ОБЩЕСТВЕНИ КОМУНИКАЦИИ И ИНФОРМАЦИОННИ НАУКИ
PUBLIC COMMUNICATIONS AND INFORMATION SCIENCES

HOW TO CONDUCT DATA PROTECTION-COMPLIANT DATA EXCHANGE WITH INDIA

Rainer Lukas
University of Library Studies and Information Technologies

Abstract: *This study investigates the compliance of data protection frameworks in India with the European Union's General Data Protection Regulation (GDPR). With India's evolving digital economy and the absence of an EU adequacy decision for the country, this research assesses the legal robustness and operational feasibility of transferring personal data to India under GDPR stipulations. Employing a qualitative methodology, the research analyzes current Indian data protection legislation, proposed reforms, and comparative standards set by the GDPR. The analysis is grounded in a review of legal documents, draft legislations, judicial decisions, and expert commentaries. Key findings indicate that while recent draft reforms aim to enhance compliance with international standards, substantial gaps remain concerning adequacy, enforcement, and rights assurance compared to GDPR requirements. The study highlights the potential of Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) as interim mechanisms to facilitate data transfer, pending significant legal reforms in India's data protection landscape.*
Keywords: *GDPR, Data Protection, India, Data Transfer, Compliance*

INTRODUCTION

The protection of personal data is of paramount importance in democratically organized state entities. How a society, private companies or the state handle the personal data of its citizens, how much information is stored, used or passed on, why and for what purposes, can be seen as a kind of "litmus test" in terms of the rule of law. It shows how much freedom the state and private companies grant citizens and consumers. This puts a large number of fundamental rights on the agenda that can be encroached upon, e.g. telecommunications secrecy (Art. 10 GG), the fundamental right to informational self-determination (Art. 1 para. 1, Art. 2 para. 1 GG) and a large number of other fundamental rights Art. 5 GG (freedom of opinion, information and broadcasting, Art. 12 GG, Art. 13 GG, Art. 3 GG). While data protection in its beginnings was primarily directed against interference by states, which were dubbed "Leviathan" (di Martino 2005, p. 17 with reference to Thomas Hobbes "Leviathan or the Matter, Form and Power of a Commonwealth Ecclesiastical and Civil") of 1651 and Job 41, 15ff.), today it is primarily private companies that have succumbed to an al-most limitless "hunger for data". This, digitalization (Bendel 2021; Lehmann 2014, p. 4; Kusch & Malik 2017, p. 6; Wolf & Strohschen 2018) and the rapid rise of modern information and communication systems ("ICT"; Szczutkowski 2017) prompted the European standard setter to create the General Data Protection Regulation (GDPR). In doing so, it has set high standards for data exchange not only across the EU, but also on a global scale. However, an appropriate level of data protection is to be ensured not only in the European Union (EU), but also when transferring data to third countries, such as the USA (Weichert 2017, p. 10). The GDPR contains corresponding detailed provisions in its Art. 46 to 49. A level of data protection corresponding to the GDPR must be guaranteed in each case. This will be analyzed below for the ex-ample of India: Firstly, Indian law delege lata and any reform efforts are presented and then how a legally secure and GDPR-compliant data exchange can take place under current law.

Data protection in India

India is an emerging nation, one of the so-called BRIC(S) countries (acronym for Brazil, Russia, India, China and South Africa as emerging economies; Magnus 2010), i.e. one of the economically emerging countries that will play a decisive role in the globalized world economy in the future. It is assumed that the enormous poverty problems of the Indian subcontinent can be tackled with the help of ICT (Rajadhyaksha n.d., p. 29). The Indian IT sector in particular has experienced a huge boom in recent years (Messner 2008, p. 64). Accordingly, and due to the increasing exchange of goods and information with the West, data protection issues have increasingly become the focus of public interest.

Reform efforts

A comprehensive discussion and reform process is currently taking place. Recently, the draft of India's first-ever Personal Data Protection Bill (PDPB) was withdrawn by the Indian lower house of parliament (Lok Sabha) (Merle 2022). The bill was heavily criticized in many ways. It goes back to a very first draft from 2019, which was followed by a revised version in 2021. In the following, the development is traced in the necessary brevity.

