# IPBA Journal

March 2021

No 101

NEWS & LEGAL UPDATE

## Data Protection and Privacy

IPBA
INTER-PACIFIC BAR ASSOCIATION

# IPBA 2020 SHANGHAI

## 30th Inter-Pacific Bar Association Annual Meeting & Conference

18-21 April, 2021

Shanghai International Convention Center

IPBA 2020

To register, please visit: www.ipba2020.com

# IPBA Journal

The Official Publication of the Inter-Pacific Bar Association

| | |
|---|---|
| **Publisher** | Ninehills Media Limited |
| **Editor** | Paul Davis |
| **Editorial** | Kiri Cowie<br>Julie Yao |
| **Design** | Ester Wensing |

**Advertising Sales**

Jennifer Luk
E: jennifer@ninehillsmedia.com
Frank Paul
E: frank@ninehillsmedia.com
T: +852 3796 3060

ninehills media

**Ninehills Media Limited**

Level 12, Infinitus Plaza,
199 Des Voeux Road,
Sheung Wan, Hong Kong
Tel: +852 3796 3060
Fax: +852 3020 7442
Email: enquiries@ninehillsmedia.com
Internet: www.ninehillsmedia.com

ISSN 1469-6495

IPBA is incorporated in Singapore.
Company registration number:
201526931R





Cover Image:
123rf


## Contents


March 2021 No 101

INTER-PACIFIC BAR ASSOCIATION

# IPBA Leadership 2020-2021

## Officers

**President**
Jack Li
Jin Mao Partners, *Shanghai*

**President-Elect**
Miyuki Ishiguro
Nagashima, Ohno & Tsunematsu, *Tokyo*

**Vice-President**
Richard Briggs
Hadef & Partners, *Dubai*

**Secretary-General**
Michael Burian
Gleiss Lutz, *Stuttgart*

**Deputy Secretary-General**
Yong-Jae Chang
Lee & Ko, *Seoul*

**Programme Coordinator**
Shin Jae Kim
TozziniFreire Advogados, *São Paulo*

**Deputy Programme Coordinator**
Jan Peeters
Stibbe, *Brussels*

**Committee Coordinator**
Jonathan Warne
CMS Cameron McKenna Nabarro Olswang LLP, *London*

**Deputy Committee Coordinator**
Eriko Hayashi
ERI Law Office, *Osaka*

**Membership Committee Chair**
Corey Norton
Thai Union Group, *Washington, D.C.*

**Membership Committee Vice-Chair**
Melva Valdez Bello
Valdez Caluya and Fernandez, *Manila*

**Publications Committee Chair**
Priti Suri
PSA, *New Delhi*

**Publications Committee Vice-Chair**
James Jung
College of Law, *Sydney, NSW*

**Chief Technology Officer**
Varya Simpson
Law Offices of Varya Simpson, *Berkeley, CA*

**Deputy Chief Technology Officer**
Riccardo Cajola
Cajola & Associati, Milan

## Jurisdictional Council Members

**Australia:** Michael Butler
Finlaysons, *Adelaide*

**Canada:** Sean A. Muggah
Borden Ladner Gervais LLP, *Vancouver*

**China:** Jiang Junlu
King & Wood Mallesons, *Beijing*

**France:** Frederic dal Vecchio
FDV Avocat, *Neuilly-Sur-Seine*

**Germany:** Sebastian Kuehl
Huth Dietrich Hahn Partnerschaftsgesellschaft, *Hamburg*

**Hong Kong:** Myles Seto
Deacons, *Hong Kong*

**India:** Shweta Bharti
Hammurabi & Solomon Partners, *New Delhi*

**Indonesia:** Kurniawan Tanzil
SHIFT Counsellors at Law, *Jakarta*

**Japan:** Kenichi Masuda
Anderson Mori & Tomotsune, *Tokyo*

**Korea:** Jihn U Rhi
Rhi & Partners, *Seoul*

**Malaysia:** Tunku Farik
Azim, Tunku Farik & Wong, *Kuala Lumpur*

**New Zealand:** Michael Shanahan
Tompkins Wake, *Auckland*

**Pakistan:** Mohammad Abdur Rahman
Vellani & Vellani, *Karachi*

**Philippines:** Rocky Reyes
SyCip Salazar Hernandez & Gatmaitan, *Manila*

**Singapore:** Chong Yee Leong
Allen & Gledhill LLP, *Singapore*

**Switzerland:** Urs Zenhäusern
Baker & McKenzie Zurich, *Zurich*

**Taiwan:** Maxine Chiang
Chiang & Lee Attorneys-at-Law, *Taipei*

**Thailand:** Punjaporn Kosolkitiwong
Dej-Udom & Associates Ltd., *Bangkok*

**UK:** Alex Gunning
One Essex Court, *London*

**USA:** Jeffrey Snyder
Crowell & Moring LLP, *Washington, D.C.*

**Vietnam:** Net Le
LNT & Partners, *Ho Chi Minh City*

## At-Large Council Members

**China:** Xinyue (Henry) Shi
JunHe LLP, *Beijing*

**Europe:** Gerhard Wegen
Gleiss Lutz, *Stuttgart*

**India:** Manjula Chawla
Phoenix Legal, *New Delhi*

**Latin America:** Rafael Vergara
Carey, *Santiago*

**Osaka:** Kazuhiro Kobayashi
Oh-Ebashi LPC & Partners, *Osaka*

**USA:** Michael Chu
McDermott Will & Emery, *Chicago, IL*

## Regional Coordinators

**Australasia & Southwestern Pacific Islands:** Neil Russ
Russ + Associates, *Auckland*

**Hawaii & Northern Pacific Islands:** Steven Howard
Fiskars Japan Co. Ltd., *Tokyo*

**Middle East:** Ali Al Hashimi
Global Advocates and Legal Consultants, *Dubai*

## IPBA Committee Chairs/ Co-Chairs & Vice-Chairs

**Anti-Corruption & Rule of Law**
Simone Nadelhofer, LALIVE, *Zurich* – Chair
Lim Koon Huan, Skrine, *Kuala Lumpur*
Susmit Pushkar, Khaitan & Co, *New Delhi*
Susan Munro, Steptoe & Johnson LLP, *Beijing*
Eun Jae Park, Yulchon LLC, *Seoul*
Anne Durez, Total SA, *Paris*
Siva Kumar Kanagabasai, Skrine, *Kuala Lumpur*

**APEC**
Shigehiko Ishimoto, Mori Hamada & Matsumoto, *Tokyo* – Co-Chair
Wang Zhengzhi, Beijing Globe-Law Law Firm, *Beijing* – Co-Chair
Thai Binh Tran, LNT & Partners, *Ho Chi Minh City*
Raymond Goh, China Tourism Group Corporation Limited, *Hong Kong*

**Aviation and Aerospace**
Fernando Hurtado de Mendoza, Kennedys, *Lima* – Chair
Jean-Claude Beaujour, Smith D'Oria, *Paris*
Robert Wai Quon, Dentons Canada LLP, *Vancouver*
Gabriel R. Kuznietz, Demarest Advogados, *São Paulo*

**Banking, Finance and Securities**
Thomas Zwissler, ZIRNGIBL, *Munich* – Chair
Yuri Suzuki, Atsumi & Sakai, *Tokyo*
Catrina Luchsinger Gaehwiler, Froriep, *Zurich*
Vivek Kathpalia, Nishith Desai, *Singapore*
Stéphane Karolczuk, Arendt & Medernach S.A., *Hong Kong*
Vinay Ahuja, DFDL, *Bangkok*

**Competition Law**
Janet Hui, Jun He Law Offices, *Beijing* – Co-Chair
Anand Raj, Shearn Delamore & Co., *Kuala Lumpur* – Co-Chair
Sylvette Tankiang, Villaraza & Angangco, *Manila*
Vincent Wang, Tsar & Tsai Law Firm, *Taipei*
Christian Wind, Bratschi Limited, *Zurich*
Manas Kumar Chaudhuri, Khaitan & Co LLP, *New Delhi*
Sung Man Kim, Lee & Ko, *Seoul*
Eva W. Cole, Winston & Strawn LLP, *New York, NY*

**Corporate Counsel**
Jannet Cruz-Regalado, Pilipinas Shell Oil Corporation, *Manila* – Co-Chair
Christopher To, GILT Chambers, *Hong Kong* – Co-Chair
Lakshmi Nadarajah, Christopher & Lee Ong, *Kuala Lumpur*

**Cross-Border Investment**
Frederic Ruppert, FR Law - Avocat, *Paris* – Co-Chair
Sara Marchetta, Chiomenti, *Rome* – Co-Chair
Jan Bogaert, Stibbe, *Brussels*
Reinaldo Ma, TozziniFreire Advogados, *Sao Paulo*
Aimee Salamat, Cochingyan & Partners Law Offices, *Makati City*
Rohitashwa Prasad, J. Sagar Associates, *Gurgaon*
Kenichi Sekiguchi, Mori Hamada & Matsumoto, *Tokyo*
Eric Marcks, southgate, *Tokyo*
Santiago Gatica, Freshfields Bruckhaus Deringer US LLP, New York, *NY*
André Brunschweiler, Lalive, *Zurich*

**Dispute Resolution and Arbitration**
Robert Christopher Rhoda, Dentons Hong Kong LLP, *Hong Kong* – Co-Chair
Sae Youn Kim, Kim & Chang, *Seoul* – Co-Chair
Aoi Inoue, Anderson Mori & Tomotsune, *Tokyo*
Felix Dasser, Homburger AG, *Zurich*
Koh Swee Yen, WongPartnership LLP, *Singapore*
Fei Ning, Hui Zhong Law Firm , *Beijing*
Marion Smith QC, 39 Essex Chambers, *London*
Kshama Loya, Nishith Desai, *Mumbai*
Yutaro Kawabata, Nishimura & Asahi, *Tokyo*
Dorothee Ruckteschler, Dorothee Ruckteschler Dispute Resolution, *Stuttgart*
Angela Lin, Lee and Li, *Taipei*
J Felix de Luis, Legal 21 Abogados, *Madrid*
Mark Mangan, Dechert (Singapore) Pte Ltd, *Singapore*
Thomas Allen, Greenberg Traurig, LLP; *Washington, D.C*

**DRAC Investment Arbitration Sub-Committee**
Kshama Loya, Nishith Desai, Mumbai, Co-Chair
Lars Markert, Nishimura & Asahi, Tokyo, Co-Chair

**Employment and Immigration Law**
Frédérique David, Harlay Avocats, *Paris* – Chair
Jenny Tsin, WongPartnership LLP, *Singapore*
John Stamper, Support Legal, *Abu Dhabi*
Indrani Lahiri, Kochhar & Co., *New Delhi*

Björn Otto, CMS Hasche Sigle, *Cologne*
Christine Chen, Winkler Partners, *Taipei*
Pimvimol (June) Vipamaneerut, Tilleke & Gibbins, *Bangkok*

**Energy and Natural Resources**
Gmeleen Tomboc, Sidley Austin, *Singapore* – Co-Chair
Wang Jihong, Zhong Lun, *Beijing* – Co-Chair
Douglas Codiga, Schlak Ito, *Honolulu, HI*
Manoj Kumar, Hammurabi & Solomon Partners, *New Delhi*

**Environmental Law**
Mr. Alberto Cardemil, Carey, *Santiago* – Chair
Ms. Rosa Isabel Peña Sastre, Roca Junyent, *Barcelona*

**Insolvency**
Ajinderpal Singh, Dentons Rodyk & Davidson LLP, *Singapore* – Co-Chair
John Birch, Cassels Brock and Blackwell LLP, *Toronto, ON* – Co-Chair
Hiroe Toyoshima, Nakamoto & Partners, *Osaka*
Vivek Daswaney, V Law Partners, *Mumbai*

**Insurance**
Kieran Humphrey, O'Melveny & Myers, *Hong Kong* – Chair
Elaine Tay, Rajah & Tann, *Singapore*
Balakumar Balasundram, Azim Tunku Farik & Wong, *Kuala Lumpur*
Takahiko Yamada, Anderson Mori & Tomotsune, *Tokyo*
Kemsley Brennan, MinterEllison, *Sydney*

**Intellectual Property**
Frédéric Serra, HOUSE ATTORNEYS, *Geneva* – Co-Chair
Lidong Pan, Reiz Law Firm, *Guangzhou* – Co-Chair
Jose Eduardo T. Genilo, ACCRA Law, *Manila*
Christopher Kao, Pillsbury Winthrop Shaw Pittman LLP, *San Francisco*

**International Construction Projects**
Matthew Christensen, Kim & Chang, *Seoul* – Co-Chair
Alfred Wu, Norton Rose Fulbright, *Hong Kong* – Co-Chair
Karen Gough, 39 Essex, *London*

Mirella Lechna, Wardyński i Wspólnicy sp.k., *Warsaw*
Miranda Liu, Stellex Law Firm, *Taipei*
Peter Chow, King & Spalding (Singapore) LLP, *Singapore*

**International Trade**
Tracey Epps, Chapman Tripp, *Wellington* – Chair
Naoki Kondo, Oh-Ebashi LPC & Partners, *Tokyo*
Raj Bhala, University of Kansas, School of Law, *Kansas*
Devin Sikes, Akin Gump Strauss Hauer & Feld, LLP, *Washington, DC*

