Lex Scientia Law Review
Vol. 8 Issue 1 (2024) 405–432
DOI: https://doi.org/10.15294/lslr.v8i1.2081
Online since: September 22, 2024

LEX SCIENTIA LAW REVIEW
https://journal.unnes.ac.id/journals/lslr/index

Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds

Naeem AllahRakha [a]
[a] Tashkent State University of Law, Tashkent, Uzbekistan

✉ Corresponding email: chaudharynaeem133@gmail.com

Abstract

This paper examines cybersecurity regulations and practices for safeguarding digital assets like data in today's interconnected landscape. As cyber risks flourish, comprehensive frameworks outlining technical, administrative, and legal protocols are vital for securing critical systems and sensitive information. The paper's background emphasizes rising digitization, surging threat sophistication, and necessitating diligent governance. Its objectives include analyzing prominent regulations and highlighting principles around confidentiality, integrity, and availability. The qualitative study adopts a doctrinal approach and grounded theory analysis to methodically assess prominent legislation. The paper discusses legislative developments in domains like breach disclosure, identity authentication, and encryption methodologies that strengthen cyber resilience. It suggests reconciling compliance complexity through oversight alignment. The paper concludes by underscoring the need for positive incentives and public-private partnerships that collectively enhance cyber hygiene. It recommends consistent interpretation and proactive

investments in capacity building to secure our deepening digital economy against exponentially evolving threats.

KEYWORDS *Cybersecurity, Digital Assets, Privacy, Data Protection, Legal Framework*

Introduction

Digital assets refer to any information, data, or media stored in digital formats that hold potential value. Unlike physical assets, they have a virtual presence, being hosted online, in the cloud, or on devices.[1] Digital assets span a wide spectrum, from personal items like photos, emails, and social media content to financial instruments like cryptocurrencies and stable coins.[2] They also include intellectual property like trademarks, manuscripts, and artwork in digital form. With growing digitization, such virtual materials are deeply interwoven into professional and personal realms. The robust frameworks governing the usage, ownership, and transferability of digital assets become imperative. The UNIDROIT Principles 2 (2) define digital assets as "Electronic records subject to control," underscoring their significance in contemporary legal and economic frameworks.[3]

Cybersecurity involves practices and technologies safeguarding internet-connected systems like hardware, software, networks, and data against digital threats. It ensures the confidentiality, integrity, and availability of information assets against security risks.[4] As per ITU-T X.1205, cybersecurity strives to attain key properties like authenticity, traceability, recovery, and non-repudiation across systems and data by applying appropriate tools, policies,

---

1 Polanco, Rodrigo. "The Impact of Digitalization on International Investment Law: Are Investment Treaties Analogue or Digital?" *German Law Journal* 24, no. 3 (2023): 574–88. https://doi.org/10.1017/glj.2023.30.

2 Garrido, José M. *Digital Tokens: A Legal Perspective*. IMF Working Paper WP/23/151, 2023.

3 International Institute for the Unification of Private Law (UNIDROIT). *UNIDROIT Principles on Digital Assets and Private Law*. 2023. Accessed May 27, 2024. https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked.pdf.

4 Sergiienko, Nataliia, Volodymyr V. Prylovskyi, Mykhailo Burdin, Maryna O. Dei, and Hanna Z. Ostapenko. "Enforcement Actions and Their Suspension: The Concept and Legal Regulation in Ukraine, Georgia, Kazakhstan, Armenia". *Lex Scientia Law Review* 6, no. 2 (2022): 299-326. https://doi.org/10.15294/lesrev.v6i2.55974

training, and risk management. Organizations and users' assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and the user's assets against relevant security risks in the cyber environment.[5] The general security objectives comprise the availability, integrity—which may include authenticity and non-repudiation, and confidentiality.

As society grows interconnected, vast personal and professional data gets stored and transmitted online. The robust cybersecurity becomes imperative to prevent unauthorized access and criminal misuse. Comprehensive cybersecurity encompasses technology, policies, training, and risk management, guiding organizations on safe data handling. As Uzbekistan's Law on Cybersecurity No. ZRU-764 (2022) states in Article 3, cyber security "condition of security of interests of the personality, society and state from external and internal threats in cyberspace."[6] The GDPR requires that personal data be processed securely using appropriate technical and organizational measures.[7]

Robust cybersecurity is vigorous to securely sustain today's data-driven landscape across sectors. Digital liabilities can undermine rights, privacy, infrastructure stability, and organizational interests if inadequately addressed.[8] The governments worldwide are establishing holistic cybersecurity frameworks guiding technology usage policies and compliances. For instance, the EU's NIS Directive created cyber risk assessment and incident reporting obligations for operators of essential services. Similarly, the US NIST Cybersecurity Framework helps organizations align cyber risk management with business requirements and legal imperatives. Such frameworks detail control guidelines, best practices, governance principles, and standards tailored for different domains. Adhering to appropriate regimes like ISO 27001, ISO 27002, CIS

---

5 Tzavara, V., and S. Vassiliadis. "Tracing the Evolution of Cyber Resilience: A Historical and Conceptual Review." *International Journal of Information Security*, 2024. Advance online publication. https://doi.org/10.1007/s10207-023-00811-x

6 Republic of Uzbekistan. *Law of April 15, 2022 No. ZRU-764: About Cyber Security*. April 15, 2022. Accessed May 27, 2024. https://cis-legislation.com/document.fwx?rgn=139485

7 European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. GDPR-info.eu. Accessed May 27, 2024. https://gdpr-info.eu/art-5-gdpr/

8 Koos, Stefan. "Digital Globalization and Law". *Lex Scientia Law Review* 6, no. 1 (2022): 33-68. https://doi.org/10.15294/lesrev.v6i1.55092

Controls, PCI-DSS, COBIT, HITRUST Common Security Framework, or industry-specific ones sustains data integrity and system resilience.[9]

The data is information that has been translated into a form that is efficient for movement or processing. Safeguarding digital assets like data and information systems is an urgent imperative today, given the deep integration of technology across critical infrastructure. A 2020 estimate pegs the global economic impact of cybercrime at nearly 4% of global GDP, underscoring data security's profound business relevance.[10] Beyond immediate monetary losses, breaches erode consumer and partner trust, efficiency, staff morale, and competitiveness for organizations. Sectorally too, healthcare, banking, or education entities that are custodians of sensitive user data bear ethical obligations around privacy and availability assurances. The ITU has a cybersecurity capacity building program for developing countries. At least 114 national governments have adopted cybersecurity strategies and 118 have established national Computer Security Incident Response Teams (CSIRTs).[11]

In today's interconnected world, data security transcends IT departments, significantly impacting brand perception. Between 2005 and 2019, developing country households with home computers rose from 15.6% to 36.1%, while mobile phone subscriptions per 100 people tripled globally and quadrupled in low- and middle-income countries by 2020.[12] Additionally, in 2020, registered mobile money accounts surged by 12.7% globally to reach 1.21 billion, double the anticipated growth rate. Cybercrime incurred direct monetary losses of nearly USD 945 billion in 2020, almost double the figure from 2018. Cybersecurity spending for 2020 was projected to surpass USD 145 billion, constituting 1.3% of global GDP. Africa suffered an estimated USD 3.5 billion in direct losses due to cybercrime in 2017. The comprehensive economic impact of cybercrime, encompassing direct, indirect, and systemic costs, is estimated to be three times its direct cost, amounting to approximately

---

[9] Chaisse, Julien, and Christian Bauer. "Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration." *Vanderbilt Journal of Entertainment & Technology Law* 21, no. 3 (2019): 549-589.

