Scientific Journal of King Faisal University:
Humanities and Management Sciences

The Legal Framework of Legitimate Interests: A Comparative Analysis

Ahmed M. Bamashmoos
Law Department, Faculty of Science and Theoretical Studies, Saudi Electronic University, Dammam, Saudi Arabia

LINK	RECEIVED	ACCEPTED	PUBLISHED ONLINE	ASSIGNED TO AN ISSUE
https://doi.org/10.37575/h/law/250030	11/05/2025	18/08/2025	18/08/2025	01/09/2025
NO. OF WORDS	**NO. OF PAGES**	**YEAR**	**VOLUME**	**ISSUE**
7894	8	2025	26	2

Abstract

This research paper conducts a comparative analysis of the "legitimate interests" basis for personal data processing under the General Data Protection Regulation (GDPR) and the Saudi Personal Data Protection Law (PDPL). The study aims to explore how each regulatory framework defines and regulates the use of legitimate interests, focusing on the balancing test required to ensure that data subjects' rights are respected. The research methodology involves doctrinal analysis of primary legislation and a comparative approach to identify differences in procedural requirements and safeguards. The analysis reveals that while both the GDPR and the PDPL permit the use of legitimate interests, the GDPR offers a more flexible approach with a detailed balancing test, whereas the PDPL imposes stricter limitations, particularly concerning sensitive data. Key judicial precedents are examined to illustrate the application of legitimate interests in various contexts, emphasizing the importance of proportionality, transparency, and accountability. The paper concludes by suggesting best practices for data controllers in both jurisdictions and advocating for greater harmonization and procedural guidance to ensure consistency and compliance. The findings underscore the need to balance organizational interests with individual privacy rights, especially in light of increasing digital data usage, to foster trust and ensure ethical data processing.

KEYWORDS
Balancing test, data protection, GDPR, PDPL, personal data, privacy rights

CITATION
Bamashmoos, A.M. (2025). The legal framework of legitimate interests: a comparative analysis. *Scientific Journal of King Faisal University: Humanities and Management Sciences*, **26**(2), 68–75. DOI: 10.37575/h/law/250030

1. Introduction

In contemporary data-protection regimes, legitimate interests operate as an independent legal basis that permits personal-data processing without prior consent, provided that stringent safeguards are observed (European Union, 2016; Personal Data Protection Law, 2021). It offers organizations the flexibility to process data without explicit consent when certain conditions are met, aiming to balance operational needs with individuals' privacy rights (Voigt and von dem Bussche, 2017). Accordingly, the study undertakes a doctrinal comparison of how the European Union (EU)'s General Data Protection Regulation (GDPR) and the Saudi Personal Data Protection Law (PDPL) articulate and operationalize the legitimate-interest ground. By examining how each framework defines, regulates, and implements legitimate interests, the study seeks to elucidate the complexities and challenges organizations face in ensuring compliance while respecting data subjects' rights.

The GDPR has become the de facto global benchmark for data-protection regulation. Global diffusion of EU data protection standards remains pronounced: Greenleaf's latest global survey counts 172 countries with data privacy laws as of April 2025, and his successive assessments since 2021 describe "GDPR dominance," noting that most new or substantially revised laws outside the EU show significant GDPR influence (Greenleaf, 2021). Practitioner updates likewise show recent enactments and amendments in multiple regions aligning with GDPR requirements, reflecting a broader "Brussels effect". Its mature regulatory mechanisms reinforced by a substantial body of Court of Justice and supervisory-authority jurisprudence offer a tested template for applying the legitimate-interest balancing test. Setting this widely emulated framework against the Kingdom's recently enacted PDPL yields two scientific benefits: first, it provides a doctrinal yardstick that identifies where the PDPL aligns with, adapts, or departs from internationally accepted standards; second, it shows how core GDPR principles are recalibrated within Saudi Arabia's civil-law/Sharia hybrid system and socio-economic priorities. Analyzing these convergences and divergences equips scholars and policymakers with evidence-based insights for refining the PDPL and advancing global interoperability in privacy governance.

The primary objective is to dissect the definitions, requirements, and procedural safeguards that govern legitimate-interest processing in both the GDPR and the PDPL. The research addresses key questions regarding the similarities and differences between the two laws, the obligations of data controllers, and the implications for data subjects' rights. By exploring practical examples and examining judicial precedents, the paper offers a comprehensive understanding of how legitimate interests function within these legal contexts.

This study adopts a doctrinal and comparative legal methodology, analyzing primary legislation and relevant case law to provide a nuanced analysis of legitimate interests (Watkins and Burton, 2017). The findings aim to inform best practices for data controllers and contribute to ongoing discussions on harmonizing data protection laws (Hijmans, 2016). Ultimately, the paper underscores the importance of a balanced and transparent approach to legitimate interests, emphasizing the need to protect individual privacy rights amid evolving technological advancements (Gellert, 2018; Tene and Polonetsky, 2013).

1.1. Methodology:

Methodologically, the study applies a doctrinal–comparative framework that combines textual, systematic, and teleological interpretation, then evaluates each rule against accepted canons of proportionality, necessity, and effectiveness (Hutchinson and Duncan, 2012). First, the analysis cross-reads GDPR Arts. 6(1)(f), 5 and 24 with Recitals 39 and 47, and PDPL Arts. 6, 10 and 16 with PDPL IR Arts. 19 (assessment) and 20 (transparency), thereby testing internal coherence. Second, a systematic mapping links those articles to their implementing instruments most notably GDPR Recitals 39 and 47 and the PDPL Implementing Regulations, Arts 19–20—so that internal cross-references (e.g., between PDPL Art. 16 and Regulation Art 19 on balancing tests) are evaluated in context. Third,

Corresponding Author: Ahmed M. Bamashmoos 00966112613500, Asalem@seu.edu.sa

a teleological lens assesses how the balancing test advances the statutes' shared purpose of protecting fundamental privacy while enabling socially useful processing. For the GDPR, judicial and supervisory-authority jurisprudence (e.g., Volker and Markus Schecke, Court of Justice of the European Union (CJEU)) provides interpretative guidance, whereas the PDPL analysis remains strictly doctrinal because no Saudi court or administrative rulings applying the law have yet been published. This layered technique delivers a comparison that is both conceptually rigorous and practically relevant for regulators and data controllers in each jurisdiction.

