Personal Data Protection: A Preeminent EU Right for the Cypriot Legal System

Georgios Tsaousis[1]

Abstract

Data protection plays a key role in the European Union (EU) edifice. It is an invaluable tool in ensuring the mandated free movement of goods, services, capital, and persons in the internal market. Harmonisation of data protection rules between Member States (MS) was a vital step to ensure uniform implementation of this fundamental EU competence. A first attempt—Directive 95/46/EC—proved to be incomplete but was followed by the General Data Protection Regulation (GDPR), a regulatory necessity in the digital age. Although Regulations are far more coherent legislative instruments than Directives, MS are afforded some leeway when adopting national rules in certain fields. Cyprus could hardly be the exception; having integrated the GDPR into domestic law, it maintained certain 'national peculiarities', especially in the fields of court proceedings, public interest, children's consent, genetic and biometric data, and the combination of large-scale filing systems. However, some aspects of the national provisions continue to clash with the principles governing the processing of personal data (Article 5 of the GDPR). On a practical level, the Cyprus Commissioner for personal data protection should be able to reconcile such shortcomings; however, this has not been the case. This may be ascribed to either the downgrading of their role by other institutions, lack of expertise (given that the position does not require qualifications or experience in data protection), or even to the cultural attitude towards privacy in Cyprus. Despite the national peculiarities and the Commissioner's downgraded role, Cyprus' participation in the EU acquis undoubtedly ensures more effective personal data protection.

Keywords: data protection; Cyprus; GDPR; Commissioner for personal data protection; EU acquis; fundamental rights; harmonisation measures; EU secondary law

1. Introduction

Data protection plays a key role in the European Union (EU) edifice. It is a valuable tool in ensuring the free movement of goods, services, capital, and persons in

[1] Assistant Professor, Faculty of Law, University of Nicosia

the internal market. However, the uniform implementation of this fundamental EU competence has encountered obstacles in the form of disparate data protection rules, which also undermine legal certainty.[2]

The right to the protection of personal data was established by pilot Directive 95/46/EC. Its drafters were clearly influenced[3] by Convention 108 of the Council of Europe[4] and by the jurisprudence around the right to informational self-determination.[5] The Directive succeeded in harmonising the various regulatory models of the Member States (MS), specifying the basic principles of data processing and connecting the legality of their processing with clearly defined legitimate purposes. It established the rights of individuals (information, access, opposition) and set up national independent supervisory authorities (Article 28 of the pilot Directive).

It would not be an exaggeration to claim that the Directive—and the regulatory model it established—set the standard regarding the protection of informational privacy across the EU. Additionally, the requirement to ensure a satisfactory level of protection for cross-border data flow in third countries has decisively contributed to the adoption of relevant legislation in several countries in America and Asia.[6] Naturally, Cyprus, as a MS under accession, could hardly be left unaffected.

---

[2] Francis Aldhouse, 'Data protection in Europe – Some thoughts on reading the academic manifesto' (2013) 29(3) *Computer Law & Security Review* 289–292.

[3] Directive 95/46/EC, Preamble, Recital 11: 'Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention'. Available at https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng

[4] Convention 108/28.01.1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. This Convention has influenced privacy and data protection laws in Europe and beyond for over 40 years. Its modernised version (known as Convention 108+ adopted on 18 May 2018) continues to do so.

[5] Attila Kiss & Gergely László Szőke, 'Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation', in Serge Gutwirth, Ronald Leenes & Paul de Hert (eds), *Reforming European Data Protection Law* (Dordrecht Heidelberg New York London: Springer, 2015) 311; Nadezhda Purtova, 'Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table … and back on again?' (February 2014) 30(1) *Computer Law & Security Review* 6.

[6] Paul M. Schwartz, 'The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures' (May 2013) 126(7) *Foreign & Comparative Law* 1966; Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (March 2012) 2(2) *International Data Privacy Law* 77.

2. The Right to Data Protection in the Cypriot Legal System

2.1. Incorporation Of the Pilot Directive for Data Protection

Data protection is not a new right; rather, it is the codification of a right which had previously been incorporated into the 'classic' individual right to the protection of private life (Article 15 of the Cyprus Constitution). The notion of private life is not to be interpreted narrowly, since the aim is to safeguard fundamental rights. Such rights may be restricted only by law, only if judged necessary for reasons specified in Article 15 and in addition, in so far as the restriction is justified in a European democracy.[7] Regarding its application, the jurisprudence pre-dating the incorporation into internal law of Directive 95/46/EC recognised the existence of the right to the protection of personal data and included it within the protective scope of Article 15 of the Constitution without specifically referring to it. The safekeeping, use, and disposal of one's assets, personal data included, is integral to private life. Their disclosure and publication violate the right guaranteed by Article 15.1 of the Constitution. This is explicitly crystallised in a 2000 Supreme Court decision:

> The exercise of the right guaranteed by Article 15.1 cannot be interfered with, except as defined in paragraph 2 of the same Article of the Constitution. Intervention is only permitted if it is authorised by law and is exclusively necessary for one or more purposes defined in the same provision of the Constitution.[8]

Directive 95/46/EC formed part of the *acquis communautaire*, and its incorporation into national law was a prerequisite to accession for candidate MS. Furthermore, the EU Charter enshrines data protection as a fundamental right under Article 8, in addition to the right to private and family life under Article 7. In contrast to earlier rounds, candidate MS for the 2004 and 2007 EU enlargements faced the challenge of adjusting legislation[9] prior to accession to bring their laws, regulatory frameworks, and administrative practices in line with the *acquis communautaire*.[10]

The Directive was transposed into Cypriot legislation with the Personal Data Processing (Protection of the Individual) Law of 2001 (Law 138(I)/2001), which entered

[7] Achilles C. Emilianides, *Constitutional Law in Cyprus* (3rd edn., The Netherlands: Wolters Kluwer, 2024) 180.

[8] President of the Republic v House of Representatives (2000) 3 CLR 238.

[9] Candidate MS must accept the *acquis* before joining the EU. Derogations are few and limited in scope.

[10] Christophe Hillion, 'EU enlargement: A legal analysis' in A. Arnull & D. Wincott (eds), *Legitimacy and Accountability in the European Union* (Oxford: Oxford University Press, 2002) 405.

into force on 23 November 2001. On the same date, the European Convention for the Protection of Individuals from Automated Processing of Personal Data (Establishing) Law (Law 28(III)/2001), which ratified the corresponding Convention of the Council of Europe, was also published in the Official Gazette.

Article 28 of the Directive provided for the establishment of an authority charged with overseeing the implementation of national provisions enacted by the member states within its territory.

2.2. The Cypriot National Data Protection Authority

Cyprus has established Independent Administrative Authorities (IAAs) to offer faster and more targeted solutions[11] in certain areas of social life. Particularly, those areas in which the traditional administrative structure finds it difficult to respond due to the complexity of social structures but also to technological progress and the risks it entails.[12] According to EU law, the authority should exercise its duties completely independently from the legislative, and especially from the executive. In legal terms, the independence of an administrative body corresponds to its authority to make decisions at its 'complete discretion', uninfluenced by any kind of external pressure. And the quality of independence allows the *summa divisio* of the independent authorities from the traditional administrative bodies.

