LODZ CYBER HUB
University of Lodz

Legal Aspects of Computer Science — **Student Guide**

Section 3: Privacy and Data Protection

3.1 Foundations of Data Protection Law – The right to privacy and data protection principles.
3.2 The GDPR Framework – Core provisions, enforcement mechanisms, and international data transfers.
3.3 Global Data Protection Regimes – Comparative analysis: U.S., EU, and Asian models.
3.4 Balancing Privacy and Security – Ethical dilemmas in surveillance, encryption, and cybersecurity policy.

Lodz Cyber Hub - www.cyber.uni.lodz.pl

University of Lodz Law School
Dr Joanna Kulesza
Academic Year 2025/26
For internal student use only

Preliminary Note

Section 3 examines the legal foundations, regulatory structures, and contemporary challenges of privacy and personal data protection in the digital environment. It begins by situating privacy as a fundamental human right, recognised under international and European human rights law, and distinguishes it conceptually from data protection as a regulatory regime rooted in administrative law. The section explains the central role of personal data as the object of protection and introduces the core principles governing lawful data processing.

The section then provides a systematic analysis of the General Data Protection Regulation (GDPR) as the cornerstone of European data protection law. It outlines the Regulation's material and territorial scope, the conditions for lawful processing, enhanced protection for sensitive data, the rights of data subjects, and the system of enforcement and administrative sanctions. Particular attention is paid to international data transfers and the impact of the Court of Justice's jurisprudence on EU–US data flows.

A comparative perspective follows, contrasting the comprehensive, rights-based EU model with the sectoral and market-oriented approach of the United States and selected Asian regulatory frameworks. The section concludes by addressing the tension between privacy and security, analysing ethical and legal dilemmas arising from surveillance, encryption, and cybersecurity policies in democratic societies.

Recommended Reading

Kulesza, J. (2025). *Privacy and data protection.* In R. Balleste, G. Doucet & M. L. D. Hanlon (eds.), **A Research Agenda for Cybersecurity Law and Policy** (pp. 173–188). Cheltenham–Northampton: Edward Elgar Publishing.

Kulesza, J. Europe's Regulatory Sovereignty in the Age of Artificial Intelligence: A Human-Centric Response to the US–China Technological Rivalry, Sprawy Międzynarodowe (International Affairs), Vol. 78, No. 4 (2025).

Kulesza, J., & Akcalı Gur, B. (eds.), *Global Governance of Low Earth Orbit Satellites*, 218 pp., WUL 2025. Open Access

Kulesza, J., Privacy, [in:] Encyclopedia of Big Data, Schintler Laurie A., McNeely Connie L. (ed.), 2022, Springer

Additional Reading

- Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)
- Charter of Fundamental Rights of the European Union, Articles 7 and 8
- European Convention on Human Rights, Article 8
- Court of Justice of the European Union: *Google Spain SL and Google Inc. v AEPD and Mario Costeja González* (C-131/12)
- Court of Justice of the European Union: *Schrems v Data Protection Commissioner* (C-362/14) and *Schrems II* (C-311/18)
- European Court of Human Rights: *Von Hannover v Germany* (No. 1 and No. 2)
- European Court of Human Rights: *Rybolovlev and Bersheda v Monaco*
- Directive 95/46/EC (historical background)
- Secondary guidance of the European Data Protection Board (EDPB)

3.1 Foundations of Data Protection Law – The Right to Privacy and Data Protection Principles

The protection of privacy and personal data constitutes a foundational element of contemporary legal systems, particularly within Europe. Privacy is recognised as a fundamental human right, while data protection has developed as a distinct but closely related legal regime responding to the realities of automated data processing and digital technologies.

At the international and regional levels, the right to privacy is firmly embedded in human rights law. Article 8(1) of the European Convention on Human Rights (ECHR) provides that: "Everyone has the right to respect for his private and family life, his home and his correspondence." Article 8(2) allows for interferences by public authorities only where such interference is "in accordance with the law" and "necessary in a democratic society" for enumerated legitimate aims, such as national security, public safety, or the protection of the rights and freedoms of others. The jurisprudence of the European Court of Human Rights has interpreted the notion of "private life" broadly, encompassing physical and psychological integrity, personal identity, reputation, and the protection of personal information.

