IMPLEMENTATION CHALLENGES OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 IN INDIA: A CRITICAL ANALYSIS

Shaily Agrawal, Research Scholar (Law), Jagran Lakecity University

Dr. Yash Tiwari, Associate Professor (Law), Jagran Lakecity University

ABSTRACT

India's data protection laws underwent significant transformation after the Indian Constitution declared that the right to privacy is a fundamental right. The Digital Personal Data Protection Act, 2023 (DPDP Act) was enacted by India as the first comprehensive law protecting personal data considering the rapid digitization and massive processing of data conducted by both public and commercial stakeholders. The Act marks an important milestone in the legal mechanism, but its efficacy depends on the way it is implemented, institutional capacity, and effective compliance. This paper examines primary issues associated with implementing the DPDP Act, such as its constraints in the workplace, consent fatigue, enforcement mechanisms, state exemptions, cross-border data transfers, and the general population's lack of awareness. The article argues that the DPDP Act runs the risk of being nothing besides a symbolic framework until it resolves the structural and operational defects, making short comparisons with the European Union's (EU) General Data Protection Regulation (GDPR). In this study, doctrinal and comparison methods are followed to provide specific recommendations for enhancing the enforcement of the DPDP Act aligning with global digital environment.

Keywords: DPDP Act, Data Privacy, GDPR, Implementation Challenges, Data Protection Board.

1. Introduction

Digital technologies have transformed personal data into a critical asset for both public administration and private industry. In India, projects like Digital India, Aadhaar, the Unified Payments Interface (UPI), and large-scale e-governance systems made it considerably simpler to collect, process, and store personal data.[1] While the digital revolution contributed to effectiveness and creativity, it also brought up additional concerns regarding breaches of privacy and illicit use of personal data.[2]

Right to privacy was declared a fundamental right by the Supreme Court in Justice K.S. Puttaswamy v. Union of India, thereby highlighting need for a strong data privacy law in India.[3] Prior to the enactment of the DPDP Act, the Information Technology Act of 2000 was the major law to ensure right to data privacy, but it was not adequate to address contemporary data protection issues.[4] By establishing a system for safeguarding data based on consent and specifying responsibilities and rights for data principals and data fiduciaries, the DPDP Act aims to address this gap.

Nevertheless, data protection cannot be ensured just through regulation. The enforcement of the DPDP Act depends mainly on the techniques through which it is implemented and the institutional design. The capacity of DPDP Act is examined for the effective data protection considering the key barriers to its implementation.

2. Data Privacy Framework in India and European Union

The data protection framework of India has following regulations and it evolved over time-

2.1 Information Technology Act, 2000 and SPDI Rules, 2011

The Information Technology Act, 2000, which focused primarily on cybercrimes and e-commerce, was the foundation of security measures for data in India.[5] Section 43A

[1] Ministry of Electronics and Information Technology (MeitY), *Digital India*, DIGITAL INDIA PROGRAMME, https://www.digitalindia.gov.in/ (last visited Aug. 30, 2025).
[2] *Id.*
[3] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 (Supreme Court of India 2017).
[4] Digital Personal Data Protection Act, 2023 of 2023, Act no. 22 0f 2023, Government of India [hereinafter referred as DPDP Act]; Information Technology Act, 2000 of 2000, No. 21 of 2000, INDIA CODE (2000) [hereinafter referred as IT Act].
[5] IT Act, *supra* note 4.

of the Act established civil liability for inability to adhere to safety procedures, while Section 72A rendered it illegal to share personal information without consent.[6] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which added to these rules, defined sensitive personal data, and imposed limited duties on business entities, were passed in 2011.[7]

However, the IT Act failed to offer adequate rights, did not have independent governmental oversight and effective enforcement mechanisms, which made it inadequate considering expanding digital data storage and processing.

