G.C.Hadjikyprianou
& Associates LLC
ADVOCATES & LEGAL CONSULTANTS

Digital Transformation in the EU:
Recent Developments and Legal Concerns

G.C.Hadjikyprianou
& Associates LLC
ADVOCATES & LEGAL CONSULTANTS

Digital Transformation in the EU: Recent Developments and Legal Concerns

New revolutionary technologies are disrupting traditional business models and transforming organizations at an ever-increasing pace. At the same time, the increasing fast pace of digital innovation is creating new legal challenges and commercial implications requiring new legal policies and innovative structures in many areas and industries. There is thus no doubt that related socio-economic, legal and ethical impacts of newly emerged technologies have to be carefully addressed and a balance must be drawn between, on the one hand, the rights of every individual and on the other, the plethora benefits those technological advancements can offer.

In this publication, G.C.Hadjikyprianou & Associates LLC comments on the recent developments in relation to the Union's digital transformation agenda and on the related legal concerns.

Contents

I. EU Digital Transformation: A Long-Distance Race

Since the early days of 2020, the European Commission has published a number of papers in relation to the Union's digital strategy and priorities (ref, inter alia to: "Shaping Europe's Digital Future paper"; "European Data Strategy paper"; and the White Paper on Artificial Intelligence"). The ultimate goal is for the EU to achieve what is called *"tech sovereignty"* i.e. to be self-sufficient in its digital infrastructure and capabilities for the benefit of its economy and citizens, while welcoming global providers of digital products and services as long as they adhere to EU values and regulations.

The three main pillars/objectives of the EU Digital Transformation Strategy as categorised by the Commission are:

- "Tech for the People"
- "Fair and Competitive Digital Economy"; and
- "Sustainable Society".

A. Tech for the People

In recognition of the plethora benefits of an intra-Union digital transformation, the first of the three main objectives emphasises the need to invest in connectivity infrastructure (including gigabit connectivity and 5G networks) and in emerging technologies such as Blockchain and Artificial Intelligence. Besides, the promotion of a single cybersecurity market and the investment in digital skills in the workforce are also a priority. Within this context, the Commission reiterates the need that technology should be trustworthy and to this effect expert panels have been formed in order to review and amend existing EU legislations as well as to develop new legislative provisions taking into account the plethora complex related legal issues (e.g. liability of AI tools and data protection in a blockchain related transaction).

The ultimate aim here is the "[*d]evelopment, deployment and uptake of technology that makes a real difference to people's daily lives. A strong and competitive economy that masters and shapes technology in a way that respects European values*".

B. Fair and Competitive Digital Economy

A significant part of the Commission's objective to ensure a fair and competitive economy revolves around the importance of data as a "key factor of production". The Commission plans to grow the single market for data. The emphasis will not simply be on the flow of data, but on the wide availability of data, which should be easy to access, use and process.

Proposals are expected in the autumn on digital finance, including a fintech action plan, legislation around cryptoassets, and legislation to boost "operational and cyber resilience" in the financial sector.

The goal is to develop a "*frictionless single market, where companies of all sizes and in any sector can compete on equal terms, and can develop, market and use digital technologies, products and services at a scale that boosts their productivity and global competitiveness, and consumers can be confident that their rights are respected*".

C. Sustainable Society

The final pillar is to ensure that EU values and ethical rules also apply in the online digital sphere, as they would offline. In an updated and improved regulatory framework, the Commission aims to provide online platforms with legal clarity and certainty, so they can act responsibly against illicit and illegal content, while also protecting the freedom of expression. Besides, the Commission plans to integrate environmental policies with its digital strategy, including initiatives to achieve climate-neutral, energy-efficient and sustainable data centres in the EU, and to support a circular economy for information and communications technology equipment, ensuring that products are designed for durability, maintenance, dismantling, reuse and recycling, and avoiding premature obsolescence. It also plans to develop a digital model of the earth itself to support environmental forecasting and crisis management.

As the EU Commission eloquently put it: *"A trustworthy environment in which citizens are empowered in how they act and interact, and of the data they provide both online and offline. A European way to digital transformation which enhances our democratic values, respects our fundamental rights, and contributes to a sustainable, climate-neutral and resource-efficient economy*".

II. Upcoming EU 'Digital' Legislations

New revolutionary technologies are disrupting traditional business models and transforming organizations at an ever-increasing pace. At the same time, the increasing fast pace of digital innovation is creating new legal challenges and commercial implications requiring new legal policies and innovative structures in many areas and industries. There is thus no doubt that related socio-economic, legal and ethical impacts of newly emerged technologies have to be carefully addressed and a balance must be drawn between, on the one hand, the rights of every individual and on the other, the plethora benefits those technological advancements can offer.