Within the European Union, privacy and data protection are recognised as separate fundamental rights. Article 7 of the Charter of Fundamental Rights of the European Union guarantees respect

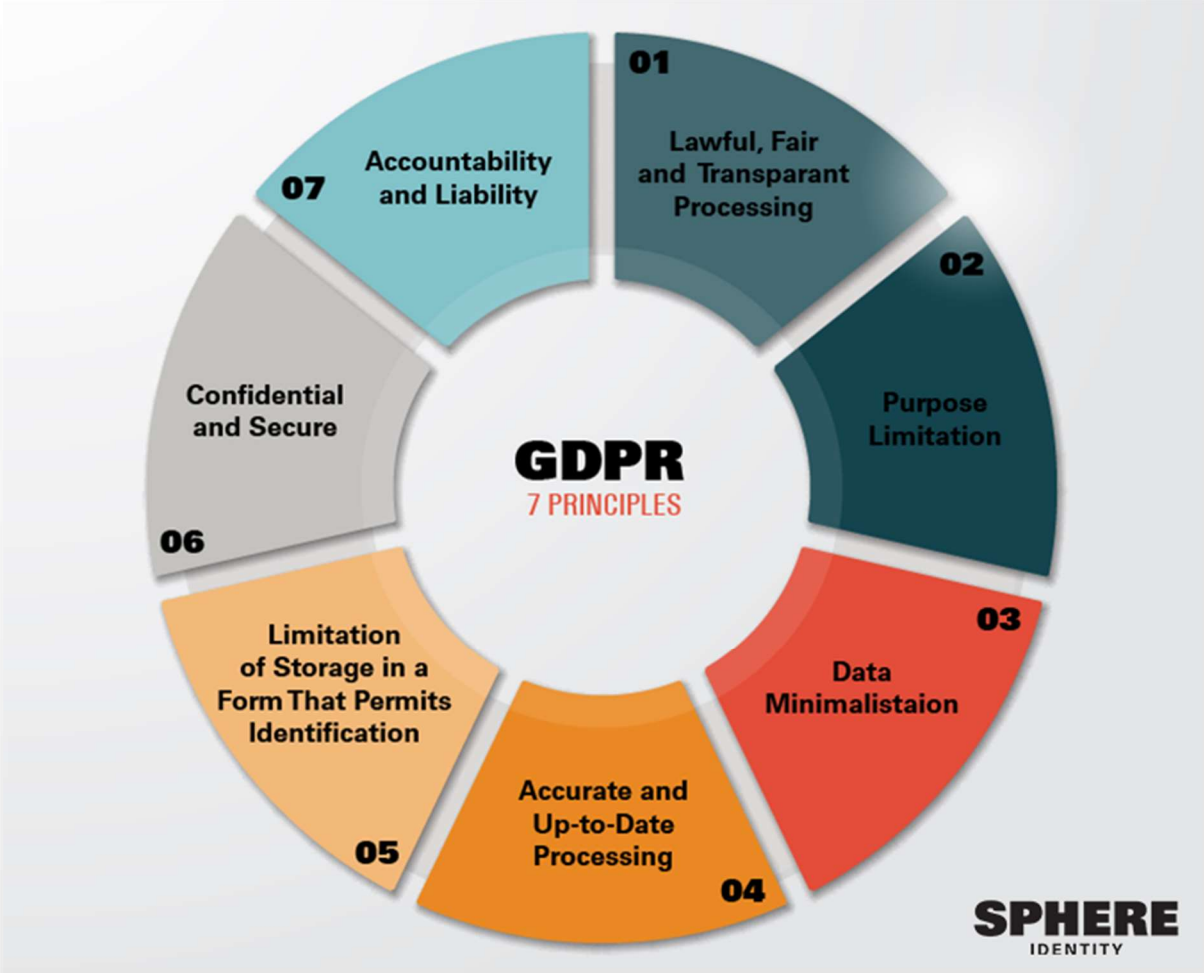
for private and family life, while Article 8 explicitly establishes a right to the protection of personal data. Article 8(1) of the Charter states that "Everyone has the right to the protection of personal data concerning him or her," and Article 8(2) requires that such data be processed fairly for specified purposes and on the basis of consent or another legitimate ground laid down by law.

The conceptual distinction between privacy and data protection is significant. Privacy traditionally functions as a personal right, rooted in civil law and human rights law, protecting individuals against unjustified intrusions into their private sphere. Data protection, by contrast, emerged as a regulatory framework grounded in administrative law, designed to govern the systematic collection, storage, use, and transfer of personal data by both public and private actors. While privacy focuses on secrecy and autonomy, data protection emphasises accountability, transparency, and procedural safeguards.

