Bharat International Journal of Humanities and Social Sciences | 2019 | Volume 08 | Issue 02 | Pages 01-06
https://bijhss-university-journal.in/en

Bharat International Journal of Humanities and Social Sciences

Research Article

व्यक्तिगत डेटा का सीमापार हस्तांतरण: यूरोपीय संघ और भारत के नियामक दृष्टिकोणों का तुलनात्मक विश्लेषण तथा सहयोग की प्रस्तावित रूपरेखा

Cross-Border Transfers of Personal Data: A Comparative Analysis of the European Union's and India's Regulatory Approaches and a Proposed Framework for Cooperation

Prof. Srikrishna Khanna [1]

[1]Prof, Atal Bihari Vajpayee Hindi University. E-mail: drikrishna.khanna@gmail.com

***Correspondence:** drikrishna.khanna@gmail.com

Submitted: 06 Jan 2019 | Revised: 17 May 2019 | Accepted: 04 Oct 2019 | Published: 22 Dec 2019

सारांश: व्यक्तिगत डेटा के सीमापार हस्तांतरण को विनियमित करने के लिए व्यक्तियों के अधिकारों की सुरक्षा, अंतरराष्ट्रीय व्यापार की आवश्यकताओं और विधि प्रवर्तन एजेंसियों सहित सार्वजनिक प्राधिकरणों के बीच सहयोग में संतुलन स्थापित करना आवश्यक है। विभिन्न न्यायक्षेत्रों में डेटा संरक्षण के उद्देश्य समान होने पर भी नियामक आवश्यकताओं में अंतर वैध हस्तांतरण को जटिल बना सकता है। यह लेख यूरोपीय संघ के सामान्य डेटा संरक्षण विनियमन (**GDPR**) और भारत के **2019** के व्यक्तिगत डेटा संरक्षण विधेयक (**PDPB**) का तुलनात्मक विश्लेषण करता है। भारतीय विधेयक को उसके विधायी प्रस्ताव के रूप में अध्ययन में शामिल किया गया है। विश्लेषण पाँच पहलुओं पर केंद्रित है—डेटा के वैध प्रसंस्करण की शर्तें, उन व्यक्तियों के अधिकार जिनसे डेटा संबंधित है, डेटा स्थानीयकरण की आवश्यकताएँ, व्यक्तिगत डेटा की सुरक्षा के उल्लंघन की स्थिति में लागू दायित्व और लेखापरीक्षा संबंधी आवश्यकताएँ। लेख यह जाँचता है कि इन क्षेत्रों में नियामक अंतर सीमापार हस्तांतरण में किस प्रकार बाधा बन सकते हैं और किन क्षेत्रों में नियमों के बीच अधिक संगतता व्यक्तिगत डेटा की सुरक्षा बनाए रखते हुए ऐसे हस्तांतरण को सुगम बना सकती है। इस तुलना के आधार पर लेख यूरोपीय संघ और भारत के बीच सहयोग की संभावित रूपरेखाओं पर विचार करता है और नीति-निर्माताओं तथा शोधकर्ताओं को यह आकलन करने का आधार देता है कि दोनों विधिक व्यवस्थाओं की भिन्नताओं को ध्यान में रखते हुए बेहतर नियामक समन्वय वैध डेटा हस्तांतरण को कैसे सुगम बना सकता है।

प्रमुख शब्द — सीमापार डेटा हस्तांतरण, व्यक्तिगत डेटा संरक्षण, **GDPR**, भारत का व्यक्तिगत डेटा संरक्षण विधेयक **2019**, डेटा स्थानीयकरण, यूरोपीय संघ–भारत नियामक सहयोग।

Abstract: Regulating cross-border transfers of personal data requires balancing the protection of individual rights with the needs of international trade and cooperation between public authorities, including law enforcement agencies. Divergent regulatory requirements can complicate lawful transfers even when jurisdictions share similar data protection objectives. This article compares the European Union's General Data Protection Regulation (GDPR) with India's Personal Data Protection Bill of 2019 as a legislative proposal. The analysis focuses on the conditions for lawful processing, the rights of data subjects, data localization requirements, obligations in the event of a personal data breach, and audit requirements. It examines how differences in these areas can hinder cross-border transfers and identifies areas in which greater regulatory compatibility could facilitate them while preserving safeguards for personal data. Drawing on this comparison, the article explores options for an EU–India cooperation framework and provides a basis for policymakers and researchers to assess how closer regulatory coordination could support lawful transfers while accommodating differences between the two legal systems.

