



Greece

George Ballas is senior and managing partner at Ballas, Pelecanos & Associates LPC. George heads the firm's IP, IT & CT practice group. He is a member of the Athens Bar Association, the International Bar Association and the International Trademark Association, an advocate before the Supreme Courts of Greece and a qualified European patent attorney. He read law at the Universities of Athens and Paris and was admitted to practice in Athens in 1972. In addition to heading the firm's litigation practice in complex pharmaceutical patents and anti-counterfeiting cases, he regularly advises clients in developing and managing strategic initiatives for optimising intellectual assets protection, exploitation and enforcement.

Theodore Konstantakopoulos is senior associate at Ballas, Pelecanos & Associates L.P.C. and member of the firm's IP, IT & CT Group. A graduate of the Athens University Law School (LLB), Theodore earned a Master of Laws degree (MLE) from Leibniz Universität, Hannover, Germany, following which he was awarded a second Master of Laws degree (LLM) from Queen Mary College, University of London in Computer and Communications Law. Theodore is a certified Data Protection Officer (DPO) (ISO/IEC 17024) and advises Fortune500 companies on all aspects of electronic communications, information technology, media, telecommunications and e-commerce law, with particular focus on data protection issues.

1 | What are the key features of the main laws and regulations governing digital transformation in your jurisdiction?

According to the European Commission (EC)'s Digital Economy and Society Index (DESI), even though Greece has one of the least advanced digital economies in the EU, during the past few years there has been remarkable progress in promoting investment in digital technologies and integration of digital technology by businesses and digital public services. The EC's Country Report Greece 2020 confirms that integration of digital technology by businesses in Greece is relatively slow, with the exception of the use of big data and electronic information sharing, which are higher than the EU average.

Greece has committed to advancing new digital technologies in line with the Digital Europe programme (The EU's programme to drive the digital transformation of Europe, covering supercomputing, artificial intelligence, cybersecurity, etc) and to investing strategically in digital technologies through EU coordinated programmes.

During the past few years, Greece has adopted legislation to support digital public administration; the Ministry for Digital Governance has a leading role in coordinating relevant government measures and in delivering several major information technology projects.

The legal framework currently in place covers, inter alia, digital governance (Law 4727/2020 and Law 4623/2019 on digital governance, also covering the accessibility of the websites and mobile applications of public sector bodies); access to public information (Law 4727/2020 on reuse of public sector information); electronic identification (eID) and Trust Services (eIDAS Regulation (EU) No 910/2014); security aspects related to digital governance (Law 4577/2018 on security of network and information systems, Greek National Cyber Security Strategy); eProcurement (Law 4601/2019 on electronic invoicing, Public Procurement Law 4412/2016); and e-commerce (Presidential Decree 131/2003).

The Greek government is currently working on its Digital Transformation Bible, which, among other things, will promote the digitisation of processes and the interoperability of information systems and will include a pipeline of IT investment projects for the entire public administration. Meanwhile, steps are being taken as regards flagship projects, which include the creation of a unified platform for electronic services; introducing digital identity cards for all citizens; developing the infrastructure on 5G networks; and increasing ultrafast broadband coverage.



- 2 | What are the most noteworthy recent developments affecting organisations' digital transformation plans and projects in your jurisdiction, including any government policy or regulatory initiatives?

The National Broadband Next Generation Access Plan (Access Plan) is the roadmap for the development and availability of modern broadband infrastructure throughout Greece and for the use by citizens and businesses of high-speed and ultra high-speed broadband services. The Access Plan generally aims at the creation of a favourable environment for private investment in next-generation networks, as well as at public support in areas with little or no interest from private players. In this context, the objectives of the Digital Agenda for Europe 2020 (one of seven flagship initiatives under the Europe 2020 strategy) have been set as minimum national targets for the deployment and service availability of high- and ultra high-speed broadband connections; namely, by the end of 2020, fast broadband (over 30 mbps) should be available to all citizens and at least 50 per cent of Greek households should have ultrafast broadband (over 100 mbps). The Access Plan is based on two main pillars: first, legislative and regulatory support (eg, Law 4463/2017 on measures to reduce

“Before implementing digital transformation, organisations need to prepare a cloud strategy tailored to their specific business needs and regulatory environment.”

the cost of deploying high-speed electronic communications networks, transposing EU Directive 2014/61); and second, government support initiatives and actions, e.g. coverage of geographic areas with low investment interest.

On 5 October 2020, the Microsoft Corporation announced its GR for Growth initiative, a plan to support government and businesses of all sizes in Greece with technology and resources. As part of the plan, Microsoft announced its intention to build new datacentres that will establish a Microsoft cloud region in Greece, which will offer access to low-latency, enterprise-grade cloud services; in this context, Microsoft also announced its plan to skill approximately 100,000 people in Greece in digital technologies by 2025.