**Legal Development & Training**
Raphael Tay, Lee Hishammuddin Allen & Gledhill, *Kuala Lumpur* – Chair
Tsuyoshi Dai, Tsuyoshi Dai & Partners, *Tokyo*
Jae Hoon Choi, Lee & Ko, *Seoul*
Keanu Ou, Jin Mao Partners , *Shanghai*
Jonathan Lai, Watanabe Ing LLP, *Hawaii*
Rosie Thuy Huong, Nguyen Van Hau & Associates, *Ho Chi Minh City*

**Legal Practice**
Emerico De Guzman, ACCRALAW, *Manila* – Chair
KL Hee Woong Yoon, Yulchon LLC, *Seoul*
Mark Lowndes, Tompkins Wake, *Auckland*
Hiroyuki Ishizuka, Nagashima Ohno & Tsunematsu, *Tokyo*
James Miller, Reynolds Porter Chamberlain LLP (RPC), *London*

**Maritime Law**
Yosuke Tanaka, Tanaka & Partners, LPC, *Tokyo* – Chair
Thian Seng Oon, Oon and Bazul, *Singapore*
Damien Laracy, Hill Dickinson Hong Kong, *Hong Kong*
Cheng Xiangyong, Wang Jing & Co., *Beijing & Shenzen*

**Next Generation**
Valentino Lucini, Wang Jing & Co. Law Firm, *China, Guangzhou* – Co-Chair
Amira Budiyano, Gateway Law Corporation, *Singapore* – Co-Chair
Ferran Foix Miralles, Gómez-Acebo & Pombo, London
Julie Raneda, Schellenberg Wittmer Pte Ltd/Attorneys at Law, *Singapore*
Ngosong Fonkem, Page-Fura PC, *Chicago, IL*

Patricia Cristina Tan Ngochua, Romulo Mabanta Buenaventura Sayoc & De Los Angeles, *Manila*
Santiago Fontana, Ferrere, *Montevideo*

**Scholarship**
Jay Lemoine, Norton, Rose, Fulbright Canada, *Vancouver* – Chair
Picharn Sukparangsee, Bangkok Global Law Offices Ltd., *Bangkok*
Mahesh Rai, Drew & Napier,
Sophia S.C. (Sheau Chyng) Lin, Primordial Law Firm, *Taipei*

**Tax Law**
Jay Shim, Lee & Ko, *Seoul* – Chair
Brigida Galbete, Cuatrecasas, Gonçalves Pereira, *Barcelona*
Alexis Katchourine, FAREWELL TAX, *Paris*
Andre De Souza Carvalho, Veirano Advogados, *Rio de Janeiro*
Tracy Xiang, Y&T Lawyers, *Suzhou*
Charles C. Hwang, Crowell & Moring LLP, *Washington, D.C.*

**Technology, Media & Telecommunications**
JJ Disini, Disini & Disini Law Office, Manila – Co-Chair
Bryan Tan, Pinsent Masons, Singapore – Co-Chair
Doil Son, Yulchon LLC, Seoul
Masaya Hirano, TMI Associates, Tokyo

**Women Business Lawyers**
Olivia Kung, Wellington Legal, *Hong Kong* – Chair
Ruby Rose Javier-Yusi, ACCRALAW, *Manila*
Diep Hoang , DILINH Legal, *Ho Chi Minh City*
Goh Seow Hui, Bird & Bird, *Singapore*
Winnie Tam SC, Des Voeux Chambers, *Hong Kong*
Zhang Yun Yan , Jincheng Tongda & Neal, *Shanghai*
Lory Anne P Manuel–McMullin, Bello Valdez Caluya and Fernandez, *Manila*

## Past Presidents

Francis Xavier (Immediate Past President 2019-2020)
Rajah & Tann LLP, *Singapore*

Perry Pe (Past President 2018-2019)
Romulo, Mabanta, Buenaventura, Sayoc & De Los Angeles, *Makati City*

Denis McNamara (2017-2018)
*Auckland*

Dhinesh Bhaskaran (2016-2017)
Shearn Delamore & Co., *Kuala Lumpur*

Huen Wong (2015-2016)
Fried, Frank, Harris, Shriver & Jacobson LLP, *Hong Kong*

William A. Scott (2014-2015)
CI Investments Inc., *Toronto, ON*

Young-Moo Shin (2013-2014)
S&L Partners, *Seoul*

Lalit Bhasin (2012-2013)
Bhasin & Co., Advocates, *New Delhi*

Shiro Kuniya (2011-2012)
Oh-Ebashi LPC & Partners, *Osaka*

Suet-Fern Lee (2010-2011)
Morgan Lewis Stamford LLC, *Singapore*

Rafael A. Morales (2009-2010)
Morales & Justiniano, *Manila*

Gerold W. Libby (2008-2009)
Zuber Lawler & Del Duca LLP, *Los Angeles, CA*

Zongze Gao (2007-2008)
*Beijing*

James McH. FitzSimons (2006-2007)
Paralympics Australia, *Sydney*

Felix O. Soebagjo (2005-2006)
Soebagjo, Jatim, Djarot, *Jakarta*

Sang-Kyu Rhi (2004-2005)
Rhi & Partners, *Seoul*

Ravinder Nath (2003-2004)
Rajinder Narain & Co, *New Delhi*

Vivien Chan (2002-2003)
Vivien Chan & Co, *Hong Kong*

Nobuo Miyake (2001-2002)
MASS Partners Law Firm, *Tokyo*

John W. Craig (2000-2001)
(retired) *Toronto, ON*

Dej-Udom Krairit (1999-2000)
Dej-Udom & Associates Ltd, *Bangkok*

Susan Glazebrook (1998-1999)
Supreme Court of New Zealand, *Wellington*

Cecil Abraham (1997-1998)
Cecil Abraham & Partners, *Kuala Lumpur*

Teodoro D. Regala (1996-1997)
(deceased) *Manila*

Carl E. Anduri, Jr. (1995-1996)
*Lafayette, CA*

Pathmanaban Selvadurai (1994-1995)
Tan Rajah & Cheah, *Singapore*

Ming-Sheng Lin (1993-1994)
(deceased), *Taipei*

Richard James Marshall (1992-1993)
Glencore International AG

Kunio Hamada (1991-1992)
Hibiya Park Law Offices, *Tokyo*

## Past Secretaries-General

Caroline Berube (2017-2019)
HJM Asia Law & Co LLC, *Guangzhou*

Miyuki Ishiguro (2015-2017)
Nagashima Ohno & Tsunematsu, *Tokyo*

Yap Wai Ming (2013-2015)
Morgan Lewis Stamford LLC, *Singapore*

Alan S. Fujimoto (2011-2013)
Goodsill Anderson Quinn & Stifel, *Honolulu, HI*

Gerald A. Sumida (2009-2011)
Carlsmith Ball LLP, *Honolulu, HI*

Arthur Loke (2007-2009)
Virtus Law LLP, *Singapore*

Koichiro Nakamoto (2005-2007)
Anderson Mori & Tomotsune, *Tokyo*

Philip N. Pillai (2001-2005)
Shook Lin & Bok, *Singapore*

Harumichi Uchida (1999-2001)
TMI Associates, *Tokyo*

Takashi Ejiri (1995-1999)
Natori Law Office, *Tokyo*

Nobuo Miyake (1991-1995)
MASS Partners Law Firm, *Tokyo*

# The President's Message

**Jack Li**
**President**

***Changing the Regional Landscape for the Legal Industry — How Does the IPBA Benefit From the Regional Comprehensive Economic Partnership?***

Dear Colleagues, Members and Friends, Brothers and Sisters,

As a member of an international lawyer's organisation, I have increasingly realised the close connection between cross-border economic and trade relations and the ecology of the legal industry. In recent days, I have placed my emphasis on the finalisation of the Regional Comprehensive Economic Partnership ('RCEP') in what is set to be the world's largest free trade agreement ('FTA').

On 15 November 2020, after the 4th Regional Comprehensive Economic Partnership ('RCEP') Summit, the 10 ASEAN and Asia-Pacific countries, including China, Japan, South Korea, Australia and New Zealand formally signed the RCEP Agreement. Initiated by ASEAN in 2012, the RCEP's conclusion would cement the ASEAN bloc's pivotal role in forging regional integration. The RCEP was devised as a forward-looking trade deal. The RCEP agreement aims to achieve a comprehensive economic partnership that covers wide-ranging issues such as trade, investments, technological cooperation, intellectual property rights, competition, e-commerce and dispute settlement, among other things. After eight years of negotiations, including three rounds of leaders' meetings, 19 ministerial meetings, 28 rounds of formal negotiations, the signing of the RCEP Agreement strengthens my long-held belief, notwithstanding the trade disputes that have arisen frequently in recent years, that frictions and confrontation are only ups and downs and cooperation and mutual benefit shall always be in the mainstream.

From the persepective as the President of the IPBA, I think that strengthening international and regional cooperation will surely become a valuable and historical opportunity for the further development of this organisation for the following reasons:

1. The RECP provides more opportunities for lawyers from the IPBA. The RCEP covers a region with a population of more than 3.5 billion, accounting for 47.4 per cent of the world, 32.2 per cent of the world's economy and 29.1 per cent of global trade. The coverage under the RCEP agreement corresponds to a great extent to the majority of the jurisdictions that the IPBA members come from.

2. The IPBA may take this advantage to strengthen and further develop the range and quality of its cohesion and connection. The legal talents from the IPBA will be valuable assets for the future development of foreign-related businesses within the RCEP signatory states and the inseparable mutually beneficial cooperation is a feature of the core competitiveness and attractiveness of the IPBA in our future international regional economic cooperation.

3. Experts from the IPBA may assist the RCEP agreement with its implementation in the long run. The signing of the RCEP is a brand new endeavour and many intractable problems need to be discovered and resolved and the transactions under different jurisdictions need to also be guided by legal experts. Many members of the IPBA have been deeply involved in their own

practices for a long time, with comprehensive regional and international perspectives, and they are capable of providing professional and safe suggestions for transnational transactions under the RCEP framework.

My fellow colleagues, ladies and gentlemen, the RCEP is an example and representative of the current and future international economic cooperation pattern. As the President of the IPBA, I would like to suggest that you keep an eye on this opportunity as well as the trends of development to achieve some mutually beneficial and win-win developments together!

Finally, I do wish you all the best and I thank you very much.

**Jack Li**
**President**

---

## Publications Committee Guidelines for Publication of Articles in the IPBA Journal

We are pleased to accept articles on interesting legal topics and new legal developments that are happening in your jurisdiction. From time to time, issues of the Journal will be themed. Please send: (1) your article to both **Priti Suri** at p.suri@psalegal.com and **James Jung** at jjung@collaw.ac.nz; (2) a lead paragraph of approximately 50 or 60 words, giving a brief introduction to, or an overview of the article's main theme; (3) a photo with the following specifications (File Format: JPG or TIFF, Resolution: 300dpi and Dimensions: 4cm(w) x 5cm(h)); and (4) your biography of approximately 30 to 50 words.

The requirements for publication of an article in the *IPBA Journal* are as follows:

1. The article has not been previously published in any journal or publication;
2. The article is of good quality both in terms of technical input and topical interest for IPBA members;
3. The article is not written to publicise the expertise, specialization, or network offices of the writer or the firm at which the writer is based;
4. The article is concise (2500 to 3000 words) and, in any event, does not exceed 3000 words;
5. The article must be written in English (with British English spelling), and the author must ensure that it meets international business standards;
6. The article is written by an IPBA member. Co-authors must also be IPBA members; and
7. Contributors must agree to and abide by the copyright guidelines of the IPBA. These include, but are not limited to
   a. An author may provide a link on the website of his/her firm or his/her personal website/ social media page to the page of the Journal on which the first page of his/her article appears; and
   b. An author may not post on any site an entire PDF of the Journal in which the article authored by him/her appears.

# The Secretary-General's Message

**Michael Burian**
**Secretary-General**

Dear IPBA Members,

As the new year has started, we are looking ahead with increasing confidence. Our lives and IPBA activities are still affected and will probably continue to be affected by the pandemic this year, but we are optimistic that the ongoing lockdown measures and the rollout of the vaccination campaigns will help to decrease infection rates. We will stay connected with all of our colleagues online to share our common interests and mutual experiences and we hope that we might get a chance to start meeting in person again in the course of this year.

The last year has been a very challenging one for the IPBA as well. The pandemic affected not only our daily routines but also the activities of the IPBA worldwide. Most of our events could not take place as initially planned. Therefore, we had to switch our activities to online lectures and seminars. At this point, I would like to express my gratitude to everyone who helped in organising and implementing those events, in particular our Program Coordinator Shin Jae Kim and our Secretariat. Only with the support and flexibility of all of you have we been able to switch to a new way of communication and therefore keep our organisation alive.

As you know, this year is a special one for the IPBA since it is the year of our 30th anniversary. The 30th Annual Meeting and Conference had to be postponed but is now scheduled to take place from 18 to 21 April 2021 in Shanghai. Due to continued travel restrictions, the conference will be held as a combined onsite/online event. Currently, almost 200 delegates have registered for the onsite conference, but, at the same time, we are afraid that it will be unlikely that many members from outside of China will be able to travel to Shanghai. As such, the Shanghai Conference Organising Committee will add online sessions accessible by delegates who have registered for the onsite conference as well as to those who only registered for the online sessions. You can still pre-register online or contact our conference organisers if you have questions about the registration or the event itself (https://ipba2020.medmeeting.org/en).

Furthermore, we are planning to hold the first-ever IPBA Virtual Conference from 15 to 19 June this year. As of today, we are planning to organise more than 25 'live' online sessions, each with the opportunity to network online in real time.