The Cypriot Constitution distinguishes between political power and administrative function. It prohibits the involvement of the government in the administrative functioning of the State. The legal basis for this is an imperative constitutional principle, recognised by jurisprudence,[13] which stipulates that the administration must operate independently of political influence. To fulfil the purpose of administrative independence, the Cypriot legislator assigned responsibility for staffing the administration to an independent body, the Public Service Commission. At the level of ex-

[11] The protection, or rather the solutions, offered by IAAs could be characterised as autonomous in the sense that they do not originate from the 'classic' administration. Rather, they stem from a legal structure that has the peculiarity of being characterised as independent since it acts, decides, and sometimes imposes sanctions without any executive-branch intervention.

[12] Jean-Bernard Auby, 'Remarques Terminales' in R.F.D.A., N° 5/2010, 931.

[13] President of the Republic v House of Representatives (No. 3) (2011) 3 CLR 777; Kakouris v District of Famagusta et al. (2004) 1 CLR 8; Frangoulides (No. 2) v Republic (1966) 3 CLR 676; R.I.K. etc. v Karagiorgis et al. (1991) 3 CLR 159; Dimokratia v Konstantinidis (No. 1) (1996) 3 CLR 206; Socrates v Democracy (1997) 3 CLR 204; Democracy v Pogiatzi (1992) 3 CLR 196; President of the Republic v House of Representatives (1991) 3 CLR 631; President of the Republic v House of Representatives (No. 2) (2009) 3 CLR 648; Pavlou a.o. v Returning Officer a.o. (1987) 1 CLR 252; Hinds a.o. v The Queen (1976) 1 All E.R. 354.

press provisions, the Cypriot Constitution explicitly establishes and safeguards the separation of powers through specific Articles—122, 124, and 125—which concern the public service and the Public Service Commission.

Cyprus' Commissioner for personal data protection ('the Data Commissioner') is an IAA charged with supervising the implementation of legislative data protection provisions and other regulations concerning the protection of individuals from the processing of their personal data. The Commissioner therefore defends fundamental rights and freedoms guaranteed by the Constitution (privacy, respect of correspondence and communication, etc.) while making regulatory interventions[14] in the field of data processing, which is constantly changing through the development of new technologies, especially artificial intelligence (AI).

The Directive states that the independent authority must be notified of the processing of any personal data included in a file by both public and private entities. In 2002–2003, the Commissioner's first year of operation, a total of 1,370 notifications were submitted for the keeping / operation of records and the processing of personal data.[15] Interest in the personal data protection framework was admittedly limited in the early years of implementation. In fact, in a 2004 European Commission survey, 60% of EU citizens had never heard of the legislation regarding the protection of personal data. This ignorance may be explained by the relatively nascent stage at which digital tools like the internet, social networks, and AI applications were two decades ago. In Cyprus, despite sustained efforts by the IAA to inform professional classes such as lawyers, journalists, and doctors (usually through their professional organisations), the lack of a substantial response has been highly problematic, as these professionals play an essential role in the processing of personal data.[16]

The Directive quickly proved to be an imperfect regulatory tool for ensuring comprehensive personal data protection, unable to meet the challenges of globalisation and rapid technological development.[17] The need to establish more coherent rules became imperative.

[14] For example, the Commissioner announced the completion of 30 audits regarding the use of cookies by news and public information websites. Then Commissioner Nikolaidou concluded some websites did not disclose the purposes for their use of cookies, while others that did provide that information did not receive users' express consent for the use of cookies. Announcement dated 08 May 2023, available at https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/99981BE9F8E399EFC22589A9002E6742?OpenDocument# (accessed on 28 April 2025).

[15] Data Protection Commissioner, Annual Report 2002-2003, 9 [in Greek].

[16] Data Protection Commissioner, Annual Report 2004, 3 [in Greek].

[17] EC Communication 04.11.2010: 'A comprehensive approach on personal data protection in the EU',

2.3. The GDPR and the Role of the Cypriot Presidency

It is a truism that the law lags behind technology. However, data protection law has reacted relatively nimbly to the digitalisation of society and the economy. While the commodification of personal information is not a new phenomenon, its expansion into the online environment is a qualitative change, possibly even a paradigm shift. The evolution of personal information on an economic scale is shown clearly across online businesses, especially in advertising practices.[18] In a globalised market, personal data has become the basic currency of the information economy.[19] Personal data is undoubtedly crucial in political communication as well,[20] with risks posed to the quality of democracy by unfair processing.[21] In short, by the end of the first decade of the 21st century, the data protection framework needed updating[22] to address the challenges of the digital age and restore eroded confidence in the regulatory and protective capacity of EU legislation.[23]

The EU General Data Protection Regulation (GDPR) must be viewed in the context of the worldwide trend—inspired by the EU itself—to adopt similar laws.[24] On the adoption of the GDPR's predecessor, Directive 95/46/EC, only around 30 countries, most in Western Europe, had similar rules; nowadays almost 130 across all continents have some form of regulatory framework in place.[25] Adopted in April 2016 and applicable as of May 2018, the GDPR is the centrepiece of the reform of the EU regulatory framework for the protection of personal data. While retaining the conceptual framework of the Directive 95/46/EC it replaced, the GDPR represents a major shift

18.

[18] Andrew Hotaling, 'Protecting personally identifiable information on the Internet: Notice and consent in the age of behavioral targeting' (2008) 16 CommLaw Conspectus 529.

[19] Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011) 140(4) *Daedalus* 34.

[20] Katharine Dommett, 'Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns' (2019) 8(4) *Internet Policy Review*.

[21] Ekathimerini.com, 'Prosecutor to probe Asimakopoulou's alleged GDPR breach' (05 March 2024) available at https://www.ekathimerini.com/news/1233321/prosecutor-launches-investigation-into-asimakopoulous-alleged-gdpr-breach/.

[22] Mira Burri & Rahel Schär, 'The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy' (2016) 6 *Journal of Information Policy* 481.

[23] Marc Rotenberg, 'On International Privacy: A Path Forward for the US and Europe' (Spring 2014) 35(4) *Harvard International Review* 24.

[24] Michelle Goddard, 'The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact' (November 2017) 59(6) *International Journal of Market Research* 705.

[25] Giovanni Butarelli, 'Forefront' in Christofer Kuner, Lee A. Bygrave & Christofer Docksey (eds), *The EU General Data Protection Regulation (GDPR) A Commentary* (Oxford: Oxford University Press, 2020).

in the regulation of data protection while reaffirming that privacy constitutes one of the fundamental rights of EU law.

Initially, certain MS raised juridical and political objections to the choice of a Regulation as the legal instrument, as its binding force restricted national approaches regarding the level and method of data protection. For example, while Germany fervently supported a high level of protection, the UK feared that such protection might act as a deterrent to the establishment of US technology companies on its soil, as the British applied a less protective regulatory framework.[26] Member States argued that a Regulation would introduce binding rules and thus limited leeway to develop alternative protection policies. In other words, it would be a centralised and monopolistic legislation contrary to the principle of subsidiarity, which runs through EU law.[27]

Denmark, which held the Presidency of the EU Council in the first half of 2012, processed the final proposal of the GDPR article by article. Cyprus then assumed the Council Presidency and continued this horizontal approach focusing on three issues: (1) delegated and implementing acts; (2) administrative burdens and compliance costs; and (3) more flexibility for the public sector. Due to its length, the Danish and Cypriot Council Presidencies reviewed less than half of the GDPR proposal by the end of 2012.

