Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: Greece

by Popi Papantoniou and Valeria Kokkinou, Bahas, Gramatidis & Partners LLP, with Practical Law Data Privacy Advisor

Country Q&A | Law stated as of 14-Jun-2021 | European Union, Greece, International

A Q&A discussing obligations for private-sector data controllers in Greece to notify, register with, or obtain authorization from the data protection authority under Greece's comprehensive data protection law before processing personal data. It also discusses any requirements for data controllers to appoint a data protection officer (DPO) and any applicable notification or registration obligations relating to DPO appointments. This Q&A does not cover notification, registration, or authorization requirements for data processors or arising under sectoral laws. For an overview of the data protection law in Greece, see Country Q&A, Data Protection in Greece: Overview.

Data Protection Authority

1. What is the name and contact information of the country's data protection authority or supervisory authority responsible for data protection?

Name

Hellenic Data Protection Authority (HDPA)

DPA Contact Information

W: dpa.gr

English Home Page

E: contact@dpa.gr

Agency Contact Webpage

For a chart with key guidance from the HDPA, see GDPR Data Protection Authority Guidance Tracker by Country (EEA): Greece.

© 2021 Thomson Reuters. All rights reserved.

Notification or Registration

2. Does the country's comprehensive data protection law require private-sector data controllers to notify or register with the data protection authority before processing personal data?

In certain circumstances. The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Country Q&A, Data Protection in Greece: Overview: Question 1). Like the GDPR, Greece's Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) does not generally distinguish between different kinds of private and public sector controllers when it comes to notification or registration requirements. For the GDPR's requirements, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: EU: Question 2.

General Notification or Registration Requirements

The Data Protection Law does not require private-sector controllers to notify or register with the Hellenic Data Protection Authority (HDPA) when carrying out personal data processing activities. The GDPR requires prior consultation with or authorization from the HDPA in certain circumstances (Article 36, GDPR). For more on prior consultation requirements, see Prior Consultation Requirements; for more on prior authorization requirements, see Question 3.

Prior Consultation Requirements

Controllers must consult with the HDPA if a data protection impact assessment (DPIA) indicates that the processing would result in a high risk to natural persons' rights and freedoms if the controller fails to take measures to mitigate the risk (Article 36, GDPR). Controllers operating in Greece may submit the prior consultation request electronically (HDPA: Prior consultation with the HDPA).

The HDPA has released guidance and a non-exhaustive list data processing activities that require a DPIA, which complements the list from the guidelines that the European Data Protection Board endorsed from the Article 29 Working Party (Article 35(4), GDPR; see HDPA: Data protection impact assessment and Opinion 7/2018 on the draft list of the competent supervisory authority of Greece regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) (September 25, 2018)).

Cross-Border Data Transfers

Controllers must inform the HDPA when transferring data to non-adequate countries on the basis that the transfer is necessary for the controller's compelling legitimate interests (Article 49(1) and Recital 113, GDPR). This may occur, for example, when controllers cannot rely on GDPR Articles 45 to 47 as the basis for a cross-border transfer because, for example, there is no adequacy decision and none of the appropriate safeguards in GDPR Article 46 or other derogations in GDPR Article 49 are applicable. The Data Protection Law does not impose any additional notification or registration requirements for cross-border data transfers. For more on cross-border data transfers in Greece, see Country Q&A, Data Protection in Greece: Overview: Question 20.

© 2021 Thomson Reuters. All rights reserved.

Authorization

3. Does the country's comprehensive data protection law require private-sector data controllers to seek authorization from the data protection authority before processing personal data?

In certain circumstances. The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Country Q&A, Data Protection in Greece: Overview: Question 1). For more on the GDPR's general authorization requirements, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: EU: Question 3.

Prior Authorization Requirements

Greece's Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) does not impose requirements for controllers to obtain authorization from the Hellenic Data Protection Authority (HDPA) before processing personal data. Controllers may have obligations based on GDPR Article 36. For more information on prior consultation requirements, see Question 2.

Cross-Border Data Transfers

The Data Protection Law does not impose additional authorization requirements for cross-border data transfers. For the GDPR's cross-border authorization requirements, see Country Q&A, Data Protection in the EU: Overview: Question 20.

