ELENA ARGYROPOULOU
& ASSOCIATES LLC
Advocates | Legal Consultants

April 2018

**The EU General Data Protection Regulation (GDPR) – Are you ready?**

The **EU General Data Protection Regulation (GDPR)** is evidently one of the most important developments in the area of data privacy regulation in the past 20 years and unlike a Directive it does not require any enabling legislation to be passed locally by the Member States, meaning that it will apply directly in all Member States.

After several years of preparation and following heavy debates, the GDPR was **finally approved** by the EU Parliament on **14 April 2016** with its enforcement date being the **25 May 2018**. Organizations which are not compliant by the fast approaching enforcement date, may face heavy fines.

The GDPR replaces the Data Protection Directive 95/46/EC and has been explicitly designed to harmonize data privacy laws across Europe, in order to protect and empower all EU citizens data privacy and to improve as much as possible the way organizations across the region approach data privacy.

No-one would question the fact that the protection of natural persons in relation to the processing of personal data is a fundamental right that everyone should respect and cherish.

The said development was inevitable taking into consideration the economic and social integration resulting from the functioning of the internal market that has led to a substantial increase in cross-border flows of personal data.

159, Leontiou Str. | Maryvonne Building
1st Floor | Office 103 | 3022 Limassol-Cyprus
Tel: +357 25349949 | Fax: +357 25349849
E-mail: info@argyropouloullc.com
Website: www.argyropouloullc.com

**Whom does GDPR affect?**

The arrival of the GDPR will have a wide-ranging impact on all organisations processing personally identifiable information whether such organisations are identified as "controllers"[1] or "processors"[2] of such information in the EU.

This is so:

A. where the activities relate to offering goods or services to EU citizens, irrespective of whether a payment from Data Subjects is required,

**OR**

B. where the activities of the organisation relate to monitoring of behaviour that takes place within the EU;

**AND**

I. irrespective of whether the processing takes place in the EU or not,
II. irrespective of whether the processor or controller is established in the EU,
III. irrespective of whether the processing operation is undertaken wholly or partly by automated or non-automated means, and
IV. irrespective of whether the processing operation is undertaken actively or passively (i.e. if the data is intended to be processed and used or if the data form part or is intended to form part of a filing (archiving) system).

In simple words, with the above into consideration, the GDPR applies when your business:

- ⇨ Collects and files personal data whether that is for its employees or for third party clients;
- ⇨ Maintains and operates a Website online;
- ⇨ Receives and processes personal data for marketing and communication purposes;
- ⇨ Exchanges and/or transmits personal data to other entities or parties (whether locally and/or across countries) for its employees or for third party clients;
- ⇨ Operates within a group structure in different countries worldwide.

[1] A controller is the entity that determines the purposes, conditions and means of the processing of personal data.
[2] A processor is an entity which processes personal data on behalf of the controller.

**What are the penalties for non-compliance?**

Failure to comply with the GDPR will be costly both in monetary terms but also from a reputational point of view. On breaching GDPR fines may be imposed on data controllers and data processors on a two-tier basis, as follows:

- Up to 2% of annual worldwide turnover (revenue) of the preceding financial year or 10 million Euro (whichever is the greater) for violations relating to internal record keeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default.
- Up to 4% of annual worldwide turnover (revenue) of the preceding financial year or 20 million Euro (whichever is the greater) for violations relating to breaches of the data protection principles, conditions for consent, Data Subjects' rights and international data transfers.

In order to respond to these changes in data protection regulation, organisations need to conduct a clear and comprehensive analysis of where they are now and their readiness for the GDPR.

**What constitutes *"Personal Data"* and *"Special Categories of Personal Data"*?**

***Personal Data*** is information related to a natural person or "**Data Subject**" that can be used to directly or indirectly identify that person. Such information can be anything from a name, a photo, an email address, bank details, and posts on social networking websites, medical information, or a computer IP address.