With the gradual improvement of the pandemic situation and the rapid development of vaccines, we are optimistic that our meetings and conferences can soon be held in the usual format again. We all miss the opportunity to see each other in person, to meet new people and catch up with old friends. Nevertheless, the new expertise in online meetings and seminars allows us to look forward to the coming months. We are confident that the IPBA will be able to experience an extraordinary 30th-anniversary year.

**Michael Burian**
**Secretary-General**

# Message to the Reader

**Priti Suri**
**Chair – Publications Committee, IPBA**

Dear Reader,

Welcome to the March issue of the IPBA Journal. The theme for this first issue of 2021 is 'Data Protection and Privacy.' It would be correct to say data privacy and privacy in general have become two of the most defining issues of our era. As global economies shift the focus to a greater online presence and, given the size and scale of collection, use and sharing of personal information to third parties, the importance of the theme has assumed criticality at a mammoth scale. Undoubtedly, recent years have witnessed a spurt in legislation on this subject around the world, but there is a long road ahead.

The United Nations Conference on Trade and Development ('UNCTAD') created a tool to map and track the state of e-commerce legislation in various fields in its 194 member states. The current position reveals 66 per cent of countries have enacted legislation on the subject, 10 per cent have drafts ready, 19 per cent have none, and there is no information for the remaining 5 per cent. The pervasive use of technology has ensured that data is an integral part of our daily lives and people are questioning the lack of privacy and control, particularly given the possibilities of misuse and resale of personal data.

I am grateful for the positive responses I received from potential writers on this subject. In this edition, the authors have covered a wide array of related, topical themes. In the first article, titled 'Proposed Framework of Governance of Non–Personal Data in India: Unlocking Commercial and Community Benefits', Vivek Kathpalia and Aaron Kamath examine this subject from an Indian perspective. They analyse how enforcement of rights and unlocking the value of Non-personal Data ('NPD') could lead to societal progression, particularly when combined with emerging technologies. In the second article, Martin Polaine discusses 'Data Protection Experiences from Brexit' and makes a case as to how EU and UK GDPR could set the foundation, and even shape, an ASEAN and wider APAC data protection legislative regime.

The third article, 'Privacy Rights of Data of Users on Digital Technology Platforms' by Bui Cong Thanh, provides a perspective from Vietnam and explores user privacy thorough accessing, using and exploiting the benefits from websites and the boundary between legality of information collected and rights upon collection. The author notes that the lawmakers are focused on creating a safe network environment for foreign users and investors in the country. In the fourth article, Arya Tripathy explores and compares the existing legal regime and the proposed law in India. Titled 'Cross-Border Data Transfer in India: One Step Forward and Two Steps Back?' she also examines the rationale for data flow restrictions and its impact on organizations.

In the fifth article titled "Data Protection—European Roadblock or Global Guidance" the two co-authors from Germany, Dr. Björn Otto and David Windhövel, reflect how data protection can be perceived as an obstacle in the path of economic opportunities. They consider data protection issues across various jurisdictions on two levels: between individuals and companies on the one hand, and between citizens and states on the other. The final article, 'The Importance of having a Data Processing Agreement—Drafting Points" by Ekaterina Biruleva, discusses the need for and the substance in such an agreement, the requirement of which stems from EU GDPR.

In December 2020, we started a new feature titled 'Up Close and Personal' with the objective of interviewing

IPBA women members. The spotlight of this issue is on the new incoming President, Miyuki Ishiguro. I was heartened to read Miyuki's responses which have reaffirmed a fundamental personal belief for me: there may be cultural differences based on where we live, but the commonality of experiences underscores that we are all very similar!

In addition, there are details about new members between November 2020 and February 2021. Please send us your professional milestones for publication in the Members' Notes section, too.

The June 2021 edition will be focused on the 30th Annual Meeting and Conference which will be taking place in Shanghai between April 18-21 and will be hosted virtually and also in-person for our colleagues in China and others who are able to travel. And, do not forget to mark your calendars from June 15-19, 2021 for IPBA's first virtual conference 'Innovative Resilience in an Altered Legal Landscape'. I hope to see many of you there!

As always, thank you for the consistent contributions. Both James Jung, my Vice-Chair, and I remain grateful.

**Priti Suri**
**Chair – Publications Committee of IPBA**

| IPBA Upcoming Events | | |
|---|---|---|
| **Event** | **Location** | **Date** |
| **IPBA Annual Meeting and Conferences** | | |
| 30th Annual Meeting and Conference | Shanghai, China | April 18-21, 2021 |
| 31st Annual Meeting and Conference | Tokyo, Japan | April 20-23, 2022 |
| 32nd Annual Meeting and Conference | Dubai, UAE | 1st Quarter 2023 |
| **Special Event** | | |
| IPBA Virtual Conference: Innovative Resilience in an Altered Legal Landscape | Online | June 15-19, 2021 |
| **IPBA Mid-Year Council Meeting** | | |
| 2021 Mid-Year Council Meeting and Regional Conference | Jakarta, Indonesia | November, 2021 |
| **IPBA Webinars** | | |
| COVID Business Interruption Insurance - the UK Supreme Court decision on coverage | Zoom | March 1, 2021 |
| Use and abuse of state funding in the Covid-19 era | Zoom | March 4, 2021 |
| EPC Contracts in Renewable Energy Projects: Challenges and Strategies | Zoom | March 31, 2021 |
| More details can be found on our web site: http://www.ipba.org<br>The above schedule is subject to change. | | |

IPBA
Legal
Update

# Proposed Framework for Governance of Non-Personal Data in India: Unlocking Commercial and Community Benefits

Since the Supreme Court of India declared the right to privacy as a fundamental right, the Government has been in the process of preparing an extensive personal data protection law. Recently, a Government-appointed committee proposed a framework for governance of non-personal data as well, to confer rights to a community over such data, protect individuals against the risk of re-identification and abuse, and facilitate data sharing for economic and social benefits.

## Introduction

### Background

India has 504 million active internet users and is the world's largest internet market after China with immense potential for growth to a seamless data-driven economy.[1] It is crucial for a country like India to take stock of the rules and regulations that decide how data is protected, utilised and shared.

India was the world's highest smartphone data user in 2019[2] and has become a noticeably data-aware nation. Spurred in part by the European General Data Protection Regulation ('GDPR') in 2016, and growing cybersecurity incidents, data privacy and cyber security have been buzzwords in law-making circles. In a momentous shift in India's privacy jurisprudence, a nine-judge bench of the Supreme Court of India ('Supreme Court') in August 2017 unanimously affirmed that the 'right to privacy is a fundamental right' of an individual and 'an intrinsic part of the right to life and personal liberty' under the Constitution of India.[3]

### Recent Focus on Personal Data

While the aforementioned case was pending before the Supreme Court, the Indian Government's Ministry of Electronic and Information Technology ('MeitY') constituted a committee on 31 July 2017 ('Expert Committee') to study data protection issues in India and suggest principles for data protection. The Expert Committee submitted its report[4] to MeitY on 27 July 2018 and recommended a draft Personal Data Protection Bill, 2018.[5] The Government deliberated and tabled a significantly revised draft, that is, the Personal Data Protection Bill, 2019[6] ('PDP Bill') before the Indian Parliament in December 2019. Subsequently, it was referred to a joint parliamentary committee ('JPC') for deliberation.[7] An official report and a revised draft of the PDP Bill is expected from the JPC during the ongoing Budget Session of Parliament.

### Unlocking Non-personal Data

The JPC's inclination to give due consideration to Non-Personal Data ('NPD') is reflective of a bigger shift in the worldview on data regulation. Europe has been active in regulating NPD[8] albeit to a limited extent. The European Commission recognised the need for creating high-value, publicly held datasets in crucial sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills for a more advanced economy.[9]

Data is at the heart of any vibrant economy of the twenty-first century. Unlocking the value of NPD could lead to huge advancements in society when combined with emerging technologies such as AI, AR/VR, drones, IoT, telemedicine and autonomous vehicles. One can determine the fastest route through traffic or decide the right coordinates for the navigation of a weather satellite. NPD can improve efficiency in healthcare information processing, optimise multimodal transport and manage traffic flows, help to make evidence-based decisions on environmental concerns and improve public administration.[10]

On 13 September 2019, MeitY set up a committee ('NPD Committee') to study issues relating to NPD and to suggest regulation of such NPD.[11] The NPD Committee published its first version of the report proposing an NPD governance framework and sought public comments.[12] The report appeared to lack clear articulation of definitions, provisions and the purpose of regulating NPD. Upon consideration of stakeholder comments, the NPD Committee published a revised Report on the NPD Governance Framework on 16 December 2020 ('Report')[13] and sought public comments until 31 January 2021.[14] The Report clarifies the definition of NPD, legal basis of right vested with the State and various communities, scope of High-Value Datasets ('HVDs') and purposes of data sharing. The proposed NPD framework ('Framework') in the Report appears to be more streamlined and objective-oriented.

## Ambitions for Non-Personal Data Governance

### Goals

The Report has twin goals of enforcing rights and enabling value creation. First, it seeks to establish enforceable community rights and protect individual privacy rights threatened by the risk of re-identification and subsequent abuse of NPD. Second, it seeks to enable a data sharing system to unlock the economic value of NPD.

### Guiding Principles

Keeping these goals and benefits in mind, and akin to the privacy principles set out in the PDP Bill (such as consent, purpose limitation, storage limitation and data minimisation), the Report sets out these guiding principles for regulation of NPD: (1) the rights of the sovereign State over any NPD; (2) accruing benefits to India and the world; (3) protection of privacy of an individual against harm; (4) simplicity and unambiguity of NPD; and (5)

open access to the NPD for the purposes of innovation and entrepreneurship.

## Scope of NPD

### Definition and Categories of NPD

The Report defines NPD as data that is not 'Personal Data' as defined under the PDP Bill[15] or data devoid of any personally identifiable information. NPD may either be: (1) data not related to an identified or identifiable natural person, such as air quality data or data on wind power turbines; or (2) data that was previously personal data but has since been anonymised such as an anonymised dataset of individuals within an age bracket. The Report breaks down NPD into two categories, that is, NPD collected either from a private entity or a public entity.

### NPD Collected From a Private Entity

The Report further categorises NPD on the basis of data collected from private or public domains and parallelly on the basis of data collected from databases created from private collection mechanisms or public collection mechanisms. So, a private entity may collect mobile data usage information of people in a city which is data from the private domain (that is, data relating to an individual) either from:

1. a telecom company housing collective mobile data usage of its users in the city (that is, a database created from a public collection mechanism); or

2. a telecom company which has anonymised data of each individual's mobile data usage (that is, a database created from a private collection mechanism).

Similarly, a private entity may collect information about electricity towers in a city which is data from the public domain (that is, data relating to a community or a public space) either from:

a. a company which has done a city-wide survey (that is, a database created from a public collection mechanism); or

b. a company which has data from individual monitoring sensors on each electricity tower (that is, a database created from a private collection mechanism).

### NPD Collected From a Public Entity

The Report further categorises NPD collected by a public entity on the basis of data collected from the private or public domains and parallelly on the basis of data collected from databases created from private collection mechanisms or public collection mechanisms. So, a public entity may collect information to create a database about the number of cars owned by individuals in a neighbourhood which is data from the private domain (that is, data relating to an individual) either from:

1. government-installed cameras in the neighbourhood that identify cars (that is, a database created from a public collection mechanism); or

2. the government's transport department having data on each registered car in that neighbourhood (that is, a database created from a private collection mechanism).

Similarly, a public entity may collect information about water quality in a city which is data from the public domain (that is, data relating to a community or a public space) either from:

a. the water processing plant of that particular city (that is, a database created from a public collection mechanism); or

b. from individual meters installed by the concerned water supply department of the local government (that is, a database created from a private collection mechanism).

### High-value Datasets:

1. ***For Public Good and Societal Benefit***
   High-value Datasets ('HVDs') are NPD containing datasets for public-good and societal benefit, and are capable of generating insights. For example, a dataset of anonymised health information of COVID-19 patients with a history of pulmonary diseases useful for vaccination purposes.

2. ***Granularity of HVDs***
   HVDs consist of NPD of varying degrees of granularity such as:

1. raw/factual/transactional-level data such as anonymised data of each COVID-19-positive individual in a particular society;

2. aggregate-level data, such as an aggregated data set of those COVID-19-positive individuals grouped by age and pre-existing disorders; and

3. inferred data, such as a study of how different pre-existing disorders affect individuals who test positive for COVID-19.

***3. Creation of HVDs***

HVDs can only be created by 'Data Trustees' by collecting NPD from Data Custodians, that is, data collecting entities (see below). The Report recommends that a Data Trustee may only request specific subsets of a raw dataset ensuring data minimisation. Unlike requests to a private entity, a Data Trustee cannot request a public entity for inferred data related to national security issues.

Data Trustees must uniformly request NPD from all major custodians in creation of a HVD. If any custodian refuses to share NPD, the trustee can raise a request to the Non-Personal Data Authority ('NPDA') (described below) to direct the custodian to share the NPD.

HVDs are offered a higher degree of protection owing to their utility and potential for misuse. The Report recommends the following safeguards:

1. *NPD that is prone to de-anonymisation*: The sensitivity of personal data must also be inherited into its NPD form. For example, Telecom laws require anonymised location data gathered from telecom customers to be localised.

2. *Monitoring tools*: NPD stored in the cloud must be regularly monitored for risks and reports must be submitted by cloud service providers.

3. *Safeguarding vulnerability*: Organisations must be indemnified for losses caused due to exposed vulnerabilities even when they have adequate security standards in place.