The Regulation was chosen (instead of the Directive) to achieve coherence between the legislative arrangements of the MS. The Regulation contributed to better harmonisation due to its direct applicability (Article 288, Treaty on the Functioning of the European Union)[28] into national law without the need for national rules. In other words, it has a direct effect and prevails, thanks also to the primacy of EU law, over any contrary national regulations.[29]

2.4. The New GDPR Regulatory Framework

European Union Regulations produce a direct legal effect; consequently, MS are not required to transpose them into their national legal order. By providing a uniform set

[26] Luke Danagher, 'An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data? (2012) 3(3) *European Journal of Law and Technology*.

[27] Paul. M. Schwartz, 'The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures' (May 2013) 126(7) *Foreign & Comparative Law* 1966–2008.

[28] According to the criteria of *Van Gend en Loos*.

[29] C. Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law' (6 February 2012) *Bloomberg BNA Privacy and Security Law Report* 1–15.

of rules, the GDPR creates a coherent framework and largely achieves balanced data protection across the geographical boundaries of the EU, crystallising an environment of legal certainty from which economic operators and individuals can benefit as 'data subjects'.

In Cyprus, as part of the qualitative upgrading of key individual rights, a reference was added to the preamble of the Constitution in 2016, referencing Article 8(2) of the European Convention of Human Rights (ECHR) and mentioning the introduction of an additional exception to the right to privacy. Regarding the implementation of the GDPR, on 31 July 2018, the Law on the Protection of Natural Persons Against the Processing of Personal Data and the Free Movement of such Data was published in the Official Gazette (Law 125(I)/ 2018). Its purpose was implementing provisions of the GDPR, which affords MS a degree of discretion.[30] It should be noted that in 2018, a Parliamentary Legal Committee report on the above law made a reference to the EU Charter of Fundamental Rights (EUCFR). The President of the Republic had returned the draft law to the House of Representatives for reconsideration. Certain provisions were found to be incompatible with the Charter and were therefore removed from the draft.[31] In particular, the initial bill (as formulated by Parliament) did not fully define *who* could lawfully process personal data. According to the President of the Republic, this made the law problematic because it conflicted with the letter and spirit of the GDPR, on which it was based.

The GDPR is a notably dense and complex legal text (consisting of 99 articles and 173 recitals in the preamble) that attempts to cover all cases of data processing. However, the continuous evolution of technology, as well as political and economic relations, requires a continuous updating—or, more correctly, crystallisation—of the regulatory framework to ensure a high and uniform level of protection in data processing among MS. For this reason, the GDPR established the European Data Protection Board (EDPB), an independent EU body tasked with coherently applying data protection rules throughout the EU and facilitating cooperation between the data protection authorities of MS.[32] The EDPB has the competence to issue general

[30] Consequently, with the entry into force of the provisions of Law 125(I)/2018, the Personal Data Processing (Protection of the Individual) Laws of 2001 to 2012 were repealed.

[31] FRA, The EU Charter of fundamental rights in Cyprus, available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-eu-charter-in-cyprus_en.pdf (last accessed 28 April 2025).

[32] The EDPB is based in Brussels and replaces the Article 29 Working Group of Directive 95/46/EC. It is composed of representatives of the national data protection authorities and the European Data Protection Supervisor (EDPS). The European Commission is entitled to participate without voting rights in the activities and meetings of the EDPB.

guidance documents[33] (including guidelines, recommendations, and best practices) to clarify EU legislative acts concerning data protection, thus clarifying rights and obligations to stakeholders.[34] The body can also issue binding decisions on national supervisory authorities to ensure consistent implementation. The EDPB launched a coordinated enforcement framework (CEE) action for 2024, an initiative to implement right of access, which will involve 31 data protection authorities (DPAs) across the European Economic Area.[35]

2.5. The Role of the Data Commissioner

The GDPR has maintained and to some extent upgraded the role and powers of the Cypriot independent data protection authority.[36] The Cypriot Data Commissioner has issued guidelines and recommendations on the following: commercial promotions, public administration, labour relations, banking and financial transactions, camera surveillance systems, the insurance sector, the provision of health services and especially biometric data, academic research, education, the internet and wider technological developments, mass media, social media, and local authorities.[37] The Commissioner has proven to be particularly proactive, updating instructions or giving opinions and issuing notices even on somewhat unusual or particularly complex cases (e.g. consent in the context of direct marketing, renaming of Facebook groups / pages, announcements in relation to existing transmission licenses, etc.). Adherence to duty is clearly viewed as crucial, as it effectively ensures a higher level of personal data protection institutionally. Dedication to duty and efficiency are not self-evident, given that the Data Commissioner is part of the administrative structure and must therefore deal with the chronic dysfunctions of 'traditional' State institutions as well as frequent cases of wrong civil servant mentality. For example, its Greek counterpart

[33] E.g. 'Guidelines 2/2023 on Technical Scope of Art. 5(3) of e-Privacy Directive', 'Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)', 'Guidelines 01/2022 on data subject rights – Right of access', '*EDPB Best practices for the organization of EDPB Plenary meetings*' etc., all available at: https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en (last accessed 28 April 2025).

[34] Shervin Nahid, *'Data Protection and Compliance*' edited by Stewart Room, BCS Learning & Development Limited (2021) ProQuest Ebook Central, p. 189.

[35] Howard, R. Jason '*EDPB begins coordinated privacy enforcement*' (2024) Cybersecurity Policy Report, 1.

[36] The mission and competences of the Commissioner are described in Articles 57 and 58 of the GDPR as well as in Articles 24 and 25 of Law 125(I)/2018.

[37] A list of the most important instructions of the Commissioner is provided below the references.

(the HDPA) unfortunately never managed to live up to the expectations and the great challenges it faced.

The Commissioner can intervene in a regulatory capacity as well as impose civil and administrative sanctions. The legality and proportionality of these penalties can be brought on an ad hoc basis before the Administrative Court.[38] According to Article 28 of Law 125(I)/2018, 'every natural or legal person has the right to appeal against a decision of the Commissioner before the Administrative Court'. The right to appeal against a decision by the Commissioner is, however, only granted if the latter has caused moral or material damage.[39]

Things are more complicated in practice, with cooperation between the Commissioner and the institutions remaining problematic. In fact, in a recent discussion of the Office's budget in the Parliamentary Finance Committee, the Commissioner expressed concern about the incorrect use of the personal data protection framework in cases where transparency issues may arise. The Commissioner's Office is permanently understaffed, while the Commissioner's request to recruit staff through special examinations has not moved forward.[40]

3. The Review of the Sanctions Imposed Through Current Jurisprudence

The Data Commissioner in Cyprus must hold the same qualifications as a Supreme Court judge (Article 19(2) of Law 125(I)/2018). This means appointees are well acquainted with legislation and the administrative procedures alike. The decisions of the Commissioner are nevertheless frequently annulled, a fact that has a negative effect on both legal certainty and the proper observance of GDPR principles regarding effective data protection. The reasons are many and varied and may be found in the systemic administrative shortcomings and dysfunctions as well as the national culture towards privacy. The pathologies of the administrative mechanism tend to become ingrained, while Cypriot society remains a predominantly traditional society

[38] Breikot Management LTD v. Republic through Personal Data Protection Commission, Case no. 962/2019, 16/12/2022.