[10] Wicaksono, Raden Mas Try Ananto. "Reviewing Legal Justice, Certainty, and Legal Expediency in Government Regulation Number 24 of 2018 Concerning Electronically Integrated Business Services". *Lex Scientia Law Review* 5, no. 1 (2021): 1-24. https://doi.org/10.15294/lesrev.v5i1.44905

[11] Tariq, U., Ahmed, I., Bashir, A. K., and Shaukat, K. "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review." *Sensors* 23, no. 8 (2023): 4117. https://doi.org/10.3390/s23084117

[12] Haganta, Raphael. "Legal Protection of Personal Data as Privacy Rights of E-Commerce Consumers Amid the Covid-19 Pandemic". *Lex Scientia Law Review* 4, no. 2 (2020): 77-90. https://doi.org/10.15294/lesrev.v4i2.40904

USD 4 trillion in 2020, aligning with forecasts projecting annual global cybercrime costs of USD 6 trillion in 2021.[13]

Digital systems and sensitive information assets face a multitude of cyber threats that can have severe disruptive consequences. Critical infrastructure risks paralysis through attacks targeting industrial control systems, power grids, or manufacturing networks, including top companies like Yahoo, LinkedIn, Facebook, and Marriott International. Smartphones are everywhere; not only are they used for personal connection and communication, but they are often essential for business, which makes them even more vulnerable to cyber threats. Even ransomware that encrypts data can cripple functionality. The breaches erode consumer trust and reputation. It is true that cybersecurity teams often use powerful, cutting-edge technologies to protect data and other corporate assets. But it is also true that many threats can be mitigated using less-advanced methods.[14]

Cybersecurity regulations are indispensable in today's digital landscape, serving as a critical framework for protecting sensitive data and mitigating cyber threats. These regulations establish comprehensive standards and guidelines that organizations must adhere to, ensuring the robust safeguarding of information assets.[15] Without such regulations, businesses risk overlooking crucial security measures, leaving themselves vulnerable to a myriad of cyber threats, including malware, phishing attacks, and unauthorized access. Similar to how workplace safety regulations have become ingrained in ensuring employee welfare, cybersecurity regulations are imperative for fostering a culture of awareness and accountability in addressing evolving cyber risks. Foregoing regulatory steps like multifactor authentication, pen tests, and threat hunts is the cyber equivalent of a surgeon not washing their hands before operating or a traffic patrol officer starting work without a regulation safety vest.[16]

The primary purpose of this study is to provide a comprehensive examination of cybersecurity regulations and practices for safeguarding digital

---

[13] Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. "Digital Technologies: Tensions in Privacy and Data." *Journal of the Academy of Marketing Science* 50, no. 5 (2022): 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

[14] Javaid, M., Haleem, A., Singh, R. P., & Suman, R. "Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends." *Cyber Security and Applications* 1 (2023): 100016. https://doi.org/10.1016/j.csa.2023.100016

[15] Inggarwati, Melodia Puji, Olivia Celia, and Berliana Dwi Arthanti. "Online Single Submission dor Cyber Defense and Security in Indonesia". *Lex Scientia Law Review* 4, no. 1 (2020): 83-95. https://doi.org/10.15294/lesrev.v4i1.37709

[16] Dunn Cavelty, Myriam, and Andreas Wenger, eds. *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*. London: Routledge, 2022. https://doi.org/10.4324/9781003110224

assets, particularly data, in today's interconnected landscape. The objective is to analyze the legal frameworks, principles, and guidelines that govern the protection of sensitive information and mitigate cyber threats. The study delves into prominent regulations, such as the EU's NIS Directive, GDPR, and Uzbekistan's cybersecurity laws, as well as international standards like ISO 27001 and CIS Controls. By exploring these authoritative sources, the research aims to highlight the fundamental principles of confidentiality, integrity, and availability that underpin effective cybersecurity measures. Furthermore, the study seeks to elucidate the intricate relationship between cybersecurity compliance and data protection, emphasizing the legal obligations and accountability measures that organizations must adhere to in order to safeguard digital assets and uphold privacy rights. It examines the technical, administrative, and legal protocols that collectively contribute to fostering a robust cybersecurity posture, addressing issues such as breach disclosure, identity authentication, encryption methodologies, and incident response mechanisms.

RQ: How can cybersecurity regulations and practices effectively safeguard digital assets in today's interconnected landscape?

H 1: Comprehensive cybersecurity regulations that encompass technical, administrative, and legal protocols are crucial for securing critical systems and sensitive information against evolving cyber threats.

H 2: Adherence to international standards and best practices, such as ISO 27001 and CIS Controls, enhances an organization's ability to protect digital assets by implementing proven security measures and risk management strategies.

H 3: Effective cybersecurity practices, including robust encryption, multi-factor authentication, and incident response mechanisms, play a pivotal role in upholding the principles of confidentiality, integrity, and availability of digital assets.

The significance of this study lies in its timeliness and relevance in the face of the rapidly evolving cybersecurity landscape. As digitization pervades every aspect of modern society, the protection of digital assets, particularly sensitive data, has become a paramount concern for individuals, organizations, and governments alike. The study contributes to the growing body of knowledge surrounding cybersecurity regulations and practices, providing valuable insights for policymakers, legal professionals, cybersecurity experts, and organizational decision-makers. Furthermore, the study's emphasis on principles such as confidentiality, integrity, and availability highlight the

fundamental objectives that cybersecurity measures aim to achieve, ensuring the protection of sensitive information and the continuity of critical systems. Ultimately, the significance of this study lies in its potential to inform and guide stakeholders in navigating the complexities of the digital landscape, promoting a collaborative approach to cybersecurity that involves regulatory bodies, industry leaders, and individuals alike.

This study adopts a qualitative methodology using doctrinal research and grounded theory analysis to examine cybersecurity regulations and practices for safeguarding digital assets. Qualitative methods enable an in-depth, nuanced exploration of complex legislative and policy frameworks governing technology usage and data protection. The inductive nature of qualitative research supports constructing robust understandings grounded in the rigorous study of authoritative legal sources. This aligns with a doctrinal approach centered on analyzing primary legal materials like statutes, case law, and regulatory guidance. Doctrinal research facilitates a systematic assessment of legal principles, rights, obligations, and evolving jurisprudence around digital governance.[17]

For this study, key legislation, including the EU's NIS Directive, GDPR, and recent cybersecurity regulations in Uzbekistan, as well as prominent international standards like ISO 27001, were reviewed. These authoritative doctrinal sources formed the primary data corpus analyzed using grounded theory methods. Grounded theory entails the iterative coding of qualitative data to derive conceptual categories and identify explanatory relationships through an inductive process. As categories and theoretical linkages emerge from the textual data, they guide further targeted analysis in successive coding cycles, termed constant comparison. Eventually, conceptual saturation results in a coherent framework rooted in the original information. This data-driven inductive approach prevents preconceptions from narrowing findings, allowing substantive theories to emerge directly from legislative patterns.[18]

The study's analytical techniques encompass systematic content analysis of legal provisions, principles, and obligations around cybersecurity, data protection, and privacy safeguards. Detailed line-by-line coding of texts identified core themes like confidentiality, availability, purpose limitation, breach notification duties, etc. Extensive memo writing tracked code choices

---

[17] Hamilton, A. B., & Finley, E. P. "Qualitative Methods in Implementation Research: An Introduction." *Psychiatry Research* 280 (2019): 112516. https://doi.org/10.1016/j.psychres.2019.112516

[18] Chun Tie, Y., Birks, M., and Francis, K. "Grounded Theory Research: A Design Framework for Novice Researchers." *SAGE Open Medicine* 7 (2019): 2050312118822927. https://doi.org/10.1177/2050312118822927

and category evolution. Concept mapping visualizes relationships between codes like "accountability," "transparency," and "fairness principles" in gripping process intricacies. By repeatedly moving between data snippets and higher-level abstractions in clearly documented stages, robust, theoretically grounded interpretations arose directly from cybersecurity regulations.[19]

