

## How will national DPAs impose fines for GDPR violations?

---

The GDPR introduced an antitrust-type sanction regime with fines which, for severe infringements, may amount up to 20 million euros or 4% of the annual turnover, whichever is greater. The Working Party of Article 29 recently issued its much expected draft Guidelines for the consistent application of such fines. The intention of these Guidelines is to ensure that similar fines will be imposed by the national DPAs for similar cases, resulting in a uniform application of the GDPR throughout the EU (principle of equivalence).

The Guidelines constitute an elaboration on the assessment criteria set forth by the GDPR itself and should be applied on an *ad hoc* basis by the national DPAs. The most significant criteria are the following:

### **(a) The nature, gravity and duration of the infringement and the categories of personal data concerned**

The above should be assessed taking into consideration the number of the individuals affected (e.g. the number of registrants in a database, users of an application or customers etc.), the specified purpose of the processing and the use of the data in a compatible manner with that purpose, as well as the level of damages occurred. Whether the personal data affected are sensitive is of equal importance for assessing the severity of the breach.

### **(b) Intentional or negligent infringement**

Circumstances that are indicative of intention might be the unlawful processing authorised by the top management or in disregard of existing privacy policies known to the employees. On the other hand, failure to read and abide by existing policies, human error, failure to apply technical updates in a timely manner or failure to adopt (rather than simply failure to apply them) are indicators of a negligent behaviour.

### **(c) Responsibility of the controller/processor regarding technical and organisational measures**

Examples of what is practically assessed here is whether technical, organisational and security measures at all levels of the organisation have been taken, whether privacy policies are known and actually applied, whether best practice regimes are followed or whether organisations have adhered to approved codes of conduct and certification mechanisms.

**(d) Action to mitigate the damage suffered by the individuals**

Even when no such measures were taken, organisations that have admitted to their infringement and taken responsibility to correct or limit the impact of their actions might be treated with some flexibility.

**Recommendation**

In view of the entry into force of the GDPR and the draft Guidelines, there may be a significant shift of the approach to be adopted by the Hellenic DPA on the level of fines. By way of practical advice to organisations acting either as controllers or processors, the strengthening of their position at the current stage and prior to the occurrence of a GDPR infringement can be effected through a solid GDPR compliance exercise that should include:

1. Design and implementation of appropriate data protection policies and procedures;
2. Review and implementation of appropriate technical and organisational measures that would protect the personal data within their organisation and outside it (when data are processed by service providers); and
3. Training of employees and increase of their awareness to improve understanding of the GDPR and to ensure actual implementation of the relevant policies and procedures (ongoing task).

For advice on the GDPR compliance actions and other data protection issues, please contact:

**Takis Kakouris****Partner**

T (+30) 210 69 67 097

E t.kakouris@zeya.com

**Mary Deligianni****Senior Associate**

T (+30) 210 69 67 106

E m.deligianni@zeya.com

Established in 1893, Zepos & Yannopoulos is one of the leading and largest Law firms in Greece providing comprehensive legal and tax services to companies conducting business in Greece.

280, Kifissias Ave.  
152 32 Halandri  
Athens, Greece

newsletters@zeya.com  
Tel.: (+30) 210 69 67 000  
Fax: (+30) 210 69 94 640

[www.zeya.com](http://www.zeya.com)

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, or stored in any retrieval system of any nature without prior permission. Application for permission for other use of copyright material including permission to reproduce extracts in other published works shall be made to the publishers. Full acknowledgment of author, publisher and source must be given.

Nothing in this newsletter shall be construed as legal advice. The newsletter is necessarily generalised. Professional advice should therefore be sought before any action is undertaken based on this newsletter.