The cornerstone of modern European data protection law is the concept of "personal data." Under Article 4(1) GDPR, personal data means: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

This definition is deliberately broad and technology-neutral. Information qualifies as personal data whenever it relates to an identifiable individual, regardless of the format or medium in which it is processed. Identifiability may be direct (for example, by name) or indirect (through combinations of data points). Importantly, personal data that has been pseudonymised or encrypted remains within the scope of the GDPR if re-identification is reasonably possible. Only data that has been rendered truly anonymous, such that identification is no longer possible by any means reasonably likely to be used, falls outside the scope of data protection law.

European data protection law is structured around a set of core principles that govern all processing of personal data. Article 5(1) GDPR provides that personal data shall be:
(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation");
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation");
(d) accurate and, where necessary, kept up to date ("accuracy");
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ("storage limitation");
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage ("integrity and confidentiality").



Article 5(2) GDPR introduces the principle of accountability, providing that "the controller shall be responsible for, and be able to demonstrate compliance with" these principles. This obligation fundamentally reshapes regulatory expectations by shifting the burden of compliance onto data controllers and requiring proactive organisational and technical measures.

3.2 The GDPR Framework – Core Provisions, Enforcement Mechanisms, and International Data Transfers

The General Data Protection Regulation (GDPR), applicable since 25 May 2018, represents the most comprehensive and influential data protection framework to date. As a regulation, it is directly applicable in all EU Member States, ensuring a high degree of harmonisation across the internal market.

The GDPR applies to the processing of personal data wholly or partly by automated means, as well as to non-automated processing where personal data forms part of a filing system. Its territorial scope is extensive: under Article 3 GDPR, the Regulation applies not only to controllers and processors established in the EU, but also to entities outside the EU where processing activities relate to the offering of goods or services to individuals in the EU or to the monitoring of their behaviour.

Lawfulness of processing constitutes a central requirement. Article 6(1) GDPR provides that processing shall be lawful only if and to the extent that at least one of the following applies: the data subject has given consent; processing is necessary for the performance of a contract; processing is necessary for compliance with a legal obligation; processing is necessary to protect vital interests; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; or processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where overridden by the interests or fundamental rights of the data subject.

Consent is subject to strict conditions. Article 7 GDPR requires that consent be freely given, specific, informed and unambiguous. Data subjects must have the right to withdraw consent at any time, and controllers must be able to demonstrate that valid consent was obtained. In the case of children, Article 8 GDPR introduces additional safeguards, particularly in relation to information society services.

Certain categories of personal data receive enhanced protection. Article 9 GDPR prohibits the processing of special categories of data, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for identification purposes, health data, or data concerning a person's sex life or sexual orientation, unless one of the enumerated exceptions applies.

The GDPR significantly strengthens the rights of data subjects. These include the right of access (Article 15), the right to rectification (Article 16), the right to erasure ("right to be forgotten", Article 17), the right to restriction of processing (Article 18), the right to data portability (Article 20), and the right to object (Article 21). The right to be forgotten, elaborated by the Court of Justice of the European Union in *Google Spain*, requires controllers to erase personal data where processing is no longer necessary, consent is withdrawn, or processing is unlawful, subject to balancing against freedom of expression and the public interest.

Enforcement under the GDPR is entrusted to independent supervisory authorities in each Member State, operating within a framework of cooperation and consistency coordinated by the European Data Protection Board. Supervisory authorities possess extensive investigative and corrective powers, including the ability to issue warnings, reprimands, compliance orders, and administrative fines.

Article 83 GDPR establishes a robust sanctions regime. Administrative fines must be "effective, proportionate and dissuasive" and may reach up to EUR 20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. The Regulation specifies detailed criteria for determining the amount of a fine, including the nature, gravity and duration of the infringement, the number of data subjects affected, the level of damage suffered, and the degree of responsibility of the controller or processor.

International data transfers represent one of the most complex areas of GDPR compliance. Chapter V GDPR provides that transfers of personal data to third countries or international organisations may take place only where the conditions laid down in the Regulation are met. Transfers may occur on the basis of an adequacy decision (Article 45), appropriate safeguards

such as standard contractual clauses or binding corporate rules (Articles 46–47), or, in limited circumstances, specific derogations (Article 49).