Data Protection in Cybersecurity: A Development of Regulations

Cybersecurity regulations are laws that govern the types of measures an organization must take to protect itself, its data, and its customers from cyber threats and data breaches.[20] The NIS Directive, Europe's pioneering cybersecurity legislation, was updated in 2023 to adapt to increasing digitization and evolving threats. It aims to enhance the overall cybersecurity preparedness of EU Member States by mandating the establishment of vital resources like Computer Security Incident Response Teams (CSIRTs) and competent national network and information systems (NIS) authorities. It fosters cooperation among Member States through a dedicated Cooperation Group, facilitating strategic collaboration and information exchange. The directive instills a culture of security across critical sectors like energy, transportation, finance, and healthcare, mandating businesses deemed essential to implement appropriate security measures and report serious incidents to national authorities.[21]

The General Data Protection Regulation (GDPR) serves as a comprehensive framework for safeguarding personal data from various risks, encompassing both external cybersecurity threats and internal data handling procedures by employees. It emphasizes the necessity of processing personal data securely through appropriate technical and organizational measures without prescribing specific cybersecurity methods. Effective since May 25, 2018, and

---

[19] AllahRakha, Naeem. "Modernizing Criminal and Evidence Laws to Facilitate Tourism in Pakistan." *SSRN*. Accessed May 27, 2024. https://ssrn.com/abstract=4707544

[20] Cremer, Frank, Barry Sheehan, Michael Fortmann, Arash N. Kia, Martin Mullins, Finbarr Murphy, and Stefan Materne. "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability." *Geneva Papers on Risk and Insurance: Issues and Practice* 47, no. 3 (2022): 698–736. Accessed May 27, 2024. doi:10.1057/s41288-022-00266-6

[21] European Union. *Directive (EU) 2022/2555 of the European Parliament and of the Council. "On measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)."* EUR-Lex. Accessed December 14, 2022. https://eur-lex.europa.eu/eli/dir/2022/2555

later adopted into UK law post-Brexit, GDPR encompasses 99 articles covering diverse aspects of data protection and privacy, including consent, the right to erasure, and data breach notification. Notably, GDPR's extraterritorial reach extends to businesses worldwide that handle EU or UK citizens' data. For cybersecurity professionals, while the pursuit of data protection isn't novel, GDPR amplifies the focus with its detailed requirements, particularly concerning data breach reporting and substantial fines, making compliance paramount in global business operations.[22]

Non-compliance with data protection laws carries significant financial penalties. According to the GDPR, companies may face fines of up to 4% of their global annual turnover, or €20 million, for violations. Similarly, in other jurisdictions, fines can reach comparable levels. For serious breaches, authorities may impose fines of up to £17.5 million or 4% of the annual worldwide turnover, whichever is higher. Regulatory bodies typically adopt a risk-based approach to enforcement. In cases of particularly severe violations outlined in Article 83(5) of the GDPR, fines can escalate up to €20 million, or 4% of the undertaking's annual turnover. Compliance with data protection regulations is imperative to avoid such substantial penalties.

Until April 15, 2022, Uzbekistan lacked specific legislation on cybersecurity, with only general mentions in existing laws. However, with the enactment of Law No. ZRU-764 on Cybersecurity, effective July 17, 2022, the country aims to regulate cybersecurity comprehensively. This law, establishes the framework for regulating activities related to cyber security within the country. It delineates key concepts such as cybercrime, cyberspace, cyber threat, and cyber security incidents, providing a clear understanding of the scope of cyber security concerns.[23] The law aims to safeguard the interests of individuals, society, and the state from both external and internal threats in cyberspace, emphasizing the importance of protecting critical information infrastructure. It outlines measures for cyber protection, including legal, organizational, and technical aspects, to prevent cyber-attacks, identify vulnerabilities, and ensure

---

[22] European Parliament, & Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. EUR-Lex. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

[23] AllahRakha, N. "Demystifying the Network and Cloud Forensics' Legal, Ethical, and Practical Considerations." *Pakistan Journal of Criminology* 16, no. 2 (2024): 119-132. https://doi.org/10.62271/pjc.16.2.119.132

the stability and reliability of telecommunication networks and information systems.[24]

The Law of the Republic of Uzbekistan on Personal Data, adopted on April 16, 2019, aims to regulate the handling of personal data within the country. This legislation, comprising this law and other related legal acts, governs various aspects of personal data processing and protection. It applies universally, encompassing all activities involving the handling of personal data, irrespective of the methods used for processing, including digital technologies.[25] However, certain exemptions are outlined, such as personal data processing for non-commercial or domestic purposes, archival document management, and data pertaining to state secrets or law enforcement activities. The law defines key terms such as 'personal data,' 'data subject,' 'personal database,' 'processing of personal data,' 'operator,' 'owner,' and 'third party.' Emphasizing principles such as respecting constitutional rights, ensuring the legality and accuracy of data processing, maintaining confidentiality and security, and upholding equality among stakeholders, the law underscores the significance of safeguarding individual rights, societal welfare, and national interests.[26]

The recent amendments to Article 46-2 of the Administrative Responsibility Code stipulate fines for violations of personal data laws, with citizens facing fines typically ranging from 3 to 5 times the minimum wage, while officials may incur fines from 5 to 10 times the minimum wage. However, under amendments to Article 141-2 of the Criminal Code, repeat offenses within a year could lead to more severe penalties, including fines of up to 150 times the minimum wage, deprivation of certain rights for up to 3 years, or up to 2 years of correctional work. These measures aim to enforce compliance with personal data regulations and deter future infractions, highlighting the importance of safeguarding individuals' privacy rights in accordance with the law.[27]

---

[24] AllahRakha, N. "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations." *Mexican Law Review* 16, no. 2 (2024): 23-54

[25] International Conference on Engineering and Computer Science. 2022. "The Use of Innovative Technology in Accelerating Problems Sustainable Development." *AIP Conference Proceedings* 3109, no. 1 (April 9, 2024): 030007. https://doi.org/10.1063/5.0204895

[26] Republic of Uzbekistan. *Law on Personal Data (No. LRU-547, 02.07.2019)*. Retrieved from https://lex.uz/docs/4831939

[27] Republic of Uzbekistan. *The Code of the Republic of Uzbekistan about the Administrative Responsibility (No. 2015-XII, September 22, 1994) (as amended on 15-11-2023)*. CIS Legislation. Retrieved from https://cis-legislation.com/document.fwx?rgn=751

The National Institute of Standards and Technology (NIST) has released the latest version of its Cybersecurity Framework (CSF), known as CSF 2.0. This update is intended to be accessible to a wide range of users, including small organizations, schools, and large corporations, regardless of their level of cybersecurity expertise.[28] CSF 2.0 has a broader scope, extending beyond critical infrastructure to encompass all types of organizations. It introduces a new focus on governance, highlighting the importance of informed decision-making in cybersecurity strategy at the senior leadership level. It was organized around six key functions: identify, protect, detect, respond, recover, and the newly added govern function. Together, these functions offer a comprehensive approach to managing cybersecurity risk throughout its life cycle.[29]

The Cybersecurity Framework (CSF) Profile for Genomic Data offers voluntary guidance to aid organizations in managing cybersecurity and privacy risks associated with processing genomic data. Developed in collaboration with stakeholders from industry, academia, and government, it builds upon NIST Internal Report (IR) 8467 and responds to directives from Congress and the White House. The profile outlines 12 genomic-related mission objectives and prioritizes relevant CSF subcategories, facilitating organizations in understanding and improving their cybersecurity practices pertaining to genomic data.[30] It enables organizations to assess current practices, develop tailored organizational profiles, and prioritize cybersecurity investments aligned with their mission objectives. While intended as a supplement to existing standards and regulations, the profile emphasizes the importance of addressing privacy risks alongside cybersecurity concerns, with plans for a complementary Privacy Framework Profile in the future.[31]