2.2 Transition to the DPDP Act, 2023

Following the 2019 Personal Data Protection Bill was withdrawn, India chose a fresh, streamlined method with the DPDP Act of 2023.[8] The focus of the Act is confined to digital personal data only and the structure based on consent, data principal rights, data fiduciary obligations, and heavy penalties for breaches.[9] The limited scope and type of organizational framework given by the DPDP Act, pose serious challenges for its implementation, in spite of following international standards for data protection.

2.3 Digital Personal Data Protection (DPDP) Act, 2023

After numerous debates, India finally enacted the DPDP Act, 2023, known as its recent data protection law. Some key characteristics are: -

2.3.1 Processing based on consent - It requires users to give explicit consent to processing.[10]

2.3.2 Rights of data principals - Users have rights like data correction, erasure, and grievance redressal.[11]

[6] IT Act §§ 43A, 72A.
[7] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 of 2011, G.S.R. 313(E) [hereinafter referred as SPDI Rules].
[8] PRS Legislative Research, *The Personal Data Protection Bill, 2019*, PRS LEGISLATIVE RESEARCH (2019), https://prsindia.org/billtrack/the-personal-data-protection-bill-2019.
[9] DPDP Act §§ 5–16.
[10] DPDP Act § 6.
[11] DPDP Act §§ 11–14.

2.3.3 Obligations of Data Fiduciaries - Businesses need to be certain that purpose limitation, security procedures, and accountability are effective.[12]

2.3.4 Cross-border data flow - The DPDP Act permits data be transferred to trusted countries, that are allowed by the central government.[13]

2.3.5 Government exemptions - The Act allows government departments to manage data without consent for national security and governance, which caused fears about government oversight.[14]

The DPDP Act has some strengths, but it lacks autonomy from independent organizations to lay out fines like the GDPR exerts.

2.4 The General Data Protection Regulation

The European Union has enacted the GDPR in 2016, which came into force in 2018. This is considered as the most comprehensive and stable data protection regulation worldwide. Many nations have enacted their data protection regulation based on GDPR.[15] The DPDP Act is no exception as it is also based on GDPR. The main features of the GDPR are: -

2.4.1 Legal, fair, and Transparent Processing - According to GDPR, the processing personal data needs to be conducted in a legitimate, fair, and transparent way.[16]

2.4.2 Data Subjects' Extended Rights - The GDPR gives right to access, rectify, erase, limit, port, and object which are more detailed than the DPDP Act.[17]

2.4.3 Strict Consent Rules - The consent must be freely given, explicit, informed, clear, and can be revoked.[18]

[12] DPDP Act §§ 8–10.
[13] DPDP Act § 16.
[14] DPDP Act § 17.
[15] 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), 2016 O.J. (L 119) 1[hereinafter referred as GDPR].
[16] GDPR art. 5.
[17] GDPR arts. 12–22.
[18] GDPR arts. 4(11), 7.

2.4.4 Accountability and Compliance - The data controller has a duty to show compliance through records, and internal assessments.[19]

2.4.5 Privacy By Design and By Default - Structural safeguards for privacy need to be built in from the very beginning.[20]

2.4.6 Cross-border Data Flow - International data transfers may only be carried out when there are an adequacy decision or suitable safeguards.[21]

2.4.7 Heavy Penalties - The regulatory penalties may be levied up to twenty million euros, or four percent of worldwide yearly revenue of the data, controller found in breach of GDPR rules.[22]

Although the DPDP Act is based on the GDPR but there are some apparent shortcomings which are discussed in next section.

3. Comparative Analysis of The GDPR and The DPDP Act

The DPDP Act is analogous to the GDPR in several respects, however there are notable divergences or shortcomings as well. These are outlined below: -

3.1 Scope

The GDPR applies to all organizations that process the personal data of residents of European Union, regardless of whether they are within or outside the European Union. This is known as its extra-territorial application.[23] The DPDP Act also applies to all businesses and organizations that are managing digital personal data of Indian citizens within or outside India. However, in comparison to the GDPR, it has a limited scope as it excludes offline or non-digital data, and due to its regulatory approach, and offers comparatively weaker protection of individual rights than the GDPR.[24]

[19] GDPR arts. 24–30.
[20] GDPR art. 25.
[21] GDPR arts. 45–50.
[22] GDPR art. 83.
[23] GDPR art. 3.
[24] DPDP Act § 2.