Also announced recently is the beginning of the process for the establishment and operation of an ESA Business Incubation Centre (ESA BIC) in Greece, an initiative supported by the Ministry of Digital Governance (General Secretariat for Telecommunications and Posts) and the European Space Agency (ESA), aiming at the transformation of space-connected business ideas into commercial start-ups companies, via the ESA intellectual properties, space technologies and know-how transfers from space applications to everyday applications.

3 | **What are the key legal and practical factors that organisations should consider for a successful Cloud and data centre strategy?**

Before implementing digital transformation, organisations need to prepare a cloud strategy tailored to their specific business needs and regulatory environment. A critical element for the successful development of such strategy is the involvement and participation of all key departments and stakeholders from day one. The said stakeholders should include decision-making individuals in management, legal, procurement, finance and IT. This way, objectives and expectations are set on a more realistic basis, increasing the chances of a smooth transition to the cloud. A cloud strategy should define specific evaluation criteria, on the basis of which the organisation will be able to decide whether cloud migration has been successful and has offered anticipated business value.

Organisations are advised to ensure and verify that they outsource cloud services to providers who follow compliance guidelines, standards and regulations which apply to their respective industries, for instance, HIPAA, ISO 27000, PCI DSS, GDPR, etc.

Moreover, it is often the case that a cloud service provider has further outsourced part of its operations or infrastructure to third parties. Organisations need to have a complete understanding and evaluate the relationship of the cloud service provider with the said underlying providers. In compliance with data protection regulation,

where the cloud service provider (under its capacity as processor) engages another processor for carrying out specific processing activities on behalf of the organisation (controller), the same data protection obligations, as set out in the data processing agreement between the organisation and the cloud service provider, must be contractually imposed on that other processor..

Cloud service agreements often also offer providers the ability to unilaterally proceed with changes to the terms of the service agreement at any time with a specified level of advance notice. Organisations should consider developing and having in place an exit strategy, ie, a business plan to migrate workloads to alternate cloud providers, or back on-premise, in the event that a change in service terms is unacceptable.

From a practical, purely technological perspective, cloud migration may come with certain transformation challenges and risks, which organisations should be aware of and prepare for, especially organisations relying significantly on legacy systems or running legacy applications that will most likely need to go through a refactoring procedure and re-architecture and redesign the said applications, in order to adapt to the cloud environment and take full advantage of the cloud-based features and benefits (elasticity, flexibility, high availability, high resilience). Refactoring migration could be costly and time-consuming, but most importantly, it might entail risks, since this can be a complex exercise including application code changes, which could affect the functionality of the application.

4 | What contracting points, techniques and best practices should organisations be aware of when procuring digital transformation services at each level of the Cloud 'stack'? How have these evolved over the past five years and what is the direction of travel?

Before procuring digital transformation services, organisations need to evaluate whether and which specific cloud offerings can effectively satisfy each organisation's particular reliability, integrity, confidentiality, regulatory compliance and security requirements.

Relevant for all levels of the cloud stack is the issue of data protection and data localisation. Generally speaking, it is important that organisations make sure that, at all times, they retain full control and ownership over their data; in certain cases, where regulatory obligations apply, organisations should have the ability to choose the geographic locations (eg, specific data centres) in which to store their data.

In particular, government and public sector entities (due to their size and complex structures, and also due to the sensitivity and criticality of the data that they typically hold and process) should negotiate and agree on cloud service terms,



which offer access to cloud portability and interoperability tools and services; it is advisable that they also avoid strict, long-term contracts.

Organisations should look out for possible data preservation rules included in cloud service agreements. Upon termination of the agreement, providers may delete all data immediately or (more often) after a certain period of time.

Also relevant for all levels of the cloud stack is the issue of secure data deletion. From a data protection law perspective, it is important that cloud service providers are contractually obligated to offer a mechanism for effectively, reliably and permanently deleting an organisation's personal data upon the organisation's instruction to do so.

An issue particularly relevant for software as a service (SaaS) and platform as a service (PaaS) solutions is the possible lack of portability, namely the ability to move and suitably adapt data and applications between SaaS clouds and PaaS clouds, as this could take considerable effort to transform the data and applications from their form on the source system to the form required by the target system. Organisations are advised to consider cloud service providers who offer compliance with relevant

international standards, like ISO/IEC 19941:2017 which specifies cloud computing interoperability and portability types.

5 | In your experience, what are the typical points of contention in contract discussions and how are they best resolved?