ISO/IEC 27001:2022 is the globally recognized standard for information security management systems (ISMS), providing guidance for organizations of all sizes and sectors to establish, implement, and continually improve their security protocols.[32] Compliance with ISO/IEC 27001 signifies

---

[28] Allen, Brian, Brandon Bapst, and Terry Allan Hicks. *Building a Cyber Risk Management Program*. "O'Reilly Media, Inc.", 2023, pp. 20-21

[29] National Institute of Standards and Technology. "NIST Releases Version 2.0 of Landmark Cybersecurity Framework." Published February 26, 2024. Accessed May 27, 2024. https://www.nist.gov/cyberframework

[30] Saeed, Saqib, Neda Azizi, Shahzaib Tahir, Munir Ahmad, and Abdullah M. Almuhaideb. *Strengthening Industrial Cybersecurity to Protect Business Intelligence*. IGI Global, February 14, 2024

[31] NIST. "Cybersecurity Framework Profile for Genomic Data (NIST IR 8467, Initial Public Draft)." June 15, 2023. https://csrc.nist.gov/pubs/ir/8467/ipd

[32] Watkins, Steve G. *ISO/IEC 27001:2022: An Introduction to Information Security and the ISMS Standard*. IT Governance Publishing, 2022. https://doi.org/10.2307/j.ctv30qq13d

that an organization has implemented a robust system to manage risks associated with data security, adhering to internationally accepted best practices. In an era where cyber threats are prevalent and evolving rapidly, ISO/IEC 27001 fosters a proactive and comprehensive approach to cybersecurity, encompassing people, processes, and technology. Certification to this standard demonstrates a commitment to information security excellence and provides assurance to stakeholders that an organization is effectively managing its cyber risks and enhancing operational resilience.[33]

ISO/IEC 27002 is an international standard providing guidance on cybersecurity best practices for implementing an information security management system protecting organizational data assets. It complements ISO/IEC 27001, which outlines the requirements for an ISMS. As cyber risks proliferate with deepening digitization, ISO/IEC 27002 equips businesses to take a proactive and systematic approach to safeguarding critical information against threats like data breaches, unauthorized access, and reputational hazards. The standard gives, a risk-based framework leveraging industry best practices around access controls, human resource protocols, encryption, and incident response. Following ISO/IEC 27002 guidelines signifies an enterprise's commitment to fostering trust and accountability among stakeholders through robust cybersecurity policies and procedures.[34] It forms part of the ISO 27000 family of standards driving end-to-end organizational resilience in today's complex digital environment.[35]

The Center for Internet Security's CIS Critical Security Controls comprise a prioritized, risk-based set of cybersecurity best practices that provide a blueprint for organizations to improve protections against prevalent threats.[36] Consolidating safeguards by functional activities rather than infrastructure management, these controls evolved from the SANS Critical Security Control (SANS Top 20) guidelines to the current framework of 18 actionable controls spanning diverse domains like access management, data protection, awareness training, and incident response. These are now officially called the CIS Critical Security Controls (CIS Controls). Backed by global collaboration between security experts, technology partners, and customers, the CIS Controls tackle

---

[33] ISO/IEC. "Information security, cybersecurity and privacy protection (ISO/IEC 27001:2022)." Accessed May 27, 2024. https://www.iso.org/standard/27001

[34] ISO. *Information security, cybersecurity and privacy protection.* (ISO/IEC 27002:2022). Accessed May 27, 2024. https://www.iso.org/standard/75652.html

[35] ISO. *Information security management.* (ISO/IEC 27000 family). Retrieved from https://www.iso.org/standard/iso-iec-27000-family

[36] Center for Internet Security. *CIS Controls.* (2021). Retrieved from https://www.cisecurity.org/controls

increasingly sophisticated attack types while supporting innovation and operational objectives. They signify an enterprise's commitment to holistic cyber-risk governance centered on collective knowledge, pragmatic controls, and metrics-driven maturity. CIS also houses the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).[37]

The Payment Card Industry Security Standards Council (PCI SSC) serves as a global platform for collaboration among stakeholders in the payments industry, aiming to establish and promote data security standards for secure transactions worldwide. These standards, such as the PCI Data Security Standard (PCI DSS), are designed to safeguard payment account data across various stages of the payment process, discouraging theft by making such data less valuable to cybercriminals.[38] PCI DSS outlines specific requirements for entities involved in processing, storing, or transmitting cardholder data, mirroring established security best practices. Key objectives include maintaining a secure network and systems, protecting cardholder data through encryption and access controls, implementing vulnerability management programs, monitoring networks regularly, and upholding information security policies.[39]

COBIT, which stands for Control Objectives for Information and Related Technology, is a framework developed by the ISACA (Information Systems Audit and Control Association) to assist managers in bridging the gap between technical aspects, business risks, and control requirements within an organization. It serves as a guideline applicable to any industry, ensuring the quality, control, and reliability of information systems, a critical aspect of modern business operations. COBIT 5, the latest version, serves as the overarching framework for the governance and management of enterprise IT. It outlines five principles, including meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach, and separating governance from management. These principles, alongside the seven supporting enablers, provide a comprehensive

---

[37] Center for Internet Security. *Elections Infrastructure Information Sharing & Analysis Center*. (2020). https://www.cisecurity.org/elections-isac/

[38] Ronit, Karsten. "The Governance of Global Industry Associations: The Role of Micro-Politics." In *Elgar Politics and Business series*, 200-204. Edward Elgar Publishing, 2022

[39] PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard* (2023). Retrieved from https://otm.finance.harvard.edu/files/otm/files/pci_security_standards.pdf

approach to the governance and management of IT, effectively aligning organizational goals with IT strategies effectively.[40]

The HITRUST Common Security Framework (CSF) stands as a certifiable framework designed to assist healthcare organizations and their providers in demonstrating security and compliance in a streamlined manner. Unlike ISO audits, which involve a less collaborative process, the Approach incorporates both assessment and review by HITRUST alongside validation by an independent third party. Leveraging nationally and internationally accepted security and privacy-related regulations, standards, and frameworks such as ISO, NIST, PCI, HIPAA, and GDPR, the CSF offers a comprehensive set of controls while continually integrating additional authoritative sources. The CSF provides clarity, consistency, and ultimately reduces the compliance burden for organizations globally, ensuring certainty in data protection compliance.[41]

Analysis of Data Protection in Cybersecurity: Problems and Challenges

The fundamental principles governing cybersecurity in law are the tenets of information security: confidentiality, integrity, and availability.[42] Every element of the information security program must be designed to implement one or more of these principles.

1) The principle of confidentiality serves to uphold privacy rights by restricting access to sensitive data solely to individuals who require it for their designated roles within an organization.
2) The principle of integrity guarantees that data remains accurate and dependable, free from unintended or malicious alterations. It encompasses safeguarding against unauthorized modifications such as additions, deletions, or alterations to the data.

---

[40] Lee, I. "What Is COBIT (Control Objectives for Information Technology)? 5 Main Principles." *Wallarm Learning Center*, 2023. Accessed May 27, 2024. https://www.wallarm.com/what/what-is-cobit-control-objectives-for-information-technology

[41] Abohatem, A. Y., Ba-Alwi, F. M., & Al-Khulaidi, A. A. "Suggestion Cybersecurity Framework (CSF) for Reducing Cyber-Attacks on Information Systems." *Sana'a University Journal of Applied Sciences and Technology* 1, no. 3 (2023). https://doi.org/10.59628/jast.v1i3.248

[42] Marquenie, T., & Quezada, K. "Operationalization of Information Security through Compliance with Directive 2016/680 in Law Enforcement Technology and Practice." In *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, edited by A. Vedder, J. Schroers, C. Ducuing, & P. Valcke, 97–128. Intersentia, 2019

3) The principle of availability pertains to ensuring that a system, including its software and data, remains fully accessible to users whenever they require it or at predetermined times. The primary goal of availability is to guarantee that the technological framework, applications, and data are readily accessible whenever they are necessary for an organizational function or to serve the needs of the organization's clientele.