3.2 Consent

Under GDPR, consent must be clear, specific, freely given, and informed, and can be revoked at any time.[25] Similarly, the DPDP Act also states that consent must be free, informed, specific, clear, and revocable.[26] However, the DPDP Act is not as stringent and there are some exceptions allowing processing without consent for legitimate reasons.

3.3 Rights of Data Subjects and Data Principals

The data subjects are granted numerous rights under the GDPR, including the power to access, rectify, erase, limit, object, transfer, and secure their data from automated decision-making.[27] Several rights such as right to access, correction, erasure, dispute redressal, and nomination are provided to the data principals under the DPDP Act. But certain rights are not provided by the DPDP Act like right to data portability, and right against automated decision-making.[28]

3.4 Duties of Data Controllers and Data Fiduciaries

The GDPR requires that controllers must keep detailed records of their processing operations, perform data protection impact assessments (DPIAs), and build systems that protect privacy by design and by default.[29] The DPDP Act outlines duties dealing with security measures and the responsibilities of Significant Data Fiduciaries (SDFs). However, it gives less detail on DPIAs or privacy by design, making it less strict in terms of accountability as compared to the measure of accountability imposed by GDPR.[30]

3.5 Cross-Border Data Transfers

The GDPR only allows cross-border transfers if there is an adequacy decision or if there are proper safeguards and the EU will ensure this is accurate.[31] Section 16 of the DPDP

[25] GDPR arts. 4(11), 7.
[26] DPDP Act §§ 6–7.
[27] GDPR arts. 12–22.
[28] DPDP Act §§ 11–14.
[29] GDPR arts. 24–30
[30] DPDP Act §§ 8–10.
[31] GDPR arts. 45–50.

Act regulates cross-border transfers and restricts it to countries or territories that the government had notified. Compliance procedure gives more authority to executives and fewer regulatory directives.[32]

3.6 Government Exemptions

Under the GDPR, exemptions are only allowed in certain situations and are closely defined. They need to be necessary and proportional, and have legislative safeguards.[33] On the other hand, the DPDP Act gives the government lot of exemptions for public order, security, and sovereignty. The broad Indian provisions, driven by executives could weaken data principal rights.[34]

3.7 Enforcement and Penalties

As per GDPR fines for noncompliance may amount up to €20 million, or 4% of global yearly revenue. Supervisory authorities can investigate, order, and enforce compliance.[35] In the DPDP Act, fines are smaller relative to the annual turnover of a company and the Data Protection Board, which currently has limited authority to operate autonomously imposes these penalties.[36]

3.8 Approach

The GDPR is focused on rights and accountability. It highlights principles of transparency, privacy by design, and provides data subjects greater authority. On the other hand, the DPDP Act focuses primarily on accountability of than on ensuring strong individual rights. The regulation considers the governance concerns and adapts to the policy and regulatory setting of India.

4. Illustrative Case Studies on Data Protection under the DPDP Act and the GDPR

4.1 Justice K.S. Puttaswamy against the Union of India

This case recognized that the right to privacy is a fundamental right under the Indian

[32] DPDP Act § 16.
[33] GDPR art. 23.
[34] DPDP Act § 17.
[35] GDPR art. 83.
[36] DPDP Act § 33.