***Special Categories of Personal Data*** is personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms and include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**What are the Key Elements of GDPR and how should Organisations endeavor to address them?**

| Key concepts | What should Organisations be doing now? |
|---|---|
| **Greater harmonisation.**<br><br>The GDPR introduces a single legal framework that applies across all EU member states.<br><br>This means that Organisations will face a more consistent set of data protection compliance obligations from one EU member state to the other. | Organisations should, *inter alia,* start considering the manner in which they will verify the age of each Data Subject *(particularly where there is no relationship in person)* and obtain parental or guardian consent prior to engaging any services and put systems in place.<br><br>Member states will have some flexibility over decisions, for example, the age at which online service providers must verify that parental consent has been given before providing the service can be set at 13 to 16 years of age. In Cyprus that is likely to be set at the age of 14 however this proposal is still subject to final parliamentary approval. |
| **Expanded territorial scope.**<br><br>Non-EU Organisations (whether identified as data controllers or data processors) will be subject to the GDPR if they either:<br><br>(a) Offer goods or services to Data Subjects in the EU irrespective of whether payment is received.<br><br>(b) Monitor Data Subjects' behaviour that takes place within the EU. | Organisations established outside the EU should consider whether any of their entities are subject to the GDPR.<br><br>If so, such an Organisation should review the compliance obligations of its affected entities under the GDPR.<br><br>Non-EU Organisations processing Personal Data of EU citizens will also have to appoint a representative in the EU. |

| | |
|---|---|
| **Consent, as a legal basis for processing, will be harder to obtain.**<br><br>GDPR requires a very high standard of consent, which must be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to their personal data being processed, such as by a written, electronic or oral statement.<br><br>A Data Subject's explicit consent is still required to process special categories of personal data.<br><br>Organisations must be able to demonstrate that the Data Subject gave their consent to the processing and they will bear the burden of proof that consent was validly obtained.<br><br>When the processing has multiple purposes, the Data Subject should give their consent to each of the processing purposes.<br><br>The Data Subject shall have the right to withdraw their consent at any time.<br><br>The execution of a contract or the provision of a service cannot be conditional on consent to processing or use of data that is not necessary for the execution of the contract or the provision of the service.<br><br>Data controllers cannot rely on consent as a legal basis for processing if there is a "clear imbalance" between the parties (for example, the employer and employee relationship) as consent is presumed not to be freely given. | Organisations that rely on consent, as a legal basis for processing personal data, will need to carefully review their existing practices to ensure that any consent they obtain indicates affirmative agreement from the Data Subject.<br><br>Organisations must also consider how they will discharge the evidential burden of demonstrating that consent has been obtained.<br><br>Organisations must ensure that a natural person can withdraw their consent at any time. It must be as easy to withdraw consent as to give it.<br><br>Changes to consent mechanisms will require careful review, and may take time to implement. |

| | |
|---|---|
| **The risk-based approach to compliance.**<br><br>The GDPR adopts a risk-based approach to compliance, under which Organisations bear responsibility for assessing the degree of risk that their processing activities pose to data subjects. This can be seen in several of the provisions, for example, the new accountability principle and requirement for data controllers to maintain documentation, privacy by design and default, privacy impact assessments, data security requirements and the appointment of a data protection officer in certain circumstances.<br><br>**Low-risk processing activities may face a reduced compliance burden**. | As this may involve substantial changes to existing compliance strategies and arrangements Organisations should start their preparation now. Organisations should, *inter alia,*<br><br>⇨ Create awareness among the senior decision makers.<br><br>⇨ Audit and document the personal data they hold, recording where it came from and who it is shared with.<br><br>⇨ Review the legal basis for the various types of processing that they carry out and document this.<br><br>⇨ Review privacy notices and put in place a plan for making any changes to comply with the GDPR. |
| **The "one-stop shop".**<br><br>Where an Organisation has more than one establishment in the EU, the GDPR anticipates that they will have a main establishment, and work with the national supervisory authority for the main establishment where cross-border processing is involved ("**leading national supervisory authority**").<br><br>The leading national supervisory authority will be responsible for all regulation of cross-border processing activities carried out by that Organisation. It must work with all other "concerned national supervisory authorities". All concerned national supervisory authorities have a say in decisions on enforcement relating to cross-border processing activities. | For Organisations that only operate within a single EU member state, and only process the personal data of data subjects residing in that member state, interaction with the local national supervisory authority under the GDPR will be straightforward.<br><br>Multi-nationals and Organisations that operate in more than one EU member state will need to interact with a single national supervisory authority as their "lead authority". |