A typical point of contention in cloud agreements is the contractual definition of service availability. Such service level obligation usually comes with a number of technical conditions, which organisations should carefully consider and analyse in order to choose a cloud solution that suits their business needs and importantly also covers their regulatory obligations. In this context, also relevant is the agreement on scheduled outages and force majeure events, which typically do not count as failure to perform. Organisations should, prior to entering into discussions, evaluate the frequency and duration of outages that they can tolerate without adversely impacting their business processes and their resiliency alternatives availability in the case of incidents involving a prolonged outage. Moreover, the agreed level of cloud service availability and offered capabilities for disaster recovery should be addressed in the organisation's contingency and business continuity plan, in order to ensure recovery and restoration of disrupted cloud operations via alternative services, equipment and locations, as needed.

Service availability expectations are often balanced with remedies offered by cloud service providers for failure to perform. Such remedies are usually contractually limited and capped.

In compliance with data protection legislation, organisations should negotiate and agree on a right to audit the cloud environment. The said right needs to be contractually defined in detail, in order to allow for effective audit of the cloud service provider's practices and compliance with the cloud service agreement and the law. Service providers will often try to restrict the right to audit and suggest alternatives, like self-evaluation reports.

Obviously, the smaller the size of the organisation the less flexible cloud service providers can be in contract discussions. With the notable exception of government procurement cases, for most organisations cloud service agreements are usually non-negotiable.

6 | How do your jurisdiction's cybersecurity laws affect organisations on their digital transformation journey?

Use of cloud services extends an organisation's IT footprint, which, theoretically at least, increases the risk of cyberattacks. This calls for the implementation of

“The agreed level of cloud service availability and offered capabilities for disaster recovery should be addressed in the organisation’s contingency and business continuity plan.”



technical and organisational measures which can adequately manage such risks and ensure regulatory compliance, importantly, with Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)). Organisations procuring cloud services should understand that transfer of certain (security) risk management responsibilities to cloud service providers does not limit their liability in case of security incidents, as organisations remain primarily accountable for regulatory compliance and possible damage caused to third parties, eg, to their customers.

That said, when organisations discuss cloud service agreements, special attention needs to be placed on recovery time objectives (RTOs) and the contractually agreed disaster-recovery provisions and processes, as this would significantly affect an organisation's ability to apply its business continuity plan.

Greece has developed and implemented a National Strategy on Cybersecurity and has also transposed the NIS Directive (EU) 2016/1148 in the Greek legal system (Law 4577/2018). Law 4577/2018 has introduced measures with a view to achieving a high level of security of network and information systems and applies to operators of essential services (eg, entities in the energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, and digital


infrastructure sectors) and to Digital Service Providers (online marketplaces, online search engines, and cloud computing services).

7 | How do your jurisdiction's data protection laws affect organisations as they undergo digital transformation?

Digital transformation is substantially affected by applicable data protection laws in Greece, most importantly the GDPR. Certain GDPR provisions (eg, on security of processing, on the use of data processors, transfers of personal data to third countries, etc.) directly affect the relationship between organisations and digital transformation service providers.

According to the GDPR accountability principle, an organisation (under the capacity of controller) is responsible for, and must, at all times, be able to demonstrate compliance with the GDPR principles relating to processing of personal data (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality). Compliance with the accountability principle can be a challenging exercise when processing of the data is outsourced to third-party data processors (like cloud service providers). The general principle is that where processing is to be carried out on behalf of a controller (as could be the case of procuring cloud services), the controller must use only processors (cloud service providers) providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the GDPR requirements. Contents of the data processing agreement between the organisation and the cloud service provider is specifically regulated by the GDPR. In practice, challenging can often be the exercise of the organisation's right (and obligation) to audit the cloud service provider's compliance with the GDPR and the data processing agreement.

GDPR provisions on data transfers to third countries and industry specific legislation imposing data localisation rules, can also affect and determine the choice of cloud service provider. In principle, a transfer of personal data to a third country may take place where the European Commission (EC) has adopted an adequacy decision or, in the absence of a decision, if the transfer is subject to the safeguards of Article 46 of the GDPR, eg, Standard Contractual Clauses (SCC) adopted by the EC. Notably, the recent *Schrems II* landmark judgment delivered by the Court of Justice of the EU (CJEU) (Case C-311/18) had a significant impact on data transfers to third countries, including to the US, where major cloud service providers are located. *Schrems II* essentially declared the EU-US Privacy Shield invalid and, most importantly, questioned and put into perspective the extent to which EU-based organisations can still rely on the SCC for data processing outsourced to certain



“Industry-specific regulation can impose an obligation for organisations to retain and store certain data locally.”

providers in the US and globally. The CJEU found that, before a transfer of data may occur, there must be a prior assessment of the context of each individual transfer, that evaluates the laws of the country where the recipient is based, the nature of the data to be transferred, the privacy risks to such data, and any additional safeguards adopted by the parties to ensure that the data will receive adequate protection, as defined under EU Law. Further, the data importer is required to inform the data exporter of any inability to comply with the standard data protection clauses. If such protection is lacking, the parties are obligated to suspend the transfer, or terminate the contract. While the SCC remain valid, their continued validity is subject to an additional step: the obligation to conduct the equivalent of a data protection impact assessment to ensure that the adequate protection is and will be provided and, subsequently, continuously monitored.