With that said, now, more than ever before, it is time to look towards the future, to the laws that will be required to facilitate the operation of our societies which are under a digital transformation. We hereunder provide a chronological timeline of upcoming digital laws and legislative amendments which can be expected to come into effect in the very near future.

A: Evagorou 31, Evagoras Tower, Office 32, 1066 Nicosia, Cyprus | Valaoritou street 7, Kolonaki, Athens 10671, Greece.
T: +357 22760727 / +357 22760726 E: gch@hadjikyprianoulaw.com W: www.hadjikyprianoulaw.com

Legislative developments expected at the end of 2020:

1. **Network and Information Security Directive**

   As a result of the numerous cyberattacks, inter alia, in hospitals; hotels and universities across the Union, the EU Commission has entered into a long consultation process to amend the existing regulatory landscape and/or introduce new measures targeting a higher level of protection. Towards this goal, the EU Commission set out a new EU Security Union Strategy for the period 2020 to 2025, focusing on priority areas where the EU can bring value to support Member States in fostering security for all those living in Europe. From combatting terrorism and organised crime, to preventing and detecting hybrid threats and increasing the resilience of EU critical infrastructure, to promoting cybersecurity and fostering research and innovation, the strategy lays out the tools and measures to be developed over the next 5 years to ensure security in both the physical and digital environment. In concrete terms, by the end of this year, one can expect added measures on Critical Infrastructure Protection, as well as a review of the NIS Directive which may lead to a widened scope of operators of essential services, as defined therein.

2. **5G**

   5G will play a key role in the future development of Europe's digital economy and society. It will be a major enabler for future digital services in core areas of citizens' lives and an important basis for the digital and green transformations. With worldwide 5G revenues estimated at €225 billion in 2025, 5G is a key asset for Europe to compete in the global market and its cybersecurity is crucial for ensuring the strategic autonomy of the Union. Billions of connected objects and systems are concerned, including in critical sectors such as energy, transport, banking, and health, as well as industrial control systems carrying sensitive information and supporting safety systems.

   In the shadow of the extensive public discussions, inter alia, as to the potential health side effects of the 5G tech, the launch of 5G across the EU is currently slated for the end of 2020, at the latest, with plans for ongoing infrastructural work to have wider 5G coverage across EU by 2025.

3. **New Competition Tool**

   Competition law plays a key part in the digital economy and this is especially true with so many new online business platforms emerging. The EU Commission is planning to launch a new 'competition tool' by the end of the year to curb anti-competitive behaviour and better address abuses of dominant market positions.

A: Evagorou 31, Evagoras Tower, Office 32, 1066 Nicosia, Cyprus | Valaoritou street 7, Kolonaki, Athens 10671, Greece.
T: +357 22760727 / +357 22760726 E: gch@hadjikyprianoulaw.com W: www.hadjikyprianoulaw.com

4. **Digital Services Act**

One of the most expecting new EU legislation in this area is the EU Digital Services Act. The new law will regulate further the use of online platforms; smart contract and e-advertising.

As pointed out the EU Commission: "*Europe needs a modernised regulatory framework to reduce the ever increasing regulatory fragmentation across Member States, to better ensure that everyone across Europe is protected online as they are offline and to offer to all European businesses a level playing field to innovate, grow and compete globally. Users' safety as well as the respect of their fundamental rights, in particular their freedom of expression, must be systematically guaranteed*."

Legislative developments planned for 2021:

1. **Gaia-X Initiative**

Through the Gaia-X initiative, EU aims to create a 'European data ecosystem', to achieve what is called 'digital sovereignty'. With that said, GAIA-X's aim is to develop common requirements for a European data infrastructure. Therefore openness, transparency and the ability to connect to other European countries are central to GAIA-X. 'Project GAIA-X' connects centralised and decentralised infrastructures in order to turn them into a homogeneous, user-friendly system. The resulting federated form of data infrastructure strengthens the ability to both access and share data securely and confidently.

2. **Regulation on AI**

The European Union has long been interested in artificial intelligence (AI). Back in 2014, the EU first investigated the issue by producing guidelines on the regulation of robotics. Since then, they have continued to work on this area, with a strong focus on the regulation of AI.

A follow-up to the White Paper the Commission had published in February 2020, can be expected sometime early in 2021.

3. **Digital Tax**

The digitalisation of the economy and society poses new tax policy challenges. One of the main questions is how to correctly capture value and tax businesses characterised by a reliance on intangible assets, no or insignificant physical presence in the tax jurisdictions where commercial activities are carried out (scale without mass), and a considerable user role in value creation. Current tax rules are struggling to cope with the emerging realities of these new economic models.

