OVERVIEW

Data Protection & Cybersecurity

LEARN MORE

READ OUR LATEST NEWS

Digital transformation has made compliance with data protection and cybersecurity regulations a key challenge to businesses worldwide.

Our firm's data protection and cybersecurity team is one of the longest established and highly specialised practices in Greece, offering top quality expertise to our clients -typically multinational companies- and practical solutions that make impact on their business.

Our long-term involvement has helped us develop in-depth legal capabilities and gain a true understanding of the technologies we encounter as part of our work. We consider that these features, combined with our holistic and business-friendly approach to clients, make our offering truly unique.

We have been involved in the most innovative and complex data protection projects that have taken place in the recent years, such as cloud computing, applications and software platforms used by individuals in the context of medical, insurance and other services, connected devices, implementation of biometric methods and identification technology, implementation of AI technologies, handling of cyber-attacks, assessment of legality of data analytics and processing of big data, implementation of monitoring mechanisms in the workplace that aim to prevent data breaches and disclosures of confidential information and profiling activities through automated systems.

Our work covers the usual regulatory compliance, GDPR audits, due diligence on data protection and privacy issues, privacy impact assessments, whistleblowing schemes and other privacy policies, data breaches, analytics, data processing agreements, cross-border data transfers, data security, data retention obligations, privacy training and data investigations and litigation.

Also, over the years, we have built a close, constructive and interactive relationship with the Hellenic Data Protection Authority and have contributed to the formation of the prevailing regulatory approach on several matters.

Clients in this practice include leading high-tech and telecom companies, pharmaceuticals, insurance and financial sector companies, commercial retailers, logistics and transportation companies, energy sector organisations, digital service providers, media companies, as well as education and non-profit organisations.

One-stop shop

Using our 40+ years' experience in this area, we advise leading multinational companies, many of which are heavily regulated, on data protection, privacy and information security, covering all angles (legal and IT) and all lines of service (counselling & compliance, DPO as a service, data breach management, DPIAs, litigation), delivering practical and implementable advice.

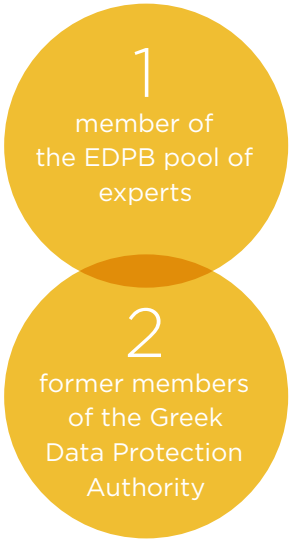
Our team of experts includes a member of the European Data Protection Board (EDPB) pool of experts for the fields of “Technical expertise in New Technologies and Information Security” and “Legal expertise in New Technologies”; also, two former members of the Greek Data Protection Authority, who have been involved in the development of the regulator’s case law in this critical area.

A holistic approach to compliance and security

- One of the largest teams of leading experts on data protection, privacy and cybersecurity in Greece.
- In-house IT and cybersecurity experts
- Strategic partnerships with cybersecurity and forensic companies
- International exposure and experience advising Fortune 500 clients on numerous cross-jurisdictional (EMEA) projects

Six lines of service

1. Regulatory advice
2. GDPR compliance audits
3. Data breach management
4. DPO as a Service
5. Data Protection Impact Assessment
6. Litigation



1. Regulatory advice

We provide compliance support to help our clients keep pace with the changing regulatory landscape in data protection and cybersecurity and minimise legal compliance risks in their day-to-day operations. Our team has the depth of resources to provide creative and practical advice on data protection and privacy matters faced by the organisations we support.

We advise a broad range of leading organisations **across numerous sectors**, including banking, insurance, IT, telecommunications, health, pharmaceuticals, retailers, logistics, automotive, marketing, energy, internet services and platforms, media, etc.

Our range of services includes:

/ data protection notices to data subjects and consent forms (customers, users of websites, etc.)

/ data protection and cybersecurity policies

/ HR data and privacy at work (notices to employees, device use policies, use of biometrics, use of AI technologies for hiring, employee monitoring, use of DLP tools, background and criminal checks, operation of CCTV systems, etc.)

/ data processing agreements

/ development of cross-border data transfer solutions (intra-group and with third parties)

/ e-privacy issues in the telecoms sector

/ health data (medical records, health tracking apps, clinical trials, medical devices, etc.)

/ electronic surveillance and law enforcement access

/ operation of websites and online shops

/ cookies and other tracking technologies

/ advertising and marketing (adtech, profiling, etc.)

/ data subject rights (DSR) management

/ data retention and data localisation

/ whistleblowing schemes and policies

/ trainings and seminars

/ legislative monitoring and assessment (including ePrivacy, NIS Directive, AI Act, AI Liability Directive, vertical industry specific legislation, etc.)