## Legal Basis of Processing NPD

The Framework is intended to solely apply to NPD and not personal data. Recognising the risk of de-anonymisation of NPD, the Report recommends that individuals be informed that their data would be anonymised and that they may withdraw consent.

It is clear that once an individual's consent for anonymisation is withdrawn, the data would once again be personal data. However, it could pose practical hurdles for data that has already run through analytics and thereafter an individual's consent is withdrawn. If some individuals have consented to provide their anonymised driving licence data and that NPD is consequently used to prepare a larger data set of licence holders of a particular category, it is unclear what would happen to the larger data set if they withdrew their consents.

Further, businesses would be required to scale up and introduce consent mechanisms for undertaking processing of NPD of their customers too, raising costs comparable to the processing of personal data. Normally businesses could often adopt anonymisation at the point of collection to offset these costs.

## Stakeholders

Non-Personal Data Authority

Similar to the Data Protection Authority ('DPA') proposed to be set up under the PDP Bill, the Report recommends the establishment of a Non-Personal Data Authority ('NPDA') through industry participation, which would function harmoniously with the DPA, the Commission of India ('CCI') and other industry regulators. While the DPA or the CCI's role is towards protecting individual rights or ensuring a fair market, the NPDA would seek to foster innovation and effective use of the Framework. That being said, the NPDA would still carry out more traditional supervisory activities such as adjudicating data requests made by Data Trustees, ensuring that HVDs are used for only sanctioned purposes, etc.

### Data Businesses

***1. Definition and Registration of Data Businesses***

Any entity which is a public or private entity that collects, processes, stores or otherwise manages data is defined as a 'Data Business' under the Report. There are certain Data Businesses which the Report recommends should be obligated to register with

the NPDA, based on parameters such as revenue, magnitude of information and sources of data. It is unclear if the requirement applies to foreign entities too. Other Data Businesses may also register with the NPDA voluntarily.

***2. Data Custodians and Processors***

Data Businesses are categorised further into Data Custodians and Data Processors:

1. *Data Custodians*: Data Custodians are akin to 'data fiduciaries'[16] under the PDP Bill and 'data controllers' under the GDPR. They undertake collection, storage, processing, use, etc., of data and typically collect data from an individual. The Report recommends a 'duty of care' by them towards the community.

**HVDs can only be created by 'Data Trustees' by collecting NPD from Data Custodians.**

2. *Data Processors*: Data Processors are similar to 'data processors' as defined in the PDP Bill. They process NPD on the instructions of Data Custodians. However, Data Processors are responsible for the processing of NPD relating to their own business.

As a welcome addition, the Framework exempts Data Businesses from liability caused by any accidental harm. In a world of increasing cyber-attacks with cybersecurity playing catch up, Data Businesses may indulge in innovation without the fear of being penalised.

***3. Data Trustees***

'Data Trustees' are Data Businesses which are responsible for the creation, maintenance, and sharing of HVDs in India. They may be government organisations or private non-profit organisations. They are voluntarily created by persons intending to create, share and store HVDs and owe a duty of care to the community from where the HVDs are sourced. For example, a non-profit company may create a HVD on the number of diabetic patients in a particular section of the population. This non-profit company, being a Data Trustee, would have a duty of care towards such diabetic patients in that community.

## Data Sharing Framework

### Grounds for Sharing NPD

Data sharing is recommended to be undertaken on the basis of three purposes:

***1. Sovereign Purposes***

Data requests for sovereign purposes may only be made by government or public entities to maintain national security, law and order and public administration activities. The Report recognises that government actors already possess the power to request data under various extant laws. For example, a municipal body may ask Facebook for the number of people who tend to like online gaming through their accounts in that municipality.

***2. Public Good***

HVDs may be used for 'public good', that is for a community benefit, research and development, policy development or other societal benefit purposes. The Report is silent on whether NPD other than HVDs can be shared for public good. For example, a private organisation may request a soil testing laboratory for information on the soil in an area to improve farming practices. However, more clarity on what constitutes public good would help stifle any potential misuse of NPD.

***3. Commercial Purposes***

The Report recognises that for-profit entities share NPD for commercial purposes as an existing practice and hence does not provide any recommendations. For example, Facebook may request anonymised app usage data of WhatsApp's customers.

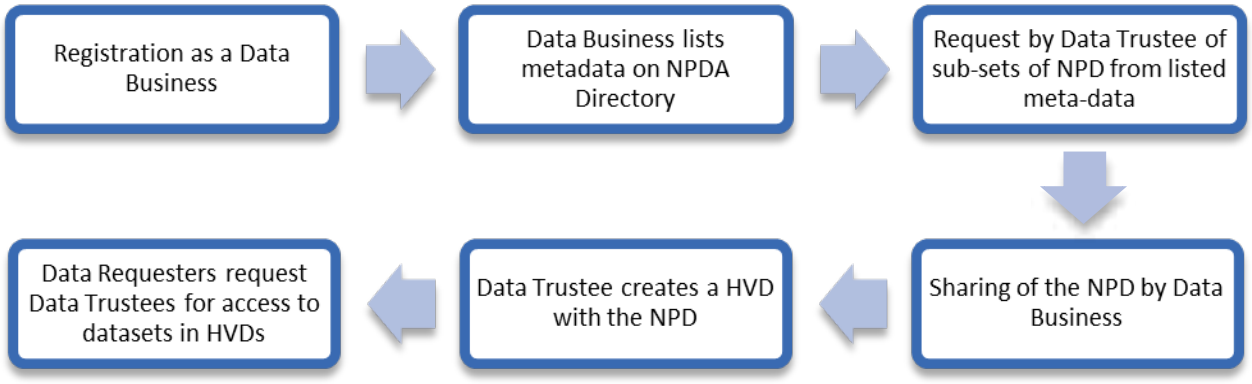
### Metadata Directory

All Data Businesses are required to share metadata and underlying data with the NPDA. The NPDA will create a publicly accessible directory of metadata sourced from all Data Businesses in India. However, the necessity of sharing underlying data for the purpose of a metadata directory is unclear. Open access to the metadata directory would be provided to registered organisations in India.

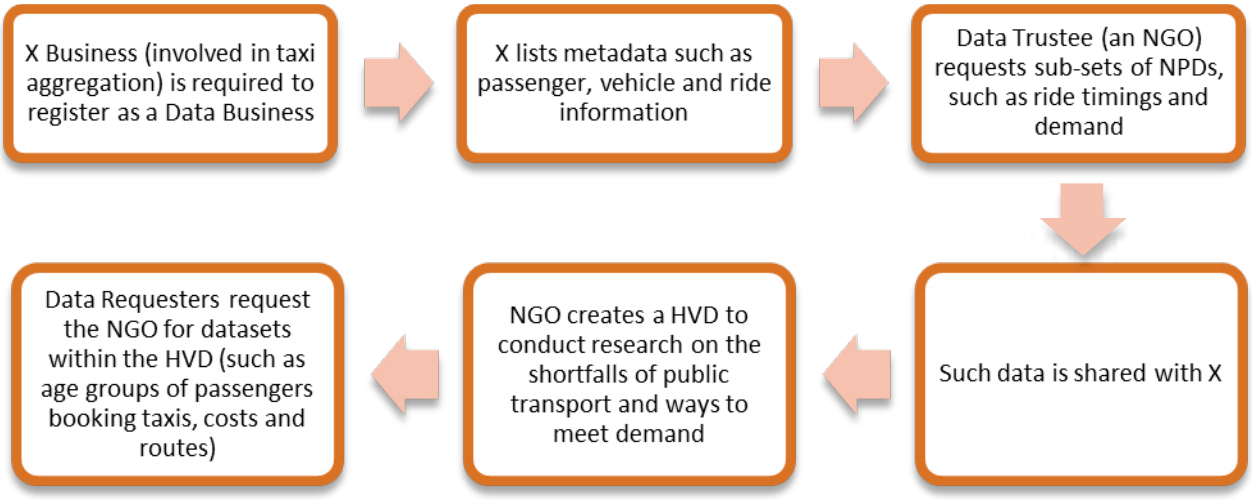
### Sharing of HVD

The Report recommends that sharing of HVDs must be subject to data minimisation, purpose limitation and must benefit the 'greater public good'. Concerns have been raised on the Framework allowing sharing of HVDs to 'create new businesses—startups and SMEs' which some fear would lead to a conflict of business interests.

Proposed Data Flow




To illustrate with an example:




## Benefactors of the Framework

### The Sovereign State

It is abundantly clear that one of the primary benefactors of the Framework is the State. One of the main goals of the Framework is to vest rights over NPD with India although the nature of the exact rights is unclear. However, NPD shared for a sovereign purpose would benefit security of the State and public administration. For example, the State can request NPD from cab aggregators to determine and improve transport patterns during a COVID-19-induced lockdown.

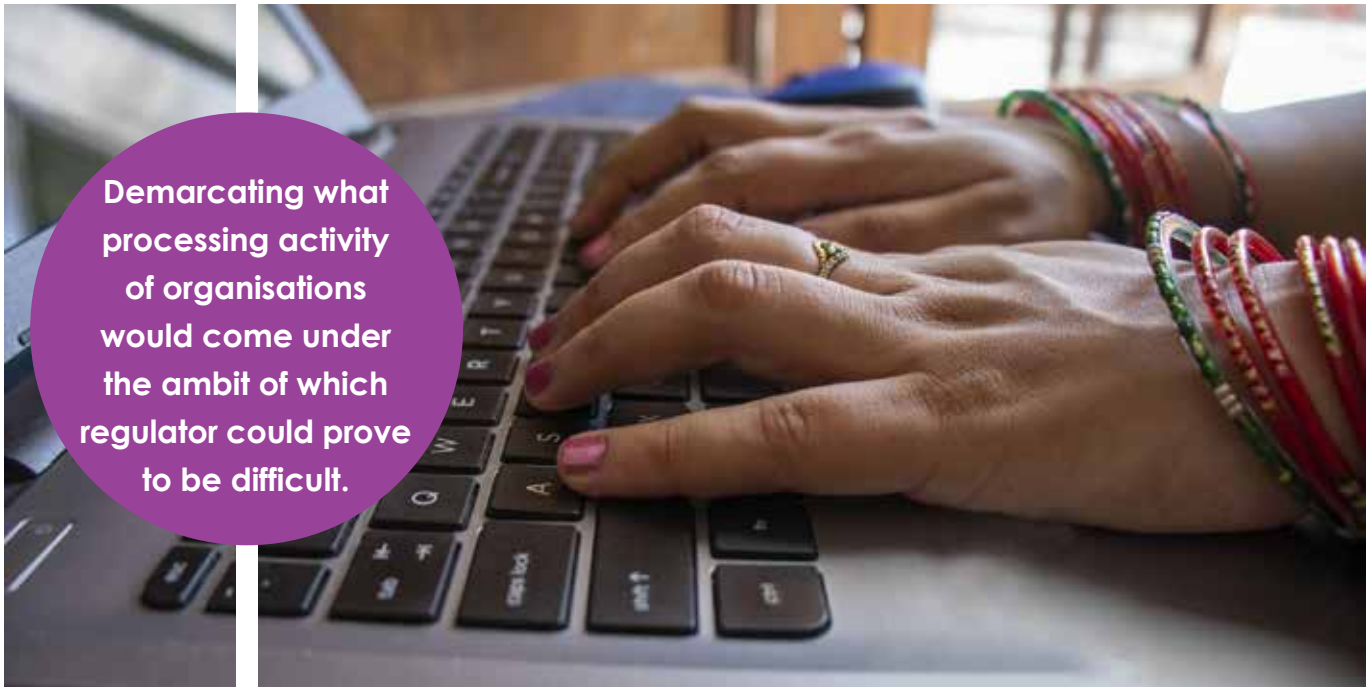
### The Community

The Report intends to create rights vested in a community, unlike in individuals, over their personal data. A community is defined as any group of people bound by common interests and purposes and involved in social and/or economic interactions. These communities have the right to raise a complaint with the NPDA through non-profit entities.

Since the NPD Committee has chosen to keep the definition of a 'community' broad and vague, the scope of who would be affected by exercise of 'community rights' could be fluid.

### Private Entities

While private entities may not be the biggest benefactors of data sharing processes under the Framework, the Report recognises that certain rights over copyrights and proprietary rights of private entities need to be protected.



Demarcating what processing activity of organisations would come under the ambit of which regulator could prove to be difficult.

## Interplay Between the NPD Framework and PDP Bill

### Anonymised Data

The Report recognises that the PDP Bill grants authority to the government to request anonymised data from organisations and to that effect, recognises the conflict of jurisdiction with the Framework. It recommends that the provisions related to anonymisation be removed from the PDP Bill. With reports coming in (as described above) that the scope of the PDP Bill would be revised too, it would be interesting to see how anonymised data would be governed by the PDP Bill.

### The NDPA and the DPA

Data Custodians under the Framework may, in all probability, be data fiduciaries under the PDP Bill. Entities will be accountable to both the NPDA and the DPA. While the NPDA would focus on unlocking value in NPD, the DPA would supervise prevention of personal harm. This could prove tricky for an organisation that processes a mix of NPD and personal data. Demarcating what processing activity of organisations would come under the ambit of which regulator could prove to be difficult.

## Parting Thoughts

While there are still some issues to be ironed out, the Framework is a commendable step to deriving societal and economic benefit out of the behemoth of a resource that India is. The European Commission has forayed into this space to a limited extent with its regulation for a framework for the free flow of non-personal data. It has also proposed a 'Data Governance Act' aimed at creating trust between data intermediaries and strengthening data-sharing mechanisms.[17] The Framework, though, is a more comprehensive, first-of-its kind regulation and the Report recognises that.