Constitution, marking its significance as a landmark judgement. The groundwork for India's privacy protection structure is laid down by this judgement which highlighted key concepts like consent, purpose limitation, and the protection of data principal rights. It provides the legal foundation for the DPDP Act.[37]

4.2 Aadhaar Case challenging Data Management by Unique Identification Authority of India (UIDAI)

The Aadhaar case examined the concerns relating to the security of personal data being shared and used without consent by UIDAI biometric authentication services. The duties of data fiduciaries, including grievance redressal and consent management, highlights the significance of the rights of data principals for ensuring data privacy.[38]

4.3 Case - Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos

Right to be forgotten was recognized in this judgement making it quite significant. The GDPR's approach gives individuals more control over their personal data as compared to the DPDP Act, especially in terms of access, erasure, and objection, is highlighted in this case.[39]

4.4 Schrems II —Cross-border Data Flow

The Schrems II ruling struck off the EU–US Privacy Shield system because it failed to protect personal data that was transferred outside of the European Union to the U. S. A. The ruling demonstrates strict GDPR rule regarding cross-border data transfers. In contrast, the trans-border data transfer under the DPDP Act is primarily based on executive decisions with no regulatory provisions.[40]

4.5 British Airways data breach

The case demonstrates the way the GDPR emphasizes upon holding companies accountable by levying heavy fines based on their global revenue. Heavy fines are

[37] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[38] Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018) 1 SCC 1 (Supreme Court of India 2018).
[39] Google Spain SL v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González, Case C-131/12, EU:C:2014:317.
[40] Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, Case C-311/18, EU:C:2020:559.

levied by the DPDP Act as well, up to ₹250 crore, but the fines are not based on the company's revenue. In contrast, the GDPR uses a distinct monitoring procedure and punishments based on turnover to ensure systematic compliance.[41]

Table 4.1 – Comparison of the GDPR and The DPDP Act based on Case Studies

FEATURE	GDPR	DPDP ACT	CASE
SCOPE	PROCESSING BOTH DIGITAL AND NON-DIGITAL PERSONAL DATA.[42]	PROCESSING DIGITAL PERSONAL DATA ONLY.[43]	*PUTTASWAMY V. UNION OF INDIA* – CONSTITUTIONAL FOUNDATION FOR PRIVACY.[44]
CONSENT	FREELY GIVEN, INFORMED, SPECIFIC, UNAMBIGUOUS, REVOCABLE.[45]	FREE, INFORMED, SPECIFIC, CLEAR, WITHDRAWABLE.[46]	UIDAI / AADHAAR CASE – IMPROPER SHARING HIGHLIGHTED CONSENT IMPORTANCE.[47]
RIGHTS OF DATA SUBJECTS AND DATA PRINCIPALS	ACCESS, RECTIFICATION, ERASURE, RESTRICTION, OBJECTION, PORTABILITY, AUTOMATED DECISION-MAKING SAFEGUARDS.[48]	ACCESS, CORRECTION, ERASURE, GRIEVANCE REDRESSAL, NOMINATION.[49]	*GOOGLE SPAIN SL* – RIGHT TO BE FORGOTTEN; DPDP RIGHTS NARROWER.[50]
DATA CONTROLLER AND DATA FIDUCIARY OBLIGATIONS	ACCOUNTABILITY, DPIAS, SECURITY, PRIVACY BY DESIGN AND BY DEFAULT[51]	SECURITY SAFEGUARDS, SDF OBLIGATIONS, COMPLIANCE DUTIES.[52]	BRITISH AIRWAYS BREACH – GDPR ENFORCEMENT; DPDP HAS LOWER PENALTIES.[53]

[41] Information Commissioner's Office, Penalty Notice to British Airways, Case Ref. COM0783542 (Oct. 16, 2020).
[42] GDPR art. 3.
[43] DPDP Act § 2.
[44] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[45] GDPR arts. 4(11), 7.
[46] DPDP Act § 6.
[47] *Justice K.S. Puttaswamy (Aadhaar) v. Union of India* (2018) 1 SCC 1.
[48] GDPR arts. 12–22.
[49] DPDP Act §§ 11–14.
[50] Google Spain SL v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González, Case C-131/12, EU:C:2014:317.
[51] GDPR arts. 24–30
[52] DPDP Act §§ 8–10.
[53] Information Commissioner's Office, Penalty Notice to British Airways, Case Ref. COM0783542 (Oct. 16, 2020).