Advised Deutsche Telekom on various data protection issues (employee background checks, whistleblowing channel)

Advised a US cloud computing giant on data protection law issues related to security measures in data centres

2. GDPR compliance audits

Complying and demonstrating compliance with data protection and cybersecurity regulations is a significant and growing challenge for organisations. We carry out compliance and re-designing projects for our clients' GDPR-readiness in synergies with (inhouse and external) IT and cybersecurity experts.

GDPR compliance program

We have designed and we offer a holistic, end-to-end GDPR compliance program, which we fine tune and adapt to the industry and particular needs of the organisations we support, helping them (a) develop and maintain an appropriate framework for data processing across the entire data lifecycle and (b) demonstrate accountability for GDPR requirements.

Our legal and IT experts, working closely with stakeholders across your organisation, will:

- map the data processing activities
- map and review the IT and security infrastructure relating to the processing activities
- review existing policies and procedures governing data processing and security, data protection notices and consent forms and services agreement with service providers
- conduct a gap analysis to assess compliance levels against the GDPR, the ePrivacy law, other sector-specific Greek data protection legislation and the decisions and guidelines of the Hellenic Data Protection Authority
- prepare practical advice for compliance with the GDPR with recommended actions prioritised following a risk-based approach

Multi-jurisdictional projects

Our established relationships with international law firms and our participation to global networks of law firms enable us to undertake and manage large scale, multi-jurisdictional GDPR compliance projects.

We typically support Greece-based multinationals, covering all aspects of GDPR audit and compliance in the respective jurisdictions.

Support in M&A transactions

We help organisations understand and navigate data protection-related legal risks and obligations linked with M&A and project development projects. We work with our M&A and project development colleagues to perform data protection due diligence and include the necessary reps and warranties in the SPA and other transactional documents.

Technology M&A

Personal data protection issues are key considerations in M&A concerning technology companies, as such companies are inherently data-driven or data-related. Ensuring compliance with the applicable data protection legislation throughout the transaction process is critical, e.g. when the target company shares documents identifying individuals (customers, personnel, etc.) and, importantly, where a transaction involves the transfer of such documents outside the EU/EEA.

Dawn Raids

Our firm has extensive expert experience in dawn raid procedures from regulatory authorities. We prepare organisations to deal with dawn raids by the Hellenic Data Protection Authority and the Hellenic Authority for Communication Security and Privacy and we advise and support them during the entire process.

Before the dawn raid, we provide trainings to employees, and we prepare relevant internal policies. We also conduct mock exercises.

During the dawn raid, our team supports the organisation, so that their rights are protected throughout the procedure, importantly ensuring that the audit remains within the legal scope.

After the dawn raid, we advise on next steps, and we offer support on follow-up procedures with and enforcement by the supervisory authorities.

We offered our holistic (legal and IT), end-to-end GDPR compliance service to Navarino, and we supported L'Oréal for the needs of a global GDPR compliance audit. We also supported various due diligence projects

3. Data breach management

In a cyberattack or in the case of a personal data breach, the first 72 hours are critical, when informed decisions need to be made and immediate actions needs to be taken.

Our cybersecurity and data protection team can help you prepare for and respond decisively to any data breach incident (unauthorised access, data leakage, ransomware, etc.), offering immediate legal advice and assistance with breach notification procedures, also assistance with internal and external investigations, to mitigate compliance, liability and reputational risks.

Our established partnerships with IT (cybersecurity and forensics) experts, offer added value to our services, ensuring an affective and timely management of obligations and risks.

Data breach response planning

Organisations need to be able to detect, investigate, risk-assess, record and, when needed, report any data breaches. Having effective processes and policies in place is critical in order to comply with time sensitive regulatory requirements.

We support organisations in developing incident-response policies and crisis management strategies tailored to the specifics of their business and the regulatory requirements of their industry.

To ensure that our clients are fully prepared in the case of a cyber-attack, we provide training to executives and staff, so that they able to recognise security incidents and know how to escalate investigate, record and further manage personal data breaches.

Data breach management

We offer an end-to-end incident management service helping organisations comply with all relevant regulatory and contractual requirements:

- Assessment of the facts and advice on legal obligations and immediate actions
- Assistance with internal and external investigations
- Communication of the data breach to the individuals affected
- Notification to and interaction with supervisory authorities
- Management of contractual obligations towards clients and suppliers
- Preparation of recovery plans and support with implementation
- Assistance with follow on claims and litigation
- Assistance with post-event investigations and enforcement by supervisory authorities and challenging of administrative sanctions

Incident response service

In the event of a suspected or identified data incident you can reach our breach response team at databreach@zeya.com. We will advise you on and guide you through the steps to take to ensure compliance with regulatory obligations and mitigation of liability and reputational risks.

Assisted clients with the identification and investigation of security incidents, advised on legal obligations, also prepared and filed relevant notifications to competent authorities

4. DPO as a Service

As a strategic service line, we provide DPO as a Service in order to help our clients outsource the role of a Data Protection Officer (DPO) thus securing the desired GDPR compliance level.

