INDEX COPERNICUS INTERNATIONAL

№63
MARCH, 2026

ISSN 2710-3056

The issue of journal contains:

Proceedings of the X Correspondence International Scientific and Practical Conference

SCIENCE OF POST-INDUSTRIAL SOCIETY: GLOBALIZATION AND TRANSFORMATION PROCESSES

held on March 6th, 2026 by

NGO European Scientific Platform (Vinnytsia, Ukraine)
LLC International Centre Corporative Management (Vienna, Austria)

GRAIL OF SCIENCE
PERIODICAL SCIENTIFIC JOURNAL

ISSN 2710–3056

INTERNATIONAL SCIENTIFIC JOURNAL

GRAIL OF SCIENCE

№ 63 (March 2026)

with the proceedings of the:

X Correspondence International Scientific and Practical Conference

SCIENCE OF POST-INDUSTRIAL SOCIETY: GLOBALIZATION AND TRANSFORMATION PROCESSES

held on March 6th, 2026 by

NGO European Scientific Platform (Vinnytsia, Ukraine)
LLC International Centre Corporative Management (Vienna, Austria)

МІЖНАРОДНИЙ НАУКОВИЙ ЖУРНАЛ

ГРААЛЬ НАУКИ

№ 63 (березень, 2026)

за матеріалами:

X Міжнародної науково-практичної конференції

SCIENCE OF POST-INDUSTRIAL SOCIETY: GLOBALIZATION AND TRANSFORMATION PROCESSES

що проводилася 06.03.2026

ГО «Європейська наукова платформа» (Вінниця, Україна)
ТОВ «International Centre Corporative Management» (Відень, Австрія)

Вінниця – Відень, 2026

DOI 10.36074/grail-of-science.06.03.2026

ГРААЛЬ НАУКИ : міжнар. наук. журнал. – Вінниця : ГО «Європейська наукова платформа»; НУ «Інститут науково-технічної інтеграції та співпраці», 2026. – No 63. – 936 с.

Видання розраховане на науковців, викладачів, аспірантів, студентів, усіх, хто прагне отримати ґрунтовні знання теоретичного і прикладного характеру.

Рекомендовано до видання Вченою Радою Наукової установи «Інститут науково-технічної інтеграції та співпраці». Протокол № 8 від 05.03.2026.

Головний редактор: Танасійчук Альона Миколаївна, д-р. екон. наук, доцент (Україна)
Заступник головного редактора: Ємельянов Олександр Юрійович, д-р. екон. наук, професор (Україна)
Голова оргкомітету конференції: Голденблат Марія (Україна)
Заступник голови оргкомітету конференції: Рейчел Апаро (Австрійська Республіка)
Відповідальний секретар: Рабей Настасія Романівна (Україна)

ЧЛЕНИ РЕДАКЦІЙНОЇ КОЛЕГІЇ:
Квасницька Раїса Степанівна - д-р. екон. наук, професор (Україна); **Jakhongir Shaturaev** - канд. екон. наук, доцент (Республіка Узбекистан); **Заднєпровська Ганна Ігорівна** - канд. екон. наук (Україна); **Занора Володимир Олександрович** - канд. екон. наук, доцент (Україна); **Маркович Ірина Богданівна** - канд. екон. наук, доцент (Україна); **Яковенко Роман Валерійович** - канд. екон. наук, доцент (Україна); **Поливана Людмила Анатоліївна** - канд. екон. наук, доцент (Україна); **Гевчук Анна Вікторівна** - д-р. екон. наук, професор (Україна); **Маслій Олександра Анатоліївна** - канд. екон. наук, доцент (Україна); **Євтушенко Наталія Миколаївна** - канд. екон. наук, доцент (Україна); **Москвічова Олена Сергіївна** - канд. екон. наук, доцент (Україна); **Ясишена Валентина Валеріївна** - д-р. екон. наук, професор (Україна); **Михайлишин Лілія Іванівна** - д-р. екон. наук, професор (Україна); **Гавриленко Наталія Вікторівна** - канд. екон. наук, доцент (Україна); **Гіулі Гігуашвілі** - д-р. екон. наук, професор (Грузія); **Тамар Макасарашвілі** - д-р. екон. наук, професор (Грузія); **Мерабі Ванішвілі** - д-р. екон. наук, професор (Грузія).

НАУКОВІ КОНСУЛЬТАНТИ:
Онікієнко Сергій Володимирович - д-р. екон. наук, професор (Україна); **Marko Timchev** - д-р. екон. наук, доцент (Республіка Болгарія); **Khatuna Tabagari** - д-р. екон. наук, професор (Сакартвело); **Грень Лариса Миколаївна** - д-р. наук з держ. управління, професор (Україна); **Михаліцька Наталія Ярославівна** - канд. наук з держ. управління, доцент (Україна); **Ткаченко Павло Ігорович** - аспірант (Україна); **Купріянова Дарина Сергіївна** - практикуючий юрист (Польща); **Губаль Галина Миколаївна** - канд. фіз-мат. наук, доцент (Україна); **Козуб Галина Олександрівна** - канд. техн. наук, доцент (Україна); **Козьма Антон Антонович** - канд. хім. наук (Україна); **Морозова Тетяна Василівна** - канд. біол. наук, доцент (Україна); **Купріянова Лариса Сергіївна** - канд. мед. наук, доцент (Україна); **Лисенко Дмитро Андрійович** - канд. мед. наук, доцент (Україна); **Цубанова Наталя Анатоліївна** - д-р. фарм. наук., професор (Україна); **Олійник Світлана Валентинівна** - канд. фарм. наук, доцент (Україна); **Полєжаєв Юрій Григорович** - канд. наук із соц. ком., доцент (Україна); **Mukhabbat Khakimova** - д-р. пед. наук, професор (Республіка Узбекистан); **Куліченко Алла Костянтинівна** - д-р. пед. наук, доцент (Україна); **Фурман Тарас Юрійович** - канд. пед. наук, доцент (Україна); **Бажан Станіслав Миколайович** - д-р. філософії (Україна); **Ямполь Юрій Віталійович** - аспірант (Україна); **Антипова Жанна Ігорівна** - старший викладач (Україна); **Яцик Мар'яна Романівна** - канд. пед. наук, доцент (Україна); **Корбозерова Ніна Миколаївна** - д-р. філол. наук, професор (Україна); **Ковальська Наталя Аркадіївна** - канд. філол. наук, доцент (Україна); **Присяжнюк Оксана Ярославівна** - канд. філол. наук, доцент (Україна); **Мелех Галина Богданівна** - канд. філол. наук, доцент (Україна); **Корнус Анатолій Олександрович** - канд. геогр. наук, доцент (Україна); **Фомін Андрій Володимирович** - канд. іст. наук, доцент (Україна); **Рубан Микола Юрійович** - д-р. філос. з іст. та археології (Україна); **Гірна Наталія Мирославівна** - канд. іст. наук, доцент (Україна); **Устінова Ірина Ігорівна** - д-р. арх., професор (Україна); **Катерина Діденко** - канд. арх. (Україна); **Воскобойнікова Юлія Василівна** - д-р. мист. (Україна); **Крипчук Микола Володимирович** - канд. мист., доцент (Україна); **Лугова Тетяна Анатоліївна** - канд. мист., доцент (Україна)

Верстальник: *Білоус Тетяна (Україна).* ***Дизайнер:*** *Казьміна Надія (Україна).* ***Коректор:*** *Дудник Григорій (Україна).*

«Грааль науки» є офіційно зареєстрованим мультидисциплінарним науковим виданням з міжнародною сферою поширення, що підтримує політику відкритого доступу. **Ідентифікатор медіа R30-02704** (рішення № 430 від 22.02.2024 Національної Ради України з питань телебачення і радіомовлення).