CROSS-BORDER DATA TRANSFERS	ADEQUACY DECISIONS OR SAFEGUARDS REQUIRED.[54]	RESTRICTED TO NOTIFIED COUNTRIES.[55]	*SCHREMS II* – INVALIDATION OF EU-US PRIVACY SHIELD.[56]
GOVERNMENT EXEMPTIONS	ONLY FOR SPECIFIC CASES; NECESSITY, PROPORTIONALITY, LEGISLATIVE SAFEGUARDS.[57]	BROAD EXEMPTIONS FOR SOVEREIGNTY, SECURITY, PUBLIC ORDER.[58]	UIDAI / AADHAAR CASE – STATE SURVEILLANCE CONSIDERATIONS.[59]
ENFORCEMENT AND PENALTIES	FINES UP TO €20M OR 4% OF GLOBAL TURNOVER; STRONG REGULATORY OVERSIGHT.[60]	FINES AND PENALTIES LOWER; ENFORCED VIA DATA PROTECTION BOARD.[61]	BRITISH AIRWAYS BREACH – EXAMPLE OF GDPR ENFORCEMENT AS COMPARED TO DPDP ACT'S LIMITED ENFORCEMENT.[62]
APPROACH	RIGHTS-CENTRIC, TRANSPARENCY, ACCOUNTABILITY, EMPOWERMENT.	COMPLIANCE-DRIVEN, PROCEDURAL, ORGANIZATIONAL FOCUS.	COMPARATIVE INSIGHT – GDPR PRIORITIZES DATA SUBJECT EMPOWERMENT, DPDP EMPHASIZES COMPLIANCE

5. Key Implementation Challenges

The challenges to implement the DPDP Act are following: -

5.1 Data Protection Board and Institutional Capacity

The Data Protection Board of India (DPB) is the primary body responsible for implementing the provisions of the DPDP Act.[63] The selection procedure of the Board and managerial independence are linked to the executive decisions, as opposed to the autonomous regulatory bodies under the GDPR.[64] This raises questions regarding

[54] GDPR arts. 45–50.
[55] DPDP Act § 16.
[56] Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, Case C-311/18, EU:C:2020:559.
[57] GDPR art. 23.
[58] DPDP Act § 17.
[59] *Justice K.S. Puttaswamy (Aadhaar) v. Union of India* (2018) 1 SCC 1.
[60] GDPR art. 83.
[61] DPDP Act § 33.
[62] Information Commissioner's Office, Penalty Notice to British Airways, Case Ref. COM0783542 (Oct. 16, 2020).
[63] DPDP Act § 18.
[64] DPDP Act § 19.

the autonomy, transparency, and accountability, especially in terms of processing State data.

5.2 Complex Consent Prerequisites and Hidden Tricks

Consent has been accorded a lot of importance in the DPDP Act, but complex privacy notices, digital illiteracy, and hidden patterns reduce its efficacy. As a result, consent often becomes a formalistic exercise rather than an informed and rational decision because people often give it without fully understanding the purpose.[65]

5.3 Weak Enforcement and Penalty Execution

Heavy fines are levied by the DPDP Act, but they can be effective as a deterrent due to unclear rules for enforcement, investigative authority, or administrative transparency. India's regulation system has still not completely developed, unlike the GDPR's system.[66]

5.4 State Exemptions

The broad exemptions given to State agencies for grounds like national security and public order is the most disputed provisions of the DPDP Act. These exemptions might affect the constitutional protections laid out in Puttaswamy judgement and can result in unlimited surveillance with no proper checks and balances.[67]

5.5 Cross-Border Data Transfers

The DPDP Act allows data to be transferred to those countries that are notified by the government as trusted nations.[68] However, unlike GDPR, the lack of specific requirements and protections confuses the multinational firms and might damage India's reputation as a participant in international data flows.[69]

---

[65] Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 JOURNAL OF ECONOMIC LITERATURE 442 (2016), https://pubs.aeaweb.org/doi/10.1257/jel.54.2.442.
[66] DPDP Act § 22.
[67] Puttaswamy, 2017 S.C.C. 1.
[68] DPDP Act § 16.
[69] GDPR art. 45.