Our team of legal and IT counsels, acting as DPO, is a key player in the data governance system and main instrument for promoting compliance within your organisation. We will play a key role in fostering a data protection culture within your organisation and will help to implement essential elements of the GDPR, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing, and notification and communication of data breaches. Our team will be acting as intermediary between data subjects and your organisation.

Importantly, part of our DPO service is monitoring of compliance with the GDPR, for the needs of which we (a) collect information to identify processing activities; (b) analyse and check the compliance of processing activities, and (c) inform, advise and issue recommendations to the organisation.

We will cooperate with the Hellenic Data Protection Authority and act as a contact point, to facilitate access by the supervisory authority to the documents and information for the performance of its tasks, as well as for the exercise of its investigative, corrective, authorisation, and advisory powers.

Our DPO team has all required skills and expertise, including:

- In-depth understanding of the GDPR and other data protection and privacy legislation and relevant vertical - industry specific rules
- Exposure to and understanding of the business and processing operations carried out by clients in a significantly broad range of sectors and industries.
- Understanding of information technologies and data security
- Ability to promote a data protection culture within organisations

"EU Representative" service

Our team can be designated as an EU Representative for non-EU companies doing business within the EU and being subject to the GDPR. We will act as a local point of contact for EU individuals and EU data protection supervisory authorities.

Offered DPO services to Cerved

5. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process that helps organisations identify and minimise the data protection risks of a processing activity, project, tool or offering. Organisations are obligated to carry out a DPIA for processing operations that is likely to result in a high risk to individuals. This includes:

- use of AI tools and technologies (e.g., for recruitment and evaluation of employees, credit risk assessment of business partners, consumer profiling, home appliances, etc.)
- use of CCTV systems
- implementation of whistleblowing reporting channels
- evaluation or scoring of individuals
- credit risk assessment of customers by financial sector institutions
- monitoring of employees' workstation, internet activity, etc.
- use of Internet of Things (IoT) technology devices
- gathering of public social media data for generating profiles
- processing of patients' genetic and health data by healthcare organisations
- use of smart technologies (including wearables)
- profiling for the purpose of promoting products and services
- processing of electronic communications data (content, metadata, location data)
- monitoring of drivers and passengers' behaviour using cameras in vehicles
- cloud migration and use of cloud computing services

We have undertaken DPIA projects for private and public sector organisations across numerous industries, including financial institutions, retailers and government agencies.

We have developed a **DPIA methodology** and templates, having built on methodologies suggested by various EU supervisory authorities, having also considered relevant guidelines and international risk assessment and risk management standards.

This allows the systematic description of the purposes of the processing and the processing operations and the assessment of their necessity and proportionality in relation to the purposes. We assess the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR.

We are able and we have the capacity to handle high volumes of DPIA work within tight deadlines, because of the size of our data protection and cybersecurity practice, strength of support services and rigorous quality controls.

Importantly, teams carrying out DPIAs include both, **legal** and **IT experts**, who work closely with internal and, as the case might be, external stakeholders, including consultation with the data subjects affected by the envisaged data processing.

Carried out a DPIA for "Zeus" Electronic Voting system, operated by GRNET (under the Ministry of Digital Governance) and used by public and private sector entities, organisations, institutions and bodies

6. Litigation

We advise and represent organisations across the full spectrum of data protection, cybersecurity and privacy-related complaints, claims and disputes, including from cases of alleged unlawful processing and GDPR violations through to claims for damages arising out of personal data breaches.

Our data protection team is supported by our dispute resolution experts, with decades of unparalleled experience, gained in courts at all levels of jurisdictions and particular expertise in cross-border litigation.

Depending on the characteristics of each data protection litigation case, we build a team of data protection and dispute resolution specialists, who work closely with you; when and to the extent needed, our inhouse or outside IT experts contribute to our work. Although with us you have numerous experts at your disposal, you only have to deal with one person in our firm – a dedicated contact who leads our team that conducts and manages your case.

Represented Cisco in two class actions filed by teachers and parents of school students, concerning the use of the Webex Meetings Platform for distance learning

For further information please contact

Theodore Konstantakopoulos
Partner | Head of TMT & Data

t.konstantakopoulos@zeya.com

Yolanda Antoniou-Rapti
Senior Associate

y.antoniou@zeya.com

Iliana Papantoni
Associate

i.papantoni@zeya.com

Vasileios Tzikas-Sotiriadis
Associate

v.tzikas@zeya.com

Data protection bulletin

In our monthly bulleting we bring you the latest and most important local developments in data protection and cyber-security; we also keep you up to date on EU legal news with impact on the local market.

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
Tel.: (+30) 210 69 67 000
Fax: (+30) 210 69 94 640

www.zeya.com
subscribe
LinkedIn