The EU and other international bodies have been discussing these issues for some time. In March 2018, the EU introduced a 'fair taxation of the digital economy' package. It contained proposals for an interim and long-term digital tax. The European Parliament supported both proposals, widening their scope and coverage and backing integration of digital tax into the proposed Council framework on corporate taxation. However, there was no immediate political agreement in the Council. As finding a global solution at Organisation for Economic Co-operation and Development (OECD) level or a coordinated EU approach was not yet feasible, some Member States started implementing or designing national digital taxes. As an indication of difficulties around this issue, the introduction of these taxes in France heightened trade tensions between the EU and the United States of America, with the latter favouring a 'voluntary' tax system – a position which may prevent a global agreement.

Over the last few years, the OECD has nevertheless made progress on developing a global solution and proposed a two-pillar system: while the first pillar (unified approach) would grant new taxation rights and review the current profit allocation and business location-taxation rules, the second (GloBE) aims to mitigate risks stemming from the practices of profit-shifting to jurisdictions where they can be subjected to no, or very low, taxation. The EU is committed to supporting the OECD's work, but if no solution is found by the end of 2020, it will again make a proposal for its own digital tax.

In light of the above, and despite the already expressed concerns by a number of Member States, the EU Council has formally requested the Commission to develop a proposal on Digital Tax by the first quarter of 2021 should no international agreement is reached within 2020.

4. Data Act

Over the last few years, digital technologies have transformed the economy and society, affecting all sectors of activity and the daily lives of all Europeans. Data is at the centre of this transformation and more is to come. Data-driven innovation will bring enormous benefits for citizens, for example through improved personalised medicine, new mobility and through its contribution to the European Green Deal. In a society where individuals will generate ever-increasing amounts of data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules. Citizens will trust and embrace data-driven innovations only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules. At the same time, the increasing volume of non-personal industrial data and public data in Europe, combined with technological change in how the data is stored

and processed, will constitute a potential source of growth and innovation that should be tapped.

Hence, tying in to Gaia-X and the Digital Services Act mentioned above, the EU Commission is seeking to create a 'data reservoir' of sorts, a European market for data, where both private and public entities can pool together large amounts of data which can be categorised accordingly into various different sectors such as energy, agriculture and healthcare. This could be further regulated by a Data Act, projected to be launched in 2021, whereby an EU data governance body would also be established to oversee the administration of such data in the public interest. On the basis of this strategy, the Commission has launched a comprehensive consultation on the specific measures that could be taken to keep the EU at the forefront of the data-agile economy, while respecting and promoting the fundamental values that are the foundation of European societies.

5. E-Privacy Regulation

On June 3, 2020, the Presidency of the Council of the European Union published a progress report on the proposed Regulation concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), better known as "the Draft ePrivacy Regulation".

In 2020 the ePrivacy Directive was scheduled to be reviewed for potential updates. However, when the Draft ePrivacy Regulation was announced, this review was sidelined given the ePrivacy Directive was to be repealed by the ePrivacy Regulation. Now, with the review of ePrivacy Directive arriving early next year, stakeholders have suggested that a better approach would be to scrap the ePR altogether, and instead to update the ePrivacy Directive and use the GDPR to fill the gaps. In the meantime, the rules in the EU around electronic tools such as cookies and spam will remain a patchwork of national laws, and companies will have to check their compliance on a country by country basis.

The aforementioned Progress Report indicates that subsequent deliberations on the draft ePrivacy Regulation were cancelled due to the COVID-19 crisis and that the Croatian Presidency will now work closely with the incoming German Presidency to facilitate further discussions and ensure a smooth handover of the file.

6. A New 'Privacy Shield'

On Thursday 16th July 2020, the Court of Justice of the European Union ('CJEU') ruled that the 'Privacy Shield' agreement allowing for the transfer of personal data between the European Union and the United States of America does not provide sufficient protection from US surveillance to EU citizens. With the demise

A: Evagorou 31, Evagoras Tower, Office 32, 1066 Nicosia, Cyprus | Valaoritou street 7, Kolonaki, Athens 10671, Greece.
T: +357 22760727 / +357 22760726 E: gch@hadjikyprianoulaw.com W: www.hadjikyprianoulaw.com

of the Privacy Shield, and the requirement that the "standard contractual clauses" should be judged on a case by case basis, the uncertainty surrounding international data transfers is set to continue. Our projection for the future in this area is that both the US and the EU will try to find a longer-lasting solution for international data transfer in the near future.

III. An Overview of the AI Regulation in Europe

Artificial intelligence (AI) has become an area of strategic importance and a key driver of economic and social development across the world. Enterprises around the world are rapidly incorporating artificial intelligence (AI) into existing and new products and processes. This effort is not just to improve such offerings and services, but to achieve a qualitatively higher level of capability not possible before. This emerging technology can bring solutions to many societal challenges from treating diseases to minimising the environmental impact of farming. However, related socio-economic, legal and ethical impacts have to be carefully addressed and a balance must be drawn between, on the one hand, the rights of every individual and on the other, the plethora benefits this technology can offer.