Keywords: Cross-border data transfers, personal data protection, GDPR, India's Personal Data Protection Bill 2019, data localization, EU–India regulatory cooperation.

1. प्रस्तावना

सीमापार डेटा हस्तांतरण डिजिटल सेवाओं, अंतरराष्ट्रीय व्यापार और सार्वजनिक संस्थाओं के सहयोग का अभिन्न भाग है। कोई संगठन एक देश में डेटा एकत्र कर सकता है, दूसरे में उसका विश्लेषण कर सकता है और किसी तीसरे देश में स्थित सेवा प्रदाता से भंडारण या सहायता प्राप्त कर सकता है। इस प्रक्रिया में संबंधित व्यक्ति, डेटा के उपयोग का निर्णय लेने वाला संगठन और उसके लिए काम करने वाला प्रसंस्करणकर्ता अलग-अलग विधिक व्यवस्थाओं के अधीन हो सकते हैं। एक क्षेत्र में वैध संग्रह अपने आप दूसरे क्षेत्र में हस्तांतरण का अधिकार नहीं देता। डेटा का विदेश जाना उस व्यक्ति के लिए अधिकारों के प्रयोग को कठिन बना सकता है जिससे डेटा संबंधित है। दूसरी ओर, हर प्रकार के डेटा पर एक समान स्थानीय भंडारण या अनुमोदन की शर्त लगाने से लागत बढ़ सकती है। इसका असर उन छोटे संगठनों पर विशेष रूप से पड़ सकता है जिनके पास अलग-अलग देशों में अनुपालन और तकनीकी व्यवस्था चलाने के सीमित साधन हैं। अध्ययन का केंद्रीय प्रश्न यह है कि अधिकारों का प्रभावी संरक्षण बनाए रखते हुए दो अलग-अलग विधिक व्यवस्थाओं के बीच वैध हस्तांतरण कैसे संभव बनाया जाए।

2. अध्ययन की पद्धति और तुलना का दायरा

© 2019 By the Authors. This Open Access Article Was Published Under a Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/).

मूल अध्ययन तुलनात्मक विधिक विश्लेषण पर आधारित है। यूरोपीय संघ के विनियमन, भारतीय विधेयक, न्यायिक निर्णय और नियामक दस्तावेज़ों को संस्थागत तथा व्यावसायिक अनुपालन के संदर्भ में पढ़ा गया है। मूल लेख में उद्योग और डेटा गोपनीयता से जुड़े विशेषज्ञों के साथ साक्षात्कार और चर्चाओं का भी उल्लेख है। इन चर्चाओं को व्यावहारिक संदर्भ के रूप में समझा गया है।

तुलना के तीन स्तर हैं। पहला स्तर यह पूछता है कि डेटा का प्रसंस्करण किन आधारों पर वैध है। दूसरा स्तर विदेश में डेटा भेजने की अतिरिक्त शर्तों पर केंद्रित है। तीसरा स्तर जाँचता है कि अधिकार लागू करने, शिकायत का निवारण करने और उल्लंघन की सूचना देने की ज़िम्मेदारी किसकी है। इससे समान शब्दावली और वास्तविक विधिक संगतता के बीच अंतर स्पष्ट होता है।