[39] T.A. v Republic through Personal Data Protection Commission, Case No. 1612/2019, 21/08/2023.

[40] Sigmalive.com, 'The Personal Data Protection Authority is seeking personnel with special exams' (04 November 2024) available at https://www.sigmalive.com/news/local/1253809/prosopiko-me-eidikes-eksetaseis-zita-i-ep-prostasias-prosopikwn-dedomenon [in Greek] (last accessed 28 April 2025)

that finds it difficult to understand and assimilate the more specific aspects of privacy, as they develop and evolve through technological progress.

However, perhaps most crucial of all is the Commissioner's potential lack of expertise. The legislation does not require candidates for Data Commissioner to have expertise either in data protection law, or in EU law, or even in administrative law, the fundamental principles of which apply in all its administrative actions and when imposing sanctions. The volatility of the data protection regulatory framework, combined with the complexity of the cases brought before it, make it more than imperative that the Data Commissioner is specialised in personal data protection law and technology regulation. The effectiveness of the Data Commissioner's task has a direct impact on the level of protection of citizens' rights as well as on the day-to-day business of companies and will thus play a significant role in the success of the GDPR.[41] It is therefore also important to acknowledge and highlight the need to ensure that DPAs possess adequate human and financial resources to successfully carry out their mission.[42]

An interim decision held that the applicant had been deprived of documents essential to the support of his case:

> The purpose of Article 61(1) of Regulation (EU) 2016/679 [...] is to provide information and mutual assistance so that the Regulation is implemented and applied in a coherent manner [...] The subject who appeals to justice must have the same weapons in presenting and arguing his case as the administration had when investigating the case before it. Potentially, an element that the administration investigated but ultimately decided not to rely on is evidence that helps the case of the administrator and thus, its non-disclosure effectively deprives him of the opportunity for a fair trial (Article 6 (1) ECHR).[43]

In another case, the challenged decision imposing a fine was annulled due to improper provision to the applicant of the right to be heard on all the elements of the

[41] Andra Giurgiu & Tine A. Larsen, 'Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?' (2016) 2(3) *European Data Protection Law Review* 352.

[42] FRA, 'Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)' (2010), p. 50, available at: https://op.europa.eu/en/publication-detail/-/publication/994e9977-d4c7-4f28-8221-9e10f916e330/language-en (last accessed 23 September 2025)

[43] LGS Handling LTD & Ors v Republic through Personal Data Protection Commission, Case No. 14/2020, 10/1/2022.

case; more specifically, the administration did not notify the applicant of the complaint or offer it for inspection, as required, before the applicant was found liable or sentenced.[44]

A recent ruling held that the Commissioner's decision had been made under legal and factual error, without due investigation or reasoning. The Commissioner:

> accepted that the applicants' processing of the complainant's data was lawful, and that there was no evidence to prove that the person who, according to the complainant's claim, disseminated his data, had gained access to his personal file. On the contrary, this person was demonstrably not present at the contested session of the applicants in which reference was made to the complainant's data. However, he arbitrarily concluded that the applicants had breached their obligations.[45]

Another decision also follows the same lines, according to which the Commissioner:

> did not investigate the origin of the information but contented himself with generalizing the applicant's status as a politically exposed person. Even such a person, however, is not exempt from the protection provided by the Law. Therefore, the decision suffers from lack of due research and erroneous interpretation of the law and the facts.[46]

Finally, a decision from 2024 focused on both the error of the Commissioner and his failure to conduct an adequate investigation: 'Before arriving at the final decision, the Commissioner should have clarified the contradictory positions of the applicants to clarify the actual conditions of application of the processing'.[47]

4. The Particularities of National Data Protection Law

The GDPR harmonises data protection rules throughout the EU and is directly and consistently applicable in all MS. Cyprus enthusiastically welcomed the new era of

[44] Arctinos Publications LTD v Republic through Personal Data Protection Commission, Case No. 92/2019, 3/2/2022.

[45] Municipality of Strovolos v Republic through Personal Data Protection Commission, Case No. 1596/2018, 17/5/2022

[46] B.G. v Republic through Personal Data Protection Commission, Case No. 95/2020, 26/10/2023.

[47] LGS Handling LTD et al. v Republic through Personal Data Protection Commission, Case No. 14/2020, 23/1/2024.

data protection. In fact, it was one of the leading MS in imposing fines during the first year of application of the Regulation.[48]

It must be noted that the GDPR is in fact the result of a compromise between politicians and powerful business interests in the technology and IT sectors. For this reason, according to recital 10,[49] MS are afforded some leeway to maintain or introduce national provisions to further determine the application of the data protection rules established by the GDPR or to adapt more specific rules in certain fields; perhaps the most salient of these is data protection in labour relations.[50] The GDPR contains 'opening clauses'[51] that allow MS to further specify its application in these areas—these specifications are commonly used in 'harmonization measures of EU secondary law'[52] as a compromise to facilitate political agreement on the law.

The GDPR allows MS to establish targeted rules in specific areas to ensure an effective level of data protection while respecting political, social, and economic particularities. Cypriot legislation has few such variations. Some are considered necessary either for the proper functioning of institutions (e.g. in data processing in the courts, or to protect the public interest), or for the proper functioning of the market (e.g. processing the data of minors). Others, however, are considered problematic or, rather, disproportionate in relation to the intended purpose (e.g. data of fire department employees, large-scale data interconnection). To date, the compatibility of national regulations with the GDPR has not (yet) been subjected to judicial review; this is likely imminent, especially for the consent of minors and the databases of security forces (the police and fire departments).

[48] Catherine Barrett, *'Emerging trends from the first year of EU GDPR enforcement' (2020) Chicago*: American Bar Association. 16(3): 24.

[49] 'This Regulation does not exclude Member State law that sets out the circumstances for specific processing situations, including determining more precisely the conditions under which the processing of personal data is lawful'.

[50] Halefom H. Abraha, 'A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace' (2022) 12(4) *International Data Privacy Law* 277.

[51] For a complete list of the opening clauses found throughout the GDPR, see Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Cham, Switzerland: Springer International, 2017) 220.

[52] Emilia Miscenic & Anna-Lena Hoffmann, 'The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)' (2020) *EU and comparative law issues and challenges series (ECLIC)* 51

4.1. Court Proceedings

Article 55(3) of the GDPR excludes the competence of national DPAs to supervise data processing performed by courts.[53] This is not the case under Cyprus law. Perhaps Cypriot legislators did not specify on the matter intentionally, as there is a relevant rule in the Regulation. However, this gives rise to a practical issue. As Cypriot law is silent on the matter, this supervision falls de facto under the competence of the DPA. Having noted this deficiency, the Supreme Court temporarily suspended the publication of court decisions pending the introduction of a legislative framework implementing the obligations imposed under the GDPR. The Court also formulated several proposals to ensure compliance with Article 55(3) of the GDPR. Finally, the Supreme Court (with a circular dated 19/07/2018)[54] regulated the pending issues of harmonising the publication of decisions with the GDPR: The decisions intended for publication/editing on the internet would be published with reference only to the surnames of natural person parties without reference to any other personal identifiers and especially without reference to pseudonyms.