2. Literature Review

This literature review begins by tracing the historical development of data protection laws to contextualize the emergence of "legitimate interests" as a lawful basis for data processing. It then explores how the GDPR and the PDPL define and regulate legitimate interests, examining the legal frameworks, challenges, and requirements associated with this concept. The review focuses on how these laws balance organizational needs with the rights of data subjects, highlighting key judicial precedents and the inherent challenges in applying legitimate interests in practice.

2.1. Historical Development of Data Protection Laws:

Early European instruments (ECHR, 1950; Convention 108, 1981; OECD Guidelines, 1980; Directive 95/46/EC, 1995) laid the doctrinal foundations later refined by the GDPR and, in Saudi Arabia, the PDPL.

2.2. Judicial Precedents on Legitimate Interests:

This section distils four leading CJEU judgments—*Schecke, Breyer, Jehovan todistajat, Fashion ID*—each mapped to one of the comparison criteria above, thereby demonstrating the practical calibration of purpose, necessity, and balancing. These precedents provide important insights into how courts balance organizational needs with individuals' privacy rights, offering guidance that informs both the GDPR and the PDPL frameworks.

2.3. Volker und Markus Schecke Case (CJEU, 2010):

The *Volker und Markus Schecke* case (Joined Cases C-92/09 and C-93/09) dealt with the publication of beneficiaries of EU agricultural subsidies, where the European Commission mandated that names of recipients and amounts received be published online. The CJEU ruled that this measure was disproportionate and infringed on individuals' privacy rights, as it did not properly balance the interest in transparency against the fundamental rights of the data subjects. The Court stressed that blanket justifications for processing such as promoting transparency in public spending were not sufficient without considering less intrusive alternatives and the impact on privacy. This ruling underscores the need for a thorough assessment whenever legitimate interests are relied upon as a basis for data processing. It also highlights the importance of respecting data subjects' rights, particularly regarding sensitive personal information. The decision set an important standard, especially for public authorities, on how they must justify their actions under the legitimate interests basis to ensure compliance with data protection laws.

2.3.1. Breyer v Germany (CJEU, 2016)

In *Breyer* (C-582/14) the Court held that website operators may log visitors' dynamic IP addresses to defend against cyber-attacks, recognizing server security as a legitimate interest. Crucially, the Court stressed proportionality: retention periods must be limited and data disclosed only where strictly necessary, illustrating that even security interests require a calibrated balancing of risks and safeguards.

2.3.2. Jehovan todistajat (CJEU, 2018)

In *Tietosuojavaltuutettu v Jehovan todistajat* (C-25/17) the Court confirmed that a religious community canvassing door-to-door could rely on legitimate interests, but only if data subjects reasonably expected such processing and appropriate opt-out mechanisms were provided. The ruling sharpened the "reasonable expectations" limb of Recital 47 and underscores the need for context-specific balancing.

2.3.3. Fashion ID (CJEU, 2019)

In *Fashion ID GmbH* (C-40/17) the Court found that an online retailer embedding a Facebook "Like" plug-in pursued a commercial legitimate interest in optimizing publicity. Nonetheless, the controller had to ensure transparent disclosure and obtain user consent for any tracking cookies, demonstrating that commercial gain alone is insufficient where intrusive technologies are employed.

3. Challenges of Using "Legitimate Interests" as a Legal Basis for Data Processing

The use of "legitimate interests" as a lawful basis for data processing presents several challenges due to its inherent flexibility and the necessity of balancing the interests of data controllers with the fundamental rights of data subjects (Dolenc, 2020). These challenges are complex and multifaceted, affecting both parties involved.

3.1. Complexity of the Balancing Test:

Relying on legitimate interests necessitates conducting a balancing test (GDPR Art. 6(1)(f), Recital 47; PDPL Art. 16(1)(b)). This test involves evaluating whether the controller's legitimate interest outweighs the fundamental rights and freedoms of the data subject. Factors such as the nature of the data, the relationship between the data subject and the controller, the data subject's expectations, and the potential impact of processing must be considered. The subjective nature of this evaluation, without clear guidelines on weighting different interests, makes the assessment complex and potentially inconsistent across organizations (Zufall *et al.,* 2022).

3.2. Lack of Predictability for Data Subjects:

Assessing the data subject's reasonable expectations regarding the processing of their personal data is critical (Wachter and Mittelstadt, 2019). What is considered "reasonable" can vary greatly among individuals, resulting in a lack of predictability for data subjects who may not understand why their data is processed without explicit consent (Balboni *et al.,* 2013). This subjectivity challenges the protection of individual privacy and can erode trust between data subjects and controllers.

3.3. Compliance Burden for Data Controllers:

Data controllers are required to perform and document the balancing test, justifying their decision to rely on legitimate interests (PDPL Implementing Regulations, Art. 16(3)). Under the GDPR, this involves conducting a Legitimate Interests Assessment (LIA), which can be resource-intensive (Freitas and Mira da Silva, 2018). The accountability principle mandates that controllers demonstrate compliance, adding legal and operational risks if they fail to justify their processing adequately (GDPR Art. 5(2); PDPL Art. 16).

3.4. Conflicts with Data Subject Rights:

Data subjects have various rights, such as the right to object to processing, access their data, and restrict processing (GDPR Arts. 15, 18 and 21; PDPL Art. 4). Using legitimate interests can create tensions between these rights and the needs of controllers. For example, when a data subject objects to processing, the controller must assess whether their legitimate interest overrides the individual's rights, which may not always be straightforward. This can lead to disputes and enforcement actions by data protection authorities.

3.5. Interim Summary on Challenges:

The challenges associated with using "legitimate interests" as a lawful basis for data processing highlight the importance of cautious and transparent application. The inherent flexibility and ambiguity can lead to inconsistencies and potential misuse, affecting both data controllers and data subjects. A thorough understanding of these challenges is essential for organizations to navigate the complexities of data protection laws effectively and to maintain trust with individuals whose data they process.