3. यूरोपीय संघ और भारत के डेटा संरक्षण ढाँचे

3.1 यूरोपीय संघ

GDPR व्यक्तिगत डेटा को किसी पहचाने गए या पहचाने जा सकने वाले प्राकृतिक व्यक्ति से संबंधित सूचना के रूप में देखता है। डेटा नियंत्रक प्रसंस्करण के उद्देश्य और साधन निर्धारित करता है। प्रसंस्करणकर्ता नियंत्रक की ओर से डेटा का उपयोग करता है। यूरोपीय संघ में प्रतिष्ठान की गतिविधियों के संदर्भ में होने वाले प्रसंस्करण के अलावा कुछ स्थितियों में यूरोपीय संघ के बाहर स्थित संगठन भी इसके दायरे में आते हैं। उदाहरण के लिए, संघ में स्थित व्यक्तियों को वस्तुएँ या सेवाएँ देने अथवा संघ के भीतर उनके व्यवहार की निगरानी से जुड़े प्रसंस्करण पर अनुच्छेद 3 लागू हो सकता है।

अनुच्छेद 5 वैधता, निष्पक्षता, पारदर्शिता, उद्देश्य-सीमा, डेटा न्यूनीकरण, शुद्धता, भंडारण-सीमा और सुरक्षा के सिद्धांत निर्धारित करता है। अनुच्छेद 6 सहमति, अनुबंध का निष्पादन, विधिक दायित्व, जीवन-संबंधी हित, सार्वजनिक हित या सार्वजनिक प्राधिकार का प्रयोग, और वैध हित जैसे प्रसंस्करण आधार निर्धारित करता है। अनुच्छेद 9 के अंतर्गत विशेष श्रेणियों के प्रसंस्करण के लिए अलग शर्तें हैं। आपराधिक दोषसिद्धि और अपराधों से संबंधित डेटा के लिए अनुच्छेद 10 अलग व्यवस्था करता है।

3.2 भारत का 2019 का विधेयक

भारतीय विधेयक में 'डेटा प्रिंसिपल' उस व्यक्ति को कहा गया है जिससे व्यक्तिगत डेटा संबंधित है। 'डेटा फिड्यूशियरी' वह पक्ष है जो प्रसंस्करण के उद्देश्य और साधन निर्धारित करता है। मूल अध्ययन रेखांकित करता है कि भारत में प्रसंस्करण होने से कुछ ऐसी गतिविधियाँ भी विधेयक के दायरे में आ सकती थीं जिनमें डेटा भारतीय व्यक्तियों से संबंधित न हो। विदेश में होने वाले प्रसंस्करण के लिए भारत में कारोबार, सेवाओं की पेशकश या प्रोफाइलिंग जैसे संबंध भी प्रासंगिक थे।

विधेयक सामान्य व्यक्तिगत डेटा, संवेदनशील व्यक्तिगत डेटा और सरकार द्वारा अधिसूचित किए जाने वाले 'महत्त्वपूर्ण व्यक्तिगत डेटा' के बीच अंतर करता था। संवेदनशील श्रेणियों में वित्तीय डेटा, आधिकारिक पहचानकर्ता, जाति या जनजाति तथा ट्रांसजेंडर या इंटरसेक्स स्थिति जैसी मदें शामिल थीं। स्वास्थ्य, आनुवंशिक और बायोमेट्रिक डेटा जैसे कुछ क्षेत्रों में यूरोपीय और भारतीय व्यवस्थाओं का पर्याप्त मेल था। यूरोपीय सूची में नस्लीय या जातीय मूल, दार्शनिक विश्वास और ट्रेड यूनियन सदस्यता जैसी श्रेणियाँ थीं। दोनों ढाँचों में किसी श्रेणी का समान नाम होने पर भी उसकी परिभाषा और लागू शर्तें अलग हो सकती हैं।

भारत के प्रस्ताव में सहमति के अलावा विधि द्वारा अपेक्षित प्रसंस्करण, चिकित्सा आपातस्थिति, रोजगार और विनियमों में निर्धारित युक्तिसंगत उद्देश्यों के लिए प्रावधान थे। GDPR के 'वैध हित' और विधेयक के 'युक्तिसंगत उद्देश्य' में कुछ समानता थी, पर उनके निर्धारण का तरीका अलग था। भारतीय प्रस्ताव में डेटा संरक्षण प्राधिकरण की भूमिका विशेष रूप से महत्त्वपूर्ण थी।