In the last two years, there has been a wealth of new publications, guidelines and political declarations from various EU bodies on AI. These provide insight into the future of AI in Europe – including on how it will be regulated, what governments will promote, who will be liable for defects in AI and how safety standards will be enforced. These insights are of value both to legal practitioners operating in the emerging technologies sector and to organisations developing, using or considering the procurement of AI products. AI products and services will be covered by numerous areas of the law, including privacy, data security, products liability, intellectual property, and antitrust, among others. Further, it is expected that these various areas of law will change in response to AI.

Below we highlight some regulatory EU initiatives in relation to the development of the AI EU legislative landscape.

EU Legislative Landscape on Artificial Intelligence:

2018:

i. The first and most important EU initiative in relation to AI was the **Declaration of Cooperation on Artificial Intelligence**, signed at the beginning of 2018 by the majority of Member States of the EU. The ultimate aim of this important initiative was to assemble a unified intra-union approach to the most important issues relating to AI.

ii. Following the aforementioned first initiative, **the Communication from the Commission to the European Parliament, The European Council, the Council, the European Economic and Social Committee and the Committee Of The Regions On Artificial Intelligence For Europe** was published.

The aim of this Communication was to set out an Intra-Union initiative in order to:

"

a) *Boost the EU's technological and industrial capacity and AI uptake across the economy, both by the private and public sectors . This includes investments in research and innovation and better access to data.*
b) *Prepare for socio-economic changes brought about by AI by encouraging the modernisation of education and training systems, nurturing talent, anticipating changes in the labour market, supporting labour market ransitions and adaptation of social protection systems. and*
c) *Ensure an appropriate ethical and legal framework, based on the Union's values and in line with the Charter of Fundamental Rights of the EU. This includes forthcoming guidance on existing product liability rules, a detailed analysis of emerging challenges, and cooperation with stakeholders, through a European AI Alliance, for the development of AI ethics guidelines."*

iii. As a result of the aforementioned call to EU countries to join forces in order to develop Europe's AI regulatory landscape, the Joint Research Centre of the European Commission published a report called "**Artificial Intelligence: A European Perspective**" aiming to provide an independent and balance assessment on the opportunities and underlying challenges/complexities presented by AI in Europe as well as to assess the positioning of the EU in the AI global chessboard.

2019:

Without a doubt, 2019 was a year full of great initiatives and developments in relation to AI in Europe. The European Commission in consultation with the High-Level Expert Group on AI has published a number of papers aiming to further mature the AI EU regulatory landscape covering a number of complex legal issues, including inter alia, trustworthiness in the AI decision making process and liabilities. Those reports were the following:

i. The **Ethics Guidelines for Trustworthy Artificial Intelligence Report**;

ii. The **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Building Trust in Human Centric Artificial Intelligence**;

iii. The **Policy and Investment Recommendations for Trustworthy Artificial Intelligence Report**; and

iv. The **Liability for Artificial Intelligence and other Emerging Digital Technologies**.

2020:

Building upon the recommendations and consultation initiatives mentioned above, the European Commission under the presidency of Ursula Von der Leyen has made the first major step towards an EU legislative proposal on AI in February 2020 by publishing a **"White Paper on Artificial Intelligence - A European Approach To Excellence And Trust".**

The purpose of the AI White Paper is to seek input and proposals on the development of a common EU framework for the regulation of AI. The European strategy for data, which accompanies this White Paper, aims to enable Europe to become the most attractive, secure and dynamic data-agile economy in the world – empowering Europe with data to improve decisions and better the lives of all its citizens. The strategy sets out a number of policy measures, including mobilising private and public investments, needed to achieve this goal. Finally, the implications of AI, Internet of Things and other digital technologies for safety and liability legislation are analysed in the Commission Report accompanying this White Paper.

AI is a strategic technology that offers many benefits for citizens, companies and society as a whole, provided it is human-centric, ethical, sustainable and respects fundamental rights and values. AI offers important efficiency and productivity gains that can strengthen the competitiveness of European industry and improve the wellbeing of citizens. It can also contribute to finding solutions to some of the most pressing societal challenges, including the fight against climate change and environmental degradation, the challenges linked to sustainability and demographic changes, and the protection of our democracies and, where necessary and proportionate, the fight against crime.

For Europe to seize fully the opportunities that AI offers, it must develop and reinforce the necessary industrial and technological capacities. As set out in the accompanying European strategy for data, this also requires measures that will enable the EU to become a global hub for data.

The European approach for AI aims to promote Europe's innovation capacity in the area of AI while supporting the development and uptake of ethical and trustworthy AI across the EU economy. AI should work for people and be a force for good in society.