4. Comparative Matrix – Analytical Criteria

The comparison follows three criteria (1) scope, (2) procedural safeguards, and (3) judicial or regulatory interpretation summarized in Table 1 below.

Table 1. Comparative Matrix of Legitimate-Interest Requirements in the GDPR and the PDPL

Criterion	GDPR Highlight	PDPL Highlight	Key Precedent / Reg
1. Scope	Art. 6(1)(f) – broad purposes permitted	Arts. 6 and 16 – excludes sensitive data	Breyer (security scope)
2. Safeguards	Arts. 24 (LIA) and 25 (privacy by design)	PDPL IR Art. 19 (documented assessment)	Schecke (proportionality)
3. Interpretation	CJEU case-law shapes balancing	No case-law yet; textual + Reg 19	Jehovan todistajat (CJEU 2018), Fashion ID

5. The GDPR Legitimate Interests

5.1. Definition and Scope of Legitimate Interests Under the GDPR:

Under the GDPR, Article 6(1)(f) provides a legal basis for processing personal data when it is necessary for the purposes of legitimate interests pursued by the data controller or a third party, except where these interests are overridden by the interests or fundamental rights and freedoms of the data subject (GDPR Art. 6(1)(f); European Data Protection Board, 2024; Article 29 Working Party, 2014). This legal basis serves as a flexible option that enables data controllers to process data for various purposes that benefit their operations, provided that the rights of individuals are not unduly affected (Voigt and von dem Bussche, 2017). Recital 47 of the GDPR provides further clarification by emphasizing that the concept of legitimate interests requires the balancing of the interests of data controllers with those of data subjects (Lachaud, 2018). It highlights that the expectations of the data subject are crucial in determining whether legitimate interests may apply (Lachaud, 2018). The reasonable expectations of individuals based on their relationship with the data controller must be taken into account, particularly in cases where the data subject is an existing customer or employee (Voigt and von dem Bussche, 2017). Textually, the qualifier "necessary" in Art. 6(1)(f) must be read in light of Recital 39's proportionality aim, a view endorsed in *Breyer v Germany* (C-582/14).

5.2. The Three-Part Test for Legitimate Interests:

To apply the legitimate interests basis, controllers must satisfy a three-part test: the purpose test, the necessity test, and the balancing test (Article 29 Working Party, 2014). Each of these tests must be passed for legitimate interests to be considered a valid legal basis for data processing under the GDPR (Voigt and von dem Bussche, 2017).

5.2.1. Purpose Test

The purpose test involves examining the legitimacy of the interest pursued by the data controller or a third party. The interest must be lawful, explicit, and specific, meaning that the data controller must have a clearly defined reason for processing that complies with relevant legal and ethical standards (Lynskey, 2015). Legitimate interests can encompass a wide range of purposes, such as fraud prevention, ensuring network security, or engaging in direct marketing activities (Article 29 Working Party, 2014). However, this interest must be genuinely legitimate, without conflicting with the laws or rights of others. If the controller's purpose is unlawful or unethical, then it will not pass the purpose test (González Fuster, 2014).

5.2.2. Necessity Test

The necessity test requires data controllers to analyze whether the processing is necessary to achieve the stated purpose (Voigt and von dem Bussche, 2017). This involves determining whether the same outcome can be achieved through other, less intrusive means. The necessity test ensures that the data processing is not excessive and that the chosen means are proportionate to the intended purpose (Lynskey, 2015). If an alternative approach exists that involves less or no personal data, the controller must consider that option. For instance, in direct marketing, if personalized advertisements can be delivered without using personally identifiable information, that method should be preferred over one that involves extensive profiling (González Fuster, 2014).

5.2.3. Balancing Test

The balancing test evaluates the competing interests between the data controller and the data subject. This test requires the controller to determine whether the interests of the organization outweigh the rights and freedoms of the data subject (Article 29 Working Party, 2014). Several factors are considered during this assessment, including the potential impact on the data subject, the sensitivity of the data being processed, the reasonable expectations of the data subject, and whether adequate safeguards are in place to protect the individual's rights (European Data Protection Board, 2019). For example, if the processing involves sensitive data, such as health information, the rights of the data subject are likely to outweigh the legitimate interests of the controller, especially if processing is not essential to the controller's purpose (Lynskey, 2015). To mitigate the impact on individuals, controllers must implement safeguards, such as data minimization, privacy notices, and the possibility for individuals to opt out of processing (Voigt and von dem Bussche, 2017).

5.3. Challenges for Data Controllers Under the GDPR:

The use of legitimate interests as a lawful basis under the GDPR comes with several challenges. One of the main challenges is the requirement to conduct an LIA, which involves documenting each of the three parts of the test (Information Commissioner's Office, 2019). Controllers must provide a comprehensive explanation of the purpose of the processing, why it is necessary, and why they believe the data subject's rights do not override their interests (Voigt and von dem Bussche, 2017). This assessment must also be documented to demonstrate compliance with the GDPR's accountability principle, meaning that data controllers must be ready to justify their use of legitimate interests to supervisory authorities if required (GDPR, Art. 5(2)).

Another challenge is maintaining transparency (Goddard, 2017). The GDPR requires that data controllers be transparent with data subjects about the use of their data (GDPR Arts. 13–14). When relying on legitimate interests, organizations must clearly inform data subjects about the processing, the specific interests pursued, and the rights available to them, such as the right to object to processing (European Data Protection Board, 2019). Maintaining this level of transparency can be complex, particularly when processing is carried out for multiple purposes that may not be immediately apparent to the data subject.

Furthermore, data controllers must ensure that appropriate safeguards are in place to protect data subjects (GDPR, Art. 25). These safeguards include measures like data minimization, which limits the data collected to only what is strictly necessary, and the implementation of privacy-enhancing technologies (European Union Agency for Cybersecurity, 2018). Without such safeguards, data processing is more likely to have a negative impact on data subjects, which could mean that the processing would not meet the balancing requirement of Article 6(1)(f) (Lynskey, 2015).