The 2019 draft

The 2019 draft was preceded by extensive consultations at various levels (Prasad & Menon 2020, p. 1). Of particular importance was not only the adoption of the GDPR, but also the fact that the Supreme Court of India in Justice K.S. Puttaswamy v Union of India had previously recognized the fundamental right to data protection or informational self-determination, which was first developed and recognized worldwide by the Federal Constitutional Court (BVerfG) (BVerfGE 65.1), as a fundamental right within the meaning of Articles 14, 19 and 21 of the Constitution in 2017 (Supreme Court of India 2017). India thus followed a global trend of using the adoption of the GDPR as an opportunity and starting point for far-reaching reforms. In addition, the previous regulation from 2011 had been recognized as inadequate (Prasad & Menon 2020, p. 2 fn. p. 24). Of central importance in the draft was the introduction of data protection principles that correspond to the GDPR standard (PDPB 2018, Section 3 Clause 14), in particular the principle of prior consent to data processing. It also provided for the establishment of a data protection authority (Art. 41 of the draft) and the abolition of Sec. 43A of the IT Act (Merle, Herzner & Schmitz-Bauerdick 2022). The draft was submitted to the House of Commons on 11 December 2019 (Merle, Herzner & Schmitz-Bauerdick 2022). The Information Technology Act, 2000 (IT Act), which was amended by the Information Technology (Amendment) Act, 2008, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, have been authoritative to date. Sec. 43A and 72A of the IT Act, which were added with the revision, provide for claims for damages and sanctions in the event of a data protection breach (Merle, Herzner & Schmitz-Bauerdick 2022).

Criticism of the 2019 draft and new rules of the 2021 draft

On 16 December 2021, the Joint Parliamentary Committee (JPC) submitted a report and a draft "Data Protection Bill, 2021" to the Indian Parliament, which included provisions on data localization and non-personal data (Merle, Herzner & Schmitz-Bauerdick 2022). The new draft of 2021 (PDPB 2021) (Tripathy & Sehgal 2021), takes up the suggestions of the JPC and now contains provisions on personal and non-personal data (Tripathy & Sehgal 2021). Extensive amendments were proposed. In particular, the regulations for company founders were considered too complex (Barik 2022). The JPC submitted 81 supplementary proposals and 112 recommendations. The scope of the new provisions should also cover non-personal data. Furthermore, provisions on the regulation of social networks and data security when using smartphones etc. are also proposed. Social media companies should also be able to be held liable for the content of their users (Barik 2022). Provisions on data localization are also proposed, as are regulations on data transfer only to countries with a comparable level of data protection (Barik 2022).

RESEARCH METHODOLOGY

This research aims to analyze the legal and procedural frameworks for GDPR-compliant data exchange between the European Union and India, focusing on the current laws and reforms within India related to data protection. This study employs a qualitative research design, utilizing documentary analysis as the primary method. This approach allows for a comprehensive review of existing legal texts, reform drafts, expert commentaries, and judicial decisions relevant to data protection in India and the European Union.

Data for this research was collected from multiple sources to ensure a robust analysis:

- **Legal Documents:** Examination of the GDPR, specifically Articles 44 to 49, and relevant Indian legislation such as the Information Technology Act 2000 and its amendments.
- **Draft Legislation:** Analysis of the evolving drafts of India's Personal Data Protection Bill, including the withdrawn 2019 draft and the proposed 2021 amendments.
- **Judicial Decisions:** Review of significant court rulings such as the Supreme Court of India's judgment in Justice K.S. Puttaswamy v Union of India, which recognized privacy as a fundamental right.
- **Scholarly Articles and Reports:** Consultation of academic publications and expert analyses on data protection and privacy laws in both the EU and India.

The study uses a thematic analysis framework to identify key themes related to data protection standards, compliance challenges, and the alignment of Indian laws with GDPR requirements. The analysis focuses on:

- **Comparative Legal Analysis:** Comparing GDPR standards with Indian data protection measures to evaluate compliance levels.
- **Regulatory Evolution:** Tracking the progress and changes in Indian data protection laws through various draft stages.
- **Impact Assessment:** Assessing the implications of legal frameworks on data transfers between the EU and India, considering both compliance and operational impacts.

Evaluation Criteria:

- **Adequacy of Protection:** Assessing whether Indian data protection laws provide adequate safeguards as required by GDPR.
- **Legal Robustness:** Evaluating the legal mechanisms in place to enforce data protection rights and resolve disputes.
- **Operational Feasibility:** Examining the practical aspects of implementing GDPR-compliant data transfer mechanisms like Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs).

The study acknowledges potential limitations due to the rapidly changing landscape of data protection legislation in India and the interpretation of GDPR compliance, which can vary significantly based on legal and technological developments.