The Report is clear that the Framework is only intended to regulate the NPD of Indians and not foreigners. With data being hyper-connected in any information system today, Data Custodians could face more difficulties in segregating their datasets to ensure compliance.

The Framework may overlap with attempts at the sectoral level to regulate NPD such as in the securities market. The Securities and Exchange Board of India ('SEBI') constituted a Market Data Advisory Committee[18] that seeks to define different forms of NPD and recommend an operational framework for sharing such NPD under the oversight of SEBI. Jurisdictional challenges may arise between SEBI and the NPDA, in addition to how NPD is treated by either of the regulators.

The Framework's overlap with the PDP Bill must be closely watched too. The PDP Bill is the priority of the Government and its final draft would determine if NPD regulation

would form part of the PDP Bill itself or if there would be an independent regulation as the Report recommends. The Government has been receptive to public comments and suggestions on its first version of the Report, it can be expected that once the deadline for submission of public comments on the Report closes, there may well be a third version of the Framework issued.

## Notes

[1] IAMAI, Digital In India, available at https://cms.iamai.in/Content/ResearchPapers/2286f4d7-424f-4bde-be88-6415fe5021d5.pdf (last visited 21 January 2021).
[2] Navadha Pandey, 'India's Data Usage Per Smartphone Highest in World at 9.8GB/month: Report', available at www.livemint.com/industry/telecom/india-s-data-usage-per-smartphone-highest-in-world-at-9-8gb-per-month-report-1560936943979.html#box_1560936943979 (last visited 21 January 2021).
[3] Justice KS Puttaswamy (Retd) & Anr v Union of India & Ors, W.P. (Civil) No. 494 of 2012 (Order dated 24 August 2017), available at https://indiankanoon.org/doc/91938676 (last visited 19 January 2021).
[4] Report of the Committee of Experts under the Chairmanship of Justice BN Srikrishna, A Fair and Free Digital Economy: Protecting Privacy, Enpowering Indians, available at www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited 21 January 2021).
[5] The Personal Data Protection Bill, 2018, available at www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf (last visited 21 January 2021).
[6] The Personal Data Protection Bill, 2019, available at http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf (last visited 20 January 2021).
[7] See the Lok Sabha Supplementary List of Business, at http://164.100.47.193/lob/17/Second/SLOB11.12.2019_.pdf (last visited 20 January 2021).
[8] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807 (last visited 21 January 2021).
[9] European Commission, 'A European Strategy for Data', available at https://ec.europa.eu/digital-single-market/en/european-strategy-data (last visited 21 January 2021).
[10] European Commission, 'What Can Big Data Do for You', available at https://ec.europa.eu/digital-single-market/en/what-can-big-data-do-you (last visited 21 January 2021).
[11] MeitY Office Memorandum dated 13 September 2019, available at www.meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_framework.pdf (last visited 21 January 2021).
[12] Report on the Draft Non-Personal Data Governance Framework, available at www.mygov.in/task/share-your-inputs-draft-non-personal-data-governance-framework/ (last visited 21 January 2021).
[13] Revised Report on the Draft Non-Personal Data Governance Framework, available at https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf (last visited 21 January 2021).
[14] Call for inputs on Draft Non-Personal Data Governance Framework, available at www.mygov.in/group-issue/share-your-inputs-draft-non-personal-data-governance-framework/ (last visited 21 January 2021).
[15] The PDP Bill defines 'personal data' as 'data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.'
[16] The PDP Bill defines a 'data fiduciary' as 'any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.'
[17] European Commission, 'Proposal for a Regulation on European data governance (Data Governance Act)', available at https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act (last visited 20 January 2021).
[18] See the press release of SEBI constituting a 'Market Data Advisory Committee,' available at www.sebi.gov.in/media/press-releases/oct-2020/sebi-steps-up-efforts-for-data-culture-through-data-democratization-in-the-indian-securities-market-constitutes-market-data-advisory-committee-_47898.html (last visited 20 January 2021).

**Aaron Kamath**
**Nishith Desai Associates, India**

Aaron Kamath is a leader of the International Commercial Laws and Technology-Media-Telecommunication Laws Practice Group at Nishith Desai Associates. He advises clients on complex cross-border transactions including technology deals, mergers and acquisitions, private equity investments, legal and regulatory matters and commercial transactions across various sectors, with special focus on IT, digital media, e-commerce, retail and fin-tech. He is a member of the TMT Committee of the IPBA.

**Vivek Kathpalia**
**Nishith Desai Associates, Singapore**

Vivek Kathpalia is the Head of the Singapore Office of Nishith Desai Associates. Dividing his time between Singapore and India, Vivek co-leads the practices of Information Technology, Telecommunications, New Media and Education. Vivek has been advising clients in complex cross-border transactions, including technology deals, M&A, PE investments, regulatory and commercial matters across various industries. Drawing upon his foundational experiences as a litigator, Vivek brings valuable insights to the transactional and advisory practice

*The authors thank Purushotham Kittane from Nishith Desai Associates for his contribution to this article.*

IPBA
Legal
Update

# Data Protection Experiences from Brexit

## Envisaging a future data transfer framework for ASEAN

18
Mar 2021

## Introduction

The EU General Data Protection Regulation ('GDPR')[1] is regarded as a global standard for the protection of the right to privacy of an individual ('the data subject'). Whilst it creates a legal obligation for EU States, it has been used as a template for non-EU jurisdictions and is the basis of the UK's framework, the UK GDPR, following its withdrawal from the EU.

The EU GDPR and UK GDPR strike a balance between the legitimate business interests of an organisation and its ability to collect, use, process, share and transfer personal data and the interests of the data subjects, their right to privacy and right to ensure that the data held by an organisation (whether as controller or processor) is kept secure, accurate and is only used for its original intended purpose. They achieve this aim through the creation of technical, governance and organisational obligations, along with robust enforcement and stringent penalties.

In ASEAN, development of data protection frameworks has been gradual and disjointed, with some States still without an overarching law. However, the growth of trade with Europe has prompted ASEAN jurisdictions to review and reconsider their approach to data protection and privacy.

## Obligations and Responsibilities

A key question for an organisation is whether it acts as a controller, joint controller and/or processor, as this decides its obligations and responsibilities. For those UK-based organisations, the Information Commissioner's Office ('ICO') has created a checklist against which an organisation may assess its activities in order to decide its role and function, as well as consequent responsibilities and obligations. This, in turn, guides the technical and organisational measures it must put in place to achieve and demonstrate compliance under the EU and UK GDPR.

An organisation is not expected to adopt each and every measure to the fullest extent, but rather adopt those that are proportionate to the identified level of risk, including:

### 1. Technical

- Adopt a data protection framework 'by design and by default'. When an organisation is considering new processes or systems, it must consider how data protection principles and safeguards can be incorporated within such a system (for example, by ensuring that its privacy settings are set at 'high' by default).

- Ensure that technical and IT security systems are secure and can withstand any accidental or deliberate action that causes loss, alteration, unauthorised disclosure of, or access to, personal

data. Most jurisdictions have a national cyber security centre that issues guidance and tools for organisations.

**2. Governance**

Data protection compliance is a matter for an organisation's board and senior management. As with any other governance issue, an organisation is required to put in place measures that meet its risk assessment and risk appetite. Both the EU and UK GDPR lay down specific compliance measures, which include:

- Appointment of a Data Protection Officer ('DPO') for an organisation that meets the criteria set out in Article 37:
    - all public authorities, including private companies performing a public function, but not courts (as defined in national law) acting in their judicial capacity;
    - all other controllers/processors whose core activity is the regular and systematic monitoring of individuals on a large scale; and
    - all controllers/processors that process special categories of personal data on a large scale or personal data relating to criminal convictions.

In addition, domestic law may include other types of organisation where a DPO is required. Even for those without a legal obligation to appoint a DPO, there is a general encouragement to consider such an appointment on a voluntary basis. The DPO lies at the heart of the implementation of the EU GDPR (and the UK GDPR) obligations, which require an organisation to:

- Ensure data protection principles are fully integrated into business operations and staff trained to the requisite standard (depending on role and function).
- Provide for suitable communication channels and complaints mechanisms for data subjects.
- Have record keeping systems in place where an organisation has 250 or more employees. (However, given the overarching obligation for transparency and accountability, SMEs should also keep a record of their data processing).
- Report personal security data breaches to the national supervisory authority and, in appropriate circumstances, also notify data subjects.

**3. Organisational**

An organisation (in particular, any data controller) retains legal responsibility for GDPR compliance and must have clear internal policies and procedures relating to:

- Adherence to data protection principles when collecting, using, processing, sharing (including sharing with competent law enforcement agencies) or transferring (to a third State or international organisation) personal data.
- The lawfulness of data processing.
- Having a privacy notice.
- Handling of communications from data subjects in exercise of their rights granted under the EU and UK GDPR and dealing with complaints from data subjects.
- The transfer of personal data to a third State or international organisation.
- Security, including security of processing and of personal data. This includes the physical security of premises and staff access to personal data within the organisation.
- Data protection impact assessments ('DPIA'), where the organisation has identified a high risk to the rights and freedoms of data subjects.
- Notification of personal data breaches to the national supervisory authority and, where relevant, data subjects. The EU GDPR requires each member State to have one or more national supervisory authorities, and organisations that conduct cross-border operations should identify its applicable lead supervisory authority (usually where it is headquartered). Since the withdrawal of the UK from the EU, organisations must now review their operations to determine whether they fall within Article 3 of the UK GDPR and EU GDPR and whether they are subject to both the ICO and/or another European Economic Area (EU States, plus Iceland, Liechtenstein and Norway) ('EEA') supervisory authority.

## Particular Features of the UK's Data Protection Framework

The UK implemented the EU GDPR through the Data Protection Act 2018 ('DPA 2018') and took the opportunity to apply the data processing principles to other areas, including immigration, law enforcement and intelligence agencies. To that extent, UK domestic law went much further than the strict requirements of the EU GDPR.

The DPA 2018 also introduced additional requirements or exemptions, particularly in respect of notifications and data access rights. It must be remembered that data subject rights are not absolute, but restrictive. Encroachment may thus be justified if lawful, necessary and proportionate. Its Schedule sets out specific instances when the exemption applies, the extent to which it applies in respect of each right and the conditions for its application. It also permits the processing of special category data (or 'sensitive data') in any of the 10 situations listed in the GDPR, with additional conditions, varying in nature, scope and extent.

**The DPO lies at the heart of the implementation of the EU GDPR (and the UK GDPR) obligations.**

The UK's withdrawal from the EU has led to the creation of a UK-specific framework, which nevertheless remains predicated on the EU GDPR and retains, subject to specific qualification under the DPA 2018, the same key definitions as to personal data, data protection principles and the rights of data subjects, along with the wider obligations set out in the EU GDPR. The reality is that, essentially, the data protection obligations in the UK are unchanged and that is no mere coincidence. The EU GDPR standards, along with the extension to other areas and sectors, have been retained as a matter of policy to safeguard the interests of data subjects, but also to allow, without undue complication, the cross-border transfer of personal data from the UK to a third State (which now includes every EU/EEA State).

## International/Cross-border Data Transfers

The increase in the levels of collection and processing of personal data, allied to technological developments and processors more frequently being located in a jurisdiction other than that of the controller, have combined to create an additional challenge, namely, the rights of individuals not being able to be guaranteed or protected once their personal data has been transferred to another jurisdiction. At the same time, the business imperative for data transfer is captured by Recital 101 of the EU GDPR:

> … flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data … A transfer could take place only if … the conditions laid down in the provisions of this Regulation relating to the transfer of personal data … are complied with by the controller or processor.

Data transfer is the transfer of any personal data which is being processed or is intended to be processed after it has been transferred to a third State or international organisation. This is an important concept as the key is whether the data is processed or intended to be processed (which includes storage of data) in that third State. If data simply transits through a third State and is not likely to be processed in that third State, it is not data transfer.

Despite a recognition of the need for personal data transfer, it has been far from easy. Within the EU/EEA, the EU GDPR harmonised the data protection framework through, *inter alia,* the creation of common obligations and responsibilities for controllers and processors, giving data subjects the same level of legally enforceable rights in each such State, establishing equivalent sanctions in all Member States and building co-operation between national supervisory authorities. This helped to create what might be described as a 'common safe space' for personal data transfer between Member States, underpinned by each State having signed up to the same human rights standards (under the EU Charter) and data protection framework.

The wider issue, though, is whether an organisation located in an EU State may transfer personal data to a third State (that is, non-EU/EEA) or international organisation, or between a group of undertakings or enterprises engaged in joint economic activity.

Chapter V of the EU GDPR sets out the principles for transfer and the three bases of transfer: adequacy decision (Article 45), appropriate safeguards (Article 46) and derogation (Article 49). As the transition period for the UK has now ended, it is now a 'third country' for the purposes of personal data transfers between the UK and the EEA and falls to be considered under Chapter V of the EU GDPR.

Before considering each of the bases of transfer, it is worth highlighting that, under the UK–EU Trade and Cooperation Agreement, data transfers between the UK and the EU/EEA may continue for no more than six months until adequacy decisions have been adopted. For the sake of clarity, we will therefore consider the alternative basis for transfer in the event that an adequacy decision is not made for the UK.

For its part, the UK has created similar transfer mechanisms for data transfers from the UK to any third country (which includes the EEA). The three transfer conditions are: adequacy regulation (Article 45, UK GDPR), appropriate safeguards (Article 46, UK GDPR), and exception (Article 49 UK GDPR).