Наказом МОН України № 582 від 24.04.2024 виданню «Грааль науки» присвоєно Категорію Б фахових видань України з питань економіки (051 «Економіка»).

«Грааль науки» індексується в міжнародних реферативних та наукометричних базах даних:
Index Copernicus Journals Master List; «Наукова періодика України» (Національна бібліотека України імені В.І. Вернадського НАН України); Національний репозитарій академічних текстів; Google Scholar; WorldCat; Open Ukrainian Citation Index; CrossRef; Mendeley; Scite; Semantic Scholar; Scilit; OpenAIRE, PubPeer.

Конференція зареєстрована УкрІНТЕІ (Посвідчення № 76 від 26.01.2026) та сертифікована Euro Science Certification Group (Сертифікат № 23264 від 13.01.2026).

За точність викладених фактів та правильність цитування відповідальність несе автор.

© Автори статей, 2026
© ГО «Європейська наукова платформа», 2026
© НУ «Інститут науково-технічної інтеграції та співпраці», 2026
© LLC «International Centre Corporative Management», 2026

changes in property inheritance systems as key elements in the formation of the traditional family model. The paper also highlights the philosophical views of ancient thinkers on marriage and family, their role in the functioning of the state and society, and interpretations of gender roles within family relations. Historical features of the development of family structures in Ukrainian society are considered, including the influence of Christian traditions, customary law, and socio-economic transformations on the evolution of family life. Particular emphasis is placed on the changes that occurred in the twentieth and twenty-first centuries under the influence of industrialization, urbanization, social reforms, the sexual revolution, and broader processes of social modernization. The study concludes that the modern institution of marriage is undergoing significant transformation, reflected in changes in values, roles, and models of family life. It emphasizes the importance of further research into the historical foundations of family development in order to better understand contemporary processes in the marital and family sphere and to develop new approaches to analyzing the family as an important social institution.
Keywords: *marriage, family, historiography, evolution of marital relations, patriarchal family, nuclear family, gender roles, social transformations.*

2026 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

ARTICLE

DOI 10.36074/grail-of-science.06.03.2026.056

THE EVOLUTION OF DIGITAL PRIVACY RIGHTS IN COMMON LAW JURISDICTIONS. A COMPARATIVE ANALYSIS OF UK AND UKRAINIAN APPROACHES TO PERSONAL DATA PROTECTION POST-2020

Mykola Sverhun
Master's Degree
National University of Technologies and Design, Ukraine

Natalya Liubymova
Senior Lecturer
National University of Technologies and Design, Ukraine

Summary. *This paper examines the evolution of digital privacy rights and personal data protection frameworks in the United Kingdom and Ukraine following significant legal developments post-2020. The research analyses the divergent path taken by the UK after Brexit on 31 January 2020, with the implementation of the UK GDPR on 1 January 2021 and subsequent Data (Use and Access) Act 2025, alongside Ukraine's progressive alignment with European Union data protection standards whilst maintaining its distinct legal framework. Through comparative legal analysis, this study identifies key similarities and differences in approach, implementation mechanisms, and enforcement practices. The findings demonstrate that whilst both jurisdictions share fundamental principles of data protection derived from international standards and the European Convention on Human Rights, their implementation strategies reflect distinct legal traditions and geopolitical contexts shaped by Brexit and European integration respectively. The paper examines enforcement actions including the £20 million British Airways fine and £18.4 million Marriott International penalty, contrasting these with Ukraine's current maximum penalty of 34,000 hryvnias (approximately $820 USD) [20]. The research contributes to understanding how different legal systems adapt international data protection standards to their specific constitutional and regulatory environments, whilst navigating the complex balance between privacy protection, economic innovation, and international data flows.*

Keywords: *digital privacy rights, personal data protection, UK GDPR, Ukrainian data protection law, comparative legal analysis, Brexit legislation, European integration, Data (Use and Access) Act 2025, enforcement mechanisms, international data transfers.*

Introduction

The landscape of digital privacy rights has undergone fundamental transformation since 2020, with unprecedented challenges emerging from the

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

COVID-19 pandemic, Brexit, and rapid digitalisation across all sectors of society [1]. These converging forces have created what scholars term a "perfect storm" for data protection law, requiring jurisdictions worldwide to reconsider the balance between individual privacy rights, public health imperatives, economic innovation, and national security concerns.

The United Kingdom's withdrawal from the European Union on 31 January 2020 marked a pivotal moment for data protection law, initiating a transition period that concluded on 31 December 2020 [2]. During this eleven-month transition, the UK technically remained outside the EU politically whilst continuing to follow EU law, including the EU General Data Protection Regulation. From 1 January 2021, the UK GDPR came into force as domestic legislation, created through the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020, which amended the EU GDPR to function in a UK context by replacing references to "the Union" with "the United Kingdom" and transferring regulatory powers from European to British institutions [2].

The European Commission's adequacy decision, granted on 28 June 2021, represented a critical juncture in UK-EU data relations [3]. This decision, adopted with only two days to spare before the Brexit transition arrangement for data protection expired on 30 June 2021, confirmed that the UK offers a level of data protection essentially equivalent to that in the EU under the GDPR. However, the decision contains a "sunset clause" limiting its validity to four years, requiring renewal by June 2025. This temporary nature reflects ongoing concerns about potential UK regulatory divergence from EU standards and creates uncertainty for businesses relying on seamless cross-border data flows.

This comparative study examines how the UK and Ukraine have developed their data protection regimes post-2020, focusing on legislative frameworks, enforcement mechanisms, practical implementation, and future trajectories. The UK has pursued regulatory autonomy through the Data Protection Act 2018 [4] and the recent Data (Use and Access), Act 2025, which received Royal Assent on 19 June 2025 and introduces significant reforms to UK GDPR aimed at reducing regulatory burden whilst maintaining high protection standards [19]. These reforms represent the most substantial changes to UK data protection law since Brexit and signal the government's intention to create a distinctively British approach to data regulation.

Meanwhile, Ukraine continues its legislative alignment with EU standards through draft Law № 8153 on harmonisation with GDPR, submitted to Parliament in October 2022 and passed first reading on 20 November 2024 [21]. This draft law proposes transformative changes to Ukraine's data protection regime, including maximum fines up to 150 million hryvnias or 8% of annual turnover for legal entities - representing a potential 4,400-fold increase compared to current penalties [21]. The legislation's progress has been complicated by ongoing war circumstances, limited institutional capacity, and the need to balance European integration commitments with immediate national priorities.

The comparative analysis presented in this paper reveals fundamental differences in how common law and civil law traditions approach data protection, how Brexit and European integration shape regulatory choices, and how enforcement capacity affects the practical realisation of data protection rights. By

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

examining these two jurisdictions at critical junctures in their regulatory development, this research contributes to broader understanding of data protection law's evolution in an increasingly interconnected yet fragmented global digital economy.

Literature Review and Theoretical Framework

The theoretical foundation of privacy rights traces back to Samuel Warren and Louis Brandeis' seminal 1890 article "The Right to Privacy," published in the Harvard Law Review [5]. Writing in response to the perceived threats to privacy posed by newspaper gossip and emerging photographic technologies, Warren and Brandeis articulated privacy as "the right to be left alone" and argued for legal recognition of an individual's right to control information about themselves. This conceptual framework, revolutionary for its time, established privacy as both an individual right deserving legal protection and a social value essential for human dignity and democratic society.

Warren and Brandeis' formulation influenced privacy law development across common law jurisdictions, though their concept focused primarily on protection against intrusion and publicity rather than the informational processing challenges of the digital age. The article's enduring influence stems from its recognition that technological change requires corresponding legal evolution - a principle that remains central to contemporary data protection debates as artificial intelligence, biometric surveillance, and ubiquitous data collection create new threats to privacy unimaginable in 1890.