4.2. Public Interest

Data controllers may process individuals' personal data in public interest cases (e.g. tax, banking, police, etc.). Other than being necessary for the performance of a task carried out in the public interest, this processing must have a (national or EU) legal basis or be within the scope of exercise of official authority vested in the data controller. According to Cypriot law:

> the processing of personal data which is vested by virtue of a Decision of the Council of Ministers to a public authority or body for the performance of a task carried out in the public interest or in the exercise of official authority shall be performed lawfully and fairly, in a clear, precise and transparent manner in relation to the data subject, in accordance with the provisions of Article 5(1), point (a) and Article 6(1) point (e) of the Regulation.[55]

[53] However, in an important decision (Judgment of 02/03/2023 - Norra Stockholm Bygg Case C-268/21), the CJEU ruled that the GDPR applies to civil proceedings before national courts, including court orders to produce documents containing personal data as evidence.

[54] The circular is available at https://www.cyprusbarassociation.org/files/ANNOUNCEMENTS/2018/egkyklios_125.pdf

[55] Article 7 of Law 125(I)/2018.

The term 'lawfully' signifies that there must be a written rule of law that defines or allows the specific processing for the purposes of public interest. On the other hand, the 'qualitative elements' of the processing, i.e. whether the required level of protection is met, should be judged on a case-by-case basis.

4.3. Children's Consent

According to the EDPB consent guidelines,[56] persons aged 16 and above can provide consent. For those below the age of 16 (children), the data controller must request consent from a parent or legal guardian. However, the Cypriot provision sets the age bar lower:

> When the offering of information society services directly to a child is based on the child's consent, the processing of personal data shall be lawful where the child is at least fourteen (14) years old. For a child younger than fourteen (14) years old, the processing of personal data referred to in subsection (1) shall be lawful when consent is given or authorized by the holder of parental responsibility over the child.[57]

Based on recent data, a third of GDPR fines for social media platforms are linked to the protection of children's data.[58] This finding highlights the extent to which children's online activity is vulnerable to abuse. Cyprus should therefore bring the regulatory framework up to at least the standards of the EDPB.

4.4. Genetic and Biometric Data

The GDPR is the first to provide a definition of genetic data. Article 4(13) defines it as:

> the personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.[59]

---

[56] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020.

[57] Article 8 of Law 125(I)/2018.

[58] Ioanna Lykiardopoulou, 'A third of GDPR fines for social media platforms linked to child data protection' (*The Next Web*, 8 November 2023), available at: https://thenextweb.com/news/gdpr-fines-social-media-platforms-child-data-protection (last accessed 23 September 2025).

[59] Law 125(I)/2018 states: '"genetic data" shall mean personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the

Genetic data contains unique information about the data subjects and their blood relatives, highlighting the importance of privacy protection.[60] The processing of genetic data must be subject to stricter rules, since it may expose core aspects of an individual's identity (ethnic and/or racial origin, state of health, sexual life, etc.). However, by making an artificial distinction between various categories of biometric data through the use of automated data processing methods, out of respect for fundamental rights and freedoms, the GDPR fails to provide clear rules and much-needed protection.[61]

Considering the danger posed by the processing of this type of data, special regulations were introduced to establish additional safeguards and limit the risk. The Cyprus legislature focused on the processing of genetic and/or biometric data in the context of commercial practices.[62] Furthermore, the new rules on labour regulations stipulated that the processing of employees' biometric data must be necessary (e.g. for security reasons, in the case of employees working in high-risk/high-security areas such as ports, airports, military installations, etc.). If employees have provided consent for the collection and processing of their biometric data, but the process is deemed not to be necessary, the consent in no way remedies the illegality.[63] On a related note, Article 9(1) of Law 125(I)/2018 prohibits the processing of genetic and biometric data for purposes of health and life insurance. These stricter rules are specific to Cyprus, given that the GDPR does not prohibit this processing for life or health insurance purposes.[64]

---

health of that natural person and which result from an analysis of a biological sample from the natural person in question'.

[60] Mahsa Shabani & Pascal Borry, 'Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation' (2018) 26 *European Journal of Human Genetics*.

[61] Els J. Kindt, 'Having yes, using no? About the new legal regime for biometric data' (June 2018) 34(3) *The computer law and security report* 538.

[62] An Administrative Court Decision (Sub. No. 1930/2012) dated 19/05/2017 ratified the Commissioner's Decision dated 02/10/2012, which mandated a private hospital to stop collecting and processing biometric data (and delete any data already collected/processed) through their fingerprint scanning system. The system was used to monitor hours worked. The Commissioner's Decision was based on the principle of proportionality—a fundamental rule of lawful processing. The Court ruled that the operation of a system to monitor working hours constituted a disproportionate interference in private life.

[63] Data Protection Commissioner, Opinion 2/2018, p. 3.

[64] A complaint was filed against an insurance company by a complainant who claimed that her gynaecological exam (Pap test) claim was denied on the grounds that she would have to provide the result of the exam for the company to assess her claim. With the intervention of the Commissioner, the insurance company ultimately re-evaluated the complainant's claim and paid her the corresponding compensation, without requiring the submission of any examination results. Commissioner's annual report (2020) 68.

Also, where the processing of genetic and biometric data is based on a data subject's consent, the further processing of such data requires further consent. The introduction of stricter requirements for processing genetic data seems appropriate in Cyprus, in view of heightened concerns regarding potential misuses of genetic data, which could result from increased availability of said data.

Cypriot legislation also contains certain provisions that seem incompatible with the protective framework of the GDPR (especially the principles of Article 5, with an emphasis on lawfulness, minimisation, and proportionality). These provisions are found in the regulatory framework that governs the operation of the security forces (police and fire services) and mandate the collection of genetic material from new recruits. The regulation states:

> upon recruitment, each Member is photographed, and their genetic material and fingerprints are taken, which are kept in a separate file of the Fire Department, maintained in accordance with the Law on the Protection of Natural Persons Against the Processing of Personal Data and the Free Movement of Such Data, for service purposes. A Member's photograph, genetic material and fingerprints and all copies and related records are erased upon leaving the service, unless the Member is under criminal or disciplinary investigation or prosecution at the time.[65]

In principle, this regulation initially formed part of the measures to prevent and address corruption in the police,[66] but were subsequently also adopted by the fire service.[67] The contested regulation expressly states that the data collection and processing framework is governed by Law 125(I)/2018, i.e. by the GDPR, but does not reflect its fundamental provisions.

First, the collection of data is based on service purposes, albeit not restrictively defined in advance, pursuant to Article 5(2): 'Personal data shall be collected for specified, explicit and legitimate purposes'. Official reasons must be specified, as the prevention and prosecution of criminal offenses is excluded from the scope of the GDPR Also, according to Article 9(2) I of the GDPR, the processing of genetic and bi-

[65] Regulatory administrative act 196/2021 for the Police and 462/2017 for the Fire Brigade.

[66] Advisory report on the Establishment and Operation of the Police Internal Audit Service Law of 2017 (currently Law 3(I)/2018)

[67] Before becoming autonomous, the fire service operated under the legislation governing the police. The legislation which now governs the fire service is distinct, but nevertheless identical to that of the police.

ometric data is allowed (among others) for reasons of public interest. These reasons, however, must be further specified and delimited, which is not the case here.