Nevertheless, grasping international data transfer bases is far from straightforward! With that in mind, we will now turn to examine each of those bases (under both the EU GDPR and UK GDPR).

## Bases for Data Transfers: The Three Bases

As discussed above, the three bases for transfer of personal data are:

1. Adequacy decision (Article 45, EU GDPR) and Adequacy regulation (Article 45, UK GDPR).

2. Appropriate safeguards (Article 46, EU GDPR) and Appropriate safeguards (Article 46, UK GDPR).

3. Derogation (Article 49, EU GDPR) and Exception (Article 49, UK GDPR).

### 1. Adequacy Decision (EU GDPR) and Adequacy Regulation (UK GDPR)

Under the EU GDPR, the European Commission ('EC') can decide that a third State, a territory, or one or more specified sectors within a third State, or an international organisation provides an adequate level of protection for data subjects. This is the 'adequacy decision' and once it has made an adequacy decision, data transfer can take place without any further or additional authorisation.

Under the UK GDPR, the same procedure is carried out by the Secretary of State, who will make a decision under the DPA 2018 in respect of a third State, a territory, or one or more sectors within a third State, an international organisation or a description of such a State, territory, sector or organisation ('adequacy regulation') following which data transfer can then take place without any further or additional authorisation. The regulations may specify or describe a transfer; if so, only such a transfer may be made.

The factors that the EC and the Secretary of State must take into account are broadly the same. These include:

- The rule of law, respect for human rights and fundamental freedoms, access to the data by public authorities in the third State, its data protection rules, ability of data subjects to enforce their rights in that State and rules for any onward transfer to another State or international organisation.

- The existence and effective functioning of one or more independent supervisory authorities in the third State or to which an international organisation is subject that is responsible for ensuring compliance, has adequate enforcement powers, is able to advise data subjects on how to exercise their rights and its cooperation with the supervisory authority of the relevant State (in the case of the UK, the ICO).

- The international commitments entered into by the third State or international organisation.

The EC and Secretary of State each publishes a list of the third States, territories and specified sectors within third State and international organisations for which an adequacy decision has been made or set out in the adequacy regulation.

The EC has made full findings of adequacy in respect of nine States and territories and partial findings of adequacy in relation to two States (Japan and Canada). The adequacy decisions are kept under review and any additional findings are published on the EC website. It has not yet made an adequacy decision as to the UK[2]. However, as mentioned earlier, the UK–EU Trade and Cooperation Agreement has preserved the


position and personal data transfer from the EU (and the EEA) to the UK is permitted for 'no more than six months' until the EC has adopted its adequacy decisions. It is not a foregone conclusion that an adequacy decision will be made for the UK. Without an adequacy decision, personal data transfer from the EEA will need to take place under the remaining transfer bases.

The UK 'adequacy regulations' include the EEA and all States, territories and international organisations covered by the existing EC 'adequacy decisions' that were valid as of 31 December 2020. The position may change, but presently an EEA-based organisation and those covered by the EC adequacy decision may continue to transfer data to the UK.

**2. Appropriate safeguards (Article 46 EU GDPR and UK GDPR)**

In the absence of an adequacy decision or adequacy regulation, an organisation may still transfer personal data, provided it has appropriate safeguards in place and on condition that a data subject is able to enforce his/her rights and has effective legal remedies available.

Article 46(2) of both EU and UK GDPR provides six appropriate safeguards and it is for the controller or processor to decide which is most applicable to its operations and offers adequate data subject protection. The selection of the appropriate safeguard does not require approval from the relevant supervisory authority, however, the safeguard may contain elements of approval and authorisation. The appropriate safeguards are:

***Safeguard 1:*** A legally binding agreement between public authorities. Alternatively, the national supervisory authority may authorise the contractual clauses between controller or processor and the controller, processor or the recipient of the personal data in the third State or international organisation, or the provisions are set out in any administrative arrangements between public authorities or bodies.

***Safeguard 2:*** Governing transfers between a group of undertakings or enterprises engaged in joint economic activity through legally binding corporate rules ('BCR') that expressly provide for enforceable rights of data subjects and meet all 14 conditions set out in Article 47(2). Where reliance is to be placed on BCRs, they must be approved by the relevant EU State supervisory authority (EU compliance) or the ICO (UK compliance).

***Safeguard 3:*** Standard data protection clauses (Standard Contractual Clauses or SCCs) in the form of template transfer clauses adopted by the European Commission (EC) or specified in regulations made by the Secretary of State (for the UK).

The SCC safeguard was the subject of a challenge in respect of the EU–US Privacy Shield (2016/1250) on the grounds that it did not provide adequate protection against access by public authorities to the data transferred to the US. The Court of Justice of the European Union in Data Protection Commissioner v Facebook Ireland and Maximillian Schrems[3] highlighted the shortcomings in the existing EU–US Privacy Shield, in particular the lack of equivalent protection guaranteed by the EU GDPR and EU Charter and declared it invalid.

The Court confirmed that whilst GDPR applies to the transfer of personal data for commercial purposes between operators, the data may be processed by the authorities of the third State for the purposes of public security, defence and State security. The real concern is the level of protection available to the data subject in the third State which must equate to that available to the data subject in the relevant EU State and any assessment as to the level of protection 'must take into consideration both the contractual clauses agreed between the data exporter established in the EU and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country'.

The Court held that the limitations on the protection of personal data under US law, where that data is accessed or used by US public authorities, do not satisfy the equivalence requirements and that the surveillance programmes based on those domestic law provisions are not limited to that which is strictly necessary or proportionate.

The requirement now is for an operator to consider if the SCCs provide adequate protection. If not, supplementary measures need to be in place. In November 2020, the European Data Protection Board ('EDPB') published its recommendations on supplementary measures ('Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data') which set out a series of steps in order to assess whether supplementary measures are required for the intended data transfer(s).

In addition, 'Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures' require an organisation to examine the law in the third State that governs access to personal data by public authorities and whether the surveillance measures in the third State amount to justifiable interference with the rights to privacy and the protection of personal data.

If the organisation comes to the view that the surveillance measures in the third State are not sufficiently limited, nor provide effective redress to EU data subjects, then the level of protection is deemed not to be EU equivalent and any transfer must be stopped or re-considered.

***Safeguard 4:*** Standard data protection clauses adopted by a supervisory authority and approved by the Commission (EU GDPR) and standard data protection clauses specified in a document issued (and not withdrawn) by the Commissioner under section 119A of the DPA 2018 and for the time being in force (UK DPA and GDPR). For the UK, the safeguard allows organisations to enter into a contract that is specific to its area of operations, provided the contract is ICO approved.

***Safeguard 5:*** An approved code of conduct under Article 40, catering for the specific processing requirements of a sector, whilst simultaneously ensuring the application of the EU/UK GDPRs to the relevant sector and to MSMEs. The code should include binding, enforceable commitments by the data receiver (controller/processor) in the third State to apply the appropriate safeguards, including protecting the rights of individuals whose personal data is transferred. The UK ICO has not yet approved any codes of conduct.

***Safeguard 6:*** The approved certification mechanism developed under Article 42 (EU/UK GDPRs). The certification mechanism must include a binding, enforceable commitment by the data receiver (controller/processor) in the third State to apply appropriate safeguards, including enforcement of data subject rights. The certification mechanism must be approved by the relevant supervisory authority.

### 3. Derogation (Article 49 EU GDPR) and Exception (Article 49 UK GDPR)

Where the EC has not made an adequacy decision or one of the Article 46 safeguards (including BCRs) is not available, the transfer may take place through reliance upon a derogation in Article 49 (EU GDPR).

The UK GDPR takes the same approach, including the specific situations for the derogation or exception. Those are:

1. explicit consent of the data subject having been informed of all possible risks (this derogation is not available for activities by public authorities in the exercise of their public powers);

2. it is necessary for the performance of a contract, or to put in place pre-contract, measures between the data subject and the controller (not available for activities by public authorities in the exercise of their public powers);

3. it is necessary for the performance or conclusion of a contract between the controller and a person (natural or legal) other than the data subject, but which has been made in the interests of the data subject (not available for activities by public authorities in the exercise of their public powers);

4. it is necessary for important reasons of public interest made under domestic law–for the UK, it is the Secretary of State who by regulation will specify if the transfer should be restricted;

5. it is necessary for the establishment, exercise or defence of legal claims;

6. it is necessary to protect the vital interests of a person (data subject or another) where the data subject is physically/legally incapable of giving consent; or

7. it is made from a register which, under national or EU law, is intended to provide information to the public (and is open to consultation by either the public in general or those with a legitimate interest in inspecting the register), but only to the extent permitted under the relevant law (EU or Member State law) and in accordance with any conditions stipulated therein.

Article 49(1) (EU/UK GDPRs) also creates a transfer mechanism where there has been no adequacy decision/adequacy regulation, an appropriate safeguard (including BCR) is not available and the derogation or exception situations are not available. This transfer mechanism is only available subject to the strict conditions in Article 49(1). If reliance is to be placed on this transfer mechanism, a controller must inform the relevant supervisory authority and the data subject of the transfer. It must, in addition to its ongoing obligations to the data subject under Articles 13 and 14, also inform the data subject the nature of the compelling legitimate interest it is pursuing. The conditions set out in Article 49(1) are:

a. the transfer is not repetitive (similar transfers are not made on a regular basis);

b. it involves a limited number of individuals;

c. it is necessary for the purposes of the compelling legitimate interests of the organisation, but does not override the interests of the individual; and

d. the controller has assessed all the circumstances of the transfer and, based on that, has put in place suitable safeguards to protect the personal data.

## Reflection

The EU and UK GDPRs are not an easy read and do not make for a straightforward explanation to a client. However, they do set out a comprehensive framework that seems here to stay and is likely to heavily influence, and even shape, ASEAN and wider Asia-Pacific data protection policy and legislation in the years to come.

## Notes

[1] Regulation (EU) 2016/679
[2] Since the paper was written, the EC has announced two adequacy decisions (GDPR & law enforcement respectively) for the transfer of personal data to the UK. However, both decisions await formal approval.
[3] (Case C-311/18; judgment dated 16 July 2020).

**Martin Polaine**
**Barrister, Brooke Chambers, United Kingdom**

Martin Polaine is a barrister at Brooke Chambers, London, specialising in international arbitration, international trade & investment law, and regulatory & risk.

# Privacy Rights of Data of Users on Digital Technology Platforms

Years ago, the regulations on protecting the privacy of the data collected by enterprises from e-commerce websites and mobile apps were not strong and tools for protecting data owners ('users') were not constituted clearly. With the occurrence of loss and disputes and the rapid growth of the e-commerce industry, the Vietnamese legislature has issued several provisions to create a legal instrument to protect data owners and enterprises' legitimate rights for collecting and using data. This article will discuss matters relating to user privacy through accessing, using, and exploiting the benefit from enterprises' websites and the boundary between the legality of the information collected by enterprises and their rights upon collection of such information.

## Introduction

The Fourth Industrial Revolution keeps progressing strongly even while the world is experiencing the COVID-19 pandemic. As before, digital transaction platforms have been created to optimise users' demands such as saving time or reducing travel and to enhance the flexibility and benefit of applications. For now, the effects from the pandemic and the requirement from governments on isolating, reducing direct activities and limiting gatherings have turned out to be the momentum for the digital industry to reach a climax.

In Vietnam, this is even more pronounced since the Vietnamese government has issued several consecutive policies to minimise the effect of COVID-19; that is, typically, the social isolation of international travellers entering the country, infected people and those suspected of being infected. The isolation does not apply only to the infected but also to the whole enterprise if such enterprise has employees that have had direct or indirect close contact with any infected individual. The issues arising are how enterprises can survive and operate; how authority agencies can avoid being temporarily closed; and how citizens can maintain daily activities such as studying, gatherings, consumption, entertainment, etc. Consequently, this has led to a faster growth of digital technology in Vietnam than ever before.

According to statistics from the statistical organisation in Vietnam, during the period before COVID-19 broke out in Vietnam and globally, the number of internet users in Vietnam increased by 6.2 million (10 per cent) from 2019 to 2020. As of January 2020, Vietnam currently has 68.17 million people using internet services, and social media penetration of 67 per cent.

With such growth, users' data has become goods searched and used for commercial purposes by organisations and individuals. Governments also use data collected from declaration requests to manage citizens and companies. In this context, information technology is developing programs and apps to collect information and to track and monitor individuals and enterprises extensively, at a country level and even at a global level. However, many similar programs and systems are being built and operated rampantly by authorities and economic, commercial and technological entities and others that gravely violate users' rights of privacy. Users are forced to provide information when using any technology utilities or apps, without knowing whether their data is protected or not.

## Which Data is Permissible to Collect?

User rights of privacy to their data have been promulgated in regulatory documents of Vietnam since 1946 under the first Constitution. Accordingly, they are inalienable rights which belong to the data owners. It means that the data owners shall be entitled to consider and determine the use of the data by their sole decision. In other words, in Vietnam, the data permissible to be collected is only that which the owners have allowed and provided voluntarily. What remains is that data collectors, when using data, must comply with the legal framework of Vietnam. This is based on the 'individual consent' principle, that is, the consent and acceptance of users through ticking 'I Agree', 'I understand and agree' or 'I accept' stated in commitments called 'Terms and Conditions' or 'Terms of Use'.

The understanding under Vietnamese regulations is similar to that of the rest of the world regarding user data.