Evolution from Privacy to Data Protection

Contemporary data protection scholarship recognises the distinct nature of data protection from traditional privacy concepts. While privacy protects against intrusion into personal space and unwanted publicity, data protection establishes rules for lawful processing of personal information regardless of whether such processing constitutes a privacy intrusion in the traditional sense. This distinction becomes particularly relevant in comparative analysis, where different legal traditions interpret these concepts through their constitutional frameworks and historical experiences.

The European approach to data protection evolved from several sources: the Universal Declaration of Human Rights (1948), the European Convention on Human Rights (1950), concerns about data processing under authoritarian regimes during World War II, and the recognition that transnational data flows required harmonised regulation. The Council of Europe Convention 108 (1981) represented the first binding international instrument on data protection, establishing principles that would later inform the EU Data Protection Directive (1995) and ultimately the GDPR (2016) [15].

The GDPR marked a paradigm shift by recognising data protection as a fundamental right rather than merely a regulatory framework. Article 8 of the EU Charter of Fundamental Rights establishes that "everyone has the right to the protection of personal data concerning him or her," elevating data protection to constitutional status within EU law. This framing influences how European institutions interpret data protection obligations and balance them against other rights and interests.

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

Comparative Legal Methodology

This research employs comparative legal analysis to examine how different legal systems address similar challenges in protecting personal data. The UK represents a common law tradition emphasising precedent, incremental development through case law, and practical problem-solving, whilst Ukraine reflects a civil law tradition influenced by both Soviet legal heritage and contemporary European continental systems, emphasising systematic codification and hierarchical legal structures.

Zweigert and Kötz's functional approach to comparative law guides this analysis, focusing on how different legal systems solve similar problems rather than merely comparing formal legal rules. This methodology recognises that seemingly similar legislative provisions may operate differently within distinct institutional contexts, legal cultures, and enforcement environments. Understanding these contextual factors proves essential for meaningful comparison of data protection regimes.

The UK Framework: Post-Brexit Evolution

The United Kingdom's modern data protection regime has evolved through several legislative iterations, reflecting both domestic privacy concerns and international harmonisation requirements. The Data Protection Act 1984 implemented the Council of Europe Convention 108, establishing the Data Protection Registrar (later renamed Information Commissioner) and basic fair processing principles. The Data Protection Act 1998 implemented the EU Data Protection Directive, significantly expanding protection scope and individual rights.

The Data Protection Act 2018, which received Royal Assent on 23 May 2018, represents the current primary legislation governing data protection in the United Kingdom [4]. This comprehensive statute, consisting of seven parts and twenty-three schedules spanning over 200 pages, serves multiple purposes: implementing the EU GDPR (whilst the UK remained an EU member), updating provisions for law enforcement data processing to implement the Law Enforcement Directive, establishing a framework for intelligence services data processing, and creating provisions for specific sectors including health research, journalism, and immigration.

The Act works alongside the UK GDPR to create a comprehensive two-tier framework. The UK GDPR maintains substantially equivalent provisions to the EU GDPR but operates as independent UK legislation enforced by UK authorities. This relationship sometimes creates complexity, as practitioners must navigate between the primary Act and the GDPR, determining which provisions apply in particular circumstances and how they interact.

The distinction between data controllers and processors represents a fundamental aspect of data protection accountability under UK GDPR. Controllers determine the purposes and means of processing and bear primary responsibility for compliance, whilst processors act on behalf of controllers and must implement appropriate technical and organisational measures. The European Data Protection Board's detailed guidance on these concepts, whilst not directly binding on the UK post-Brexit, provides interpretative framework that the ICO considers when determining responsibility and liability [17]. This clear delineation of roles proves

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

essential for enforcement actions, as seen in cases where organisations outsourced processing operations whilst remaining accountable for security failures. Understanding the global context of data protection also requires recognising that regulatory frameworks operate within increasingly complex international ecosystems. OECD research demonstrates that the digital data landscape features diverse regulatory approaches, technological architectures, and business models that interact across borders [18]. The UK's post-Brexit position must therefore balance domestic regulatory autonomy with international alignment to maintain cross-border data flows whilst protecting fundamental rights.

The Failed Reform: Data Protection and Digital Information Bill

Following extensive consultation initiated with the 'Data: A New Direction' paper from September to November 2021, the UK government developed ambitious plans to reform data protection law [10]. This consultation, signed by Oliver Dowden as Secretary of State for Digital, Culture, Media and Sport, sought views on proposals to "seize the opportunities of our new regulatory freedom" post-Brexit whilst maintaining high data protection standards and the EU adequacy decision.

The government introduced the Data Protection and Digital Information Bill to Parliament on 18 July 2022, subsequently re-introducing it as version "No. 2" on 8 March 2023 after the initial Bill fell when Parliament prorogued [11]. The Bill proposed significant changes including: replacing the GDPR's accountability principle with a more flexible approach; introducing new recognised legitimate interests for data processing; modifying subject access request procedures; reforming the ICO's governance structure; and creating new powers for data sharing between public bodies.

However, the Bill failed to complete passage before Parliament was dissolved on 30 May 2024 for general elections. This failure reflected several factors: concerns from privacy advocates about reduced protection standards potentially jeopardising EU adequacy; business uncertainty about implementation costs and timelines; parliamentary time pressures; and changing government priorities. The Bill's demise demonstrated the challenge of reforming data protection law in a contentious political environment whilst maintaining international equivalence requirements.

Data (Use and Access) Act 2025

The newly elected Labour government introduced fresh data protection reforms through the Data (Use and Access) Act 2025, which received Royal Assent on 19 June 2025 and represents the most substantial reform of UK data protection law since Brexit. Unlike its predecessor, this Act focuses on targeted reforms rather than comprehensive restructuring, aiming to reduce regulatory burden whilst maintaining EU adequacy and high protection standards [19].

Key provisions of the 2025 Act include:

- Recognised Legitimate Interests: The Act introduces an exhaustive list of recognised legitimate interests for which organisations can process personal data without applying the balancing test required under general legitimate interests provisions. These include: crime prevention and detection; safeguarding vulnerable individuals; internal fraud prevention; maintaining network and information security; and ensuring the physical security of premises. This change aims to provide greater legal certainty for common processing activities whilst maintaining appropriate safeguards.

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

- Automated Decision-Making: The Act substantially revises Article 22 UK GDPR's restrictions on solely automated decision-making. Under the new framework, the general prohibition applies only to automated decisions involving special category data (such as ethnicity or health information). For decisions not involving special category data, organisations may deploy automated decision-making systems subject to appropriate transparency and fairness obligations, reducing the previous regime's restrictive approach that proved burdensome for legitimate uses of artificial intelligence and algorithmic systems.
- International Data Transfers: The Act simplifies international transfer mechanisms by introducing new provisions for data bridge arrangements with countries sharing equivalent protection standards. This creates a faster pathway for approving data flows to trusted partners without full adequacy decisions, potentially facilitating trade agreements and digital economy partnerships whilst maintaining protection standards through contractual safeguards and oversight mechanisms.
- Children's Data Protection: Responding to concerns about age-appropriate design and children's online safety, the Act enhances requirements for processing children's personal data. Organisations must conduct age-appropriate design impact assessments for services likely to be accessed by children, implement appropriate default privacy settings, and provide clear, child-friendly privacy information. These provisions complement the ICO's Age Appropriate Design Code whilst creating statutory obligations.
- Smart Data Schemes: The Act establishes frameworks for smart data schemes in regulated sectors, beginning with financial services. These schemes allow individuals to authorise secure sharing of their data between organisations to access better products, switch services more easily, and benefit from competition. The framework includes robust security requirements, customer authorisation procedures, and liability provisions.
- Most provisions will come into effect in December 2025 following a transition period for organisations to implement necessary changes. The Act represents a distinctly British approach to data protection reform: pragmatic, sector-specific where appropriate, and focused on reducing unnecessary compliance burden whilst maintaining high protection standards and international adequacy.