Moreover, industry-specific regulation can impose an obligation for organisations to retain and store certain data locally. For instance, there is typically an obligation for telecom providers (‘providers of publicly available electronic communication services or of public communication networks’) to carry out in-country data retention (‘in physical media which are located exclusively in Greece’) of traffic data

and location data and the related data necessary to identify the user (Law 3917/2011 transposing Data Retention Directive 2006/24/EC). However, in the light of the CJEU judgment invalidating the EU Data Retention Directive (Cases C-293/12 and C-594/12) and also considering very recent CJEU judgments, delivered on 6 October 2020 (Cases C-623/17, C-511/18, C-512/18, C-520/18), the validity and enforceability of the Law 3917/2011 is questionable, although it is still technically in force.

8 | What do organisations in your jurisdiction need to do from a legal standpoint to move software development from (traditional) waterfall through Agile (continuous improvement) to DevOps (continuous delivery)?

DevOps generally aims at the development and delivery of software code, applications and services more efficiently and at high velocity via corporate culture, practices and tools, which invest on and improve close collaboration between software development and operations teams. Commercially available DevOps solutions increasingly tend to be cloud-based.

In cases where an organisation outsources DevOps implementation, from a legal standpoint, challenging can be the contractual definition of deliverables, in other words, what is the progress and what are the operational improvements that an organisation should expect, in which time frame and, most importantly, how deliverables will be measured (eg, how can cultural shift be measured?).

Moreover, ensuring data and application security into DevOps (at every stage of the DevOps implementation, starting with the planning and design phases) must be a priority for organisations (DevSecOps). DevSecOps offers continuous risk management and importantly promotes data protection and data security awareness in the organisation. This continuous testing and monitoring has a positive impact on delivered applications, which tend to be more secure and compliant, allowing for security flaws and generally regulatory risks to be identified and dealt with early in the design, development and delivery pipeline.

9 | What constitutes effective governance and best practice for digital transformation in your jurisdiction?

Digital transformation projects must be based on a well-prepared digital transformation strategy, which should be aligned with the organisation's overall business strategy (taking into account risk management, governance and legal requirements) and which should be supported by a financial analysis justifying the investment.

Organisations should be aware that digital transformation, in most cases, will require a shift in corporate culture and management attitudes; inevitably, organisations become less self-reliant and more dependent on third-party providers of scalable and flexible (and often more cost efficient) services. This transformation and the increasing dependence from third-party cloud service providers comes with certain inherent risks, mostly in the area of security and protection of personal data.

It is important that the organisation's digital transformation strategy is frequently reviewed and, as or if needed, adjusted, so that the rapidly changing technological environment and evolving business objectives are taken into account.

Last but not least, missing digital skills can be a significant barrier to digital transformation. Organisations are advised to invest on trainings and knowledge management initiatives, which will help personnel develop and expand their digital skills and will enable the organisation to enjoy the maximum benefit of digital transformation.

George Ballas

george.ballas@balpel.gr

Theodore Konstantakopoulos

theodore.konstantakopoulos@balpel.gr

Ballas, Pelecanos & Associates L.P.C.

Athens

www.ballas-pelecanos.com

The Inside Track

What aspects of and trends in digital transformation do you find most interesting and why?

Digital transformation technology enables and supports the development of new business models and services delivered based on the three foundational cloud services: SaaS, PaaS and IaaS. For instance, business process as a service (BPaaS) is a form of business process outsourcing, which sits on top of SaaS, PaaS, and IaaS. BPaaS, making use of its cloud foundation, can scale ondemand to accommodate changes in business process needs.

What challenges have you faced as a practitioner in this area and how have you navigated them?

Effective digital transformation primarily requires a shift in business mentality, and the development of certain digital skills. Legal counsel advising in digital transformation projects with high operational impact often need to play a balancing role when having to handle employee pushback and the clash of conflicting business expectations within the organisation. When digitising operational processes and methods, organisations often find it difficult to step out of their 'corporate comfort zone' and deal with new procedures and changed routines. Legal counsels need to provide the stability, confidence and the assurances from a legal perspective, that will enable the organisation to have a successful digital transformation with optimal long-term business benefits.

What do you see as the essential qualities and skill sets of an adviser in this area?

Advisers in this area must have a solid understanding of the technical aspects of digital transformation technologies and the applicable regulatory framework.

Over the past 40 years, Ballas, Pelecanos & Associates LPC has developed and maintained a strong reputation as a leading technology law firm, regularly advising multinational IT clients that are at the frontline of technological innovation. We have equally long experience in the field of general technological developments, due to our specialisation and continuous engagement with issues of inventions and demanding litigation over them.