With this White Paper and the accompanying Report on the safety and liability framework, the Commission launches a broad consultation of Member States civil society, industry and academics, of concrete proposals for a European approach to AI. These include both policy means to boost investments in research and innovation, enhance the development of skills and support the uptake of AI by SMEs, and proposals for key elements of a future regulatory framework. This consultation will allow a comprehensive dialogue with all concerned parties that will inform the next steps of the Commission.

In light of the above, anyone involved in the development of AI technologies or investing in AI should keep a close eye on further developments, so as to have a head start in getting to grips with a new legal and economic landscape for AI as it is gradually put into place by the EU and its Member States.

IV. Liability for Artificial Intelligence and Other Emerging Digital Technologies: A Lacuna in the Applicable Local and EU Legislations

In recognition of the importance to stay at the forefront of this technological revolution, the European Commission has put forward a European approach to Artificial Intelligence and Robotics. Within this context, the Commission has published a **"Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies"** which details the findings of a Group of Experts on the liability rules specifically applicable to damages and losses resulting from the use of emerging digital technologies such as AI.

Assessment of existing liability regimes across the European Union

The Group examined whether and to what extent existing liability schemes are adapted to the emerging market realities following the development of new technologies such as artificial intelligence, advanced robotics, the internet of things and cyber security issues. In particular, they were asked to examine whether the current liability regimes across the Member States are 'adequate to facilitate the uptake of new technologies' and to assess their suitability to deal with damages and losses resulting from the use of such technologies.

In its assessment, the New Technologies Formation of the Expert Group has concluded that the liability regimes currently in force in the Member States ensure *merely a basic protection* of victims whose damage is caused by the operation of such new technologies. More specifically, they have found that, while the laws of the Member States do ensure basic protection of rights, also referred to as primarily damages in tort and contract, these laws are not specifically applicable to this dynamic, complex and fast developing area. The specific characteristics of these technologies and their applications – including complexity, modification through updates or self-learning during operation, limited predictability, and vulnerability to cybersecurity threats – may make it more difficult to offer individuals a claim for compensation in all cases where this seems justified. It is also sometimes the case that the allocation of liability is unfair or inefficient.

An example of technology given by the Group to highlight the complexities in this field is a smart home system, which has a number of interacting devices and programmes. Someone who has suffered damages as a result of a failure of this system would have a number of financial and technical obstacles to overcome in order to prove causation i.e. that the software design or algorithm caused the failure of the device or system. The more systems involved and interacting the more costly and complex this becomes. According to the Report, in order to rectify this gap, certain adjustments need to be made to existing EU and national liability regimes.

Key findings of the Group

What follows is a summary of the key findings of the Group on how liability regimes should be designed and, where necessary, changed to adapt to this evolving area of digital technology:

1. A person operating a permissible technology that nevertheless carries an increased risk of harm to others, for example AI-driven robots in public spaces, should be subject to strict liability for damage resulting from its operation.

2. In situations where a service provider ensuring the necessary technical framework has a higher degree of control than the owner or user of an actual product or service equipped with AI, this should be taken into account in determining who primarily operates the technology.

3. A person using a technology that does not pose an increased risk of harm to others should still be required to abide by duties to properly

select, operate, monitor and maintain the technology in use and – failing that – should be liable for breach of these duties if at fault.

4. A person using a technology which has a certain degree of autonomy should not be less accountable for ensuing harm than if the said harm had been caused by a human auxiliary.

5. Manufacturers of products or digital content incorporating emerging digital technology should be liable for damage caused by defects in their products, even if the defect was caused by changes made to the product under the producer's control after it had been placed on the market.

6. For situations exposing third parties to an increased risk of harm, compulsory liability insurance could give victims better access to compensation and protect potential tortfeasors against the risk of liability.

7. Where a particular technology increases the difficulties of proving the existence of an element of liability beyond what can be reasonably expected, victims should be entitled to facilitation of proof.

8. Emerging digital technologies should come with logging features, where appropriate in the circumstances, and failure to log, or to provide reasonable access to logged data, should result in a reversal of the burden of proof in order not be to the detriment of the victim.

9. The destruction of the victim's data should be regarded as damage, compensable under specific conditions.

10. It is not necessary to give devices or autonomous systems a legal personality, as the harm these may cause can and should be attributable to existing persons or bodies.

What should manufacturers and operators of such technologies do for now?

Given the identified ambiguities, it is advisable for manufacturers and operators of such technologies to make it clear, through warnings, instructions, marketing, and otherwise, that emerging technologies are being used and obtain the consent of the general public before interacting with them. Besides, all AI and/or technology driven decisions should always be reviewed by individuals/experts and a cost-benefit analysis

and risk assessments should always be made before incorporating and applying such technologies.