5.4. Practical Examples of Legitimate Interests:

One common example where legitimate interests can be applied is fraud prevention. Data controllers may process personal data to identify and prevent fraudulent activities, as fraud prevention is in the interests of both the organization and society at large (Voigt and von dem Bussche, 2017). For example, banks may process transaction data to detect unusual patterns that indicate fraudulent activities. In such cases, the legitimate interests of fraud prevention often outweigh any minimal privacy intrusion, particularly when safeguards like encryption and anonymization are in place (Goddard, 2017).

Another example is direct marketing. Recital 47 of the GDPR expressly recognizes that processing personal data for direct marketing purposes may be pursued under the legitimate-interest legal basis. Where permitted by the ePrivacy Directive's "soft opt-in," organizations may send marketing communications to existing customers on an opt-out basis, provided they respect data subjects' preferences and offer an easy way to opt out of future communications (European Union, 2016, Recital 47; Directive 2002/58/EC, art. 13(2)). In this case, the balancing test is essential to determine whether the data subject's rights override the marketing interests of the controller, and organizations must ensure that individuals are not subjected to excessive or unexpected intrusions (Lynskey, 2015).

In conclusion, the use of legitimate interests under the GDPR involves a structured assessment process designed to ensure that the rights of data subjects are respected. Controllers must clearly define the purpose of processing, ensure that processing is necessary to achieve that purpose, and carefully balance their interests against the rights of individuals. This requirement for accountability and the expectation of thorough assessments pose challenges for data controllers but also ensure that personal data is processed lawfully and ethically, maintaining trust between organizations and individuals (González Fuster, 2014).

6. The PDPL's Legitimate Interests

6.1. Definition and Scope of Legitimate Interests Under the PDPL:

Under the PDPL, the concept of legitimate interests is provided for in Articles 6 and 16 (Personal Data Protection Law [PDPL], 2021; see criteria 1–3). Article 6 states that the processing of personal data may be carried out without obtaining consent from the data subject if it is necessary for achieving the legitimate interests of the controller, provided that it does not conflict with the rights and interests of the data subject and no sensitive data is processed (PDPL Art. 6). Sensitive data includes information related to racial or ethnic origin, religious beliefs, health, genetic data, and others that could pose a greater risk to individuals' privacy if mishandled (PDPL Art. 2). Article 16 provides further details on how legitimate interests are defined within the context of data processing. This article requires data controllers to ensure that processing for legitimate interests is balanced against the rights and interests of the data subject (PDPL Art. 16). The balancing test involves determining whether the controller's interests significantly impact the data subject's rights, taking into consideration factors such as the nature of the data and the reasonable expectations of the data subject (PDPL Art. 16). The PDPL is particularly strict regarding the use of sensitive data, clearly stating that such data cannot be processed based on legitimate interests, which limits the scope of this basis compared to the GDPR (PDPL Arts. 6 and 16). Systematically, PDPL Art. 16's balancing duty must be read alongside Implementing Regulation Art 19, which supplies proportionality factors absent from the statutory text.

6.2. Requirements for Controllers:

The PDPL sets out specific requirements for data controllers when relying on legitimate interests as a basis for processing (PDPL Art. 16). One of the key requirements is that data controllers must conduct and document an assessment of the processing activities to demonstrate compliance with the law (PDPL Implementing Regulations). This assessment includes evaluating the necessity of processing, its legitimacy, and its potential impact on the data subjects (PDPL Implementing Regulations, Art. 19). If there is any potential for negative impacts or an infringement of the data subject's rights, the data controller must amend the proposed processing or rely on another legal basis (PDPL Implementing Regulations, Art. 19). This documentation is essential for ensuring accountability and for responding to inquiries from regulatory authorities (PDPL Art. 21).

Moreover, there are additional constraints on public authorities under the PDPL. Public authorities cannot rely on legitimate interests as a basis for processing unless it serves a specific statutory purpose, such as security or fulfilling a judicial requirement (PDPL Art. 16). This limitation ensures that governmental bodies do not overreach in using personal data, thereby protecting the privacy rights of individuals (PDPL Art. 16). Additionally, sensitive data is explicitly excluded from being processed under legitimate interests, imposing further restrictions on the scope of this legal basis (PDPL Art. 6).

The PDPL's Implementing Regulations provide further guidance on the application of legitimate interests (PDPL Implementing Regulations). They require data controllers to include specific safeguards to protect data subjects, such as data minimization, transparency measures, and offering data subjects the right to object to processing (PDPL Implementing Regulations, Arts. 19 and 20). These safeguards are designed to ensure that the data subject's privacy rights are prioritized and that processing activities are proportionate to the intended purpose (PDPL Implementing Regulations, Art. 20).

6.3. Comparative Examples:

The use of legitimate interests as a basis for data processing in Saudi Arabia differs from its application under the GDPR in several ways, particularly due to the cultural and regulatory context. For example, while fraud prevention is a common application of legitimate interests under both the GDPR and the PDPL, the Saudi law imposes stricter limitations on the types of data that can be processed (PDPL, 2021). Fraud prevention may involve analyzing transaction data, but any sensitive information, such as biometric or health data, cannot be used in Saudi Arabia without explicit consent (PDPL Art. 6).

Another example is direct marketing. Under the GDPR, direct marketing is explicitly recognized as a legitimate interest, provided that data subjects are informed and can easily opt out (GDPR Recital 47; Voigt and von dem Bussche, 2017). In contrast, the PDPL's approach is more restrictive. Direct marketing can only be conducted if the data subject has consented, which indicates that the legitimate interests basis may not be sufficient for such activities unless the consent is obtained separately (PDPL Art. 10). This difference highlights a more conservative approach in Saudi Arabia towards data processing that could impact individual privacy.

Overall, the PDPL incorporates stringent safeguards for using legitimate interests, emphasizing transparency, accountability, and the exclusion of sensitive data from processing under this basis (PDPL Arts. 6 and 16). While both the GDPR and the PDPL allow data controllers to rely on legitimate interests, the PDPL's framework is notably more restrictive, focusing on minimizing privacy risks and maintaining greater oversight over processing activities (PDPL Implementing Regulations).