| | |
|---|---|
| If the concerned national supervisory authorities cannot agree on a decision, the matter is referred to the European Data Protection Board (EDPB), which has a range of powers to ensure the consistent application of the GDPR across the EU, including the power to make the final decision in enforcement cases. | |
| **Data Protection by design and by default, Privacy Impact Assessments, Prior Consultation and Standardised Icons.**<br><br>**Data Protection by design and by default**<br>Taking into account the state of the art and the cost of implementation and the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity of rights and freedoms of natural persons posed by the processing, Organisations will be required to implement appropriate technical and Organisations measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation and to integrate the necessary safeguards into the processing and to ensure that by default only personal data which are necessary for each specific purpose of the processing are processed.<br><br>**Privacy Impact Assessments (PIAs)**<br>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 the Data Subjects, the Oganisation shall need to carry out an assessment of the impact of the envisaged processing operations before it takes place. | In particular, the GDPR will require organisations to implement technical and organisational measures (such as pseudonymisation) to ensure that the requirements of the GDPR are met.<br><br>Organisations must:<br><br>➔ Take data protection requirements into account from the inception of any new technology, product or service that involves the processing of personal data, with an ongoing requirement to keep those measures up-to-date.<br><br>➔ Conduct data protection impact assessments where appropriate.<br><br>➔ Consult with the relevant national leading authority when necessary as per the provisions of the GDPR.<br><br>➔ Work on a codified system using pseudonymisation, minimisation or standardised icons to reduce the risk associated with a potential data breach. |

| | |
|---|---|
| In particular, PIAs will be required for:<br><br>➔ A systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the Data Subject or similarly significantly affect the Data Subject.<br><br>➔ Processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.<br><br>➔ A systematic monitoring of a publicly accessible area on a large scale.<br><br>The relevant leading national supervisory authority will establish and make public a list of the kind of processing operations that require a PIA.<br><br>**Prior Consultation**<br>In addition, where a PIA indicates that the processing would result in a high risk in the absence of measures taken by the Organisation to mitigate the risk, the Organisation must consult, the relevant leading national supervisory authority before any processing takes place.<br><br>**Standardised Icons**<br>In addition, information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable. | |

| | |
|---|---|
| **Strict data breach notification rules**<br><br>Under the GDPR, breach notification rules require Organisations to notify the national supervisory authority of all data breaches without undue delay after first becoming aware of the breach and particularly where a data breach is likely to "result in a risk for the rights and freedoms of individuals".<br>This must be done within 72 hours of first having become aware of the breach.<br><br>Organisations are furthermore required to notify the concerned Data Subject of the said data breach. | Organisations will need to develop and implement a data breach response plan (including designating specific roles and responsibilities, training employees, and preparing template notifications) enabling them to react promptly in the event of a data breach. |
| **Pseudonymisation**<br><br>The GDPR introduces the concept of "pseudonymisation" that is, the processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual, without the use of additional information, **provided** that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.<br><br>Pseudonymous data are still subject to the terms and provisions of the GDPR and treated as personal data, but are subject to **fewer restrictions on processing**, since evidently the risk of harm on the Data Subjects is lower. | Compliance with these guidelines is, subject to appropriate guidance by professionals, fairly straightforward for Organisations other than possibly those Organisations who need to process anonymous or pseudonymous data in multiple EU member states in different ways.<br><br>It is expected that EU-wide guidelines will be produced to address this matter in a more unifying way. |
| **The right to erasure ("right be forgotten")**<br><br>Data Subjects will have the **right to request that Organisations delete their personal data** cease further dissemination of the data, and potentially have third parties halt processing of the data. in certain circumstances (for | Organisations will need to devote additional time and resources to ensuring that these issues are appropriately addressed. |