Concluding Remarks

The law of tort of EU Member States is largely non-harmonized, with the exception of product liability law under Directive 85/374/EC, some aspects of liability for infringing data protection law (Article 82 of the General Data Protection Regulation (GDPR), and liability for infringing competition law (Directive 2014/104/EU). There is also a well-established regime governing liability insurance with regard to damage caused by the use of motor vehicles (Di-rective 2009/103/EC20), although without touching upon liability for accidents itself. EU law also provides for a conflict of tort laws framework, in the form of the Rome II Regulation. On a national level, it can generally be observed that the laws of the Member States do not as of yet contain liability rules specifically applicable to damage resulting from the use of emerging digital technologies such as AI.

While it is possible to apply existing liability regimes to emerging digital technology, as these technological developments are constantly evolving, steps should be taken now to consider how to implement the recommendations of the Group. The EU's first dedicated AI legislation is expected to be published very soon and it will be very interesting to see if any of the above issues are addressed in that draft in order to mitigate the risks due to the confirmed lacuna in the law.

V. European Commission's White Paper on AI: Temporary Facial Recognition Ban

In accordance with a draft white paper on Artificial Intelligence, the European Commission is currently considering measures to impose a temporary ban on technologies dealing with facial recognition in public places. More specifically, the paper, which gives an insight of the latest EU's approach to Artificial Intelligence, stipulates that a future regulatory framework could "include a time–limited ban on the use of facial recognition technology in public spaces" and continues by adding that the "use of facial recognition technology by private or public actors in public spaces would be prohibited for a definite period (e.g. 3–5 years) during which a sound methodology for assessing the impacts of this technology and possible risk management measures could be identified and developed".

It is thus understood that the purpose of such a ban is to provide a transitional period within which data privacy concerns posed by the already widespread deployment of the technology will need to be assessed. Those who have adopted the technology would maintain that it conveys valuable social benefits, maintains public safety and security and prevents crime. However, the technology has attracted considerable

A: Evagorou 31, Evagoras Tower, Office 32, 1066 Nicosia, Cyprus | Valaoritou street 7, Kolonaki, Athens 10671, Greece.
T: +357 22760727 / +357 22760726 E: gch@hadjikyprianoulaw.com W: www.hadjikyprianoulaw.com

resistance and a number of EU citizens have made known their objections, publicly protesting against its use.

What will be borne out of the Commission's final report and how a balance between social security and privacy will be achieved remains to be seen. In any case, if the ban is finally implemented, the use facial recognition technologies in airports; train stations; sports events (ie through the Sports Fan ID Cards) and other public places would need to be postponed and regulated.

VI. Blockchain Technology and Data Protection Challenges in the EU

The data protection and privacy regulatory landscape can appear overwhelming to a business of any size. Related compliance failures can give rise to significant reputational damage; substantial regulatory fines; claims for damages as well as loss of corporate value. Thus, data protection and privacy compliance constitutes one of the key risk avoidance strategies for companies today.

The EU General Data Protection Regulation (the "GDPR") came into force on 25 May 2018 and introduced a new intra-union legal framework for privacy and data protection. The GDPR replaced the 1995 Data Protection Directive, which had been transposed into each EU member state's national legislations. While the GDPR resembles the principles of the 1995 Data Protection Directive, it has some important new key elements.

Since the introduction of the GDPR in our lives however, we have seen rapid developments in new revolutionary technologies such as Blockchain. Without a doubt, blockchain technology is disrupting traditional business models and transforming organizations at an ever-increasing pace. At the same time, the increasing fast pace of digital and blockchain related innovation is creating new legal challenges and commercial implications requiring new legal policies and innovative structures in many areas and industries especially as far a data protection is concerned. With that said, we hereunder set out the main tensions between the EU data protection regulatory landscape and blockchain technology.

Blockchain and Data Protection – Introductory Remarks

The security standards of blockchains are so high that it is virtually impossible to erase information. What might be a good feature under some circumstances can be a legal problem in other situations, for example, if personal data is concerned. Most privacy laws, especially the GDPR require that personal data must only be stored for lawful purposes, for so long it is necessary to serve the purpose, must be corrected if incorrect, and the concerned person has a right of access to the stored information. All this does not mean, however, that blockchains are invariably incompliant with data

A: Evagorou 31, Evagoras Tower, Office 32, 1066 Nicosia, Cyprus | Valaoritou street 7, Kolonaki, Athens 10671, Greece.
T: +357 22760727 / +357 22760726 E: gch@hadjikyprianoulaw.com W: www.hadjikyprianoulaw.com

protection laws, but it is a challenge to design the blockchain architecture and applications in a way that they respect privacy

Data Controller

Data Controllers have a key role to play under the GDPR being the architects and main points of accountability for data processing. In other words, the identification of the data controller and the extend of data processing activity identified by those persons are the foundations of all the rules and principles established by the GDPR. Conversely, essential to blockchain is the decentralization of data processing. Processing does not take place at one entity, but is distributed over all active participants in the blockchain network. A first crucial question – for each processing incidentally – is who should be regarded as "data controller", responsible for the processing? Therefore in such a decentralised system, the identification of the data controller becomes somewhat problematic and this deadlock has already stimulated an interesting academic debate.