7. Balancing Test and Procedural Requirements: the GDPR vs. the PDPL

7.1. The GDPR Approach:

7.1.1. Balancing Test Criteria

The GDPR requires data controllers to undertake a balancing test when relying on legitimate interests as the legal basis for data processing under Article 6(1)(f) (Regulation (EU) 2016/679, 2016). The test is designed to determine whether the interests of the data controller or a third party outweigh the rights and freedoms of the data subject (Article 29 Working Party, 2014). The balancing test considers several key criteria:

Transparency. Data controllers must be transparent with data subjects about the purposes of processing and the legitimate interests pursued. This requirement entails providing clear privacy notices that explain why the data is being processed, what legitimate interest justifies the processing, and how individuals' rights are protected (GDPR, Art. 13–14).

Accountability. Controllers are obligated to maintain documentation that demonstrates compliance with the GDPR's principles, including the outcomes of the balancing test (GDPR, Art. 5(2)). This accountability is enforced through an LIA, which provides detailed reasoning on the necessity of processing and the measures taken to protect data subjects (Information Commissioner's Office, 2019).

Rights of Data Subjects. The balancing test must consider the rights of data subjects, including the right to be informed about processing, the right to object, and the right to access their data (GDPR, Art. 12–22). Controllers must ensure that these rights are respected and that any negative impact on individuals' rights is mitigated (Voigt and von dem Bussche, 2017). If the processing would infringe on the rights or cause significant detriment to the data subject, the basis of the legitimate interest cannot be used (Article 29 Working Party, 2014).

7.1.2. Balance Between Interests

The GDPR emphasizes balancing the legitimate interests of the controller against the reasonable expectations and rights of the data subjects (GDPR, Recital 47). In determining whether processing is permissible, controllers must consider factors such as the nature of the data and the context of the data collection (Lynskey, 2015). For example, if the data subject has an established relationship with the controller (e.g., being a customer), they might reasonably expect certain uses of their data (GDPR, Recital 47). On the other hand, if processing involves sensitive data or is unrelated to the purpose for which the data was originally collected, the data subject's interests are more likely to outweigh the controller's interests (González Fuster, 2014). The GDPR stresses that appropriate safeguards——such as data minimization, encryption, and pseudonymization——should be applied to reduce any negative impact on data subjects (GDPR Arts. 25 and 32; EDPB, 2019).

7.2. The PDPL Approach:

7.2.1. Balancing of Interests

The PDPL takes a similar approach to the GDPR in requiring a balancing of interests, but it incorporates stricter procedural requirements for assessing and documenting the justification for processing based on legitimate interests (PDPL Art. 16). Under Article 16 of the PDPL, controllers must conduct an assessment to ensure that the legitimate interests do not infringe upon the rights of the data subjects (PDPL Art. 16). This assessment must document the specific purpose of processing, verify that it is aligned with the requirements of the law, and analyze the impact on the data subjects (PDPL Implementing Regulations, Art. 19).

The PDPL explicitly requires controllers to conduct a balancing test to ensure that the processing is justified and does not unduly affect the privacy or rights of the data subjects (PDPL Art. 16). The balancing test also involves assessing whether the data subjects could reasonably expect such processing based on their relationship with the controller (PDPL Implementing Regulations, Art. 19). Similar to the GDPR, the PDPL mandates that the assessment process be documented, and the controller must be prepared to demonstrate compliance to regulatory authorities upon request (PDPL, 2021, Art. 21). However, the PDPL imposes more stringent restrictions by excluding sensitive data from being processed under legitimate interests (PDPL Art. 6).

7.2.2. Preconditions for Processing

The PDPL sets out several preconditions for processing data under legitimate interests. These preconditions include:

- No Processing of Sensitive Data: Unlike the GDPR, which allows processing of sensitive data under certain conditions with heightened safeguards (GDPR, 2016, Art. 9), the PDPL prohibits processing sensitive data under legitimate interests (PDPL Art. 6).
- Specific Constraints on Public Authorities: The PDPL restricts the use of legitimate interests by public authorities unless it serves a clearly defined statutory purpose (PDPL Art. 16).
- Documentation of Assessments: Controllers must conduct a documented assessment that includes details about the purpose of processing, its legitimacy, and whether the processing aligns with the data subject's expectations (PDPL Implementing Regulations, Art. 19). If the assessment finds that the processing negatively impacts the rights of data subjects, controllers must either amend their approach or use another lawful basis for processing (PDPL Implementing Regulations, Art. 19).

7.2.3. Case Study Comparison: Fraud Prevention Example

The GDPR. Under the GDPR, a bank may use personal data for fraud prevention purposes, relying on legitimate interests as the lawful basis (GDPR Art. 6(1)(f); GDPR Recital 47). In conducting the balancing test, the bank would need to assess whether its interest in preventing fraud outweighs the rights and freedoms of the data subjects involved (Article 29 Working Party, 2014). Since fraud prevention is a critical objective that benefits both the organization and society, and the impact on data subjects is typically minimal when adequate safeguards (e.g., encryption) are in place, the legitimate interests of the bank would likely prevail (Voigt and von dem Bussche, 2017). Transparency measures, such as informing customers that their data may be used for fraud prevention and providing an option to object, would also be implemented to satisfy the GDPR requirements (GDPR Arts. 13–14).

The PDPL. In a similar scenario under the PDPL, the bank must follow a more stringent process to use legitimate interests as a legal basis (PDPL Art. 16). The PDPL would require the bank to conduct a documented assessment and demonstrate that fraud prevention aligns with the requirements of the law without infringing upon the data subjects' rights (PDPL Implementing Regulations, Art. 19). Unlike the GDPR, the PDPL strictly prohibits using sensitive data (e.g., health or biometric information) for this purpose without explicit consent, even if it is relevant to the fraud detection process (PDPL Art. 6). Additionally, the bank must ensure that the processing does not involve any public authorities unless there is a statutory basis for doing so (PDPL Art. 16).