**Figure 1**


*Source: Synthesised from the Digital Marketing Report of WeareSocial and Hootsuite.*

Accordingly, 'user data' means any information solely owned by the user such as his/her identity (name, age, date of birth, residence, ID); an enterprise's information if the users are enterprises such as residency and workplace; finances (income, assets, bank accounts, card numbers, savings, etc.); and users' interests, habits, needs, etc. This information is provided by interacting or sharing individual data with organisations from transactions on platforms serviced by them. The data is also collected when the user connects to and uses websites to search for information, digital apps for work or entertainment purposes, etc. In this way, users, by default, have provided their information to the provider and this enables organisations to collect data.

At present, Vietnam only has general provisions but no regulatory documents promulgated specifically about data — for example, which data is permissible to collect, how users can manage or monitor organisations which collect and use data, on using data for its original purpose such as when users are entitled to adjust their information and the method of adjustment, the right to delete the data previously provided, etc. All of this has resulted in data not being protected in the best way and illegal data trading also frequently happening.

## The Scope of Data Collection by Organisations

Data belongs to users under their rights of privacy and the laws give back authority to data owners. Accordingly, the law regulates that the information collector can use the collected data only upon obtaining consent of data owners and can exploit the data only within the scope of what the user has agreed, that is, data collectors can use data only to the extent agreed by users.

The above principle is recorded in the 'Law on Cyber-information Security 2015'. Accordingly, before processing individual information such as collecting, adjusting, using, saving, providing, sharing, etc., the owner's consent will be required. As for collecting organisations, they need to take measures to ensure data security. However, the current provision only stops at a general level of the government's orientation and has not caught up with the development of digital technology activities in Vietnam.

## What the Government Has Done to Ensure the Security of User Data

Users have privacy rights to their individual data, particularly the right to user data which is collected by providers, website owners, e-commerce platforms which require users to provide their own data in order to access, collect information, utilise services from providers or to perform their obligations. Apart from when users use services through websites, data is collected when users perform obligations to authorities. Users here are not only individuals but also enterprises.

In Vietnam, the regime for protecting the right to privacy of individual data was established with the 1946 Constitution and has been specifically supplemented at different periods to catch up with the development of digital technology. The current Constitution regulates as follows:

1. Everyone has the right to inviolability of their private life, personal secrets and family secrets; and has the right to protect his or her own honour and reputation. The safety and confidentiality of information on private life, personal secrets and family secrets of citizens are ensured by law.

2. Everyone has the right to confidentiality of correspondence, telephone, telegraph and other forms of private communications. No one may open, control or seize illegally correspondence, telephone, telegraph and other forms of private communications of other people.

Article 38 of the Civil Code 2015 on the 'Right to private life, personal privacy and family privacy' regulates:

1. Private life, personal privacy and family privacy are inviolable and protected by law.

2. The collection, storage, use, and publication of information related to the private life or personal privacy of an individual must have the consent of that person, and the collection, storage, use, and publication of information related to family privacy must have the consent of the family members, except where otherwise prescribed by law.

3. The safety of the mail, telephone, telegraph, electronic database and other forms of private electronic information exchange of an individual shall be ensured and kept confidential. The opening, control and seizure of the mail, telephone, telegraph, electronic database and other forms of

private electronic information exchange of another person may only be conducted in the cases provided by law.

4. A party to a contract may not disclose information on the private life, personal privacy or family privacy of the other party or parties known to it during the process of contract establishment and performance, unless otherwise agreed.

The Law on E-transactions 2005 in Article 46 'Information confidentiality in e-transactions', provides:

...

2. Agencies, organizations and individuals must not use, provide or disclose information on private and personal affairs or information of other agencies, organizations and/or individuals which is accessible by them or under their control in e-transactions without the latter's consent, unless otherwise provided for by law.

**At present, Vietnam only has general provisions but no regulatory documents promulgated specifically about data.**

The Law on Cyber-information Security 2015 also regulates 'Principles of protecting personal information in cyberspace', and accordingly provides:

1. Individuals shall themselves protect their personal information and comply with the law on provision of personal information when using services in cyberspace.

2. Agencies, organizations and individuals that process personal information shall ensure cyber information security for the information they process.

The Law on Cybersecurity 2018, at first had required that enterprises providing services in cyberspace shall notify directly to users if their data is violated, broken or lost. The Criminal Code of Vietnam has specified criminal acts for violating the privacy right of users and, based on the violation and damage level to users, to impose the respective administrative penalty or imprisonment.

In the scope of international transactions, the Vietnamese Government also proves its commitment to protect privacy rights by participating in the International Covenant on Civil and Political Rights ('ICCPR'), in which Article 17 states:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

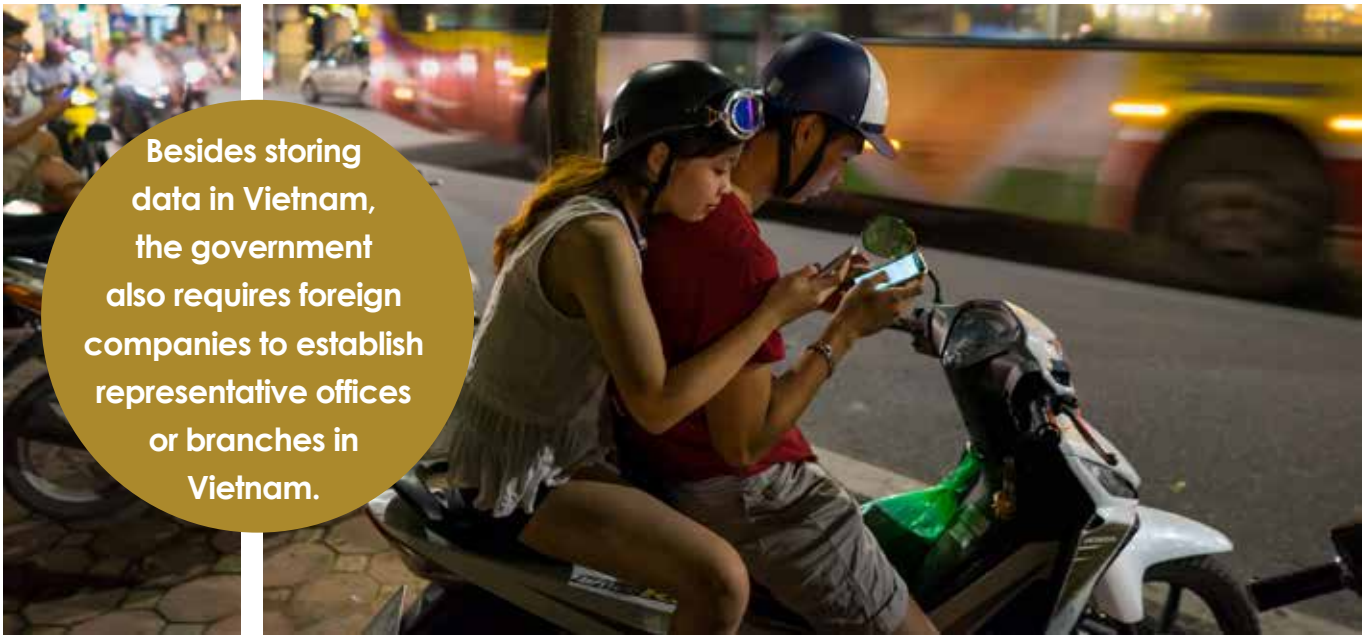
## The Difference Between Vietnamese and International Provisions on Privacy Right Security

Currently, the most provisions on data privacy right security is the General Data Protection Regulation ('GDPR') of the European Union. The GDPR was issued under the opinion that the right to privacy is an fundamental right of individuals who shall be entitled to manage the data provided to enterprises, including the right to know about usage purposes, parties which access their data, archive terms and the right to correct, delete, restrict or object to data usage, etc. The GDPR also requires that data collectors or hosts shall collect the data in a legitimate way and manage it to avoid illegally exploiting the data.

As for Vietnam, legal instruments are being adjusted to catch up with the development of digital technology. Especially, the provisions of the Law on Cybersecurity issued in 2018 have taken effect since 2019, forcing enterprises to enhance measures to ensure the security of user data, in particular:

> To apply technical solutions and other necessary measures to ensure security during the process of collecting information and to prevent the risk of revelation, damage to or loss of data; and in the case of occurrence or possible occurrence of the revelation, damage to or loss of data about user information, to immediately provide response solutions, and at the same time notify the user and report to the Cybersecurity Task Force in accordance with this Law;

The provisions of the Law on Cybersecurity have some similarities to the GDPR in recording the responsibilities of data collectors, hosts and exploiters. However, the Vietnamese laws have not yet specified the rights of




data owners as the GDPR has and it also gives the government the right to control the data to ensure the security of the flow of information and to secure the important cyber infrastructure of the nation. Therefore, organisations inside and outside of Vietnam providing services in cyberspace are obliged to store the data in Vietnam. Typically, the Law on Cybersecurity provides:

> Domestic and foreign service providers on telecom networks and on the Internet and other value added services in cyberspace in Vietnam [cyberspace service providers] carrying out activities of collecting, exploiting [using], analyzing and processing data [being] personal information, data about service users' relationships and data generated by service users in Vietnam must store such data in Vietnam for a [specified] period [to be] stipulated by the Government.

Foreign enterprises referred to in this clause must have branches or representative offices in Vietnam.

Thus, besides storing data in Vietnam, the government also requires foreign companies to establish representative offices or branches in Vietnam. This requirement shall apply to any foreign company providing telecommunications or internet services that collect, process, exploit or analyse individual data of service users. The provision has covered quite an extensive scope of enterprises operating in digital technology such as telecommunication companies, data storage companies or data sharing companies like those providing cloud services, domestic or international domains to serve users in Vietnam, e-commerce websites, online payment companies, payment intermediaries, shipping connectivity apps, social media, electronic games and e-mail.

However, all current provisions have stopped at separate provisions and have not been collated into a single regulatory document which would provide all the provisions for protecting privacy rights from other regulatory documents clearly and specifically. Also, all current provisions only exist at the most general level, but do not specify and have sanctions for each level of damage to users due to leakage or loss of data collected from such users.

## Legal Effect of the Commitment Between Users and Collectors as Data Messages

Similar to the rest of the world, in Vietnam, websites, e-commerce platforms, mobile applications, etc., record the commitment between users and data collectors on the responsibility of providing the user information and the rights of data collectors to manage and use the user information through the formality of 'Terms and Conditions'. To catch up with the worldwide developments and the conformity of the digital industry, Vietnam has acknowledged the effect of

these commitments and, accordingly, the agreement between users and organisations receiving information shall be abided by the parties and exist as a 'data message' and it will be lawful evidence to protect one of the parties when any disputes arise that relate to using the data. Particularly, the regulations on e-transactions of Vietnam have prescribed as follows:

> Article 11. Legal validity of data messages
>
> Information in data messages cannot have its legal validity disclaimed for the sole reason that it is expressed in the form of data messages.
>
> Article 12. Data messages being as valid as documents
>
> Where the law requires information to be in writing, a data message shall be considered having met this condition if the information contained therein is accessible and usable for reference when necessary.'
> ...
> Article 14. Data messages being as valid as evidence
>
> 1. A data message cannot be disclaimed in terms of its validity as evidence for the sole reason that it is a data message.
>
> 2. The validity as evidence of a data message shall be determined based on the reliability of the method by which the data message was generated, stored or communicated; the method to ensure and maintain the integrity of the data message; the method by which its originator was identified, and on other relevant factors.

Thus, it can be seen that even though the legal frameworks of Vietnam have not yet summarised all violation acts that can affect the privacy rights to users' data, the basic terms have recognised data protection and the legality of the agreement between users and the organisations receiving information on a digital technology platform.

## Current Situation in Vietnam

We understand that data plays an important role, but in Vietnam, users are not really aware of this. Thus, much of user data has become a commodity for commercial purposes. In other words, the protection of users' and customers' data has not been very focused. In fact, only when incidents and damages occur will legal measures and remedies be considered. Business fields such as real estate, health care and insurance activities are groups of services where there is a great need for accessing information of users and the mentioned data will be construed as a basis for service offering and marketing. Under different transaction forms, users' data is exchanged and illegally traded on a large scale for marketing and sales purposes, showing that customers' data is being very loosely protected. Users themselves understand this illegal use, however, there are no tools for users to request termination of illegal use of information.

At the beginning of the article, the speed of using and exploiting utilities based on digital technology, extremely popular apps in Vietnam and that the frequency of usage increases dramatically each year was discussed. In addition, the impact of government policies to minimise the impact of the COVID-19 pandemic has created momentum for the development of the digital industry in Vietnam. Another thing that significantly affects the appearance of many electronic applications, trading floors, etc., is the tax exemption and reduction policy, the investment incentive policy of the Vietnamese government. Given the speed of development, Vietnam's lawmakers are gradually drafting regulations on the protection of privacy and the safety of users' data based on the general regulations of the world, creating a safe network environment for foreign users and investors in Vietnam. In addition, the Vietnamese government is implementing many policies to propagate for users to change their views on the privacy of their own data, the data of enterprises and other individuals.

**Bui Cong Thanh (James Bui)**
**Managing Partner, PLF Law Firm, Vietnam**

Mr Bui Cong Thanh is the Managing Partner of PLF Law Firm. He is also a member of the Vietnam Business Lawyers Club, Ho Chi Minh City Bar Association and Vietnam Bar Federation. He specialises in real estate and M&A deals related to enterprises operating in various sectors, such as services, retailing, manufacturing, technology and F&B.