4. सीमापार हस्तांतरण के विधिक मार्ग

4.1 GDPR के अंतर्गत विदेश में हस्तांतरण

GDPR का अध्याय V तीसरे देशों और अंतरराष्ट्रीय संगठनों को व्यक्तिगत डेटा के हस्तांतरण का ढाँचा प्रदान करता है। अनुच्छेद 45 के अंतर्गत यूरोपीय आयोग किसी देश, क्षेत्र, निर्दिष्ट क्षेत्रक या अंतरराष्ट्रीय संगठन के संरक्षण स्तर को पर्याप्त घोषित कर सकता है। ऐसी समीक्षा में लागू कानून, स्वतंत्र निगरानी और अधिकारों को लागू करने की उपलब्ध व्यवस्था प्रासंगिक हैं।

पर्याप्तता निर्णय के अभाव में अनुच्छेद 46 के अंतर्गत उपयुक्त सुरक्षा उपायों के आधार पर हस्तांतरण संभव हो सकता है, बशर्ते व्यक्तियों के अधिकार प्रवर्तनीय हों और प्रभावी विधिक उपचार उपलब्ध हों। इसके उदाहरण हैं मानक संविदात्मक खंड (SCC), बाध्यकारी कॉरपोरेट नियम (BCR), स्वीकृत आचार संहिता और उपयुक्त बाध्यकारी प्रतिबद्धताओं के साथ प्रमाणन। किसी बहुराष्ट्रीय समूह के भीतर हस्तांतरण के लिए BCR विशेष रूप से प्रासंगिक हैं। अनुच्छेद 49 में विशिष्ट परिस्थितियों के लिए सीमित अपवाद दिए गए हैं, जिनमें जोखिमों की जानकारी दिए जाने के बाद स्पष्ट सहमति, कुछ अनुबंधों का आवश्यक निष्पादन और महत्त्वपूर्ण सार्वजनिक हित शामिल हैं।

मूल अध्ययन में उल्लिखित Schrems II निर्णय बताता है कि संविदात्मक खंडों की मौजूदगी अपने आप प्रभावी संरक्षण सुनिश्चित नहीं करती। प्राप्तकर्ता देश के कानून और व्यवहार, विशेषकर सार्वजनिक प्राधिकरणों की डेटा तक पहुँच और उपलब्ध उपचार, का भी मूल्यांकन आवश्यक है। न्यायालय ने EU–US Privacy Shield संबंधी पर्याप्तता निर्णय को अमान्य किया और मानक संविदात्मक खंडों के उपयोग में वास्तविक संरक्षण की जाँच की आवश्यकता स्पष्ट की (C-311/18, 16 जुलाई 2020)।

4.2 भारतीय विधेयक में स्थानीयकरण और हस्तांतरण

विधेयक की धारा 33 संवेदनशील व्यक्तिगत डेटा को विदेश में प्रसंस्करण के लिए भेजने की अनुमति देती थी, पर उसे भारत में भी संग्रहीत रखना आवश्यक था। धारा 34 के तहत ऐसे हस्तांतरण के लिए स्पष्ट सहमति के साथ विधेयक में निर्दिष्ट आधारों में से एक की आवश्यकता थी। इनमें प्राधिकरण से अनुमोदित अनुबंध या समूह के भीतर की योजना, केंद्र सरकार द्वारा अनुमत गंतव्य, या निर्दिष्ट उद्देश्य के लिए प्राधिकरण की अनुमति शामिल थी। अनुमोदित व्यवस्थाओं में आगे होने वाले हस्तांतरण के दौरान भी व्यक्तियों के अधिकारों की सुरक्षा प्रासंगिक थी।

महत्त्वपूर्ण व्यक्तिगत डेटा के लिए मूल नियम भारत में प्रसंस्करण था। धारा 34 में सीमित अपवाद प्रस्तावित थे। इनमें तत्काल कार्रवाई के लिए आवश्यक स्वास्थ्य या आपातकालीन सेवाओं से जुड़े हस्तांतरण और ऐसे अनुमत हस्तांतरण शामिल थे जिनसे भारत के सुरक्षा और रणनीतिक हितों पर प्रतिकूल प्रभाव न पड़े। चूँकि इस श्रेणी की पहचान सरकारी अधिसूचना पर निर्भर थी, संगठन पहले से सभी प्रभावित डेटा प्रवाहों का निर्धारण नहीं कर सकते थे।