Adhering to cybersecurity policies like confidentiality and availability is now intertwined with legal compliance across sectors. Cybersecurity compliance means adhering to industry regulations, standards, and laws related to information security and data privacy.[43] Regulation's mandate safeguarding sensitive information, while GDPR requires security controls aligned with privacy principles. Such laws expose non-compliant entities to lawsuits, financial penalties, and reputational damages for data breaches due to poor cyber hygiene. Frameworks like ISO 27001 that encode security best practices into auditable standards are seeing greater adoption. Technical measures around access controls and encryption complement administrative compliance efforts in data sharing protocols, mandated reporting, and risk management programs. Ultimately, sound cybersecurity strengthens the compliance capacities needed to operate in heavily regulated digital economies worldwide.[44]

In September 2023, Ireland's Data Protection Commission concluded its investigation into TikTok's handling of children's data, finding multiple GDPR infringements like setting underage accounts to public by default and inadequate transparency for young users. This inquiry examined TikTok's data processing practices from July to December 2020 to audit its conformity with GDPR standards on issues like platform privacy settings, age verification, and communication protocols. Ultimately, the DPC issued a €345 million penalty against TikTok for the identified violations, including those around the legal principles of data protection, accountability, fairness and transparency. Alongside the record fine, TikTok must rectify its non-compliant data

[43] Harris, Mark A., and Ronald Martin. "Promoting Cybersecurity Compliance." In *Research Anthology on Privatizing and Securing Data*, edited by Information Resources Management Association, 1990-2007. Hershey, PA: IGI Global, 2021. https://doi.org/10.4018/978-1-7998-8954-0.ch097

[44] Marotta, Anthony, and Stuart Madnick. "Analyzing the Interplay between Regulatory Compliance and Cybersecurity." Working Paper CISL# 2020-06. Massachusetts Institute of Technology, Cambridge, 2020. Accessed May 28, 2024. https://web.mit.edu/smadnick/www/wp/2020-06.pdf

processing within 3 months to align with the GDPR's safeguards and enhance platform security for teenage users.[45]

In accordance with Article 5(2) of the GDPR, controllers and processors must uphold accountability by ensuring compliance with data protection principles and demonstrating such adherence. To foster a culture of accountability, organizations should first familiarize themselves with the six key principles outlined in the GDPR, encompassing legality, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality.[46] Establishing a robust internal privacy governance structure is pivotal, incorporating measures such as documented processes and policies, conducting data protection impact assessments (DPIA), implementing recommended data security protocols, adhering to principles of data protection by design and by default, appointing a Data Protection Officer (DPO) for significant data processing activities, maintaining records of processing activities, and complying with industry codes of conduct, self-certification, data breach notification, and transparency obligations.[47]

The €1.2 billion GDPR fine imposed on Meta by the Irish Data Protection Commission underscores a significant breach of privacy regulations concerning the transfer of personal data from the EU/EEA to the U.S. Despite Meta's efforts to update Standard Contractual Clauses (SCCs) and implement supplementary measures, the arrangements failed to adequately address risks to users' rights and freedoms, as highlighted by a European Court of Justice ruling. This decision signifies a pivotal moment in data protection regulation, emphasizing the necessity for tech giants to adhere to stringent standards. Meta's response, including its intention to appeal the decision and seek legal recourse, underscores the gravity of the situation.[48]

Article 6 of the General Data Protection Regulation (GDPR) delineates the legal bases for processing personal data, which include consent, contract performance, legal obligations, protection of vital interests, public interest tasks,

---

[45] Weckler, Adrian. "TikTok to learn whether sanctions will be imposed by Irish regulator on use of kids' data." *Irish Independent*, August 3, 2023. https://www.independent.ie/business/tiktok-to-learn-whether-sanctions-will-be-imposed-by-irish-regulator-on-use-of-kids-data/a1303646791.html

[46] Quelle, Claudia. "Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach." *European Journal of Risk Regulation* 9, no. 3 (2018): 502–26. https://doi.org/10.1017/err.2018.47

[47] Bateman, R. "6 Privacy Principles of the GDPR." 2023. Retrieved from https://www.termsfeed.com/blog/gdpr-privacy-principles/

[48] EDPB. "1.2 billion Euro Fine for Facebook as a Result of EDPB Binding Decision." Press release, May 22, 2023. Accessed from https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

and legitimate interests. Processing must align with at least one of these bases to be lawful. Additionally, Member States can enact specific provisions to tailor the application of GDPR rules for certain processing situations, particularly concerning legal obligations and public interest tasks. The purpose of processing must be determined by relevant Union or Member State laws, ensuring it serves a public interest objective and remains proportionate.[49] If personal data are to be processed for a purpose other than their initial collection, the controller must assess compatibility factors, such as the relationship between the purposes and the nature of the data, to ensure lawful processing. Recital 82 emphasizes the right to compensation for individuals who suffer harm due to GDPR infringements, underscoring the regulation's accountability measures.[50]

The Luxembourg National Commission for Data Protection (CNDP) imposed a record-breaking fine of €746 million ($888 million) on Amazon Europe Core S.a.r.l. for breaching the General Data Protection Regulation (GDPR), marking a significant milestone in GDPR enforcement. This fine, stemming from a complaint filed by 10,000 individuals in May 2018, underscores the growing scrutiny over how companies handle personal data. Amazon's infringement, related to its advertising targeting system lacking proper consent, highlights the stringent requirements of GDPR regarding transparent data processing practices. Despite Amazon's intention to appeal, the magnitude of this fine signals a pivotal moment demonstrating GDPR's enforcement capabilities and its pivotal role in safeguarding data privacy rights within the European Union.[51]

Article 21 of Directive (EU) 2022/2555 requires entities to implement appropriate encryption as part of cybersecurity risk management measures safeguarding confidentiality. Robust encryption upholds privacy by preventing unauthorized access to sensitive personal information. Pseudonymization and anonymization similarly rely on transforming identifiers to manage privacy risks in analytics. Under Article 14, processing and sharing threat data containing

---

[49] Molnár-Gábor, Fruzsina, Julian Sellner, Sophia Pagil, Santa Slokenberga, Olga Tzortzatou-Nanopoulou, and Katarina Nyström. "Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden." *Seminars in Cancer Biology* 84 (September 2022): 271-283. https://doi.org/10.1016/j.semcancer.2021.12.001

[50] Kostadinova, Z. R. "Purpose Limitation under the GDPR: Can Article 6(4) Be Automated?" Tilburg University, 2019. https://arno.uvt.nl/show.cgi?fid=146471

[51] Shead, Sam. "Amazon Hit with $887 Million Fine by European Privacy Watchdog." *CNBC*, July 30, 2021. https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-.html

personal information must follow GDPR consent, purpose, and storage principles. It focuses on the principles of transparency in instances where data is collected indirectly, e.g., from a third party.[52] In such circumstances, controllers need to provide information to data subjects at the point of collection or immediately following. Article 28(3) states that the contract (or other legal act) must include the following details about the processing: the subject matter and duration of the processing; the nature and purpose of the processing; the type of personal data and categories of data subject; and. the controller's obligations and rights.[53]