The jurisprudence of the Court of Justice in *Schrems I* and *Schrems II* has profoundly shaped this area. In *Schrems II*, the Court invalidated the EU–US Privacy Shield, holding that U.S. surveillance laws failed to provide a level of protection essentially equivalent to that guaranteed within the EU. While standard contractual clauses remain valid in principle, controllers must assess, on a case-by-case basis, whether supplementary measures are necessary to ensure adequate protection in practice.

3.3 Global Data Protection Regimes – Comparative Analysis: U.S., EU, and Asian Models

Data protection regimes around the world reflect differing legal traditions, constitutional structures, and policy priorities. The European Union model is characterised by comprehensive, rights-based regulation grounded in fundamental rights. By contrast, the United States has traditionally adopted a sectoral and market-oriented approach, while many Asian jurisdictions combine elements of both models.

In the EU, data protection is conceived as a fundamental right, enforced through a centralised regulatory framework with strong supervisory authorities. The GDPR applies across sectors and technologies, imposes extensive obligations on controllers and processors, and provides individuals with enforceable rights.

The United States lacks a single, comprehensive federal data protection law. Instead, privacy and data protection are regulated through a patchwork of sector-specific statutes, such as the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), and the Gramm-Leach-Bliley Act (GLBA), supplemented by state-level legislation, most notably the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). Enforcement is often framed in terms of consumer protection and unfair or deceptive practices, rather than fundamental rights.

Asian data protection regimes are diverse. Japan's Act on the Protection of Personal Information, South Korea's Personal Information Protection Act, and Singapore's Personal Data Protection Act illustrate comprehensive frameworks influenced by European principles, while maintaining flexibility to support innovation and economic development. China's Personal Information Protection Law combines strong state oversight with broad regulatory powers, reflecting distinct constitutional and governance priorities.

Comparative analysis highlights persistent tensions between economic interests, state surveillance, and individual rights. These differences complicate cross-border data flows and necessitate mechanisms for regulatory interoperability.

3.4 Balancing Privacy and Security – Ethical Dilemmas in Surveillance, Encryption, and Cybersecurity Policy

3.4 Balancing Privacy and Security – Ethical Dilemmas in Surveillance, Encryption, and Cybersecurity Policy

The digital environment has significantly intensified long-standing tensions between the protection of privacy and the pursuit of security. States increasingly rely on advanced surveillance technologies to address threats such as terrorism, organised crime, and cybercrime, while private actors deploy extensive data analytics to optimise services, manage risks, and secure digital infrastructures. These developments raise profound legal and ethical questions concerning the permissible scope of data collection, the limits of state power, and the protection of individual autonomy in data-driven societies.

At the heart of this tension lies a structural dilemma: security measures often depend on the large-scale collection and analysis of personal data, while privacy and data protection law seek to limit, structure, and render accountable such practices. European legal frameworks do not conceptualise privacy and security as mutually exclusive values. Rather, they require that interferences with privacy be carefully justified, legally grounded, and constrained by procedural and substantive safeguards.

Under Article 8 of the European Convention on Human Rights, any interference with the right to respect for private life must satisfy three cumulative conditions: it must be "in accordance with the law," pursue a legitimate aim, and be "necessary in a democratic society." The European Court of Human Rights has consistently interpreted these requirements as imposing strict obligations on states to ensure clarity, foreseeability, proportionality, and effective oversight in surveillance regimes.

The requirement of legality demands more than the mere existence of a legal basis. The law authorising surveillance must be accessible to the public and formulated with sufficient precision to enable individuals to foresee, to a reasonable degree, the circumstances in which their communications or personal data may be subject to interception or monitoring. Vague or overly broad powers risk granting excessive discretion to public authorities and are therefore incompatible with the rule of law.

Necessity and proportionality operate as substantive constraints on surveillance practices. The Court has repeatedly emphasised that even where national security or the prevention of serious crime is invoked, measures must be strictly necessary and proportionate to the legitimate aim pursued. Blanket or indiscriminate data collection, lacking differentiation or targeting, is viewed with particular suspicion.