5. भारत और यूरोपीय संघ के बीच सूचना विनिमय

मूल लेख के समय भारत के संबंध में यूरोपीय आयोग का पर्याप्तता निर्णय उपलब्ध नहीं था। लेख इसलिए अनुबंध, समूह के भीतर लागू नियम, प्रमाणन और विशिष्ट परिस्थितियों के अपवादों पर विचार करता है। इन विकल्पों का चुनाव हस्तांतरण की दिशा, उद्देश्य और पक्षों की भूमिका के अनुसार बदलता है। उदाहरण के लिए, यूरोपीय नियंत्रक से भारतीय सेवा प्रदाता को नियमित व्यापारिक हस्तांतरण के लिए अनुबंध में प्रसंस्करण का उद्देश्य, अवधि, डेटा की श्रेणियाँ, सुरक्षा दायित्व और आगे हस्तांतरण की शर्तें स्पष्ट करना उपयोगी है। भारतीय स्थानीयकरण की प्रस्तावित शर्तों का मूल्यांकन अलग से आवश्यक होता।

सार्वजनिक प्राधिकरणों के बीच सूचना विनिमय में साझा करने वाले निकाय की वैधानिक क्षमता, प्रयोजन, गोपनीयता और व्यक्ति को उपलब्ध उपचार पर विचार करना पड़ता है। जहाँ GDPR लागू हो, उसके अनुच्छेद 46 में सार्वजनिक निकायों के लिए प्रवर्तनीय साधनों और निर्दिष्ट शर्तों वाले प्रशासनिक प्रबंधों की गुंजाइश है। आपराधिक विधि प्रवर्तन के विशिष्ट प्रयोजनों के लिए यूरोपीय संघ में निर्देश (EU) 2016/680 का अलग ढाँचा प्रासंगिक है। इसलिए व्यावसायिक और विधि प्रवर्तन हस्तांतरण को अलग विधिक मार्गों में रखना चाहिए।

मूल लेख संयुक्त राष्ट्र और यूरोपीय डेटा संरक्षण बोर्ड के बीच 2020 के संवाद को भी उद्धृत करता है। उस संवाद ने दिखाया कि अंतरराष्ट्रीय संगठनों की विशेषाधिकार और उन्मुक्ति संबंधी स्थिति तथा उन्हें डेटा भेजने वाले GDPR-अधीन संगठनों के दायित्व अलग प्रश्न हैं। यही भेद किसी द्विपक्षीय रूपरेखा में संबंधित संस्थाओं की शक्तियाँ और दायित्व स्पष्ट करने में सहायक है।

6. तुलनात्मक निष्कर्ष और अनुपालन संबंधी चुनौतियाँ

6.1 पारदर्शिता, संरक्षण और जवाबदेही

दोनों ढाँचे सूचना, उद्देश्य-सीमा, डेटा न्यूनीकरण, शुद्धता, सुरक्षा और जवाबदेही को महत्त्व देते हैं। फिर भी सूचना देने की सामग्री, शिकायत के संपर्क बिंदु और

प्रसंस्करणकर्ता के अनुबंध की आवश्यकताएँ समान नहीं थीं। GDPR का अनुच्छेद 28 प्रसंस्करणकर्ता के लिए विस्तृत संविदात्मक अपेक्षाएँ तय करता है। भारतीय प्रस्ताव में सूचना और शिकायत निवारण के अपने प्रावधान थे। डेटा प्रतिधारण के संदर्भ में भारतीय विधेयक समय-समय पर आवश्यकता की समीक्षा पर बल देता था। इस प्रकार साझा सिद्धांतों को समान परिचालन प्रक्रियाओं में बदलने के लिए अलग-अलग दायित्वों की पहचान आवश्यक है।