The research adheres to ethical standards concerning the use of published data and reports, ensuring that all sources are cited properly and that the analysis is conducted objectively and respectfully, considering the legal and cultural contexts of the countries involved.

RESULTS

Data transfer to India is analyzed in detail below. Firstly, the basics of data transfer to a third country are presented. In a second step, we will examine whether suitable safeguards pursuant to Art. 46 GDPR exist in the case of India. Finally, exemptions pursuant to Art. 49 GDPR are discussed.

Principles of data transfer to a third country

The GDPR has not only improved data exchange within the EU, but also with countries that do not have an adequate level of data protection. If this is the case, such as in the USA, binding and legally secure instruments for third country data transfers must be observed. Before data is transferred to third countries, a risk assessment must be carried out and protective measures must be taken; both must also be documented (Art. 49 para. 6 GDPR; Weichert 2017, p. 10).

According to Art. 44 GDPR, the provisions of the subsequent articles and other GDPR provisions

must be observed when transferring personal data that is already being processed or is to be processed after its transfer to a third country or an international organization. In principle, the transfer of data pursuant to Art. 45 para. 1 GDPR does not require any special authorization if an adequacy decision has been made. This presupposes that the level of data protection in the third country fulfils the requirements of the GDPR. This is not the case in India.

Such decisions have so far been made for 14 third countries, including Argentina, Uruguay, Canada, New Zealand, Japan, South Korea, Switzerland and the UK (Roßnagel 2022, p. 546). Data may be exchanged with these countries in the same way as within the EEA (Roßnagel 2022, p. 546). No separate steps are therefore required in these cases. However, India is not one of the countries with a comparable level of data protection.

Standard contractual clauses

According to Art. 46 para. 1 GDPR, a controller or processor may only transfer personal data to a third country or an international organization in the absence of a decision pursuant to Art. 45 GDPR if the controller or processor provides appropriate safeguards and if enforceable rights and effective legal remedies are available to the data subjects. Accordingly, in its Schrems II decision, the ECJ found that a level of data protection compliant with the GDPR does not exist in the USA (ECJ, judgement of 16 July 2020, C-311/18, Data Protection Commissioner/Maximillian Schrems and Facebook Ireland).

It must therefore be checked in each individual case whether such guarantees exist.

It is questionable how this will affect data transfer to India (Das 2020).

In its decision, the ECJ emphasized three aspects: 1. the level of data protection in the US, 2. the importance of efficient protection provisions for private individuals in the event of data protection violations and 3. the possibility of asserting these in a legal remedy procedure that meets the requirements of the rule of law (Das 2020; ECJ, judgment of 16 July 2020, C-311/18, Data Protection Commissioner/ Maximilian Schrems and Facebook Ireland).

The IT Act 2000 contains the relevant standards for state data monitoring. Art. 69 stipulates that data transmission can be interrupted, objected to and decrypted. The provision has a broad scope of application, applies to personal data of EU citizens and also contains sanctions for data protection offences. It also provides for certain restrictions, such as the sovereignty of the Indian state, defense aspects, national security, good relations with other states, public policy, etc. Although these provisions are vague in terms of their wording, they do provide a minimum level of protection. This is because they restrict interference with data transfer by only allowing it in these exceptional situations. US law, on the other hand, does not provide for such restrictions (Das 2020). In addition, government orders issued by Indian authorities must always be in writing (Das 2020).

As far as the second aspect of Schrems II is concerned, the Indian High Court has already recognized the importance of the right to data protection or informational self-determination in the Puttaswamy decision and thus elevated it to the rank of a constitutional guarantee. This fundamental right applies to both Indian and foreign nationals (NASSCOM 2021 p. 28).

In the Puttaswamy case, the Indian Supreme Court developed a three-stage test for reviewing state interference in data protection law:

1.The intervention may only be carried out on the basis of the law and in compliance with the regulations stipulated therein.

2.Specific purpose: The interference must be justified by a legitimate legal purpose.

3.Proportionality: The objectives and implementation of the intervention must be in reasonable proportion to each other. Accordingly, any state intervention must not only be based on the applicable law. It must also fulfil the requirements of this three-step test (NASSCOM 2021, pp. 28–29).

