Direct Line: (351) 21 324 19 08

Rua do Alecrim 26E | 1200-018 Lisboa | Portugal
Tel.: (351)21 324 19 00 | Fax: (351)21 324 19 29
www.macedovitorino.com