The Information Commissioner's Office (ICO) serves as the UK's independent data protection authority, responsible for upholding information rights and enforcing data protection, freedom of information, electronic communications, and environmental information regulations. The ICO operates with substantial independence from government, though it remains a non-ministerial government department sponsored by the Department for Science, Innovation and Technology.

John Edwards was formally appointed as Information Commissioner by Letters Patent on 21 December 2021, beginning his five-year term on 3 January 2022, succeeding Elizabeth Denham who served from 2016 to 2021 [8]. Edwards, a New Zealand lawyer who previously served as New Zealand Privacy Commissioner from 2014 to 2021, brought international experience and a pragmatic regulatory philosophy to the role. His appointment followed an extensive recruitment process including Parliamentary pre-appointment hearings.

Under Edwards' leadership, the ICO published ICO25, its Strategic Plan for 2022-2025, setting out a vision focused on three strategic goals: empowering people

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

to use data responsibly to achieve economic and social goals; giving people confidence their information will be treated with respect; and becoming a world-leading regulator [9]. The strategy emphasises a risk-based, proportionate approach to regulation, prioritising resources toward areas of greatest harm whilst supporting organisations in achieving compliance through guidance and advice.

The ICO's budget for 2024-25 exceeded £45 million, funded primarily through data protection fees paid by organisations. The ICO employs approximately 650 staff across offices in Wilmslow, London, Belfast, Cardiff, and Edinburgh, organised into directorates covering regulatory operations, policy, technology, and corporate services. This substantial institutional capacity enables the ICO to undertake complex investigations, develop detailed guidance, engage internationally, and maintain effective enforcement programs.

The ICO possesses extensive enforcement powers under UK GDPR and the Data Protection Act 2018. These powers include: conducting investigations and audits; issuing information notices requiring organisations to provide specified information; issuing assessment notices requiring organisations to permit entry and inspection of premises; issuing enforcement notices requiring organisations to take or refrain from specified actions; and imposing administrative fines up to £17.5 million or 4% of annual global turnover, whichever is greater, for the most serious infringements.

The ICO follows a Regulatory Action Policy that emphasises a graduated approach to enforcement, using the least intrusive intervention necessary to achieve compliance whilst reserving strong action for serious or deliberate non-compliance. This policy reflects the ICO's role as both regulator and advisor, seeking to promote good practice through education and guidance whilst demonstrating credible deterrence through enforcement action where necessary.

Two landmark enforcement actions in October 2020 demonstrated the ICO's approach to major data breaches and established important precedents for GDPR enforcement in the UK.

On 16 October 2020, the ICO imposed a £20 million fine on British Airways Plc for security failures that led to a significant data breach in 2018 [6]. The breach, which occurred between 22 June and 5 September 2018, affected approximately 400,000 customers whose personal data, including names, addresses, payment card numbers, and CVV codes, was harvested by attackers who had gained access to BA's systems.

The ICO's investigation found that BA failed to implement appropriate technical and organisational measures to protect personal data, specifically: failing to detect the cyber-attack for more than two months; inadequate security architecture that allowed attackers to progress from compromised user credentials to complete network access; insufficient monitoring and intrusion detection capabilities; and poor security hygiene including inadequate patch management and network segmentation.

The initial Notice of Intent in July 2019 proposed a fine of £183.39 million (approximately 1.5% of BA's 2017 worldwide turnover), which would have been the largest GDPR penalty to date. However, the final penalty of £20 million represented an approximately 89% reduction, reflecting several factors:

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

1. Detailed Representations: BA provided extensive technical information and legal arguments challenging aspects of the ICO's initial assessment, leading to revisions in the ICO's analysis of the breach's scope and BA's culpability.

2. Mitigating Actions: BA took immediate steps after discovering the breach including: notifying the ICO promptly; providing regular updates; offering compensation to affected individuals; implementing significant security improvements; and cooperating fully with the investigation.

3. COVID-19 Impact: The ICO explicitly considered the economic impact of the COVID-19 pandemic on the aviation industry, reducing the fine by £4 million to reflect BA's significantly deteriorated financial position and the broader economic context.

4. No Financial Gain: BA did not gain any financial benefit from the breach, distinguishing this case from deliberate non-compliance or processing for unlawful purposes.

5. Reputational Damage: The ICO recognised that BA had already suffered significant reputational harm and business impact from the breach and its publicity.

The case established important precedents including: cyber security failures constitute GDPR violations even when caused by sophisticated external attacks; organisations must implement appropriate security measures proportionate to their size, profile, and likelihood of being targeted; COVID-19 impacts may be considered in penalty assessments; and organisations' cooperation and remedial actions significantly affect final penalties.

On 30 October 2020, the ICO issued an £18.4 million fine to Marriott International Inc for security failures related to a prolonged cyberattack that affected an estimated 339 million guest records globally [7]. The breach originated in 2014 when attackers compromised Starwood Hotels' systems, but remained undetected until September 2018, approximately two years after Marriott acquired Starwood in September 2016.

The attack exposed various categories of personal data including guest names, email addresses, phone numbers, passport numbers (18.5 million encrypted), payment card details (9.1 million encrypted), and guest stay information. For approximately 30.1 million records, the individuals were EEA residents, with about 7 million UK residents affected.

The ICO's investigation found that Marriott failed to implement appropriate technical and organisational measures, specifically: insufficient due diligence during the Starwood acquisition to identify the ongoing breach; failure to implement adequate security measures post-acquisition; insufficient monitoring and intrusion detection; and delayed discovery of the compromise despite warning signs.

The initial Notice of Intent in July 2019 proposed a fine of £99.2 million. The final penalty of £18.4 million represented approximately an 81% reduction, reflecting: detailed representations from Marriott including technical analysis of the sophisticated attack; the fact that the breach originated before GDPR's enforcement date (though continued after); Marriott's cooperation with the investigation; improvements implemented post-discovery; the economic impact of COVID-19 on the hospitality industry; and the absence of financial gain from the breach.

The Marriott case established important precedents for: acquirer liability for pre-existing breaches in acquired companies; the need for adequate due diligence

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

in mergers and acquisitions to identify data protection risks; post-acquisition obligations to implement appropriate security measures even for legacy systems; and the fact that outsourcing security to third-party consultants does not reduce the data controller's responsibility for GDPR compliance.

Both cases remain significant as they represent the only GDPR penalties exceeding £10 million issued by the ICO to date, demonstrating the regulator's willingness to impose substantial fines for serious security failures whilst also showing flexibility in considering mitigating circumstances and economic context. Both organisations paid their fines in full and implemented significant security improvements following the enforcement actions.

International Data Transfers and Adequacy

Post-Brexit, the UK developed its own framework for international data transfers, largely mirroring EU mechanisms whilst asserting regulatory independence. The UK recognises EU member states and other countries with EU adequacy decisions as having adequate data protection, enabling free data flow. For countries without adequacy, organisations must implement appropriate safeguards such as standard contractual clauses.

On 2 February 2022, the Secretary of State issued the International Data Transfer Agreement (IDTA) and the Addendum to EU Standard Contractual Clauses under Section 119A of the Data Protection Act 2018, following consultation and Parliamentary approval. These instruments, which came into force on 21 March 2022, provide mechanisms for UK organisations to transfer personal data internationally whilst ensuring appropriate safeguards.