The Court of Justice of the European Union, in its judgment of Case C-154/21 (RW V. Österreichische Post AG) delivered on January 12, 2023, clarified the obligations regarding the disclosure of personal data recipients under Article 15 GDPR. Data subjects are entitled to receive information either about the specific recipients or the categories of recipients to whom their personal data have been or will be disclosed, with precision being paramount for effective exercise of their rights. However, the right of access may be restricted, especially when the identity of specific recipients is unknown, allowing disclosure limited to recipient categories.[54] Additionally, controllers can refuse requests deemed manifestly unfounded or excessive under Article 12(5)(b) GDPR. Consequently, controllers must prioritize providing information on specific recipients where feasible in response to access requests, ensuring compliance with GDPR provisions.[55]

Timely breach reporting and assisting affected individuals are legal duties under GDPR, as acknowledged in Article 14. But strong encryption can mask unauthorized data access, so entities may remain unaware of compromised assets. The contextually appropriate cryptography balanced with logging, analytics, and internal detection controls is vital. Authentication mechanisms

---

[52] Ducato, Rossana. "Data Protection, Scientific Research, and the Role of Information." *Computer Law & Security Review* 37 (July 2020): 105412. https://doi.org/10.1016/j.clsr.2020.105412

[53] Papathanasiou, A., Liontos, G., Liagkou, V., & Glavas, E. "Business Email Compromise (BEC) Attacks: Threats, Vulnerabilities and Countermeasures. A Perspective on the Greek Landscape." *Journal of Cybersecurity and Privacy* 3, no. 3 (2023): 610-637. https://doi.org/10.3390/jcp3030029

[54] Purtova, Nadezhda. "From Knowing by Name to Targeting: The Meaning of Identification under the GDPR." *International Data Privacy Law* 12, no. 3 (August 2022): 163–183. https://doi.org/10.1093/idpl/ipac013

[55] Court of Justice of the European Union. "Case C-154/21: RW v Österreichische Post." 2023. Accessed May 27, 2024. https://gdprhub.eu/index.php?title=CJEU_-_C-154/21_-_RW_v_%C3%96sterreichische_Post#:~:text=The%20CJEU%20held%20that%20Article,categories%20of%20recipients%20is%20sufficient

can also trace the data lineage, establishing breach accountability. And securely storing identity proofs reduces identity fraud following leaks. Additionally, Chapter VII oversight procedures verify ongoing legal compliance with security strategies. So while robust encryption and authentication strengthen data protection, their design intricacies require diligence to still fulfill notification mandates through alternate verification methods.[56]

Article 28 of Directive (EU) 2022/2555 (NIS-2) requires domain registries to establish identity verification procedures for registrants, recognizing such validation's role in addressing cybercrime like phishing. It aims to improve WHOIS data accuracy for security and contactability. E-signature regulations also demonstrate authentication's legal validity in online transactions. Encryption proves records weren't altered post-signing via keys cryptographically traceable to parties.[57] Audit trails authenticating system access and data flows can affirm compliance in disputes. Article 20 upholds accountability by enabling the clear attribution of cybersecurity liability to natural persons or legal entities. This depends on assured identities. Article 21 requires multi-factor authentication for access control security. Strong authentication fulfilling eIDAS levels enables mutual recognition across the EU.[58]

The EU digital legislative package, specifically the NIS2 Directive, mandates essential entities to promptly report cyber incidents with significant impact to the competent authority and possibly their service recipients, regardless of whether personal data is involved. These incidents include those causing severe operational disruption, financial loss, or significant harm to individuals or entities. Reporting timelines are stringent, requiring an initial alert within 24 hours of awareness, followed by formal notification within 72 hours, and a comprehensive report within one month. Moreover, entities must provide status updates and cooperate with the authority, which can compel public disclosure if necessary. Information sharing on cyber threats and

---

[56] Daigle, B., & Khan, M. The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities. *Journal of International Commerce and Economics.* (2020). Retrieved from https://www.usitc.gov/journals

[57] Reed, Christopher. "Legally Binding Electronic Documents: Digital Signatures and Authentication." *The International Lawyer* 35, no. 1 (2001): 89–106. http://www.jstor.org/stable/40707597

[58] Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. A., & Ranise, S. "The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes." *Applied Sciences* 12, no. 24 (2022): 12679. https://doi.org/10.3390/app122412679

vulnerabilities is encouraged, aiming to bolster cybersecurity and mitigate incident impacts, although it is largely voluntary.[59]

The CJEU's judgment in Case C-340/21 (VB V. Natsionalna agentsia za prihodite) clarified that fear stemming from the potential misuse of personal data can constitute non-material damage, subject to national court assessment. Controllers are liable for such damage unless they can prove they bear no responsibility, emphasizing the importance of robust security measures. The burden lies with controllers to demonstrate the adequacy of security measures under Article 32 GDPR in actions for damages under Article 82 GDPR. This ruling underscores the significance of implementing effective technical and organizational safeguards to mitigate risks associated with personal data processing, aligning with EU principles while accommodating national legal frameworks.[60]

Conclusion

Cybercrime has emerged as a severe threat to companies as attack sophistication and costs spiral. Annual global losses are predicted to hit $6 trillion by 2021. Firms across sectors face escalating risks from malware, ransomware, phishing, and even insider actions jeopardizing data security. Heightened regulations also mandate stricter safeguards, evident in rising compliance budgets. While boards now prioritize cyber risks more, persistent talent and technology constraints lead to incidents. Quantum computing's decryption capabilities could overhaul defensive strategies. Although perfect security is impossible currently, businesses must invest in multi-layered prevention coupled with response readiness to minimize breach fallout. Joint public-private efforts addressing the surging global challenge are vital. Ultimately, cyber resilience hinges on proactive governance rather than reactive measures alone to combat exponentially evolving threats.

Robust cyberforensic capabilities enabling swift evidence gathering and analysis following incidents remain inadequate presently, although digital evidence guides response protocols and policy interventions. Constraints like investigating staff shortages, limited computational resources, outdated tools struggling with expanding attack sophistication, and siloed information sharing

---

[59] Gliklich, R. E., Dreyer, N. A., & Leavy, M. B., eds. *Registries for Evaluating Patient Outcomes: A User's Guide*. 3rd ed. Agency for Healthcare Research and Quality (US), 2014. https://www.ncbi.nlm.nih.gov/books/NBK208615/

[60] Court of Justice of the European Union. "Case C 340/21: Natsionalna agentsia za prihodite." European Case Law Identifier: ECLI:EU:C:2023:986. Accessed December 14, 2023. https://gdprhub.eu/index.php?title=CJEU_-_C%E2%80%91340/21_-_Natsionalna_agentsia_za_prihodite

impede timely and accurate threat comprehension. Small teams juggling overloaded caseloads also risk investigation quality. Graduating sufficient specialists to meet diverse sectoral needs poses a systemic challenge too. Addressing the capacity lag mandates prioritizing cyber forensics infrastructure modernization, cross-agency coordination, private sector participation, training investments, and public awareness of its indispensable role in securing cyber-physical systems. Only an integrated capacity-building strategy fulfills the acute need across law enforcement, regulators, critical infrastructure entities, and cyber insurers to rely on forensic insights for informed decisions.

The EU General Data Protection Regulation aimed to provide uniform standards, enabling seamless data flows vital for the single market. However, national legislation adoption has led to fragmentation instead due to legal uncertainty around applicable rules spanning Member State divergence, as evident in domains like consent ages. The GDPR's silence on overlapping laws further compounds compliance complexity for organizations operating across borders. Divergence also risks uneven privacy safeguards for individuals, despite common principles. The consistent interpretation, oversight alignment, and enhanced cooperation are essential to reconciling national differences. Ultimately, high legal certainty and individual rights consistency necessitate maximum harmonization of data protection, especially on pivotal issues around consent, rights, and remedies through collaborative governance. But extreme rigidity risks stifling contextual innovation too. An optimal balance for sustaining EU integration mandates reconciling unity and discretion to uphold both harmony and sovereignty.