The application of these principles subsequently led to the Bombay High Court declaring the action to be unlawful in a case dealing with telephone surveillance by the intelligence agency due to non-compliance with the aforementioned criteria (NASSCOM 2021, p. 29). Overall, with regard to the second aspect of Schrems II, it can therefore be stated that data protection law in India is on the right track, as re-strictions on executive intervention are now being developed.

With regard to the third aspect, it should be noted that India, like the USA, has no independent data protection authorities. In the USA, compliance with data protection regulations is only monitored by the courts.

The European Data Protection Board (EDPB) objected to the (now withdrawn) 2021 draft, criticizing in particular the fact that the draft contains a wide range of exemptions for interventions by the executive or government. These are very far-reaching and unclear. The implementation of the draft would make it possible to access all data stored in India and thus also leave personal data of EU citizens unprotected (EDPB 2021, p. 55). Certain conditions would also have to be met for such access. However, the entire procedure is not transparent. Based on the Schrems II criteria, the protection of data is very limited and there are only a few constellations in which data subjects can claim compensation with regard to any legal remedies. In most cases, the government cannot be prosecuted for data protection violations (EDPB 2021, p. 55). All of this means that an adequacy decision for India is ruled out de lege lata and in accordance with the 2021 draft.

Accordingly, an adequacy decision by the EU Commission pursuant to Art. 45 GDPR is currently out of the question.

Thus, in the case of India, only appropriate safeguards under Art. 46 GDPR can serve as a transfer mechanism. These are the standard contractual clauses of the European Commission (SCC; Art. 46 para. 2 lit. c GDPR) and the so-called Binding Corporate Rules (BCR, Art. 46 para. 2 lit. B; Art. 47 GDPR; Schmidt & Klingen 2020, p. 331). The latter is discussed in more detail in Chapter 3.3.

The standard contractual clauses contain a general section that regulates their purpose and scope (clause 1), the effect and inalterability of the clauses (clause 2), the third-party beneficiary of the data subject (clause 3) and the interpretation (clause 4). Of particular importance is the principle that the standard contractual clauses take precedence over all other agreements (clause 5). The data transfer pro-cess is also described (clause 6). Finally, additional parties can also join the contract and submit to the clause (clause 7). Clause 8 establishes an obligation for the data exporter to check in advance, as far as can reasonably be expected, whether the recipient of the data transfer is able to fulfil the obligations arising from the clause by implementing technical and organizational measures. Module 1 then contains pro-visions on the trans fer of data between two or more controllers. The purpose limitation of the transfer of personal data, transparency (informing the data subject about the transfer) and the principle that data must be accurate and up-to-date and only transferred if it is required and that it is deleted after use are decisive.

A working paper by the globally active Finnish IT company Basware (Basware 2021) explains in detail how to proceed when using standard contractual clauses. A total of six steps are described there:

1. identification of the intended data transfer;
2. ensuring proper transmission mechanisms;
3. review of the legal situation in the third country;
4. identification and implementation of supplementary measures (i.e.: SCC or BCR);
5. examination of any disadvantages for private individuals resulting from the transfer;
6. decision on the transfer and enforcement measures (Basware 2021).

Binding company and group rules

A third option for data transfer to India is the agreement of binding corporate rules (BCR; Art. 46 para. 2 lit. B; Art. 47 GDPR). This instrument can only be considered without further ado for groups of companies and multinational corporations (Stutz & Seiter, 2022, para. 174). Such regulations can be used to work particularly efficiently in terms of data protection law. On the other hand, the effort involved in developing internal company standards is enormous. Instruments must be developed with which rights and obligations can be enforced both internally and externally. It must also be possible to defend and, if necessary, justify these to supervisory authorities. Finally, internal enforcement in large companies can also encounter difficulties (Stutz & Seiter 2022, para. 174). BCRs have the advantage that they are in line with the data protection requirements of the GDPR (compliance), data processing is standardized across the group, risks in third country transfers are avoided and a sep-

arate contract does not have to be concluded for each individual data transfer. In addition, the special data protection standards can also be used effectively in the context of corporate marketing. Finally, the BCR provide internal company guide-lines for employees (Stutz & Seiter, 2022, para. 175).

Art. 47 GDPR contains detailed provisions on the requirements and scope of what BCRs must contain. The Art. 29 Working Party of the EU Data Protection Supervisors has developed various working papers on detailed issues. Working Paper 256, for example, contains a checklist of which provisions must be included in the BCR. Working Paper 244 also states which authority is the lead authority (Stutz & Seiter 2022, para. 175).

For global players who also have branches or subsidiaries in India, BCRs are a suitable way to transfer data to India.