5.6 Exclusion of Non-Personal and Anonymized Data

Non-personal or anonymous data are not covered by the DPDP Act as it pertains to digital personal data only. In the age of AI and big data, this may lead to violations of regulations.[70]

6. Policy Recommendations

For effective implementation of the DPDP Act, several steps need to be taken. Some of the recommendations are: -

6.1 Independence of Data Protection Board — To ensure transparency and accountability, the Data Protection Board must be free from government influence regarding functions and selection procedure of Board members.[71]

6.2 Stronger Data Subject Rights - Certain individual rights needs to be included in the DPDP Act. These rights include - right to data portability, the right to be forgotten, and grievance redressal mechanisms to give data principles stronger rights to secure personal data.[72]

6.3 Enhancement of Corporate Rules - They should ensure privacy by design and by default. They should also conduct data protection impact assessments (DPIAs) and audits regularly.[73]

6.4 Transparent Rules for data transfers across borders - It is necessary to develop clear standards regarding the list of trusted nations to have clear legal guidelines.[74]

6.5 Public Awareness Campaigns - For the DPDP Act to execute smoothly in a systematic manner, both individuals and organizations need to be educated regarding their rights to data privacy.

[70] DPDP Act § 2(f).
[71] DPDP Act § 19.
[72] GDPR arts. 12–22.
[73] GDPR arts. 24–30
[74] GDPR arts. 45–47.

7. Conclusion

A significant advancement in India's data protection framework is seen with the enforcement of the Digital Personal Data Protection Act, 2023 as it enforces the right to privacy guaranteed by the Constitution. A fundamental legal framework for digital personal data is provided by the Act, but it will not be effective unless it addresses common problems such as autonomy of institutions, enforcement capacity, consent, and regulating the supervision by state.

If the law does not get systematically enforced, it may function primarily as an instrument for providing guidelines for compliance for individuals and firms rather than a framework to protect individuals rights to secure digital personal data. By ensuring the independence of the Data Protection Board, transparent enforcement, and raising public awareness and digital literacy are vital for proper application of law. The DPDP Act can only fulfil objective of adequate data privacy protection via continuous organizational dedication and ethical implementation.

References

1. Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 Journal of Economic Literature 442 (2016), https://pubs.aeaweb.org/doi/10.1257/jel.54.2.442.

2. Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, Case C-311/18, EU:C:2020:559.

3. Digital Personal Data Protection Act, 2023 of 2023, Act no. 22 0f 2023, Government of India.

4. Google Spain SL v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González, Case C-131/12, EU:C:2014:317.

5. *ICO Statement: Intention to Fine British Airways £183.39m under GDPR for Data Breach | European Data Protection Board*, https://www.edpb.europa.eu/news/national-news/2019/ico-statement-intention-fine-british-airways-ps18339m-under-gdpr-data_en (last visited Dec. 16, 2025).

6. Information Commissioner's Office, Penalty Notice to British Airways, Case Ref. COM0783542 (Oct. 16, 2020).

7. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 of 2011, G.S.R. 313(E).

8. Information Technology Act, 2000 of 2000, No. 21 of 2000, INDIA CODE (2000).

9. Justice K.S. Puttaswamy (Aadhaar) v. Union of India (2018) 1 SCC 1 (Supreme Court of India 2018).

10. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 (Supreme Court of India 2017).

11. Ministry of Electronics and Information Technology (MeitY), *Digital India*, Digital India Programme, https://www.digitalindia.gov.in/ (last visited Aug. 30, 2025).

12. PRS Legislative Research, *The Personal Data Protection Bill, 2019*, PRS Legislative Research (2019), https://prsindia.org/billtrack/the-personal-data-protection-bill-2019.

13. 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), 2016 O.J. (L 119) 1.