Robust breach disclosure and notification protocols enable timely interventions, limiting incident harm. The norms mandating prompt internal escalation upon discovering potential unauthorized access or system anomalies are vital. Public disclosure duties also uphold accountability, provided exemptions for sensitive ongoing investigations apply. Furthermore, proactive resilience investments through cyber hygiene promotion, insurance coverage for self-policing entities, and penalty reductions incentivize continuous upgrades. Security by design principles embedded in procurement contracts and service agreements also foster supply chain diligence. Ultimately, positive incentives balanced with disclosure duties reconciling flexibility and transparency promote collective cyber risk management. But over-penalization risks discouragement, necessitating proportional approaches.

Cyber hygiene involves basic practices like software updates, access management, and employee awareness that address prevalent threats exploiting common vulnerabilities. Since untrained users are among the easiest targets, promoting organizational cyber literacy through continuous training is

essential. Beyond fundamental topics, tailored sessions informing participants of emerging risks like phishing tactics and stressing secure remote access protocols uphold readiness. Furthermore, promoting risk ownership and incident alertness as individual responsibilities binding all workforce levels fosters a proactive culture vigilant towards early anomaly detection. Ultimately, positive messaging centered on resilience through cooperative diligence sustains behavioral change more effectively than punitive measures alone. Still, reinforcement via interactive quizzes assessing comprehension ensures secure habits endure.

The potential legal and regulatory developments around data protection globally include greater convergence between privacy, competition, and consumer protection oversight, like FTC-privacy regulator partnerships addressing risks in adtech. Increased enforcement around children's data protection and responsible AI practices is also likely, given the legislative strengthening of safeguards. Mass claims around unlawful data processing may rise following favorable court judgments. Pan-regional coordination would combat cross-border incident spillovers. With more comprehensive state privacy laws in the US and key rulings on tracking litigation expected, extraterritorial applicability issues will grow in relevance. Meanwhile, the steady emergence of cybersecurity regulations and incident reporting duties would spur information sharing.

References

Abohatem, A. Y., Ba-Alwi, F. M., & Al-Khulaidi, A. A. "Suggestion Cybersecurity Framework (CSF) for Reducing Cyber-Attacks on Information Systems." *Sana'a University Journal of Applied Sciences and Technology* 1, no. 3 (2023). https://doi.org/10.59628/jast.v1i3.248

AllahRakha, N. "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations." *Mexican Law Review* 16, no. 2 (2024): 23-54

AllahRakha, N. "Demystifying the Network and Cloud Forensics' Legal, Ethical, and Practical Considerations." *Pakistan Journal of Criminology* 16, no. 2 (2024): 119-132. https://doi.org/10.62271/pjc.16.2.119.132

AllahRakha, Naeem. "Modernizing Criminal and Evidence Laws to Facilitate Tourism in Pakistan." *SSRN*. Accessed May 27, 2024. https://ssrn.com/abstract=4707544

Allen, Brian, Brandon Bapst, and Terry Allan Hicks. *Building a Cyber Risk Management Program*. "O'Reilly Media, Inc.", 2023, pp. 20-21

Bateman, R. "6 Privacy Principles of the GDPR." 2023. Retrieved from https://www.termsfeed.com/blog/gdpr-privacy-principles/

Center for Internet Security. *CIS Controls*. (2021). Retrieved from https://www.cisecurity.org/controls

Center for Internet Security. *Elections Infrastructure Information Sharing & Analysis Center*. (2020). https://www.cisecurity.org/elections-isac/

Chaisse, Julien, and Christian Bauer. "Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration." *Vanderbilt Journal of Entertainment & Technology Law* 21, no. 3 (2019): 549-589.

Chun Tie, Y., Birks, M., and Francis, K. "Grounded Theory Research: A Design Framework for Novice Researchers." *SAGE Open Medicine* 7 (2019): 2050312118822927. https://doi.org/10.1177/2050312118822927

Court of Justice of the European Union. "Case C 340/21: Natsionalna agentsia za prihodite." European Case Law Identifier: ECLI:EU:C:2023:986. Accessed December 14, 2023. https://gdprhub.eu/index.php?title=CJEU_-_C%E2%80%91340/21_-_Natsionalna_agentsia_za_prihodite

Court of Justice of the European Union. "Case C-154/21: RW v Österreichische Post." 2023. Accessed May 27, 2024. https://gdprhub.eu/index.php?title=CJEU_-_C-154/21_-_RW_v_%C3%96sterreichische_Post#:~:text=The%20CJEU%20held%20that%20Article,categories%20of%20recipients%20is%20sufficient

Cremer, Frank, Barry Sheehan, Michael Fortmann, Arash N. Kia, Martin Mullins, Finbarr Murphy, and Stefan Materne. "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability." *Geneva Papers on Risk and Insurance: Issues and Practice* 47, no. 3 (2022): 698–736. Accessed May 27, 2024. doi:10.1057/s41288-022-00266-6

Daigle, B., & Khan, M. The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities. *Journal of International Commerce and Economics.* (2020). Retrieved from https://www.usitc.gov/journals

Ducato, Rossana. "Data Protection, Scientific Research, and the Role of Information." *Computer Law & Security Review* 37 (July 2020): 105412. https://doi.org/10.1016/j.clsr.2020.105412

Dunn Cavelty, Myriam, and Andreas Wenger, eds. *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation.* London: Routledge, 2022. https://doi.org/10.4324/9781003110224

EDPB. "1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision." Press release, May 22, 2023. Accessed from https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

European Parliament, & Council of the European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. EUR-Lex. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

European Union. *Directive (EU) 2022/2555 of the European Parliament and of the Council. "On measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)."* EUR-Lex. Accessed December 14, 2022. https://eur-lex.europa.eu/eli/dir/2022/2555

European Union. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*. GDPR-info.eu. Accessed May 27, 2024. https://gdpr-info.eu/art-5-gdpr/

Garrido, José M. *Digital Tokens: A Legal Perspective*. IMF Working Paper WP/23/151, 2023.

Gliklich, R. E., Dreyer, N. A., & Leavy, M. B., eds. *Registries for Evaluating Patient Outcomes: A User's Guide*. 3rd ed. Agency for Healthcare Research and Quality (US), 2014. https://www.ncbi.nlm.nih.gov/books/NBK208615/

Haganta, Raphael. "Legal Protection of Personal Data as Privacy Rights of E-Commerce Consumers Amid the Covid-19 Pandemic". *Lex Scientia Law Review* 4, no. 2 (2020): 77-90. https://doi.org/10.15294/lesrev.v4i2.40904

Hamilton, A. B., & Finley, E. P. "Qualitative Methods in Implementation Research: An Introduction." *Psychiatry Research* 280 (2019): 112516. https://doi.org/10.1016/j.psychres.2019.112516

Harris, Mark A., and Ronald Martin. "Promoting Cybersecurity Compliance." In *Research Anthology on Privatizing and Securing Data*, edited by Information Resources Management Association, 1990-2007. Hershey,

PA: IGI Global, 2021. https://doi.org/10.4018/978-1-7998-8954-0.ch097

Inggarwati, Melodia Puji, Olivia Celia, and Berliana Dwi Arthanti. "Online Single Submission for Cyber Defense and Security in Indonesia". *Lex Scientia Law Review* 4, no. 1 (2020): 83-95. https://doi.org/10.15294/lesrev.v4i1.37709

International Conference on Engineering and Computer Science. 2022. "The Use of Innovative Technology in Accelerating Problems Sustainable Development." *AIP Conference Proceedings* 3109, no. 1 (April 9, 2024): 030007. https://doi.org/10.1063/5.0204895

International Institute for the Unification of Private Law (UNIDROIT). *UNIDROIT Principles on Digital Assets and Private Law*. 2023. Accessed May 27, 2024. https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked.pdf.