The IDTA represents a distinctively British approach to international transfer mechanisms, differing from EU Standard Contractual Clauses in structure and style. It uses plain English drafting rather than legal formalism, consolidates various transfer scenarios into a single agreement rather than modular clauses, and incorporates UK-specific requirements and terminology. The Addendum allows organisations to continue using EU SCCs for UK transfers by appending UK-specific provisions.

The UK has granted its own adequacy decisions to several countries, beginning with EU member states and continuing with jurisdictions including South Korea, Switzerland, and others. These decisions reflect the UK's independent assessment of protection standards, though in practice the UK tends to follow EU adequacy determinations closely to maintain regulatory alignment and support business operations.

The Ukrainian Framework: European Integration and National Identity

Ukraine's data protection regime is founded on Article 32 of the Constitution of Ukraine, adopted in 1996 and amended in 2020 [12]. Article 32 provides comprehensive privacy protection, stating: "No one shall be subject to interference in his or her personal and family life, except in cases envisaged by the Constitution of Ukraine." The article specifically prohibits collecting, storing, using, and disseminating confidential information about a person without his or her consent, except in cases determined by law and only in the interests of national security, economic welfare, and human rights.

Article 32 further guarantees every citizen the right to examine information about themselves that is not a state or other secret protected by law; to demand

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

correction of untrue information; and to demand deletion of any information, as well as the right to compensation for material and moral damages inflicted by the collection, storage, use, and dissemination of incorrect information. These constitutional provisions create strong formal protection but require implementing legislation to be practically effective.

The primary legislative instrument is the Law of Ukraine "On Personal Data Protection" (Law № 2297-VI), adopted on 1 June 2010 and entering into force on 1 January 2011 [13]. This law, consisting of eight chapters and forty-one articles, established Ukraine's first comprehensive data protection framework, defining key concepts, establishing processing principles, outlining data subject rights, and creating an oversight mechanism.

The law's adoption reflected Ukraine's commitments under the Council of Europe Convention 108, which Ukraine signed in 2010 and ratified in 2010, becoming the first post-Soviet state to ratify this convention. The law drew inspiration from European models but adapted them to Ukrainian legal traditions and institutional capacities. Key provisions include requirements for data controller registration, consent requirements for processing, data subject rights to access and correction, and restrictions on cross-border transfers.

However, Law № 2297-VI predated the EU GDPR and reflected an earlier generation of data protection thinking. The law contains gaps and ambiguities compared to contemporary standards: it lacks clear legal bases for processing beyond consent; provides insufficient guidance on security obligations; contains limited provisions on automated decision-making and profiling; and establishes relatively weak enforcement mechanisms and penalties. These limitations have increasingly constrained Ukraine's ability to meet European integration commitments and protect individuals in the digital economy.

European Integration Path and Association Agreement

The Association Agreement between Ukraine and the European Union, with political chapters signed on 21 March 2014 and economic chapters (including the Deep and Comprehensive Free Trade Area) signed on 27 June 2014, marks a watershed moment in Ukraine-EU relations [14]. The Agreement entered into provisional application from 1 January 2016 and full force from 1 September 2017 following ratification by all EU member states.

Chapter III of the Agreement, titled "Justice, Freedom and Security," includes Article 14 on personal data protection. This article requires the Parties to "cooperate" in ensuring an adequate level of protection of personal data in accordance with the highest European and international standards, including those of the Council of Europe. Article 14 specifically requires Ukraine to approximate its legislation to EU legislation on personal data protection, listing the Data Protection Directive 95/46/EC (later replaced by GDPR) and related instruments.

The Association Agreement creates binding obligations for Ukraine to align its data protection regime with EU standards, subject to monitoring and enforcement through the Association Agreement's institutional mechanisms. This commitment reflects both Ukraine's European aspirations and practical necessity, as inadequate data protection could create barriers to digital trade, cross-border data flows, and integration with European digital services.

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

The Agreement also establishes Association bodies including the Association Council and Association Committee, which monitor implementation progress. The European Union has consistently raised data protection reform as a priority area in these forums, linking progress to broader assessments of Ukraine's reform efforts and European integration trajectory.

Legislative Reform Efforts: Clarifying the 2020-2021 Period

Contrary to some reports, Ukraine did not implement major amendments to Law № 2297-VI during the 2020-2021 period. This clarification is important for understanding Ukraine's actual reform timeline and the challenges facing GDPR harmonisation efforts.

The most substantial amendments to the primary data protection law occurred in 2012-2014, particularly through Law № 383-VII of 3 July 2013 "On Amendments to Certain Legislative Acts of Ukraine Regarding Improving the System of Personal Data Protection," which entered into force on 1 January 2014. These amendments strengthened certain provisions, introduced criminal liability for data protection violations, and enhanced the role of the Ukrainian Parliament Commissioner for Human Rights in data protection oversight.

During 2020-2021, several developments occurred regarding data protection, but not major legislative amendments to Law № 2297-VI:

- Council of Europe Engagement: In January 2020, Council of Europe experts met with members of the Ukrainian Parliament and relevant ministries in Strasbourg to discuss concepts for new data protection legislation harmonised with GDPR and Convention 108+. These technical assistance meetings helped Ukrainian legislators understand GDPR requirements and develop drafting approaches, but did not result in enacted legislation during this period.
- Sector-Specific Laws: Parliament adopted several sector-specific laws touching data protection aspects, most notably the Law "On Stimulating the Development of the Digital Economy in Ukraine" adopted on 15 July 2021. This law created the "Diia City" special legal regime for IT companies, including specific provisions on personal data processing for participants. However, this law did not amend the general data protection framework under Law № 2297-VI.
- COVID-19 Emergency Measures: The government adopted temporary measures allowing processing of certain types of health-related data without standard consent requirements for pandemic response purposes. These emergency provisions, justified under public health exemptions, permitted contact tracing, vaccination certificate systems, and health monitoring, but expired with the state of emergency declarations.
- Reform Planning: Various draft concepts and working documents on GDPR harmonisation circulated among government agencies, civil society organisations, and international technical assistance providers during this period. However, none of these materials progressed to formal legislative proposals submitted to Parliament during 2020-2021.

The absence of major legislative action during 2020-2021 reflected several factors: Parliament's focus on other reform priorities including judicial reform, anti-corruption measures, and oligarch regulation; institutional capacity limitations in drafting complex harmonisation legislation; political instability and government

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

changes; and resource constraints affecting legislative drafting support. Additionally, the COVID-19 pandemic disrupted normal legislative processes and shifted priorities toward immediate crisis management.

Draft Law № 8153: The primary GDPR harmonisation effort materialised through draft Law № 8153 "On Personal Data Protection," submitted to Parliament in October 2022 (not during 2020-2021 as some sources incorrectly state) [21]. This comprehensive draft, developed with extensive Council of Europe technical assistance, proposes to replace Law № 2297-VI with legislation fully harmonised with GDPR and Convention 108+ [21].

The draft law passed first reading on 20 November 2024, representing significant progress after two years of Parliamentary consideration. However, it now awaits second reading, where detailed amendments will be debated and incorporated [21]. The timeline for final adoption remains uncertain, complicated by ongoing war circumstances, Parliamentary workload, and the technical complexity of the legislation requiring careful review of hundreds of potential amendments.

Key provisions of draft Law № 8153 include: comprehensive alignment with GDPR principles and provisions; expanded legal bases for processing beyond consent; detailed obligations for data controllers and processors; enhanced data subject rights including portability; requirements for data protection impact assessments; provisions on cross-border transfers; establishment of an independent data protection authority; and significantly increased penalties for violations [21].