While the Data Protection Law does not provide any derogations, based on the GDPR, controllers must obtain prior authorization from the HDPA to transfer personal data to a non-European Economic Area (EEA) country without an adequacy decision when relying on:

- Contractual clauses that deviate from:
    - the European Commission's (EC) standard contractual clauses (SCCs); or
    - the standard clause that a supervisory authority has adopted and the EC has approved.
- Binding corporate rules (BCRs). The HDPA must approve an organization's BCRs before controllers may rely on them as a mechanism to provide adequate protection for non-EEA cross-border data transfers. However, once approved, controllers do not need to obtain the HDPA's authorization for each cross-border transfer that are subject to the BCRs.
- Codes of conduct. Associations and other similar bodies representing certain categories of controllers may prepare codes of conduct according to the requirements that GDPR Article 40 sets out. These require the HDPA's approval before:

© 2021 Thomson Reuters. All rights reserved.

- adoption; or
- amendment of existing documents.

(Articles 46(3)(a), (4), and 63, GDPR.)

To date, the HDPA has not adopted any standard data protection clauses for cross-border transfers under GDPR Article 46(2)(d). From June 27. 2021, controllers may use the new SCCs the EC has adopted as appropriate safeguards for cross-border transfers based on GDPR Article 46. For more information on the EC's implementing decision and annex with the new SCCs, see Legal update: archive, European Commission adopts final versions of standard contractual clauses under EU GDPR.

Controllers should regularly monitor guidance from the HDPA and the European Data Protection Board, as specific recommendations on responding to the July 16, 2020 decision from the EU Court of Justice (ECJ) on the validity of SCCs as a mechanism to provide adequate protection for transferred personal data may continue to evolve (Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Case C-311/18) EU:C:2020:559 (*Schrems II*); see Legal Update, Schrems II: controller to processor standard contractual clauses valid but EU-US Privacy Shield invalid (ECJ) and see Practice Note, EU Cross-Border Data Transfers: Regulatory Guidance Post Schrems II Tracker).

Data Protection Officers

4. Does the country's comprehensive data protection law require private-sector data controllers to appoint a data protection officer?

In certain circumstances. The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Country Q&A, Data Protection in Greece: Overview: Question 1). For the GDPR's requirements for appointing a data protection officer (DPO), see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: EU: Question 4.

Greece's Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) only requires public bodies to appoint a DPO (Article 6, Data Protection Law).

5. If the comprehensive data protection law requires private-sector data controllers to appoint a data protection officer (DPO), do data controllers have any obligations to notify or communicate the DPO's contact details to the data protection authority or register with the data protection authority?

© 2021 Thomson Reuters. All rights reserved.

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) applies directly in Greece (see Country Q&A, Data Protection in Greece: Overview: Question 1). For the GDPR's requirements on notifying the Hellenic Data Protection Authority (HDPA) about data protection officer (DPO) appointments, see Country Q&A, Data Protection Authority Registration and Data Protection Officer Requirements for Data Controllers: EU: Question 5.

While Greece's Law 4624/2019 on the Protection of Individuals Regarding Processing of Personal Data (Data Protection Law) provides guidance on the information public bodies must submit to the HDPA about their appointed DPOs, the law does not require private controllers to appoint a DPO or notify the HDPA of a DPO's contact information.

Public bodies may submit their DPOs' contact information electronically (HDPA: Notification of DPO designation to the Authority).

For the HDPA's contact information, see Question 1.

Contributor Profiles

Popi Papantoniou, Senior Associate

Bahas, Gramatidis & Partners LLP
T + 30 210 3318170

F + 30 210 3318171

E p.papantoniou@bahagram.com

W https://www.bahagram.com/attorneys/senior-associates/popi-papantoniou/

Professional qualifications. Greece, Attorney

Areas of practice. Civil law; commercial/corporate law and commercial litigation; data protection; and information technology law.

Valeria Kokkinou, Junior Associate

Bahas, Gramatidis & Partners LLP
T + 30 210 3318170

F + 30 210 3318171

E v.kokkinou@bahagram.com

© 2021 Thomson Reuters. All rights reserved.

W www.bahagram.com

Professional qualifications. Greece, Attorney

Areas of practice. Civil, commercial, and personal data protection law.

END OF DOCUMENT

© 2021 Thomson Reuters. All rights reserved.