The differences between the GDPR and the PDPL are apparent in the level of restrictions and documentation required. While the GDPR allows for flexibility in processing, provided that a balancing test and adequate safeguards are in place, the PDPL imposes stricter limitations, particularly regarding sensitive data and the role of public authorities (PDPL Arts. 6 and 16). The emphasis on documenting assessments and excluding sensitive data reflects a more conservative approach aimed at prioritizing individual privacy in Saudi Arabia (PDPL Implementing Regulations).

8. Challenges and Criticisms

8.1. Criticisms of Legitimate Interests Under the GDPR:

The use of "legitimate interests" as a lawful basis for data processing under the GDPR has drawn several criticisms (Kamara and de Hert, 2018). These concerns primarily revolve around the over-reliance on legitimate interests by data controllers and the lack of consistency in its application across EU member states (Mahieu *et al.,* 2019). These issues create uncertainties for both organizations seeking to use personal data and individuals aiming to understand their rights under data protection laws (Gellert, 2018).

8.1.1. Over-reliance on Legitimate Interests by Data Controllers

One of the key criticisms of the use of legitimate interests under the GDPR is the potential for over-reliance by data controllers (Tikkinen-Piri *et al.,* 2018). As outlined in Article 6(1)(f) of the GDPR, legitimate interests provide a flexible legal basis for processing personal data without requiring explicit consent from data subjects (European Union, 2016). This flexibility has led many organizations to prefer this basis over more restrictive grounds, such as consent or contractual necessity (Kamara and de Hert, 2018). There is an expressed concern that legitimate interests should not be treated as a "last resort" or an easy option when other grounds for processing do not apply (Article 29 Working Party, 2014). Instead, the legitimate interests basis requires careful consideration and balancing of interests to ensure that the rights of data subjects are respected (Lynskey, 2015).

This potential over-reliance is exacerbated by the fact that legitimate interests, unlike consent, do not require a positive action from the data subject, making it an attractive option for data controllers (Gellert, 2018). However, the reliance on legitimate interests can result in the weakening of data subjects' rights, as individuals are often unaware that their data is being processed based on this basis, especially in contexts where privacy notices are not sufficiently clear or detailed (Tikkinen-Piri *et al.,* 2018). The lack of direct engagement, such as asking for consent, creates an environment where data subjects have less control over their personal data (Lynskey, 2015). This over-reliance also raises concerns about transparency, as data subjects may not be fully informed about the legitimate purposes justifying the use of their data (European Data Protection Board, 2019).

8.1.2. Lack of Consistency in National Applications

Another major criticism concerns the lack of harmonized application of the legitimate interests basis across EU member states (Kuner *et al.,* 2019). Despite the GDPR's goal of creating a unified legal framework for data protection across the EU, the interpretation and application of legitimate interests vary significantly between jurisdictions (Hijmans, 2016). For example, some member states have adopted a stricter interpretation of the legitimate interests basis, while others have been more lenient in allowing data controllers to rely on it (Mahieu *et al.,* 2019). This inconsistency can result in an uneven playing field for businesses operating across different EU countries, as they may be subject to varying levels of regulatory scrutiny depending on the member state (Svantesson, 2019).

The lack of consistency also affects data subjects, who may experience different levels of privacy protection depending on where they reside (Kuner *et al.,* 2019). This divergence undermines the GDPR's core principle of ensuring a uniform level of data protection across the EU (Hijmans, 2016). It also complicates the task of data controllers who operate in multiple jurisdictions, as they must navigate differing interpretations of what constitutes a legitimate interest and how to perform the required balancing test (Kamara and de Hert, 2018). The CJEU has occasionally addressed these inconsistencies, emphasizing the need for a more harmonized approach (CJEU, 2018). However, practical challenges remain, with national courts and regulators interpreting the balancing requirements differently (Brkan, 2019).

8.1.3. Balancing Test and Accountability

Controllers must consider various factors, including the nature of the interest, the impact on the data subject, and whether the data subject would reasonably expect their data to be processed in such a way (Lynskey, 2015). This test is not a simple one-time assessment but requires careful consideration of all relevant factors to ensure the protection of data subjects' rights (Voigt and von dem Bussche, 2017).

However, the subjective nature of the balancing test has led to concerns about accountability (Gellert and Gutwirth, 2013). Without clear, objective criteria, different organizations may come to different conclusions about whether their interests outweigh the rights of the data subject (Tene and Polonetsky, 2013). This lack of a standardized approach makes it difficult for regulators to enforce compliance consistently and for data subjects to challenge decisions effectively (Gellert, 2018). The GDPR does require data controllers to document their assessments and justify their reliance on legitimate interests, but the quality and thoroughness of these assessments can vary widely (Kamara and de Hert, 2018). The absence of a standardized framework or a common set of criteria for performing the balancing test contributes to the inconsistencies observed across the EU (Gellert, 2018).

8.2. Challenges of Legitimate Interests in the PDPL:

The PDPL faces several challenges in the application of legitimate interests as a lawful basis for data processing. This section explores the issues related to public bodies' processing practices and the lack of detailed procedural guidance, which create uncertainties for both data controllers and data subjects under the PDPL (PDPL Arts. 6 and 16).

One significant challenge with the PDPL is the treatment of public bodies and their ability to use legitimate interests as a basis for data processing. According to Article 6 of the PDPL, public entities are permitted to process personal data if it serves a legitimate interest or for security purposes (PDPL Art. 6). However, unlike the GDPR, which requires a balancing test to ensure that the interests of the controller do not override the rights and freedoms of the data subject, the PDPL provides limited procedural details and transparency regarding how public bodies must balance these interests against the rights of individuals (PDPL Implementing Regulations).

Public entities are granted considerable leeway in the processing of personal data for purposes such as national security or judicial requirements, which raises concerns about the adequacy of checks and balances to protect individual privacy. The absence of detailed procedural requirements for public entities can potentially lead to unchecked data processing practices that may undermine individuals' rights (PDPL Art. 6). Furthermore, Article 6 explicitly prohibits the processing of sensitive data under the legitimate interests basis, adding a layer of protection, but this restriction might still be insufficient if the scope of what constitutes a "legitimate interest" remains undefined for public authorities (PDPL Art. 6).