ISO. *Information security management*. (ISO/IEC 27000 family). Retrieved from https://www.iso.org/standard/iso-iec-27000-family

ISO. *Information security, cybersecurity and privacy protection*. (ISO/IEC 27002:2022). Accessed May 27, 2024. https://www.iso.org/standard/75652.html

ISO/IEC. "Information security, cybersecurity and privacy protection (ISO/IEC 27001:2022)." Accessed May 27, 2024. https://www.iso.org/standard/27001

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. "Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends." *Cyber Security and Applications* 1 (2023): 100016. https://doi.org/10.1016/j.csa.2023.100016

Koos, Stefan.. "Digital Globalization and Law". *Lex Scientia Law Review* 6, no. 1 (2022): 33-68. https://doi.org/10.15294/lesrev.v6i1.55092

Kostadinova, Z. R. "Purpose Limitation under the GDPR: Can Article 6(4) Be Automated?" Tilburg University, 2019. https://arno.uvt.nl/show.cgi?fid=146471

Lee, I. "What Is COBIT (Control Objectives for Information Technology)? 5 Main Principles." *Wallarm Learning Center*, 2023. Accessed May 27, 2024. https://www.wallarm.com/what/what-is-cobit-control-objectives-for-information-technology

Marotta, Anthony, and Stuart Madnick. "Analyzing the Interplay between Regulatory Compliance and Cybersecurity." Working Paper CISL# 2020-06. Massachusetts Institute of Technology, Cambridge, 2020. Accessed May 28, 2024. https://web.mit.edu/smadnick/www/wp/2020-06.pdf

Marquenie, T., & Quezada, K. "Operationalization of Information Security through Compliance with Directive 2016/680 in Law Enforcement Technology and Practice." In *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, edited by A. Vedder, J. Schroers, C. Ducuing, & P. Valcke, 97–128. Intersentia, 2019

Molnár-Gábor, Fruzsina, Julian Sellner, Sophia Pagil, Santa Slokenberga, Olga Tzortzatou-Nanopoulou, and Katarina Nyström. "Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden." *Seminars in Cancer Biology* 84 (September 2022): 271-283. https://doi.org/10.1016/j.semcancer.2021.12.001

National Institute of Standards and Technology. "NIST Releases Version 2.0 of Landmark Cybersecurity Framework." Published February 26, 2024. Accessed May 27, 2024. https://www.nist.gov/cyberframework

NIST. "Cybersecurity Framework Profile for Genomic Data (NIST IR 8467, Initial Public Draft)." June 15, 2023. https://csrc.nist.gov/pubs/ir/8467/ipd

Papathanasiou, A., Liontos, G., Liagkou, V., & Glavas, E. "Business Email Compromise (BEC) Attacks: Threats, Vulnerabilities and Countermeasures. A Perspective on the Greek Landscape." *Journal of Cybersecurity and Privacy* 3, no. 3 (2023): 610-637. https://doi.org/10.3390/jcp3030029

PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard* (2023). Retrieved from https://otm.finance.harvard.edu/files/otm/files/pci_security_standards.pdf

Polanco, Rodrigo. "The Impact of Digitalization on International Investment Law: Are Investment Treaties Analogue or Digital?" *German Law Journal* 24, no. 3 (2023): 574–88. https://doi.org/10.1017/glj.2023.30.

Purtova, Nadezhda. "From Knowing by Name to Targeting: The Meaning of Identification under the GDPR." *International Data Privacy Law* 12, no. 3 (August 2022): 163–183. https://doi.org/10.1093/idpl/ipac013

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. "Digital Technologies: Tensions in Privacy and Data." *Journal of the Academy of Marketing Science* 50, no. 5 (2022): 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

QUELLE, Claudia. "Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-

Based Approach." *European Journal of Risk Regulation* 9, no. 3 (2018): 502–26. https://doi.org/10.1017/err.2018.47

Reed, Christopher. "Legally Binding Electronic Documents: Digital Signatures and Authentication." *The International Lawyer* 35, no. 1 (2001): 89–106. http://www.jstor.org/stable/40707597

Republic of Uzbekistan. *Law of April 15, 2022 No. ZRU-764: About Cyber Security*. April 15, 2022. Accessed May 27, 2024. https://cis-legislation.com/document.fwx?rgn=139485

Republic of Uzbekistan. *Law on Personal Data (No. LRU-547, 02.07.2019)*. Retrieved from https://lex.uz/docs/4831939

Republic of Uzbekistan. *The Code of the Republic of Uzbekistan about the Administrative Responsibility (No. 2015-XII, September 22, 1994) (as amended on 15-11-2023)*. CIS Legislation. Retrieved from https://cis-legislation.com/document.fwx?rgn=751

Ronit, Karsten. "The Governance of Global Industry Associations: The Role of Micro-Politics." In *Elgar Politics and Business series*, 200-204. Edward Elgar Publishing, 2022

Saeed, Saqib, Neda Azizi, Shahzaib Tahir, Munir Ahmad, and Abdullah M. Almuhaideb. *Strengthening Industrial Cybersecurity to Protect Business Intelligence*. IGI Global, February 14, 2024

Sergiienko, Nataliia, Volodymyr V. Prylovskyi, Mykhailo Burdin, Maryna O. Dei, and Hanna Z. Ostapenko. "Enforcement Actions and Their Suspension: The Concept and Legal Regulation in Ukraine, Georgia, Kazakhstan, Armenia". *Lex Scientia Law Review* 6, no. 2 (2022): 299-326. https://doi.org/10.15294/lesrev.v6i2.55974

Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. A., & Ranise, S. "The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes." *Applied Sciences* 12, no. 24 (2022): 12679. https://doi.org/10.3390/app122412679

Shead, Sam. "Amazon Hit with $887 Million Fine by European Privacy Watchdog." *CNBC*, July 30, 2021. https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-.html

Tariq, U., Ahmed, I., Bashir, A. K., and Shaukat, K. "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review." *Sensors* 23, no. 8 (2023): 4117. https://doi.org/10.3390/s23084117

Tzavara, V., and S. Vassiliadis. "Tracing the Evolution of Cyber Resilience: A Historical and Conceptual Review." *International Journal of Information*

Security, 2024. Advance online publication. https://doi.org/10.1007/s10207-023-00811-x

WATKINS, STEVE G. *ISO/IEC 27001:2022: An Introduction to Information Security and the ISMS Standard*. IT Governance Publishing, 2022. https://doi.org/10.2307/j.ctv30qq13d

Weckler, Adrian. "TikTok to learn whether sanctions will be imposed by Irish regulator on use of kids' data." *Irish Independent*, August 3, 2023. https://www.independent.ie/business/tiktok-to-learn-whether-sanctions-will-be-imposed-by-irish-regulator-on-use-of-kids-data/a1303646791.html

Wicaksono, Raden Mas Try Ananto. "Reviewing Legal Justice, Certainty, and Legal Expediency in Government Regulation Number 24 of 2018 Concerning Electronically Integrated Business Services". *Lex Scientia Law Review* 5, no. 1 (2021): 1-24. https://doi.org/10.15294/lesrev.v5i1.44905

***

Acknowledgment

I would like to express my sincere gratitude to all those who contributed to this research, either directly or indirectly, through their support, guidance, or feedback. This help and guidance have been invaluable in the completion of this work.

Funding Information

None.

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

History of Article

Submitted : March 2, 2024
Revised : May 28, 2024; August 21, 2024
Accepted : September 15, 2024
Published : September 22, 2024