Current Enforcement Regime and Penalties

The current enforcement regime under Article 188-39 of the Code of Ukraine on Administrative Offences provides for significantly lower penalties than EU GDPR equivalents [20]. Critical correction required: Previous versions of this analysis contained a calculation error regarding penalty amounts. The correct penalties are:

For individuals (natural persons):

• Part 1 (first violation): 100–200 NTMIC

Calculation: 100–200 × 17 UAH = 1,700–3,400 UAH

• Part 2 (failure to comply with the Ombudsperson's lawful demands): 200–300 NTMIC

Calculation: 200–300 × 17 UAH = 3,400–5,100 UAH

• Part 3 (repeat within one year of Part 1 or Part 2): 300–500 NTMIC

Calculation: 300–500 × 17 UAH = 5,100–8,500 UAH

• Part 4 (violation causing unlawful access / infringement of data subject's rights): 100–500 NTMIC

Calculation: 100–500 × 17 UAH = 1,700–8,500 UAH

• Part 5 (repeat within one year of Part 4): 1,000–2,000 NTMIC

Calculation: 1,000–2,000 × 17 UAH = 17,000–34,000 UAH [20].

These calculations use the fixed non-taxable minimum of 17 hryvnias established in 1996 under the Tax Code of Ukraine for administrative penalty calculations. This figure differs substantially from the tax social benefit (currently 1,514 hryvnias in 2025, equal to 50% of the minimum subsistence level for able-bodied persons), which is used for other purposes including qualifying thresholds for certain offences but not for calculating administrative penalties.

2026 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

The use of the 17 hryvnia figure reflects legislative inertia: when Ukraine transitioned from Soviet-era regulations, lawmakers fixed this amount to prevent penalties from becoming meaningless through inflation whilst debates continued about comprehensive penalty reform. Nearly three decades later, this anachronistic figure remains in force, resulting in penalties that are negligible for most violations and provide minimal deterrent effect.

To illustrate the enforcement gap: the maximum possible penalty under current Ukrainian law (34,000 hryvnias or approximately $820) equals approximately 0.0047% of the UK ICO's maximum £20 million British Airways penalty. Even adjusting for economic differences and company size, this represents an enormous disparity in enforcement capacity and deterrent effect [20].

Draft Law № 8153 proposes transformative changes to this enforcement regime. Under the proposed framework, penalties would align with GDPR levels:

- For most serious violations: up to 150 million hryvnias or 8% of annual turnover, whichever is greater
- For less serious violations: up to 75 million hryvnias or 4% of annual turnover
- These amounts represent potential increases of 4,400-fold and 2,200-fold respectively compared to current maximum penalties [21].

The Ukrainian Parliament Commissioner for Human Rights serves as the primary data protection oversight body, though enforcement mechanisms remain significantly less developed compared to EU member states or the UK [16]. The Ombudsperson's office operates with limited budget and staff dedicated to data protection functions, relying primarily on complaints received from individuals and conducting occasional proactive reviews. The office issues recommendations and can refer matters to law enforcement or administrative authorities for potential penalties, but lacks direct fine-imposing authority.

Institutional Capacity and Implementation Challenges

Ukraine faces substantial challenges in implementing effective data protection regulation beyond legislative text. These challenges include:

- Limited Regulatory Capacity: Current oversight mechanisms lack the institutional capacity, technical expertise, and resources needed for effective data protection supervision. The Ombudsperson's office, while performing valuable work, cannot replicate the functions of specialised data protection authorities in EU member states or the UK ICO.
- Enforcement Weakness: Low penalty levels combined with limited enforcement actions create minimal deterrent effect. Many organisations, particularly large international companies and digital platforms, face little practical consequence for non-compliance with current requirements.
- Low Awareness: Public awareness of data protection rights remains limited, reducing demand-side pressure for compliance. Many individuals do not understand their rights or how to exercise them, limiting the effectiveness of complaint-based oversight mechanisms.
- Resource Constraints: Ukraine's economic challenges, exacerbated by ongoing war, limit resources available for regulatory development, staff training, technology infrastructure, and other capacity-building needs.

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

- War Impact: Russia's full-scale invasion since February 2022 has disrupted all aspects of governance and public administration, diverting resources to defence and immediate humanitarian needs whilst creating additional data protection challenges related to displaced persons, occupied territories, and wartime data processing.

Despite these challenges, Ukraine has made progress in certain areas: developing digital government services through the Diia platform whilst incorporating privacy-by-design principles; engaging with civil society organisations advocating for stronger data protection; participating in international capacity-building programs with the Council of Europe and EU; and maintaining momentum on draft Law № 8153 despite difficult circumstances.

Comparative Analysis: Divergence and Convergence

Both the UK and Ukraine share commitment to fundamental data protection principles derived from international standards, particularly the Council of Europe Convention 108 and its modernised version Convention 108+ [15]. These shared principles include:

1. Lawfulness and Fairness: Processing must have legal basis and be conducted fairly toward data subjects. Both jurisdictions require organisations to identify and rely on specific lawful bases for processing (though they differ in how they define and apply these bases). Fairness encompasses obligations to process data in ways that data subjects would reasonably expect and that do not cause unjustified adverse effects.

2. Purpose Limitation: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. This principle prevents "mission creep" where data collected for one purpose is repurposed without appropriate legal basis or data subject awareness. Both jurisdictions recognise exceptions for compatible purposes such as research and archiving in the public interest, subject to appropriate safeguards.

3. Data Minimisation: Only data adequate, relevant, and limited to what is necessary for the specified purposes should be processed. This principle challenges common organisational tendencies toward maximal data collection "just in case" and requires organisations to carefully consider what data they actually need. Implementation requires regular review of data processing activities to eliminate unnecessary collection and retention.

4. Accuracy: Organisations must ensure data accuracy and take reasonable steps to update or erase inaccurate data. This principle reflects both fairness to individuals and practical need for accurate information in decision-making. It requires organisations to implement processes for verification, correction, and updating of personal data, particularly when used for significant decisions affecting individuals.

5. Storage Limitation: Data should be retained only as long as necessary for the specified purposes. Both jurisdictions require organisations to establish retention periods and procedures for secure deletion or anonymisation when data is no longer needed. This principle conflicts with organisational tendencies toward indefinite retention and requires active data lifecycle management.

6. Integrity and Confidentiality: Appropriate technical and organisational measures must protect against unauthorised or unlawful processing and accidental

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

loss, destruction, or damage. This security principle requires risk-based approaches considering the nature of data processed, potential consequences of breaches, and available protective measures. Both jurisdictions recognise that security is not absolute but must be appropriate in the circumstances.

These shared principles reflect international consensus on core data protection requirements. However, their implementation differs significantly between jurisdictions, reflecting distinct legal traditions, institutional capacities, and enforcement philosophies.

Key Differences in Approach and Implementation

The UK approaches data protection through its common law tradition, emphasising:

- Pragmatic Application: Focus on practical problem-solving and specific situations rather than abstract principles
- Case Law Development: Incremental refinement through judicial decisions and regulatory enforcement actions that establish precedents
- Regulatory Guidance: Extensive guidance from the ICO providing detailed practical advice on compliance
- Risk-Based Flexibility: Emphasis on proportionate approaches that consider organisational context and risk levels

Ukraine's civil law tradition, influenced by both European continental systems and Soviet legal heritage, emphasises:

- Systematic Codification: Preference for comprehensive legislative texts establishing clear hierarchical rules
- Formal Requirements: Greater emphasis on procedural compliance and formal registration or notification obligations
- Administrative Law Framework: Integration of data protection within broader administrative law systems including standardised penalty regimes
- Limited Role for Precedent: Lesser weight given to specific cases compared to formal legislative provisions
- These fundamental differences in legal methodology affect how data protection operates in practice, even when formal rules appear similar. For example, the UK's risk-based approach allows tailored implementation based on organisational circumstances, whilst Ukraine's more formal approach tends toward standardised requirements regardless of context.