Exceptional provisions (Art. 49 GDPR)

If the data transfer cannot be based on an adequacy decision or a suitable guarantee, it is only permitted if one of the exceptions standardized in Art. 49 GDPR ap-plies. However, the European Data Protection Board (EDPB) interprets the provisions very narrowly. Accordingly, this standard only has a very limited scope of ap-plication in practice (EDPB 2018; Schmidt & Klingen 2020, p. 331).

CONCLUSION

In light of the above, data transfers to India must still overcome certain rule of law hurdles in order to be GDPR-compliant. In individual cases, the recommendations for action issued by the EDPB (EDPB 2020a; EDPB, 2020b) should always be observed. In this context, the EDPB once again mentioned that when data is transferred and personal data is exchanged with third countries, the high level of data protection in the EU and the European Economic Area means that data protection "travels with you" (Schmidt & Klingen 2020, p. 332). Accordingly, the strict criteria of the GDPR must always be observed without any restrictions.

It is to be hoped that the necessary adaptation measures to the EU level of data protection will be implemented quickly. Although the level of data protection in India is higher than in the USA, it does not justify an adequacy decision, at least not at present. The current reform efforts are an indication that India is doing everything it can to enable secure data exchange due to the great economic importance of Indian-European trade.

REFERENCES

Barik, S. (2022, August 6). Explained: Why the Govt has withdrawn the Personal Data Protection Bill, and what happens now. The Indian Express. Retrieved from https://indianexpress.com/article/explained/explained-sci-tech/personal-data-protection-bill-withdrawal-reason-impact-explained-8070495/ [viewed on: 10 May 2024].

Basware (2021). White Paper. Transfer of Personal Data to Third Countries in Basware Services. Retrieved from https://www.basware.com/getmedia/6df1c624-3f25-4784-b46b-e8eeb29f92be/Basware-White-Paper-personal-data-transfer-to-third-countries-customers-v10082021.pdf [viewed on: 10 May 2024].

Bendel, O. (2021, July 13). Digitalisierung. Gabler Wirtschaftslexikon. Retrieved from https://wirtschaftslexikon.gabler.de/definition/digitalisierung-54195/version-384620 [viewed on: 10 May 2024].

Das, A. (2020, August 25). How would India's surveillance regime stack up in a ‚Schrems II' scenario? iapp. Retrieved from https://iapp.org/news/a/how-would-indias-surveillance-regime-stack-up-in-a-schrems-ii-scenario/ [viewed on: 10 May 2024].

Di Martino, A. (2005). *Datenschutz im europäischen Recht.* Nomos Verlag.

EDPB (2018, May 25). Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679. datenschutzkonferenz-online. Retrieved from https://www.datenschutzkonferenz-online.de/media/dsgvo/edpb_guidelines_2_2018_derogations_de.pdf [viewed on: 10 May 2024].

EDPB (2020a, November 10). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. EDPB. Retrieved from https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf [viewed on: 10 May 2024].

EDPB (2020b, November 10). Recommendations 02/2020 on the European Essential Guarantees for surveillance measures. EDPB. Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf [viewed on: 10 May 2024].

EDPB (2021). Government access to data in third countries Final Report, EDPS/2019/02-13. Retrieved from https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf [viewed on: 10 May 2024].

Lehmann, J. (2014). *Auswirkungen der Digitalisierung auf das Retail Banking.* München: GRIN Verlag.

Magnus, G. (2010). *Will Emerging Markets Shape or Shake the World Economy?* Wiley.

Merle, J. (2022, August 8). Indien zieht Entwurf seines ersten Datenschutzgesetzes zurück. GTAI. Retrieved from https://www.gtai.de/de/trade/indien/recht/indien-zieht-entwurf-seines-ersten-datenschutzgesetzes-zurueck-879772 [viewed on: 10 May 2024].