Processing of Personal Data

Pursuant to the provisions of the GDPR, one must have a valid lawful basis in order to process personal data. As far as the relationship between blockchain technology and data processing lawfulness is concerned, there are a number of challenges that need to be considered given that the use of such technologies makes the application of certain legal basis identified by GDPR difficult ie. When and how are consents given in a transaction within blockchain? Besides, the general principles of 'purpose limitation', 'data minimisation', 'accuracy' and 'storage limitation', seem to clash with the way blockchain technology mainly functions and stores data. Reason being that such technology was developed in a manner which makes it extremely difficult to tamper with data stored on any particular block within the network.

Data Protection Rights

Without a doubt, the lack of EU Blockchain legislation poses a number of problems when it comes to the right of data subjects such as the right of access; the right to transfer data; the right to restrict processing; and the objection to the processing of personal data right. Due to the decentralised nature of blockchain technology; blockchain's immutability and difficulties in identifying a centralised data controller, it seems that the application of those rights within the blockchain realm is problematic. As such, without a specific legal instrument covering the aforementioned gaps, it seems unlikely that a data subject would ever be able to achieve the level of control over his or her personal data which the GDPR seeks to provide through these data subject rights.

A: Evagorou 31, Evagoras Tower, Office 32, 1066 Nicosia, Cyprus | Valaoritou street 7, Kolonaki, Athens 10671, Greece.
T: +357 22760727 / +357 22760726 E: gch@hadjikyprianoulaw.com W: www.hadjikyprianoulaw.com

Concluding Remarks

The decentralised and distributed structure of blockchain conflicts with the foundations of the GDPR which is based on a centralised model of data processing and this conflict creates a deep level of legal uncertainty in this area. Nevertheless, there is currently an ongoing discussion about potential solutions which may be adopted to resolve these tensions both from a legal as well as from a technical perspective.

Ultimately, a balance needs to be struck so that data protection does not become an obstacle for innovation and at the same time, technology advancements are not attained at the expense of our data protection rights. Regulation does not need to mean the end of innovation. EU can definitely develop and implement a 'blockchain friendly', innovative and technology-neutral regulatory framework that will be in line with its data protection principles. Stakeholders, such as technology experts, lawyers and other professional services, need to actively work together to promote data protection friendly blockchain legislation. Ultimately, success will depend on support from the wider community, through a mix of investment, collaboration and innovation.

VII. Schrems II: What are the Implications on the International Data Trade and on the EU Digital Transformation Agenda?

The General Data Protection Regulation EU 2016/679 ("**GDPR"**) provides that transfers of personal data to a third country (i.e. any country outside the European Economic Area ("**EEA**")) may only take place if "appropriate safeguards" are used to legitimise the transfer. Those safeguards should ensure compliance with data protection requirements appropriate to processing within the EU, including both the availability of enforceable rights and of effective legal remedies, as well as adherence to the general principles relating to personal data processing. Among those safeguards are the Standard Contractual Clauses ("**SCCs**") of which many EU companies avail themselves in order to transfer personal data outside of the EEA for their everyday business operations. Besides, the EU Commission also ruled that the EU-US Privacy shield which underpinned the transatlantic digital trade was adequate for transferring personal data from the EU to the US. In other words, the EU-US Privacy Shield, allowed US companies to sign up to stringent privacy standards providing companies governed by the GDPR with a mechanism to transfer personal data to those companies. All these were challenged however by a privacy advocate, Max Schrems, who argued that US national security laws did not go far enough in protecting EU citizens from government snooping.

As a result, in the bombshell decision of Schrems II, the Court of Justice of the European Union (CJEU) found that the Commission's decision finding the EU-US Privacy Shield to be adequate for transferring personal data from the EU to the U.S. is invalid. In what can only be seen as a double whammy, the CJEU also ruled that transferring personal data to the U.S. pursuant to SCCs adopted by the Commission could also be found to be invalid by local data protection authorities and thus SCCs must always be scrutinized by national supervisory authorities.

Prior to Schrems II, the US was the subject of a partial adequacy decision. Because the US was deemed not to provide protections equivalent to those available in the EU, the US Department of Commerce and the European Commission devised the Privacy Shield as a set of principles designed to ensure equivalent protection was provided by companies that self-certified their adherence to these principles. These companies could be placed on the Privacy Shield list and could receive data without having to take additional measures.