The enforcement capacity gap between jurisdictions is perhaps the most consequential difference:

UK Enforcement Infrastructure:

- Independent data protection authority (ICO) with annual budget exceeding £45 million
- Approximately 650 professional staff including technical specialists, lawyers, and investigators
- Power to impose fines up to £17.5 million or 4% of global turnover
- Demonstrated willingness to impose substantial penalties (£20 million British Airways, £18.4 million Marriott)
- Comprehensive investigation capabilities including compulsory information powers

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

- Regular proactive audits and assessments of high-risk sectors
- Published enforcement action policy providing transparency and consistency

Ukrainian Enforcement Infrastructure:

- Data protection oversight integrated within Ombudsperson's office alongside broader human rights mandate
- Limited dedicated staff and budget for data protection functions
- Current maximum penalty of 34,000 hryvnias (approximately $820 USD)
- Limited enforcement actions and minimal deterrent effect from low penalties
- Primarily reactive complaint-based approach due to resource constraints
- Limited technical capacity for investigating complex data processing operations
- Dependence on other authorities for penalty imposition

This capacity gap affects not only direct enforcement but also compliance incentives, public awareness, and organisational data protection cultures. UK organisations face credible regulatory scrutiny with meaningful consequences for non-compliance, whilst Ukrainian organisations face minimal practical risk from current enforcement mechanisms (though this may change if draft Law № 8153 passes) [21].

Reform Trajectories: Divergence vs. Convergence

The UK and Ukraine are moving in opposite directions regarding relationship with EU data protection standards:

UK Divergence: Following Brexit, the UK has pursued regulatory autonomy whilst maintaining substantial equivalence with EU GDPR to preserve adequacy. The Data (Use and Access) Act 2025 represents a distinctly British approach: reducing perceived unnecessary regulatory burden; creating flexibility for beneficial innovations like artificial intelligence; simplifying requirements for lower-risk processing; whilst maintaining high protection standards for fundamental rights [19]. This trajectory balances international trade interests (requiring adequacy), domestic innovation priorities, and practical compliance concerns.

Ukrainian Convergence: Ukraine follows a path toward full GDPR alignment through draft Law № 8153, implementing EU standards more comprehensive than current law requires. This reflects: European integration commitments under the Association Agreement; practical necessity for cross-border data flows with EU; technical assistance and capacity building from European institutions; and desire to demonstrate reform progress as part of EU accession aspirations. Ukraine essentially seeks to adopt the European model wholesale rather than adapting it to national circumstances.

These divergent trajectories reflect fundamentally different geopolitical positions: the UK as a former EU member asserting post-Brexit independence whilst maintaining partnership, versus Ukraine as an EU candidate seeking to demonstrate alignment and readiness for membership. Data protection policy becomes embedded in these broader narratives of national identity and international positioning.

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

Geopolitical Context and International Relations

Brexit fundamentally shapes UK data protection policy in ways that complicate simple comparisons:

UK Balancing Act: The UK must balance multiple competing considerations:

- EU Adequacy: Maintaining adequacy decision validity requires substantial equivalence with EU standards, limiting divergence options
- Trade Agreements: Negotiations with United States, India, and others include data flow provisions that may require regulatory adjustments
- Domestic Innovation: Technology sector pressure for reduced compliance burden and regulatory flexibility
- Public Trust: Maintaining public confidence in data protection to support digital economy and government services
- International Leadership: Positioning the UK as a global data protection leader and credible alternative to EU model

Ukraine's reform efforts occur within different but equally complex geopolitical circumstances:

EU Integration Priority: Data protection reform represents one component of comprehensive approximation to EU acquis required for membership. Progress signals broader reform commitment and strengthens Ukraine's negotiating position regarding accession timeline.

War Context: Russia's invasion creates immediate data protection challenges including: protecting data of internally displaced persons; ensuring secure digital government systems under cyberattack; maintaining data protection standards whilst implementing wartime measures; and preventing misuse of personal data in occupied territories.

International Support: European and other international partners provide technical assistance, capacity building, and political support for reforms as part of broader support packages. This creates positive incentives for alignment but also dependencies on external expertise.

Digital Sovereignty: For Ukraine, data protection intersects with broader questions of digital sovereignty and resilience. Strong data protection helps protect against external interference, surveillance, and information warfare whilst building trusted digital infrastructure.

These geopolitical contexts mean that data protection policy cannot be understood purely through technical legal analysis but must be situated within broader narratives of national development, international relations, and security considerations.

Practical Implications for Individuals and Organisations

The comparative analysis reveals significant practical differences in how data protection operates:

For Individuals:

- UK: Strong formal rights backed by credible enforcement, high awareness, accessible complaint mechanisms, realistic prospects of redress
- Ukraine: Strong formal rights in draft law but weak enforcement, lower awareness, limited practical redress mechanisms, minimal deterrence for violations [21].

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

For Organisations:

- UK: Substantial compliance obligations requiring significant investment, credible regulatory scrutiny, need for ongoing adaptation to regulatory evolution
- Ukraine: Currently limited practical compliance pressure despite formal requirements, significant change anticipated if new law passes [21]

For International Data Flows:

- UK: EU adequacy enables continued flows with EEA, but sunset clause creates uncertainty; developing separate adequacy and transfer arrangements with other partners
- Ukraine: No EU adequacy decision; relies on standard contractual clauses or other safeguards for transfers; GDPR alignment may eventually enable adequacy

Conclusions and Future Perspectives

This comparative analysis reveals that whilst the United Kingdom and Ukraine share commitment to fundamental data protection principles derived from international standards and European traditions, their post-2020 trajectories reflect profoundly different legal traditions, economic contexts, geopolitical positions, and institutional capacities.

The UK has pursued regulatory autonomy post-Brexit through the Data (Use and Access) Act 2025, the most substantial reform of UK data protection law since leaving the European Union [19]. This legislation demonstrates a distinctly British approach to data protection: pragmatic, focused on reducing unnecessary burden, creating flexibility for innovation, whilst maintaining high protection standards and international adequacy. The UK's mature regulatory infrastructure, exemplified by the ICO's substantial budget, professional capacity, and demonstrated enforcement effectiveness through actions like the £20 million British Airways penalty and £18.4 million Marriott International fine, enables sophisticated risk-based regulation that balances multiple competing interests.

However, the UK faces ongoing challenges including: maintaining EU adequacy beyond the June 2025 renewal; managing tensions between divergence for domestic innovation and equivalence for international partnership; adapting regulation to emerging technologies including artificial intelligence, biometric processing, and algorithmic systems; and maintaining public trust in data protection as digital transformation accelerates across all sectors.

Ukraine continues progressive alignment with EU standards through draft Law № 8153, passed first reading on 20 November 2024 and proposing transformative reforms including maximum penalties up to 150 million hryvnias or 8% of annual turnover - representing a potential 4,400-fold increase compared to current maximum penalties of 34,000 hryvnias (approximately $820) [20]. This legislative effort reflects Ukraine's European integration commitments under the 2014 Association Agreement and practical necessity for credible data protection to enable digital economy development and cross-border data flows.

Yet Ukraine faces substantial implementation challenges beyond legislative text. Current enforcement remains significantly underdeveloped compared to European equivalents, with the Ombudsperson's office lacking the institutional capacity, resources, and powers of specialised data protection authorities [21]. The research demonstrates that effective data protection requires not only appropriate

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

legislation but also: robust enforcement infrastructure with adequate budget and professional staff; meaningful penalties that create genuine deterrence; public awareness of rights and compliance obligations; organisational data protection cultures embedding privacy considerations into business practices; and political commitment to prioritising data protection within broader reform agendas.