6.2 व्यक्तियों के अधिकार

दोनों ढाँचों में पहुँच, सुधार और कुछ परिस्थितियों में डेटा मिटाने अथवा पोर्टेबिलिटी से जुड़े अधिकार थे। प्रत्येक अधिकार की शर्तें और प्रयोग की प्रक्रिया अलग थी। GDPR के अनुच्छेद 17 में मिटाने का अधिकार निर्दिष्ट आधारों और अपवादों के अधीन है। भारतीय विधेयक ने सुधार और मिटाने के अधिकार को 'भुलाए जाने के अधिकार' से अलग रखा। प्रस्तावित भुलाए जाने का अधिकार व्यक्तिगत डेटा के निरंतर प्रकटीकरण को सीमित करने से संबंधित था और उसके प्रयोग में निर्णयन अधिकारी की भूमिका थी। इसके विपरीत, GDPR में व्यक्ति सामान्यतः पहले नियंत्रक से अपने अधिकार का प्रयोग करता है और आवश्यक होने पर पर्यवेक्षी प्राधिकरण या न्यायालय का सहारा ले सकता है।

6.3 सुरक्षा उल्लंघन, प्रभाव आकलन और लेखापरीक्षा

GDPR में प्रसंस्करणकर्ता सुरक्षा उल्लंघन की जानकारी नियंत्रक को अनुचित विलंब के बिना देता है। अनुच्छेद 33 के अनुसार नियंत्रक सामान्यतः पर्यवेक्षी प्राधिकरण को जानकारी मिलने के 72 घंटे के भीतर सूचित करता है, यदि उल्लंघन से अधिकारों और स्वतंत्रताओं को जोखिम होने की संभावना को खारिज नहीं किया जा सकता। अनुच्छेद 34 में उच्च जोखिम की स्थिति में प्रभावित व्यक्ति को सूचना देने का प्रावधान है। भारतीय विधेयक में नुकसान की संभावना वाले उल्लंघनों की सूचना प्राधिकरण को देने और प्रभावित व्यक्तियों को कब सूचित किया जाए, यह तय करने में प्राधिकरण की भूमिका प्रस्तावित थी।

GDPR का अनुच्छेद 35 उच्च जोखिम वाले प्रसंस्करण के लिए डेटा संरक्षण प्रभाव आकलन की अपेक्षा करता है। भारतीय प्रस्ताव में महत्त्वपूर्ण डेटा फिड्यूशियरी और जोखिमपूर्ण प्रसंस्करण के लिए प्रभाव आकलन तथा स्वतंत्र लेखापरीक्षा की विशेष व्यवस्था थी। विधेयक में स्वतंत्र परीक्षक द्वारा वार्षिक लेखापरीक्षा और डेटा ट्रस्ट स्कोर की संभावना थी। मूल लेख इन दायित्वों को व्यावहारिक अनुपालन का प्रमुख अंतर मानता है। दोनों क्षेत्रों में काम करने वाला संगठन एक साझा सुरक्षा कार्यक्रम बना सकता है, लेकिन रिपोर्टिंग की सीमा, समय और उत्तरदायी संस्था अलग से निर्धारित करनी होगी।

6.4 निगरानी, सरकारी पहुँच और संस्थागत लागत

भारतीय विधेयक में केंद्र सरकार को कुछ परिस्थितियों में छूट देने की व्यापक शक्तियाँ प्रस्तावित थीं। यूरोपीय ढाँचे में भी राष्ट्रीय सुरक्षा और आपराधिक विधि प्रवर्तन से संबंधित अलग कानूनी व्यवस्थाएँ प्रासंगिक हैं। तुलना में तीन प्रश्न महत्त्वपूर्ण हैं—सरकारी पहुँच किस अधिकार पर आधारित है, उस पर स्वतंत्र निगरानी कैसे होती है और प्रभावित व्यक्ति को प्रभावी उपचार कैसे मिलता है। केवल निजी संगठनों के अनुबंध इन प्रश्नों का समाधान नहीं कर सकते।

भारत में संवेदनशील डेटा की प्रति बनाए रखने से भंडारण, अद्यतन, अभिगम नियंत्रण और मिटाने की प्रक्रिया में अतिरिक्त जटिलता हो सकती थी। यूरोपीय संघ के भीतर भी शिकायत की स्वीकार्यता, कार्यवाही की अवधि और विभिन्न प्राधिकरणों के बीच समन्वय के अंतर को मूल लेख ने अनुपालन की चुनौती माना है। साझा मार्गदर्शन से दोहराव घट सकता है, विशेषकर छोटे और मध्यम उद्यमों के लिए।