The collection and processing of genetic material also requires a Data Protection Impact Assessment (DPIA) (see GDPR Article 35). In this case, however, the relevant explanatory reports submitted to Parliament before the ratification of Administrative Act 462/2017 show that no DPIA meeting GDPR standards was submitted.[68] Of course, without the DPIA, the necessity and in particular the proportionality of the processing cannot be assessed and evaluated. In fact, rather bafflingly, the questionnaire/impact analysis even mentioned that the entry into force of the act would positively affect foreign investments. The Commissioner welcomed the disputed arrangements and expressed no reservations about the creation of the above files and their compatibility with GDPR requests.[69] In none of the annual reports did the Commissioner mention participation in the consultation (while doing so for other legislation), despite being expressly required to by the law (GDPR Article 11(2)), as it concerns the processing of genetic data, i.e. data that carries serious risks for the data subjects involved.

The wording of the regulatory framework makes it clear that the measure in question was adopted for ambiguous reasons. It is difficult to understand how it assists in attracting investments and this clause should probably not be taken seriously. Furthermore, it is questionable whether the fight against corruption is effectively served through the processing of a special category of personal data (biometrics). While the collection of personal data is an effective means of deterring repeat offenders, in this case, the data belongs to police and fire service professionals. As such, the prevention purpose served by recording of this special category of personal data is presumptive and markedly uncertain. Therefore, this regulation clearly contradicts both the principle of legitimacy of purpose, since it does not specify with the necessary clarity the reason for the creation of the file in question, as well as the principles of proportionality and limitation of the storage period (GDPR Article 5(1), (3), and (5)).

The law reveals a certain ambiguity: Are the rules applicable to the subsequent use of all personal data under the GDPR? Or are they limited to the subsequent use

[68] DPIA is a comprehensive description of the envisaged processing operations and the purposes of the processing, assessment of the necessity and proportionality of the processing operations in relation to the purposes, assessment of the risks to the rights and freedoms of data subjects and the measures envisaged to address the risks.

[69] Report of the Parliamentary Legal Committee 10.

of 'police or criminal justice' data?[70] The above data collection and processing should be subject to the proper regulatory framework, i.e. Directive 2016/680—more widely known as the Law Enforcement Directive (LED)—on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences, which has been transposed into national legislation with Law 44(I)/2019. This gives rise to the following paradox: A file with a special category of personal data is created for the purposes of combating corruption, which, however, does not fall within the regulatory framework of the LED, but of the GDPR, although the latter excludes from its regulatory framework the collection and processing for the purposes of preventing and suppressing crime. This is an obvious interpretative error by the legislator that needs immediate correction because the LED establishes different rules both in terms of the lawfulness of the processing and the rights of the data subject.[71] In the case of this specific file, the data collected and processed for purely official purposes is (or should be) included in the provisions of the GDPR, while the data collected and processed for the purposes of preventing and suppressing criminal offenses is included in those of the LED. However, this once again raises the issue of violation of the principle of proportionality because the data is collected preventively, with the aim of being used in a potential criminal investigation.[72]

4.5. Merging Large-Scale Filing Systems

The GDPR itself does not define what constitutes 'large-scale'. The Article 29 Working Party Guidelines on whether processing is 'likely to result in a high risk' for the purposes of the GDPR regarding 'data processed on a large scale'[73] state that 'the GDPR does not define what constitutes large-scale, though recital 91 provides some

[70] Catherine Jasserand, 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?' (2018) 4(2) *European Data Protection Law Review* 152.

[71] Due to the specificity of the scope of the LED, some rights included in the GDPR are not found in the Directive (e.g. the right to portability) or may be subject to limitations (e.g. right of access).

[72] See, Taner Kuru, 'C-205/21 VS v Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost: Indiscriminate and Generalised Collection of Biometric and Genetic Data by Law Enforcement Authorities in the EU Is Not Allowed' (2024) 10(2) *EDPL* 223 – 231; Supreme Court, first instance jurisdiction, Application No. 7/2024, 23.01.2024.

[73] WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679', available at https://ec.europa.eu/newsroom/article29/items/611236/en (last accessed 28 April 2025)

guidance'.[74] The increase in the volume of data that public authorities, businesses, and researchers handle nowadays is a consequence of technological advances, including cloud computing, the internet of things (IoT), and machine learning, as well as improvements in computational power and lower data storage costs.[75] The importance of adopting adequate legal protection for data subjects, especially when using individual-level genomic data, has been stressed in view of increased data sharing, for example, linking files for the purpose of ensuring public order, or for research purposes, for example, identification of potential correlations between diseases and underlying genetic factors.[76]

Under Cypriot law (Law 125(I)/2018, Article 10), public authorities or bodies are permitted to merge their large-scale filing systems, but only for reasons of public interest (a definition that is up to the State).[77] Wherever the merging relates to special categories of personal data or to personal data relating to criminal convictions and offences, or is to be carried out with the use of identity card numbers or any other identifiers of general application, it must be preceded by a DPIA and a prior consultation with the Commissioner, who is in charge of the manner in which the systems are merged.[78] The merging of filing systems as provided by Cypriot law is not a particularity,[79] but rather a social imperative based on the wide discretion that the GDPR

[74] Under recital 91, 2nd sentence, 'A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons…following the processing of special categories of personal data…or data on criminal convictions and offences…'.

[75] Ines Ortega Fernandez, Sara El Kortbi Martinez & Lilian Adkinson Orellana, 'Large Scale Data Anonymisation for GDPR Compliance', in John Soldatos & Dimosthenis Kyriazis (eds), *Big Data and Artificial Intelligence in Digital Finance* (Cham, Switzerland: Springer, 2022) 327.

[76] Bartha Maria Knoppers, 'Framework for responsible sharing of genomic and health-related data' (2014) 8(3) *The HUGO Journal*.

[77] 'Large scale data' is not a standard term; it can be associated with data that grows to a huge volume over time and is held by conventional data warehousing solutions. On the other hand, according to the Guidelines on the protection of individuals regarding the processing of personal data in a world of Big Data, T-PD (2017)01 of the Convention 108 Advisory Committee, big data is the growing technological ability to collect, process and extract new and predictive knowledge from great volume, velocity, and variety of data.

[78] In 2019, 14 DPIAs were submitted for consultation to the Commissioner in accordance with Article 10 of Law 125(I)/2018, for the merging of IT systems owned by public authorities, of which 12 were processed. Commissioner's annual report (2019) 147. A list of approved file associations is provided on page 148.

[79] Christiana Markou, 'Cyprus: A Look into the Law for the Effective Application of the GDPR Reports: GDPR Implementation Series' (2019) 5(3) *EDPL Review* 396.

assigns to MS to regulate issues related to sensitive areas of their national politics (e.g. policing, provision of health services, social policy etc.).

5. Conclusion

The right to the protection of personal data emerged almost 50 years ago as a special aspect of privacy requiring protection beyond traditional legal instruments.[80] Today, the protection of personal data has evolved into an independent fundamental right enshrined in EU primary law.[81] The GDPR harmonises law among EU MS, strengthening the common market while simultaneously protecting individual rights. For most MS that had not enacted corresponding national legislation (like Cyprus), data protection is a right provided to its citizens through accession to the EU.