| | |
|---|---|
| example, as outlined in article 17, if the data are no longer required for the purpose for which they were collected or the data subject withdraws their consent).<br><br>The above mentioned right does not mean to say that Organisations should neglect when in receipt of such requests to consider first and foremost the subjects' rights to "the public interest in the availability of the data". | In particular, Organisations should consider how they will give effect to the right to erasure (right to be forgotten), as deletion of personal data is not always straightforward and is subject to other legislation which may supersede the GDPR. |
| **The right to data portability**<br><br>Data subjects have **a new right to obtain a copy of their personal data from the data controller in a commonly used and machine-readable format** and have the right to transmit those data to another controller (for example, an online service provider). In exercising their right, the data subject can request the information be transmitted directly from one controller to another, where technically feasible. | Organisations that process large volumes of personal data (for example, social media businesses, insurance companies, banks) should consider how they will give effect to these rights. |
| **Data subject access requests**<br><br>Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from an Organisation confirmation as to whether or not personal data concerning them is being processed, where and for what purpose.<br><br>Organisations must reply within one month from the date of receipt of the request.<br><br>Further, the Organisation shall provide a copy of the personal data, free of charge, in an electronic format. | Organisations should plan how they will respond to data subject access requests within the new time scale and how they will provide the additional information required. |

**What is the role of a Data Protection Office (DPO) and when does your organisation need to appoint a DPO?**

Appointment of a DPO will be mandatory[3] for those organisations (a) whose core activities consist of processing operations which by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of Data Subjects on a large scale or (b) whose core activities consist of processing a large scale of special categories of data[4] and personal date relating to criminal convictions and offences[5] and (c) where the processing is carried out by a public authority or body, except of courts acting in their judicial capacity. The appointed DPO may be a staff member or an external service provider and must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices and the ability to fulfil the prescribed tasks[6]. Most importantly, the DPO shall be bound by secrecy and confidentiality concerning the performance of his or her tasks and must not carry out any other tasks that could results in a conflict of interests[7].

DPOs are deemed to have at least the following tasks:

(a) to inform and advise the organisation and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions;
(b) to monitor compliance with the GDPR, with other Union or Member State data protection provisions and with the policies of the organisation in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35 of the GDPR;
(d) to cooperate with the relevant supervisory authority;
(e) to act as the contact point for the relevant supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 of the GDPR, and to consult, where appropriate, with regard to any other matter.

[3] Article 37 of the GDPR
[4] Article 9 of the GDPR
[5] Article 10 of the GDPR
[6] Article 39 of the GDPR
[7] Article 38(6) of the GDPR

**What should your organisation do next?**

Questions that every organisation needs to address include:

- Does GDPR apply to me?

  If no, then there is absolutely nothing to be concerned about.

  If yes,

- What do I need to do to achieve compliance?
- Where are improvements required – policy, process, technology, training, risk management, forms, data collection?
- What are my priorities?
- Where do I start?

**How can we help you?**

Argyropoulou & Associates offers a wide range of privacy and data protection services locally and internationally, and can assist in:

- Performing a thorough review of existing policies, procedures, controls, privacy, security and/or identity theft prevention mechanisms maintained within an organization with a view to help build an integrated, global privacy compliance and risk framework.
- Examination of the controls adopted as to the manner of collecting and processing personal data.
- Advising in the event of improper disclosure and identity theft, breach notification, forensic investigation as well as the negotiation and ongoing compliance with the respective regulatory bodies.
- Building a privacy program business plan including applicable budgets and roadmap to help you implement and maintain it.
- Issuing of legal opinions on data protection and any related matters.
- Design and implement solutions to address key risks and areas of noncompliance; enhance data classification scheme and technical and physical security safeguards; implement appropriate global data flows.
- Drafting of agreements on Data Processing, Disclosure and Confidentiality.
- Offering advice on issues pertaining to processing of personal data by health organisations and/or insurance companies.
- Offering advice on issues pertaining to processing of personal data during employment.

***Disclaimer:*** *The information and material provided in this note are provided solely for general information purposes. None of the information and material provided herein should be relied upon and/or treated as professional or legal advice offered on a subject matter or situation and no person should act or refrain from acting on the basis of the information or material contained in this note without seeking to obtain explicit professional advice from an attorney or legal consultant. Elena Argyropoulou & Associates LLC will be glad to assist you further.*