7. सहयोग की प्रस्तावित रूपरेखा

7.1 साझा मानक और नियामक संवाद

पहला कदम उद्देश्य-सीमा, आवश्यक डेटा तक सीमित प्रसंस्करण, सुरक्षा, पारदर्शिता और प्रभावी शिकायत निवारण जैसे साझा सिद्धांतों की पहचान है। मूल लेख दोनों पक्षों के प्रासंगिक हितधारकों वाली वार्ता समिति की संभावना प्रस्तुत करता है। समिति पहले हस्तांतरण के सामान्य परिदृश्य और अनुपालन की बाधाएँ पहचान सकती है, फिर उन क्षेत्रों को अलग कर सकती है जहाँ प्रशासनिक मार्गदर्शन पर्याप्त है और जहाँ विधिक समझौते की आवश्यकता है।

7.2 व्यावसायिक हस्तांतरण के लिए संविदात्मक उपाय

मानक संविदात्मक खंड नियमित व्यापारिक हस्तांतरण में दायित्वों को स्पष्ट कर सकते हैं। उनके अनुप्रयोग में पक्षों की भूमिका, प्रसंस्करण का उद्देश्य, सुरक्षा उपाय, आगे हस्तांतरण, उल्लंघन की सूचना, डेटा की वापसी या मिटाना और शिकायत के निवारण की व्यवस्था शामिल हो सकती है। जोखिम की समीक्षा में प्राप्तकर्ता देश में सरकारी पहुँच और प्रभावी उपचार को भी शामिल करना आवश्यक है। इन शर्तों को क्षेत्र-विशिष्ट परिशिष्टों से स्पष्ट किया जा सकता है, जबकि लागू विधिक दायित्वों का स्वतंत्र मूल्यांकन बना रहता है।

7.3 प्रमाणन और अलग सार्वजनिक सहयोग मार्ग

मूल लेख मान्यता प्राप्त प्रमाणन निकायों के माध्यम से संगठन के तकनीकी और प्रशासनिक उपायों का आकलन करने का विकल्प सुझाता है। प्रमाणन से प्रारंभिक अभिकल्पना में डेटा संरक्षण, अभिगम नियंत्रण और सुरक्षा प्रक्रियाओं के दस्तावेजी प्रमाण मिल सकते हैं। हस्तांतरण का आधार बनने पर प्रमाणन के साथ लागू कानून के अनुसार बाध्यकारी प्रतिबद्धताएँ भी आवश्यक हैं।

सार्वजनिक प्राधिकरणों के लिए अलग सहयोग मार्ग में वैधानिक अधिकार, निर्दिष्ट उद्देश्य, आवश्यकता और अनुपातिकता, डेटा तक पहुँच के अभिलेख तथा स्वतंत्र निगरानी शामिल हो सकते हैं। जहाँ पर्याप्तता पर संवाद संभव हो, वहाँ यूरोपीय संघ और जापान का उदाहरण यह दिखाने के लिए प्रासंगिक है कि विशिष्ट मतभेदों को पूरक उपायों से संबोधित किया जा सकता है। भारत और यूरोपीय संघ के बीच किसी समान परिणाम की संभावना उनके संबंधित विधिक ढाँचों और संरक्षण के व्यावहारिक आकलन पर निर्भर होगी।

8. निष्कर्ष

GDPR और भारत के 2019 के विधेयक में संरक्षण के कई साझा सिद्धांत थे, किंतु उनके क्रियान्वयन में अंतर था। संवेदनशील और महत्त्वपूर्ण डेटा की परिभाषाएँ, स्थानीय भंडारण की शर्तें, व्यक्ति के अधिकार लागू करने की प्रक्रिया और सार्वजनिक प्राधिकरणों की पहुँच जैसे प्रश्न सीमापार हस्तांतरण के लिए विशेष महत्त्व रखते हैं। इनके समाधान के लिए साझा मानकों के साथ ऐसे साधनों की आवश्यकता है जो संबंधित अधिकारों को व्यवहार में लागू कर सकें।