The landscape of data protection and privacy laws in Cyprus is poised for significant transformation driven by the rapid evolution of technology, emerging cybersecurity threats, and a changing societal perspective towards individual privacy. As we advance further into the digital age, the necessity for robust regulatory frameworks that can adapt to these advancements will become increasingly critical.[82] Despite its small size, Cyprus has established itself as an international business hub, attracting foreign investment and corporate headquarters. Cyprus' status as an EU MS is an asset that, within the increased infrastructure interconnectivity of the post-pandemic era, can enable a rapid and integrated growth.[83] In this light, ensuring a high level of data protection is crucial, both for the development of the national economy (which must remain attractive for investment) and for the safeguarding of data subjects' individual rights. The Data Commissioner's annual reports confirm the satisfactory implementation of the EU regulatory framework. Certain irregularities in need of addressing are observed at the national level, in regulations established within the scope of discretion granted by the GDPR to the MS. In particular, the regulatory framework requires clarification regarding the delimitation of the public interest and

[80] The first national law for the protection of personal data was the Swedish '*Datalagen'* of 11 May 1973.

[81] Article 8 of the Charter of Fundamental Rights of the EU.

[82] Generis Global, 'Understanding Data Protection and Privacy Laws in Cyprus', available at https://generisonline.com/understanding-data-protection-and-privacy-laws-in-cyprus/ (last accessed 25 April 2025).

[83] Effie Theodoropoulou, 'Cyprus: A New, Evolving Energy Center or Possibly Hub for the European Union in the Eastern Mediterranean' (Master thesis, University of Piraeus, March 2022), available at: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/14326/Theodoropoulou.pdf?sequence=3&isAllowed=y (last accessed 23 September 2025)

more protection regarding the consent of minors. As for the processing of special categories of data based on corruption prevention policies, the legality of the measure should be examined considering the current Court of Justice of the European Union (CJEU) and European Court of Human Rights (ECtHR) case law. This is because the legitimate purpose is not always compatible with fundamental principles of personal data law, such as purpose limitation and proportionality.

In practice, numerous complaints from citizens have accumulated over time. The complaints cover the spectrum of social, political, and economic activity and concern data controllers from the private and public sectors alike. Arguably, this is because controllers or processors have been poorly informed about their duties and obligations, or the adaptation to the requirements of the GDPR has been inconsistent. The Data Commissioner plays a crucial role in this, as they supervise the implementation of the GDPR and can impose sanctions. Ultimately, Cyprus has been faster and more effective in ensuring data protection than other, more experienced countries. This, of course, does not mean that there is no room for improvement.

In addition to issuing opinions and guidelines, the Data Commissioner must prepare standard compliance policies for the standard cases of data processing (e.g. banking institutions, private and public hospitals, internet applications, etc.) and undertake deeper public outreach initiatives. To effectively perform the role of data protection guardian, the Data Commissioner must have scientific and practical knowledge of the subject and be able to monitor developments and rise to the challenges. This is particularly important as the 'conventional' protection of personal data seems easy compared to the tectonic shifts and major challenges associated with AI, for which the EU is widely viewed to be ill-prepared. Consequently, the position of the Data Commissioner must be upgraded both institutionally (harmonious cooperation with political authorities) and substantively (adequate human and other resources).

The institutionalisation of data protection at the EU level affords individual MS limited legislative and administrative flexibility. But even despite the rigidity of EU law, the little flexibility it affords can prove significant. Cyprus, as a member of both the EU and the Commonwealth of Nations, has a domestic legal framework that resembles a colourful mosaic, an amalgam of different legal traditions. The national legislator must therefore take advantage of this unique legal culture and institutionally assimilate best practices, on the one hand to maintain the country's status as an

attractive investment destination[84] and, on the other, to safeguard at-risk individual rights.

Regarding the future, the cataclysmic changes brought about by AI are sure to pose new challenges to maintaining a high level of data protection.[85] At this early stage, it is unclear whether the AI Act will be as pivotal an international benchmark for shaping AI regulation as the GDPR has been for data protection. GDPR will continue to apply to the processing of personal data in the context of AI technologies. However, the AI Act also seems to build on some of the principles under the GDPR and, in practice, the two regimes and their respective requirements coexist. It is therefore important for 'providers' and 'developers' of AI systems to understand the interplay between these two pieces of legislation. Due to its small size, Cyprus may be an ideal ecosystem for practical implementation and interactive control of AI and personal data. Therefore, the experiences of the Cyprus model can optimise legislation and good practices in a field that is constantly evolving. Moreover, Cyprus is trying, I think successfully, to meet the requirements of EU law, something it did in the case of the AI Act.[86]

The accession of Cyprus to the EU was undoubtedly a key moment in the modern history of the island. At a purely legal level, the national regulatory framework was essentially restructured to align with the requirements of the common market. Concurrently, it provided an impetus for 'maturation' and enrichment in the field of fundamental rights. Some individual rights might never have been established without an EU-imposed obligation,[87] while others would certainly have been established at some point independently of EU membership. The right to the protection of personal data

[84] Invest Cyprus, an independent, government-funded entity, aggressively promotes investment in the traditional shipping, tourism, banking, and financial and professional services sectors. Newer sectors for Foreign Direct Investment (FDI) include energy, film production, investment funds, education, research & development, information technology, and regional headquartering. U.S. Department of State: 2023 Investment Climate Statements: Cyprus, available at https://www.state.gov/reports/2023-investment-climate-statements/cyprus/

[85] Alkistis Kostopoulou, 'Artificial Intelligence and Personal Data: Topical Issues on the Occasion of the EU AI ACT' (MA thesis, University of Piraeus, 2022) 56; Ronald Leenes & al. (eds.) *Data protection and privacy: the age of intelligent machines* (Oxford, UK: Hart Publishing, 2017).

[86] Deputy Ministry of Research, Innovation and Digital Policy, Press release of 6.11.2024, First milestone for the implementation of Regulation (EU) 2024/1689 on Artificial Intelligence in Cyprus, available at https://www.gov.cy/dmrid/en/uncategorized/first-milestone-for-the-implementation-of-regulation-eu-2024-1689-on-artificial-intelligence-in-cyprus/ (last accessed 30 April 2025).

[87] CJEU, Case C-55/18, *Federación de Servicios de Comisiones Obreras (CCOO) v. Deutsche Bank SAE*, judgment 14.05.2019. Member States must force employers to implement a system of measuring the daily working time of each employee.

is undoubtedly one of the latter. The participation of Cyprus in the EU does not determine the existence, but rather the quality of the protection, i.e. the protective scope of the right. Maintaining and strengthening the common market require reasonable compromises. Practically speaking, data subjects and technology companies have an inherently unequal relationship. The power of modern-day technological giants exceeds that of States. In this light, the adoption of rules at the EU level helps MS to look oligopolies in the eye,[88] oppose their demands, and ultimately defend threatened individual liberties, following the idiom 'many hands make light work'. In the case of Cyprus, considering its size, together with the structure of its economy (headquarters of corporate giants), personal data is protected far more effectively through its participation in the EU *acquis*.

References

Abraha H., *'A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace*' (2022) International Data Privacy Law, 12(4): 276-296.

Aldhouse F., '*Data protection in Europe – Some thoughts on reading the academic manifesto*', Computer Law & Security Review (2013) 29(3): 289-292.

Auby J-B, '*Remarques Terminales*' {Terminal Remarques} in Revue Française de Droit Administratif (2010), 5: 931.