Another issue arises from the lack of independent oversight. While the PDPL establishes a supervisory authority to monitor compliance, the effectiveness of this oversight, especially concerning public entities, can be questioned (PDPL Arts. 21–22). The potential for conflicts of interest and the difficulty of ensuring accountability in the case of state actors can make it challenging to enforce data protection standards consistently.

9. Conclusion

The GDPR and the PDPL both provide for the use of legitimate interests as a lawful basis for processing personal data, but they differ significantly in their approach and application. The GDPR offers a flexible framework with clear emphasis on accountability and transparency, allowing data controllers to use legitimate interests for a variety of purposes, including fraud prevention and direct marketing, provided they conduct a thorough balancing test. Conversely, the PDPL adopts a more conservative stance, imposing stricter limitations on the use of legitimate interests, particularly concerning sensitive data and public authorities. Thus, each recommendation that follows is mapped back to the benchmark-and-adapt approach: borrowing proven GDPR mechanisms where fit, while retaining the PDPL's culturally grounded safeguards. Both frameworks require documentation of the balancing test, but the PDPL lacks detailed procedural guidance, which creates challenges for compliance and consistency.

Building on the three-part comparative matrix—scope, safeguards, and interpretation—this paper recommends greater harmonization and the issuance of detailed guidance to enhance the effectiveness of legitimate interests as a lawful basis for data processing. Both the GDPR and the PDPL would benefit from standardized balancing-test criteria to reduce inconsistencies among data controllers, particularly across jurisdictions. For the GDPR, clearer definitions of legitimate interest and structured LIA documentation would preserve the flexibility of this legal basis without inviting misuse. For the PDPL, procedural clarity is needed, especially for public bodies, to determine when and how legitimate interests apply. Harmonized guidance would also support consistent documentation and balancing-test practices.

9.1. Best Practices:

To minimize risks of infringing on data subjects' rights, the following best practices should be adopted by data controllers in both the EU and Saudi Arabia:

- Implement Rigorous LIAs: In line with GDPR Art 24 and PDPL Implementing Regulation Art 19, controllers should apply the purpose–necessity–balancing triad and maintain auditable documentation (criterion 2 – safeguards).
- Transparency and Communication: Ensuring transparency with data subjects is crucial. Data controllers should provide clear and accessible privacy notices that explain the use of legitimate interests, including the purpose of the processing and how individuals' rights are protected. This should include a clear opt-out mechanism for any processing that may not align with the reasonable expectations of data subjects (criterion 2 – safeguards).
- Apply Safeguards: Data controllers should incorporate appropriate safeguards, such as data minimization, anonymization, or encryption, to mitigate risks to data subjects. These safeguards ensure that the processing is proportionate and that the privacy impact on individuals is minimized (criterion 2 – safeguards).
- Exclusion of Sensitive Data: Reflecting PDPL Art 6's categorical ban and GDPR Art 9's higher threshold controllers should avoid relying on legitimate interests for special-category data; where unavoidable, obtain explicit consent and apply heightened safeguards (criteria 1 and 2).

In conclusion, balancing the legitimate interests of data controllers with the rights and freedoms of data subjects is essential for ensuring ethical and lawful data processing. The GDPR and the PDPL each address this balance differently, with the GDPR offering more flexibility and the PDPL emphasizing stricter safeguards. Harmonizing legitimate-interest rules and issuing clear guidance are vital for consistent compliance. By adopting best practices, ensuring transparency, and applying robust safeguards, data controllers can process personal data in a manner that respects both operational needs and privacy rights, thus achieving a balanced and responsible approach to data protection.

Data Availability Statement

No new data were created or analyzed in this study. All sources are publicly available and cited within the article.

Acknowledgment

The author thanks the anonymous reviewers for their constructive comments and insightful suggestions, which improved the quality of this paper.

Funding

This research received no external funding.

Conflicts of Interest

The author declares no conflict of interest.

Biographies

Ahmed M. Bamashmoos

Law Department, Faculty of Science and Theoretical Studies, Saudi Electronic University, Dammam, Saudi Arabia, 00966112613500, Asalem@seu.edu.sa

Dr. Bamashmoos is a Saudi scholar holding an S.J.D. in Data Protection from the University of Kansas. He earned an LL.M. in International Trade and a B.A. in Islamic Law. He has served as a legal advisor at Saudi Aramco and is currently an Associate Professor at the Saudi Electronic University. His research focuses on data privacy, Islamic law, and legal systems, with particular interest in comparing Saudi and international privacy laws, digital transformation, and privacy rights in the modern era.

https://orcid.org/0009-0006-4813-1124

References

Article 29 Data Protection Working Party. (2014). *Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (WP 217). Brussels: European Commission*. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (accessed on 10/07/2025).

Balboni, P., Cooper, D., Imperiali, R. and Macenaite, M. (2013). Legitimate interest of the data controller: New data-protection paradigm legitimacy grounded on appropriate protection. *International Data Privacy Law*, **3**(4), 244–61. DOI:10.1093/idpl/ipt019

Brkan, M. (2019). *Courts, Privacy and Data Protection in the EU: Economic Analysis and Impact on Fundamental Rights*. Cheltenham, UK:Edward Elgar Publishing.

Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms. Rome, 4.XI.1950*. Available at: https://www.echr.coe.int/european-convention-on-human-rights (accessed on 10/07/2025).

Council of Europe. (1981). *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108). Strasbourg, 28.I.1981*. Available at: https://rm.coe.int/1680078b37 (accessed on 08/07/2025).

Court of Justice of the European Union. (2010). *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, Joined Cases C 92/09 and C 93/09, ECLI:EU:C:2010:662*. Available at: https://curia.europa.eu/juris/liste.jsf?num=C 92/09 (accessed on 07/07/2025).

Court of Justice of the European Union. (2016). *Patrick Breyer v Bundesrepublik Deutschland, Case C 582/14, ECLI:EU:C:2016:779*. Available at: https://curia.europa.eu/juris/liste.jsf?num=C 582/14 (accessed on 05/07/2025).