The Court's jurisprudence in cases such as *Von Hannover v Germany* illustrates its insistence on meaningful protection of private life, even where competing interests are strong. Although *Von Hannover* primarily concerned media intrusion rather than state surveillance, the Court articulated principles of general relevance: the assessment of whether an interference is justified must consider the contribution to a debate of general interest, the degree of intrusion into private life, and the availability of less intrusive means. The case underscores that public figures do not forfeit their right to privacy and that constant exposure or monitoring can undermine human dignity and personal autonomy.

Similarly, in *Rybolovlev and Bersheda v Monaco*, the Court addressed the interception and use of private communications in the context of criminal investigations. While recognising the legitimacy of combating crime, the Court found that insufficient safeguards and excessive use of intercepted data violated Article 8 ECHR. The judgment highlights the importance of procedural guarantees, including judicial authorisation, limits on data retention, and restrictions on secondary use. Surveillance measures, even when initially justified, may become disproportionate if data is reused or disclosed beyond what is strictly necessary.

These cases illustrate a broader doctrinal point: European human rights law does not reject surveillance as such, but demands that it be embedded within a framework of legality, accountability, and rights protection. Surveillance must be exceptional rather than routine, targeted rather than indiscriminate, and subject to effective independent oversight.

The challenges posed by surveillance are compounded in the digital environment by the increasing role of private actors. Telecommunications providers, online platforms, and cloud service providers frequently act as intermediaries between individuals and the state. Legal obligations to retain or disclose data place these actors in a complex position, balancing compliance with public authority requests against their responsibilities under data protection law and their users' expectations of confidentiality. This intermediary role raises questions about privatised enforcement, transparency, and the shifting boundaries between public and private power.

Encryption represents one of the most contested issues at the intersection of privacy and security. Strong encryption is widely recognised as a cornerstone of cybersecurity and data protection. It safeguards the confidentiality and integrity of communications, protects sensitive personal and commercial information, and underpins trust in digital services. From a data protection perspective, encryption constitutes an important technical and organisational measure to ensure compliance with the principles of integrity and confidentiality.

At the same time, law enforcement and intelligence authorities argue that widespread use of end-to-end encryption impedes lawful access to evidence, creating so-called "going dark" scenarios. In response, proposals have been advanced to require service providers to implement mechanisms for lawful access, often described as "backdoors" or exceptional access solutions. These proposals raise serious legal and technical concerns.

From a legal perspective, mandatory backdoors risk undermining the principle of proportionality. Systemic vulnerabilities introduced for exceptional access purposes are not limited to specific targets or investigations; they affect all users of a system. As a result, the interference with privacy may be broad and indiscriminate rather than targeted and necessary. Moreover, such measures may conflict with data protection obligations to ensure appropriate security of personal data.

From a technical perspective, security experts consistently warn that encryption backdoors cannot be reliably limited to legitimate authorities. Any intentional weakening of encryption creates exploitable vulnerabilities that may be abused by malicious actors, including cybercriminals and hostile states. This risk has significant implications not only for individual privacy, but also for national security, economic stability, and the resilience of critical infrastructures.

The debate over encryption thus exemplifies the difficulty of reconciling short-term investigative interests with long-term systemic security. European regulatory discourse increasingly recognises that strong encryption and robust data protection are not obstacles to security, but essential components of a secure digital environment.

Cybersecurity policy further complicates the privacy–security balance. Measures such as network monitoring, intrusion detection, and threat intelligence sharing often involve the processing of large volumes of data, including personal data. While such measures are essential to protect systems and users from cyber threats, they must be carefully designed to minimise unnecessary intrusion into private life.

The GDPR provides a framework for navigating these tensions by embedding security obligations within a rights-based structure. Controllers are required to implement appropriate technical and organisational measures, taking into account the state of the art, the risks involved, and the nature of the data processed. Risk-based governance encourages proactive security while maintaining accountability and respect for fundamental rights.

At a broader level, the balance between privacy and security has significant implications for democratic governance and technological development. Excessive surveillance and weak data protection risk eroding public trust, chilling freedom of expression, and normalising intrusive forms of monitoring. Conversely, inadequate security measures can expose individuals and societies to serious harm.

European legal frameworks increasingly articulate a vision in which privacy is not treated as an obstacle to security, but as a precondition for trust, legitimacy, and sustainable digital innovation. Protecting privacy enhances confidence in digital systems, supports the adoption of new technologies, and reinforces democratic values.

In this sense, the challenge of balancing privacy and security is not merely a technical or legal problem, but a normative one. It requires continuous reflection on the kind of digital society that legal systems seek to foster, and on the role of law in shaping the architecture of power, accountability, and trust in the digital age.