Barrett C., *'Emerging trends from the first year of EU GDPR enforcement*' (2020) Chicago : American Bar Association. 16(3) : 22-25.

Burri M., Schär R., *'The Reform of the EU Data Protection Framework : Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy*', Journal of Information Policy (2016) 6: 479-511.

Butarelli G, '*Forefront*' (2020) in The EU General Data Protection Regulation (GDPR) A Commentary, Ch. Kuner, Lee A. Bygrave, Ch. Docksey (eds), Oxford University Press.

Danagher, L., *'An Assessment of the Draft Data Protection Regulation: Does it Effectively Protect Data?*' (2012) European Journal of Law and Technology, Vol. 3(3).

Dommett K., '*Data-driven political campaigns in practice: understanding and regulating diverse data-driven campaigns*', Internet Policy Review (2019) 8(4).

Emilianides A., '*Constitutional Law in Cyprus*' (2024) 3nd ed. Wolters Kluwer.

[88] Edith Hancock, 'The EU's uphill battle against Big Tech power' (*Politico* 6 March 2024), available at https://www.politico.eu/article/the-eus-uphill-battle-against-big-tech-power/ (last accessed 25 April 2025).

Fernandez I.O, Kortbi M, Adkinson L, '*Large Scale Data Anonymisation for GDPR Compliance*' in '*Large Scale Data 'Anonymisation for GDPR Compliance in Big Data and Artificial Intelligence in Digital Finance*' (2022), Springer: 325-336.

FRA, 'Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)' (2010), available at: https://op.europa.eu/en/publication-detail/-/publication/994e9977-d4c7-4f28-8221-9e10f916e330/language-en (last accessed 23 September 2025)

Giurgiu A., Larsen T., *'Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?*', Roles and Powers of National Data Protection Authorities, European Data Protection Law Review (2016) 2(3): 342-352.

Goddard M., '*The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact*', International journal of market research (November 2017) 59(6): 703-705

Greenleaf G., '*The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*' (March 2012) International Data Privacy Law 2(2): 77-111.

Gutwirth, S. et al. (eds.) 'Data protection and privacy: the age of intelligent machines' (2017) Oxford [UK]; Hart Publishing.

Hillion C, *'EU enlargement: A legal analysis' in: Arnull A, Wincott D (eds) Legitimacy and Accountability in the European Union* (2002) Oxford: Oxford University Press: 401-419.

Hotaling A, '*Protecting personally identifiable information on the Internet: Notice and consent in the age of behavioral targeting'*, 16 CommLaw Conspectus 529 (2008): 529-565.

Jasserand C., '*Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?*' European data protection law review (Internet) (June 2018) Vol.4(2): 152-167

Jason H., '*EDPB begins coordinated privacy enforcement*' (2024) Cybersecurity Policy Report, 1.

Kindt E., '*Having yes, using no? About the new legal regime for biometric data*', The computer law and security report (June 2018), Vol.34 (3): 523-538.

Kiss A. & László Szőke G, '*Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation of Data Protection Regulation*', in S. Gutwirt et al (eds), Reforming European Data Protection Law, Law, Governance and Technology Series 20 (Springer 2015): 311-331.

Knoppers, B.M. '*Framework for responsible sharing of genomic and health-related data*' (2014) HUGO J 8(3): https://doi.org/10.1186/s11568-014-0003-1

Kostopoulou A., '*Artificial Intelligence and Personal Data: Topical Issues on the Occasion of the EU AI ACT*' (2022) Master Thesis, ProQuest Dissertations Publishing, p. 56.

Kuner C, *'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*', Bloomberg BNA Privacy and Security Law Report (2012) February 6, 2012: 1-15.

Kuru T, '*C-205/21 VS v Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s organiziranata prestapnost: Indiscriminate and Generalised Collection of Biometric and Genetic Data by Law Enforcement Authorities in the EU Is Not Allowed*', EDPL (2024) vol. 10(2): 223 – 231.

Lykiardopoulou, I, 'A third of GDPR fines for social media platforms linked to child data protection' (*The Next Web*, 8 November 2023), available at: https://thenextweb.com/news/gdpr-fines-social-media-platforms-child-data-protection (last accessed 23 September 2025).

Markou C., '*Cyprus: A Look into the Law for the Effective Application of the GDPR Reports: GDPR Implementation Series*', EDPL Review (2019), 5(3): 389-396

Miscenic E., Hoffmann A.-L., '*The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR)*' (2020) EU and comparative law issues and challenges series (ECLIC): 44-61.

Nahid S., *'Data Protection and Compliance*' edited by Stewart Room, BCS Learning & Development Limited (2021) 2nd ed. ProQuest Ebook Central, p. 189.

Nissenbaum H., *'A Contextual Approach to Privacy Online'*, Daedalus (2011) 140 (4):32–48.

Purtova N., '*Default entitlements in personal data in the proposed Regulation: Informational self-determination off the table … and back on again?*' (February 2014) Computer Law & Security Review, 30(1): 6-24.

Riga E., Dionysiou, K. *'Supremacy of EU law in Cyprus legal order*', Cyprus Mail, 30.06.2021.

Rotenberg M, *'On International Privacy: A Path Forward for the US and Europe*', Harvard International Review (Spring 2014), Cambridge 35(4): 24-28

Schwartz, P., '*The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*' (May 2013) Foreign & Comparative Law 126(7): 1966-2008.

Shabani, M., Borry, P. '*Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation'* (2018) European Journal of Human Genetic 26: 149–156 https://doi.org/10.1038/s41431-017-0045-7.

Theodoropoulou, E. '*Cyprus:* A New, Evolving Energy Center or Possibly Hub for the European Union in the Eastern Mediterranean' (Master thesis, University of Piraeus, March 2022), available at: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/14326/Theodoropoulou.pdf?sequence=3&isAllowed=y (last accessed 23 September 2025)

Voigt P., Bussche A., '*The EU General Data Protection Regulation (GDPR): A Practical Guide*' (2017) Springer International.

Main topics in which Cypriot data Commissioner adopted guidelines or addressed specific instructions:

- Directive 4/2017 for right of access of employees or candidates in the public section (only available in Greek).
- Opinion 1/2018 addressed to Trade Unions in relation to the notification by the employers of lists with names of employees, their salaries, and contributions (only available in Greek).
- Opinion 2/2018 on video surveillance at work and the use of biometric systems (only available in Greek).
- Opinion 1/2019 on the access to email accounts of employee and former employee (only available in Greek).
- Opinion 1/2020 on the supervision of long distance / online exams by higher education institutions (only available in Greek).
- Opinion 1/2022 concerning transmission of messages and placing of calls with political content / promotion of candidates (only available in Greek).
- Directions about retention periods for medical data (only available in Greek).
- Interpretation of Article 10 GDPR (only available in Greek).
- Data protection officers (DPO) Guidance.
- Data Protection Impact Assessments (DPIA) Guidance.
- Data transfers (only available in Greek).
- Records of processing activities.
- Video-surveillance (only available in Greek).
- Employment relations (only available in Greek).
- Personal data breach notifications.
- Codes of conduct and certifications mechanisms.
- Exercise of the right to access by public employees (only available in Greek).
- Processing and retention period of data by banking institutions.
- Direct marketing of goods and services.
- Use of the internet and mobile phones.