Court of Justice of the European Union. (2018). *Tietosuojavaltuutettu v Jehovan Todistajat Uskonnollinen Yhdyskunta, Case C 25/17, ECLI:EU:C:2018:551*. Available at: https://curia.europa.eu/juris/liste.jsf?num=C 25/17 (accessed on 01/07/2025).

Court of Justice of the European Union. (2019). *Fashion ID GmbH and Co. KG v Verbraucherzentrale NRW eV, Case C 40/17, ECLI:EU:C:2019:629*. Available at: https://curia.europa.eu/juris/liste.jsf?num=C 40/17 (accessed on 01/07/2025).

Dolenc, D. (2020). Legitimate interest as legal grounds for processing personal data. *Bankarstvo*, **49**(3), 145–70. DOI:10.5937/bankarstvo2003145D

European Data Protection Board. (2019). *Guidelines 3/2019 on Processing of Personal Data Through Video Devices (Rev. 29/01/2020)*. Available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en.pdf (accessed on 05/07/2025).

European Data Protection Board. (2021). *Guidelines 8/2020 on the Targeting of Social Media Users (Final Version, 13/04/2021)*. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en (accessed on 07/07/2025).

European Data Protection Board. (2024). *Guidelines 1/2024 on Processing of Personal Data Based on Article 6(1)(f) GDPR (Legitimate Interest)*. Available at: https://edpb.europa.eu (accessed on 08/07/2025).

European Parliament and Council. (1995). *Directive 95/46/EC on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data. Official Journal of the European Union, L 281, 31–50*. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (accessed on 09/07/2025).

European Union Agency for Network and Information Security (ENISA). (2015). *Privacy and Data Protection by Design – From Policy to Engineering. Heraklion/Athens: ENISA*. Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (accessed on 10/07/2025).

European Union. (2016). *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 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88*. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 01/07/2025).

Freitas, M.C. and Mira da Silva, M. (2018). GDPR compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering and Management*, **3**(4), 30. DOI:10.20897/jisem/3941

Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law and Security Review*, **34**(2), 279–88. DOI:10.1016/j.clsr.2017.12.003

Gellert, R. and Gutwirth, S. (2013). The legal construction of privacy and data protection. *Computer Law and Security Review*, **29**(5), 522–30. DOI:10.1016/j.clsr.2013.07.005

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, **59**(6), 703–5. DOI:10.2501/IJMR-2017-050

González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Dordrecht, Netherlands: Springer.

Greenleaf, G. (2021). Global data-privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws and Business International Report*, **170**(n/a), 10–3.

Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy: The Story of Article 16 TFEU*. Cham, Switzerland: Springer. DOI:10.1007/978-3-319-34090-6

Hutchinson, T. and Duncan, N. (2012). Defining and describing what we do: Doctrinal legal doctrinal legal research. *Deakin Law Review*, **17**(1), 83–119. DOI:10.21153/dlr2012vol17no1art70

Information Commissioner's Office. (2019). *Guide to the General Data Protection Regulation (GDPR): Legitimate Interests. Wilmslow, UK: ICO*. Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/ (accessed on 02/07/2025).

Kamara, I. and De Hert, P. (2018). *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. Brussels Privacy Hub Working Paper, 4(12)*. Available at: https://papers.ssrn.com/abstract=3228369 (accessed on 04/07/2025).

Kuner, C., Bygrave, L.A. and Docksey, C. (2019). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford, UK: Oxford University Press.

Lachaud, E. (2018). The balancing exercise under GDPR: Legitimacy, necessity and proportionality of data processing. *Journal of Data Protection and Privacy*, **2**(3), 243–55.

Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford, UK: Oxford University Press.

Mahieu, R., Van Hoboken, J. and Asghari, H. (2019). *Responsibility for Data Protection in a Networked World. Journal of Intellectual Property, Information Technology and E-Commerce Law, 10, 85*. Available at: https://papers.ssrn.com/abstract=3256743 (accessed on 05/07/2025).

Organisation for Economic Co-operation and Development. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD*. Available at: https://web.archive.oecd.org/2013 09 05/247484-oecd_privacy_framework.pdf (accessed on 09/07/2025).

Personal Data Protection Law. (2021). *Royal Decree M/19 of 09-02-1443H (16/09/2021), Amended by Royal Decree M/148 of 05-09-1444H (27/03/2023). Kingdom of Saudi Arabia*. Available at: https://sdaia.gov.sa/en/SDAIA/about/Documents/Personal%20 Data%20English%20V2 23April2023 Reviewed-.pdf (accessed on 02/07/2025).

Saudi Authority for Data and Artificial Intelligence. (n/a). *Implementing Regulations of the Personal Data Protection Law. Riyadh: National Data Management Office*. Available at: https://sdaia.gov.sa/en/SDAIA/about/Documents/Implementing Regulation.pdf (accessed on 03/07/2025).

Svantesson, D.J.B. (2019). Introducing the global data-privacy prize. *International Data Privacy Law*, **9**(1), 64–8. DOI:10.1093/idpl/ipz002

Tene, O. and Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of age of analytics. *Northwestern Journal of Technology and Intellectual Property*, **11**(5), 239–73.

Tikkinen-Piri, C., Rohunen, A. and Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal-data-collecting companies. *Computer Law and Security Review*, **34**(1), 134–53. DOI:10.1016/j.clsr.2017.05.015

Voigt, P. and von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham, Switzerland: Springer. DOI:10.1007/978-3-319-57959-7

Wachter, S. and Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data-protection law in the age of big data and AI. *Columbia Business Law Review*, **2019**(2), 494–620. DOI:10.7916/cblr.v2019i2.3424

Watkins, D. and Burton, M. (2017). *Research Methods in Law*. 2nd edition. Abingdon, UK: Routledge.

Zufall, F., Kimura, R. and Peng, L. (2022). Towards a simple mathematical model for the legal concept of balancing of interests. *Artificial Intelligence and Law*, **31**(4), 807–27. DOI:10.1007/s10506-022-09338-3

Copyright