The war context further complicates Ukraine's reform implementation. Russia's full-scale invasion since February 2022 has disrupted governance, diverted resources to defence and humanitarian priorities, created additional data protection challenges for displaced persons and wartime processing, whilst simultaneously demonstrating the critical importance of digital resilience and data protection against external interference and information warfare.

Looking forward, several developments merit attention:

UK Adequacy Renewal: The European Commission must decide whether to renew the UK adequacy decision by June 2025. The Data (Use and Access) Act 2025's reforms will be scrutinised to determine whether they maintain sufficient equivalence. While renewal appears likely given continued substantial similarity to GDPR, the review creates uncertainty and may impose constraints on future UK divergence.

Ukraine EU Membership: Ukraine's EU membership aspirations create strong incentives for GDPR alignment regardless of immediate implementation capacity. However, the gap between legislative text and practical enforcement will require sustained attention during accession negotiations. The European Commission may require demonstrated effectiveness, not merely formal alignment, before granting membership or adequacy [21].

Emerging Technologies: Both jurisdictions must adapt regulation to address challenges from artificial intelligence, biometric surveillance, Internet of Things, and other emerging technologies that were not envisaged when current frameworks were designed. The UK's flexible approach may enable faster adaptation, whilst Ukraine's comprehensive reform provides opportunity to incorporate contemporary issues into fundamental legislation.

Global Data Governance: The UK-Ukraine comparison reflects broader global fragmentation in data governance, with different regulatory models competing for influence. The UK represents a post-Brexit "third way" between EU and US approaches, whilst Ukraine exemplifies comprehensive EU alignment by non-member states. These different pathways contribute to ongoing debates about whether convergence toward international standards or legitimate diversity in regulatory approaches better serves global digital economy needs.

Cross-Border Enforcement: Neither the UK nor Ukraine can effectively regulate global digital platforms unilaterally. International cooperation mechanisms, bilateral arrangements, and multilateral frameworks will prove essential for addressing cross-border data protection challenges. The UK's Brexit departure complicates cooperation with EU enforcement authorities, whilst Ukraine's developing infrastructure limits its capacity to participate effectively in international enforcement networks.

The comparative analysis presented in this paper contributes to understanding how different legal systems adapt international data protection

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

standards to specific contexts. The findings challenge simplistic assumptions that similar legislative texts produce similar outcomes, demonstrating instead that legal tradition, institutional capacity, geopolitical context, and enforcement resources fundamentally shape how data protection operates in practice.

For policymakers and reformers, the research suggests that successful data protection requires holistic approaches addressing not only legislative frameworks but also institutional development, resource allocation, capacity building, public awareness, and sustained political commitment. Legislative harmonisation alone proves insufficient without corresponding investment in enforcement infrastructure and organisational capabilities.

For scholars and researchers, the UK-Ukraine comparison illuminates how Brexit, European integration, war, and institutional capacity interact to shape regulatory development in complex ways that resist deterministic predictions. Future research should examine these jurisdictions' continued evolution, particularly UK adequacy renewal outcomes, Ukraine's implementation of reformed legislation if enacted, and broader implications for data protection in jurisdictions navigating between different regulatory spheres in an increasingly multipolar global digital governance landscape [21].

References:

[1] Information Commissioner's Office (2021). *Guide to the UK General Data Protection Regulation (UK GDPR)*. London: ICO. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

[2] UK Government (2020). *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020*. SI 2020/1586. Available at: https://www.legislation.gov.uk/uksi/2020/1586/made

[3] European Commission (2021). *Commission Implementing Decision on the adequate protection of personal data by the United Kingdom*. C(2021) 4800 final, 28 June 2021 Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021D1772

[4] UK Parliament (2018). *Data Protection Act 2018*. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[5] Warren, S. & Brandeis, L. (1890). 'The Right to Privacy'. *Harvard Law Review*, Vol. 4, No. 5, pp. 193-220. Available at: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html Додаток (PDF): https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf?utm_source

[6] Information Commissioner's Office (2020). *Monetary Penalty Notice: British Airways Plc* (16 October 2020). Reference: MPN/04. Available at: https://www.edpb.europa.eu/sites/default/files/article-60-final-decisions/uk_2010-10_data_breach_security_of_processing_decisionpublic_final.pdf?utm_source

[7] Information Commissioner's Office (2020). *Monetary Penalty Notice: Marriott International Inc* (30 October 2020). Reference: MPN/05. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/encryption/encryption-and-data-protection/ Додаток (PDF): https://www.edpb.europa.eu/sites/default/files/article-60-final-decisions/uk_2020-10_personal_data_breach_decisionpublic_final.pdf

[8] UK Government (2021). *John Edwards confirmed as new Information Commissioner* (21 December 2021). Available at:

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

https://www.gov.uk/government/news/john-edwards-is-confirmed-as-the-new-information-commissioner

[9] Information Commissioner's Office (2022). *ICO25: Our Strategic Plan for 2022-2025*. London: ICO. Available at: https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-plan/
Додаток (PDF): https://ico.org.uk/media2/migrated/4020926/ico25-plan-for-consultation-20221407-v1_0.pdf?utm_source

[10] UK Government (2021). *Data: A New Direction - Government response to consultation*. London: DCMS, November 2021. Available at: https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation

[11] UK Parliament (2022). *Data Protection and Digital Information (No. 2) Bill 2022-23*. Available at: https://bills.parliament.uk/bills/3430

[12] Verkhovna Rada of Ukraine (1996). *Constitution of Ukraine* (with amendments 2020). Available at: https://zakon.rada.gov.ua/laws/show/en/254%D0%BA/96-%D0%B2%D1%80?utm_source

[13] Verkhovna Rada of Ukraine (2010). *Law of Ukraine on Personal Data Protection No. 2297-VI* (1 June 2010, as amended). Available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text

[14] European Union. *Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part.* Official Journal of the European Union, L 161. URL: https://data.europa.eu/eli/agree_internation/2014/295/oj

[15] Council of Europe (2001). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108, modernised as Convention 108+). Available at: https://www.coe.int/en/web/data-protection/convention108-and-protocol

[16] Ukrainian Parliament Commissioner for Human Rights. *Annual Report on the Observance and Protection of Human and Civil Rights and Freedoms in Ukraine for 2022 to the Verkhovna Rada of Ukraine.* Kyiv: UPCHR, 2022. URL: https://ombudsman.gov.ua/report-2022/images/documents/annual-report-2022-en.pdf

[17] European Data Protection Board. *Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Final version (7 July 2021).* Brussels: EDPB, 2021. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en
Додаток (PDF): https://www.edpb.europa.eu/system/files_en?file=2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf

[18] OECD (2022). Data in an evolving technological landscape: The case of connected and automated vehicles. OECD Digital Economy Papers, No. 346. Paris: OECD Publishing. DOI: https://doi.org/10.1787/ec7d2f6b-en.

[19] UK Parliament (2025). Data (Use and Access) Act 2025. Available at: https://www.legislation.gov.uk/ukpga/2025/18/contents
https://www.legislation.gov.uk/ukpga/2025/18/pdfs/ukpga_20250018_en.pdf

[20] Verkhovna Rada of Ukraine. Code of Ukraine on Administrative Offences, Article 188-39 (as amended). Available at: https://zakon.rada.gov.ua/laws/show/80731-10#n1314

[21] Verkhovna Rada of Ukraine (2022). Draft Law № 8153 "On Personal Data Protection" (submitted 18 October 2022, first reading adopted 20 November 2024). Available at: https://itd.rada.gov.ua/billInfo/Bills/Card/40485

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License