The judgment in Schrems II invalidated the Privacy Shield and rules that it can no longer be relied upon to enable the transfer of personal data from the EEA to the US. One of the rationales behind the decision is that adherence to the Privacy Shield principles may be limited by the need to meet national security, public interest, or law enforcement requirements (Schrems II, para 164). The availability of this derogation, the limits of which are not defined, and the concomitant ability of the US government to access transferred data under US surveillance laws without adequate means of redress for affected individuals, means that, in the CJEU's view, the Privacy Shield did not ensure equivalent protection to that available in the EU (Schrems II, paras 180 and 199).

Hence, the two key takeaways from the decision are the following:

i. The Privacy Shield framework, which is used by thousands of companies to transfer data between the EU and US, does not protect the privacy of EU citizens and is declared invalid.
ii. The SCCs adopted by the European Commission for the transfer of personal data to processors established in third countries are valid, but companies will have to carefully analyse whether their SCCs are sufficient to ensure that data in third countries is treated in line with the GDPR and the EU Charter of Fundamental Rights

Ultimately the CJEU confirmed the theoretical validity of the standard contractual clauses as a mechanism for the transfer of personal data outside of the EU. However as mentioned above, this validation came with a rather large caveat: the court stressed that entering into the standard contractual clauses is not sufficient in-and-of-itself. The

controller or processor must also, on a case-by-case basis, verify that the laws of the destination country ensure adequate protection under EU law of any personal data transferred pursuant to the standard contractual clauses. Where the laws of the destination country do not ensure adequate protection, controllers must implement supplementary measures and additional safeguards to attain the required level of protection or else cease the transfer.

Furthermore, the CJEU expressly concluded that EU supervisory authorities are required to suspend or prohibit transfers to third countries pursuant to standard contractual clauses if they are of the view that the clauses are not or cannot be complied with in the third country in a way that ensures the required level of protection. Based on the court's findings in respect of the Privacy Shield, it is difficult to see how supervisory authorities would be able to avoid such a conclusion in the case of transfers to the US.

With the demise of the Privacy Shield, and the requirement that the "standard contractual clauses" should be judged on a case by case basis, the uncertainty surrounding international data transfers is set to continue. Our projection for the future in this area is that both the US and the EU will try to find a longer-lasting solution for international data transfer in the near future.

There are no easy or quick solutions to the complexities of this judgment, but it highlights how crucial it is for controllers to ensure that they review their processing and any contracts that they may have with processors. It reminds us that real compliance cannot be a tick box exercise, it must be part of a carefully considered and holistic governance framework which, done well, will protect both individuals and organisations.

Ultimately, Schrems II and the recently filed regulatory complaints will force the EU and U.S. to develop and implement a successor to EU-U.S. Privacy Shield. In the interim, however, without the benefit of predictable data protection framework, companies involved with importing personal data from the EU face significant regulatory risks and compliance challenges. We still await formal guidance from EU regulators in response to Schrems II. However, it is clear that organisations will be expected to review data transfers that rely on Privacy Shield and SCCs and to come up with an action plan to shift away from Privacy Shield and review the use of SCCs to check they are still valid. This guidance is yet to come, so organisations should be using this time to audit any data transfers to non-EEA countries to identify the mechanisms that are used and to check they are valid. In the case of Privacy Shield, the answer will be clear – and another mechanism will have to be found. For SCCs, reviewing each use on a case-by-case basis will be required, as well as looking to assess whether the local law in the destination country offers adequate protection. If not, it will need to be determined whether adequate additional safeguards are (or can be) put in place to

A: Evagorou 31, Evagoras Tower, Office 32, 1066 Nicosia, Cyprus | Valaoritou street 7, Kolonaki, Athens 10671, Greece.
T: +357 22760727 / +357 22760726 E: gch@hadjikyprianoulaw.com W: www.hadjikyprianoulaw.com

meet the Schrems II requirements. Further due diligence checks may be required. That is likely to involve asking questions of the data importer since it is likely to be best placed to describe the legal regime in which it operates.

What Companies should do next?

- *Make sure that their senior managements are aware of those important developments.*
- *Review the current transfers within and outside the EU. Companies that transfer personal data from the U.S. should review the basis for the transfers. This should include reviewing major agreements with processors, outsourcers and hosting providers to ensure that all transfers to the U.S. may be lawfully continued.*
- *Review their outsourcing agreements and conduct risk assessments. The decision of* Schrems *II decision should encourage data exporters to review the legal basis currently used for transfers outside the EEA to ensure they remain compliant. If transfers have been based on Privacy Shield, a different legal basis has to be identified and implemented. Transfers based on SCCs also have to be re-examined and risk assessments must be conducted.*

A: Evagorou 31, Evagoras Tower, Office 32, 1066 Nicosia, Cyprus | Valaoritou street 7, Kolonaki, Athens 10671, Greece.
T: +357 22760727 / +357 22760726 E: gch@hadjikyprianoulaw.com W: www.hadjikyprianoulaw.com