Merle, J., R. **Herzner** & F. **Schmitz-Bauerdick** (2022, April 18). E-Commerce und Datenschutz in Indien. GTAI. Retrieved

from https://www.gtai.de/de/trade/indien/recht/e-commerce-und-datenschutz-in-indien-524090 [viewed on: 10 May 2024].
Messner, W. (2008). Offshoring in India: Opportunities and Risks. In: Hendel, A.; Messner, W. & Thun, F. (Eds.). *Rightshore! Successfully Industrialize SAP Projects Offshore* (pp. 15–30). Springer.
NASSCOM (2021). Implication of Schrems II on EU India Data Transfers A Mapping and Analysis of Indian Privacy and Surveillance Legislation and Practical Guidance on Cross-Border Transfers. August 2021. Noida, Uttar Pradesh. Retrieved from https://nasscom.in/sites/default/files/202108_NASSCOM_Schrems_II_Study.pdf [viewed on: 10 May 2024].
Prasad, D. & S. C. **Menon** (2020). The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law. *International Journal of Law and Information Technology,* 28(1), 1–19. https://doi.org/10.1093/ijlit/eaaa003 [DOI: 10.1093/ijlit/eaaa003].
Rajadhyaksha, U. (n.d.). Work-Life in India. Boston College. Center for Work and Family. Retrieved from https://www.bc.edu/content/dam/files/centers/cwf/research/publications3/executivebriefingseries-2/ExecutiveBriefing_Work-LifeinIndia.pdf [viewed on: 10 May 2024].
Roßnagel, A. (2022). Internationaler Datentransfer. Stand und Perspektiven. In: *Datenschutz und Datensicherheit (DuD) 2022,* pp. 545–549.
Schmidt, J. & D. **Klingen** (2020, December 22). Die Schrems II Entscheidung. Düstere Aussichten für internationale Datentransfers. Legal Revolution, pp. 329–336. Retrieved from https://lrz.legal/images/pdf/Die_Schrems_II_Entscheidung_.pdf [viewed on: 10 May 2024].
Stutz, O. & S. R. **Seiter** (2022). Datenschutzmanagement im Unternehmen. In: Schläger, U. & Thode, J.-C (Eds.). *(2022). Handbuch Datenschutz und IT-Sicherheit, 2nd Edition.* Berlin: Erich Schmidt Verlag, pp. 97–185.
Supreme Court of India (2017). Urteil v. 24.08.2017, Az.: 494 OF 2012 – Justice K S Puttaswamy. Union of India and others. Retrieved from https://translaw.clpr.org.in/wp-content/uploads/2021/12/Justice-K.S.-Puttaswamy-.pdf [viewed on: 10 May 2024].
Szczutkowski, A. (2017, November 29). Informations- und Kommunikationssysteme (I.u.K.). Gabler Wirtschaftslexikon. Retrieved from http://wirtschaftslexikon.gabler.de/Archiv/11720/informations-und-kommunikationssysteme-i-u-k-v8.html [viewed on: 10 May 2024].
Tripathy, A. & R. **Sehgal** (2021, December 20). India's New Data Protection Bill, 2021 – Overview And Analysis Of JPC Draft. PSA Legal. Retrieved from https://www.psalegal.com/indias-new-data-protection-bill-2021-overview-and-analysis-of-jpc-draft/# [viewed on: 10 May 2024].
Weichert, T. (2017). EU-DGSVO – Ein Überblick. *Computer und Arbeit (CuA),* 3/2017, pp. 9–14.
Wolf, T. & J. **Strohschen** (2018). Digitalisierung: Definition und Reife. Quantitative Bewertung der digitalen Reife. *Informatik-Spektrum,* 41, pp. 56–64.

КАК ДА СЕ ИЗВЪРШИ ОБМЕН НА ДАННИ С ИНДИЯ, СЪОТВЕТСТВАЩ НА ЗАЩИТАТА НА ДАННИТЕ

Резюме: *В това проучване се оценява съвместимостта на индийските закони за защита на данните с изискванията на ОРЗД за международно предаване на данни. Чрез качествен анализ на развиващата се правна рамка на Индия, включително Закона за информационните технологии и неотдавнашните проектоизменения на Закона за защита на личните данни, в това изследване се оценяват правните механизми, с които Индия разполага, за да гарантира защитата на данните. Проучването установява пропуски в адекватността и прилагането, които възпрепятстват спазването на GDPR, като подчертава предизвикателствата пред стандартните договорни клаузи и задължителните фирмени правила като временни механизми за предаване на данни. Констатациите сочат, че са необходими значителни реформи, за да може Индия да отговори на стандартите на ЕС, като по този начин се засягат стратегиите на многонационалните компании за движение на данни.*
Ключови думи: *ОРЗД, защита на данните, Индия, съответствие, международен трансфер на данни, стандартни договорни клаузи, задължителни фирмени правила, правна реформа*

Райнер Лукас, докторант
Университет по библиотекознание и информационни технологии
E-mail: rainer.lukas@gmail.com