Question 1

European data protection law is built around a set of foundational principles that apply to all processing of personal data, regardless of sector or technology. Which of the following best captures the role of these principles within the European regulatory framework?

A. They operate as optional guidelines that organisations may follow if convenient
B. They function as binding legal standards governing how personal data may be collected, used, stored, and disclosed
C. They apply only to public authorities and not to private entities
D. They regulate only the international transfer of personal data

---

Question 2

One of the core principles of European data protection law requires that personal data collected and processed by organisations be limited to what is strictly necessary for specific purposes. What is the primary objective of this requirement in the context of fundamental rights protection?

A. To ensure that data processing is economically efficient
B. To reduce the cost of data storage and management
C. To prevent excessive or speculative data collection that may unjustifiably interfere with individual rights
D. To encourage the exclusive use of anonymised data

Question 3

In contemporary digital environments, the principle of data minimisation poses particular challenges for services that rely on large-scale data analytics and artificial intelligence. Which of the following best reflects the legal implication of this principle for such systems?

A. Artificial intelligence systems are exempt from data protection obligations due to their technical complexity
B. Organisations may collect large volumes of data initially, provided that minimisation occurs at a later stage
C. Data collection and use must be limited to what is necessary for clearly defined and legitimate purposes
D. Data minimisation applies only after an automated system has been deployed

---

Question 4

The legal framework governing transfers of personal data from Europe to the United States was fundamentally reshaped by litigation initiated by an individual data subject. What was the central concern identified by the Court when assessing the permissibility of such transfers?

A. The absence of competition between digital service providers
B. The lack of identical privacy legislation in Europe and the United States
C. The risk that personal data could be accessed by public authorities without sufficient limitations or effective remedies
D. The excessive administrative burden placed on multinational companies

---

Question 5

Prior to its invalidation, the Safe Harbor framework was widely relied upon to legitimise transatlantic transfers of personal data. Which of the following best describes the key structural weakness of that framework as identified by the Court?

A. It imposed overly strict compliance obligations on U.S. companies
B. It relied largely on voluntary commitments while failing to adequately restrict government access to personal data
C. It applied only to small and medium-sized enterprises
D. It prevented cooperation between states on national security matters

---

Question 6

Following the invalidation of Safe Harbor, a successor transatlantic arrangement was introduced but later also found to be incompatible with European data protection requirements. What broader lesson does this sequence of decisions illustrate?

A. That transfers of personal data to third countries are generally prohibited
B. That contractual or political arrangements cannot compensate for fundamental deficiencies in foreign legal systems
C. That only technical security measures are relevant for ensuring adequate protection
D. That national supervisory authorities enjoy unlimited discretion in approving transfers

---

Question 7

Among the principles governing the processing of personal data, one requires that individuals be informed about how their data is collected and used, and that processing not take place in a misleading manner. Why is this requirement particularly important in complex digital ecosystems?

A. Because digital services rarely rely on personal data
B. Because automated decision-making eliminates the need for user awareness
C. Because layered data processing practices make it difficult for individuals to understand how their data is reused
D. Because transparency replaces the need for legal safeguards

---

Question 8

European data protection law increasingly emphasises that compliance involves more than formal adherence to rules. What practical consequence does this emphasis have for organisations that process personal data?

A. Organisations must disclose proprietary algorithms to the public
B. Organisations must proactively document, assess, and justify their data processing activities
C. Organisations are liable only if actual harm can be demonstrated
D. Organisations may shift responsibility entirely to third-party processors

---

Question 9

The principle of data minimisation often conflicts with business models based on extensive data accumulation and secondary use. How does European data protection law seek to resolve this tension?

A. By prioritising economic growth over individual rights
B. By permitting unlimited data collection where consent is obtained once
C. By requiring that data use remain closely connected to specific and legitimate purposes
D. By prohibiting any reuse of personal data under all circumstances

---

Question 10

Taken together, the emphasis on core data protection principles and the judicial scrutiny of transatlantic data transfer mechanisms reflect a broader regulatory philosophy. Which of the following best captures that philosophy?

A. Data protection is primarily a technical compliance exercise
B. Data protection is a voluntary form of market self-regulation
C. Data protection functions as a rights-based framework shaping how digital systems are designed and governed
D. Data protection applies only after concrete harm has occurred