मूल लेख का प्रस्ताव क्रमिक सहयोग पर आधारित है। नियामक संवाद से बाधाओं की पहचान की जा सकती है। वैध व्यावसायिक हस्तांतरण के लिए संविदात्मक उपाय और प्रमाणन विकसित किए जा सकते हैं। सार्वजनिक संस्थाओं के बीच विनिमय के लिए प्रयोजन और निगरानी पर केंद्रित अलग व्यवस्था बनाई जा सकती है। इस प्रकार नियामक संगतता का मूल्यांकन वास्तविक संरक्षण, प्रभावी उपचार और अनुपालन की व्यावहारिक लागत के आधार पर किया जा सकता है।

आभार

मूल लेख में अंजलि कौशिक और अन्ना-मारिया ओसुला ने शोध संबंधी चर्चाओं के लिए आनंद कृष्णन, प्रशांत गुप्ता, जतिन सहगल और आशीष बंसल का आभार व्यक्त किया है। मूल लेख अन्ना-मारिया ओसुला के शोध के लिए मसारिक विश्वविद्यालय की ERDF परियोजना के समर्थन का भी उल्लेख करता है।

References

[1]. C. Kuner, Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future, Working Paper No 187 - OECD Digital Economy Papers, OECD, vol. 7 (2011)
2. Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World, COM/2017/07 final, p. 1.
3. Available at <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contribution gdprevaluation_20200218.pdf>, p. 3 accessed on 10 January 2020
4. 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) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88, Article 4 (1). Hereafter GDPR
5. GDPR, Article 9 (1).
6. GDPR, Article 9 (4).

7. Available at: <https://www.meity.gov.in/content/information-technology-act> accessed on
26 April 2020
8. Available at: <https://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf>
accessed on 26 April 2020
9. Available at: <https://meity.gov.in/writereaddata/files/Personal_Data_Protection_ Bill,2018.pdf> accessed on 26 April 2020.
10. Available at: <https://www.prsindia.org/billtrack/personal-data-protection-bill-2019> accessed on 27 April 2020.
11. GDPR, Article 9 (1).
12. A. Kaushik, Dissertation: Data Protection On Cyber Space- Issues and Concerns, Post Graduate Diploma in Cyber Law and Cyber Forensics (National Law School of India University, Bangalore, 2017), Reg. Number: CLCF/352/15).
13. GDPR, Article 44
14. GDPR, Article 45 (1).
15. Judgement of the Court (Grand Chamber) of 16 July 2020 in case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems
16. Court of Justice of the European Union, Case C-362/14, Maximillian Schrems v. Data Protection Commissioner ("Schrems"), ECLI: EU: C:2015: 650, paras. 73-74
17. Read more: . Importantly, the transborder data flow as outlined in GDPR must not be confused with the rules established for the data exchange in law enforcement purposes. In addition to the so-called "Police Directive", access to data needed for example for criminal investigations are regulated by the EU EEvidence framework and domestic criminal procedure laws, keeping in mind that EU Member States are Parties to the Council of Europe Budapest Convention. In February 2019, the European Commission proposed to start international negotiations on cross-border access to electronic evidence with the United States and for the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, pp. 89–131; See for more .
18. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance) C/2019/304/.
19. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (Text with EEA relevance) C/2019/304/. Relevant topics are also covered in the Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision, and Official representations, assurances and commitments, Annexes to the same original document.
20. Article 46(5) GDPR allows the decisions adopted by the European Commission on the basis of Article 26(4) of Directive 95/46/CE to remain in force until amended, replaced or repealed. SCCs are established on this basis still being used by organizations as appropriate safeguards under Article 46.
21. European Data Protection Supervisor, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 2020, available at: accessed on 24 April 2020.
22. Other relevant adopted documents include: European Data Protection Supervisor, Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" Ruling, 2020, available at: accessed on 22 April 2020 and Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 2020, availble at: accessed on 20 April 2020
23. Available at: accessed on 27 April 2020.