IPBA
Legal
Update

# Cross-Border Data Transfer in India: One Step Forward and Two Steps Back?

Informational privacy is recognised as a fundamental right in India, and a new data protection law is underway. The Personal Data Protection Bill, 2019 seeks to regulate cross-border data transfer through data export restrictions and localisation norms. The article compares the existing legal regime with the proposed law, delves into the rationale for data flow restrictions outside India, and analyses its potential impact for organisations.

## Introduction

Governments regulate cross-border data flow through data export restrictions, and in some cases, impose data localisation measures that mandate some or all aspects of processing to be carried out within its territorial limits.[1] Currently, Indian data protection rules are far from adequate and permit free flow of data across borders. However, a robust data protection legislation is in the pipeline. The proposed Personal Data Protection Bill, 2019 ('PDP Bill') contemplates a mix of data export restrictions and localisation for certain data sets. This article aims to explain the insufficiency of the existing data processing regime, provide an overview of the PDP Bill and specifically analyse the proposed cross-border restrictions to understand its potential impact.

## Existing law—The Information Technology Act and Rules

Personal data processing is regulated under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ('IT Rules'),[2] notified under the Information Technology Act, 2000 . They primarily apply to Indian body corporates engaged in processing personal information ('PI') of a natural person located in India. PI is defined as information relating to a natural person, which directly or indirectly, either standalone or in combination with other information, is capable of identifying the natural person. Certain categories of PI such as passwords, financial information, physical, physiological or mental health data, sexual orientation and biometric information are classified as sensitive personal data ('SPD'). The IT Rules contain only eight provisions, do not provide detailed data protection regulations and are mostly aimed at regulating the processing of SPD.

Rule 7 of the IT Rules deals with cross-border data transfer. It states that SPD can be transferred to a third party outside India, provided: (1) the foreign recipient ensures the same level of data protection as is provided under the IT Rules which, as observed earlier, is minimal; and (2) the transfer is undertaken either on the basis of an individual's consent or for a lawful contract executed with the individual. Consequently, organisations, while seeking consent or executing e-contracts for goods and/or services, add suitable terms that permit seamless and unbridled cross-border data transfer. In essence, the IT Rules enable free flow of personal data across borders without stringent data export restrictions.

## Puttaswamy Judgment—Genesis of the PDP Bill

In the Indian Supreme Court's ('SC') landmark decision of Justice KS Puttaswamy (Retd) v Union of India[3] ('Puttaswamy'), right to privacy was conclusively recognised as a fundamental right. In Puttaswamy, the constitutional validity of the AADHAAR (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ('AADHAAR Act') was questioned. The said law rolled out a system of unique citizen identification numbers for efficient delivery of government benefits and subsidies. The unique number, also called the AADHAAR number, is linked and authenticated with an individual's biometric identifiers that are stored on a central data repository controlled by a special regulator, the UIDAI. The petitioners contended that the AADHAAR Act was invasive of an individual's right to privacy as it compelled individuals to provide their biometric information for availing legal entitlements, thereby negating free consent. It was also argued that the biometric data

can be misused by third parties seeking to authenticate the AADHAAR number as well as by the state to profile citizens, track their movements and surveil them. The Government, defending the *vires* of the legislation, argued that privacy was not a fundamental right and as such there were sufficient technical measures that would maintain authenticity and confidentiality of processed personal data.

The SC ruled that privacy was a key facet of an individual's right to life and personal liberty under Article 21 of the Constitution and can only be suspended by following substantive and procedural due process of law, that is, there must be a law, the action must serve a legitimate state aim and the invasive measures must be proportionate to the goal sought to be achieved. Further, the SC expressly recognised informational privacy as inherent to individual's right to privacy. Furthermore, the SC urged the government to create a detailed data protection regime in India that marries an individual's privacy interests and legitimate state concerns such as protecting national security, preventing and investigating crimes, encouraging innovation and dissipation of social benefits. On the second question regarding constitutionality of the AADHAAR Act, the SC undertook a detailed evaluation of the privacy and data protection safeguards provided therein and upheld its constitutionality, barring few provisions which were held unconstitutional.

## PDP Bill—An Overview

In the wake of Puttaswamy, the Indian Government constituted a Committee of experts to propose a structured data protection law.[4] The Committee submitted a draft law to the Ministry of Electronics and Information Technology on 27 July 2018 and a revised PDP Bill was referred to a Joint Parliamentary Committee on 11 December 2019 for further deliberations. The Committee is at the final stages of its deliberations and it is anticipated that a final PDP Bill will be tabled before Parliament soon.

### Overview and Key Concepts

The PDP Bill is structured as a sector agnostic law regulating the processing of personal data ('PD') and, *inter alia*, provides for core data processing principles, the permissible processing basis, individual rights, technical and organisational measures, special obligations for certain kinds of processing, cross-border data transfer mechanisms and penalties for breach. It contemplates establishing an independent regulator, the Data Protection Authority of India ('DPA') that will be vested with significant powers for regulating the data ecosystem. The PDP Bill will apply to government and private entities/persons. It will also apply extraterritorially to foreign entities or persons who are engaged in any business or systematic activity of offering goods or services to persons within India, or profile them. Some of the key concepts and requirements under the PDP Bill are captured below to understand the extent of change that the PDP Bill proposes:

1. 'Processing' is defined widely to include any and all operations performed on PD such as collection, recording, organisation, structuring, storage, alteration, retrieval, disclosure, erasure and destruction of PD. Processing must be as per the core data protection principles of purpose limitation, data minimisation, storage limitation, data accuracy, accountability and transparency.

2. PD is also provided a wide scope and will mean any data about or relating to a natural person who is directly or indirectly identifiable, whether online or offline, either standalone or in combination with other information and shall include any inference drawn from such data for the purpose of profiling. An expansive definition is essential for the law to evolve organically and cater to future technological advancements.

3. Certain categories of PD that may reveal, be related to or constitute financial data, health data, an official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation will be treated as SPD. Apart from the listed SPD, Clause 15 empowers the Central Government ('CG') to notify additional categories of SPD after consultation with the DPA and concerned sectoral regulators. The definition is wide and there is a possibility that most kinds of PD qualify as SPD. For instance, one's last name in India generally relates to a person's caste and thus, a name may also qualify as SPD.

4. The PDP Bill introduces the concept of a fiduciary or trust-based relationship between the entities processing PD and the individual. Accordingly, processing under the PDP Bill involves three


stakeholders, namely (a) the data principal as the concerned natural person whose PD is being processed (akin to a data subject); (b) the data fiduciary as the state entity or the natural or legal person that determines the purposes and means of processing (similar to a controller); and (c) the data processor as the one that processes the PD for the fiduciary strictly in accordance with the instructions of and authorisation from the fiduciary. The underlying theme is that the fiduciary is best suited to determine the impact of processing and owes a responsibility to ensure the principal's privacy.

5. Consent is the primary legal basis for processing and must be free, informed, specific, clear and capable of being withdrawn. This essentially requires the fiduciary to provide detailed information about the scope and purposes of processing, manner of processing, the stakeholders involved in the data processing cycle and available remedies and rights. Apart from consent, the PDP Bill also contemplates processing on other grounds such as performance of any state function, compliance with the law, responding to any medical emergency, a breakdown of public order, a threat to public health and for reasonable purposes as may be notified subsequently by the CG. A detailed consent mechanism is a significant improvement over the IT Rules, but critics have raised concerns about absence of other grounds for processing (such as legitimate interest, reasonable repurposing and lawful contract) and overreliance on consent that is well known to result in consent fatigue.

6. Elaborate data principal rights are provided for under the PDP Bill, including the right to confirmation and access for processed PD, correction and erasure, portability and the right to be forgotten. This is an important change as the IT Rules barely provided for individual data protection rights.

7. To bolster transparency and accountability, the PDP Bill mandates a data fiduciary to prepare a privacy by design policy, provide necessary information on processing activities, implement necessary security safeguards (such as de-identification and encryption) and report any data breach to the DPA. Additionally, based on factors such as the volume of PD processed, sensitivity of PD, turnover, risk of harm to the data principal and other factors, certain data fiduciaries can be classified as significant data fiduciaries. These fiduciaries will have to comply with

specific obligations around data audit, appointment of a data protection officer, conducting data protection impact assessments and maintaining processing records.

8. For breach of the PDP Bill, the DPA is vested with wide inquiry and directive powers. It also proposes significant penalties that could range from between two to four per cent of an organisation's global turnover[5] and entitles the principal to seek compensation for harm suffered. Thus, upon implementation of the PDP Bill, organisations have to transition from a self-regulatory approach that exists under the IT Rules to a 'comply or face the consequences' approach.

## Cross-border Transfer Under the PDP Bill

The PDP Bill at Chapter VII elaborates on cross-border data transfer mechanisms and mandates data localisation for certain kinds of data. Clause 33 permits the transfer of PD freely, as long as PD is not SPD or critical PD as may be notified by the CG. The PDP Bill does not provide any guidance on what will constitute critical PD, but it is speculated that this may include data that has a bearing on Indian sovereignty, state security, defence and the economy. Where it is SPD or critical PD, fiduciaries must take into account the data localisation principles and transfer mechanisms as explained below:

**The PDP Bill at Chapter VII elaborates on cross-border data transfer mechanisms and mandates data localisation for certain kinds of data.**

1. SPD can be transferred provided it is continually stored in India, that is, partially localised. Further, transfer can only take place with the principal's explicit consent and the DPA's approval, unless it complies with any one of the following data export restrictions. The first condition requires the transfer to be made pursuant to a contract or intra-group scheme approved by the DPA. For approval, the contract or intra-group scheme must include provisions for effective protection of the data principal's rights and liability of the fiduciary for harm caused due to non-compliance of the contract or scheme. The second condition mandates that transfer is undertaken to a country, entity or class of entity in a country or an international organisation on the basis of an adequacy decision of the CG in consultation with the DPA. An adequacy finding shall take into account the level of protection that is afforded to the transferred SPD having regard to the applicable laws and international agreements of the recipient and whether such transfer will prejudice enforcement of relevant Indian laws.

2. Critical PD can only be processed in India and cannot be transferred outside. The limited exceptions to this absolute localisation are where critical PD needs to be transferred for prompt action during health or emergency services or to a foreign recipient whom the CG has confirmed through an adequacy decision, provided that the transfer in the opinion of the CG is not prejudicially affecting security and the strategic interest of the state. If any critical PD is transferred, such transfer must be notified to the DPA within such timeline as may be prescribed.

Where the fiduciary fails to comply with cross-border data transfer regulations, the fiduciary could be penalised up to INR150 million or four per cent of the total worldwide turnover in the preceding fiscal (that is, 1 April to 31 March), whichever is higher. However, prior to imposing penalties, adjudicating officers shall provide a reasonable opportunity of hearing and the orders passed can be preferred in appeal to the appellate tribunal as may be notified.

To summarise, SPD can be processed abroad subject to partial localisation, explicit consent of the principal and either with the regulator's approval or subject to compliance with data export restrictions in the nature of a contract, intra-group scheme or adequacy decision. Critical PD is subject to absolute localisation and cannot be transferred abroad, except at the discretion of the CG. In light of these conditions, organisations have to plan, strategize and invest substantial resources for physically processing data only in India and implementing adequate data protection measures. Since there are no precedents in the context of cross-border data transfer under the IT Rules, there is ambiguity around implementation. Consequently, it is expected that the government, DPA as well as courts are likely to refer to other jurisdictions and foreign jurisprudence to interpret and enforce the requirements.

## Cross-border Data Transfer Under the EU GDPR

In order to understand the impact of the PDP Bill's data localisation and export restrictions, it is helpful to take a quick look at cross-border data transfer regulations under the European Union General Data Protection Regulations ('EU GDPR'). The general principle is that PD can be transferred outside the EU only if the recipient complies with all of the applicable EU GDPR provisions, so that the data subject's interests are safeguarded. Alongside this, the controller or processor must comply with the data export restrictions as explained below:

1. PD is transferred outside based on an adequacy decision from the European Commission ('EC') or concerned supervisory authority. An adequacy decision will, *inter alia*, evaluate the recipient's state of law including its legislation and judicial redressal mechanisms, the existence and effective functioning of an independent data protection regulator and the recipient's international commitments/stance regarding personal data protection. As of date, the EC has recognised 12 jurisdictions as being adequate.[6]

2. In absence of an adequacy decision, the controller or processor can transfer only if they have provided adequate safeguards. Adequate safeguards can be provided through a legally binding and enforceable instrument between public authorities, binding corporate rules (similar to intra-group schemes under the PDP Bill), standard data protection clauses adopted or approved by the EC, approved codes of conduct or certification mechanisms. In all of these options, it is fundamental that there are binding commitments on the recipient to apply appropriate data processing safeguards, including enforcing data subject rights under the EU GDPR.[7]

3. Where (1) or (2) are not fulfilled, the EU GDPR provides for other grounds of transfer. These include transfer with the data subject's explicit consent, performance of a contract or implementation of pre-contractual measures, public interest, legal claims or for protecting the vital interests of the data subject where the data subject is incapable of giving consent.

4. Additionally, cross-border data transfer is permissible if the transfer is not repetitive, concerns only a few data subjects, is necessary for compelling the legitimate interests of the controller that are not overridden by the data subject's rights and the controller has fully evaluated and provided suitable safeguards for protection of the transferred data.

In essence, there are no data localisation norms, although getting an adequacy finding or implementing approved adequate safeguards is an uphill task. A case in point is the decision of the European Court of Justice in the Schrems II case,[8] where it was ruled that the EU-U. S. Privacy Shield failed to provide adequate safeguards for EU data and invalidated it with immediate effect. This testifies to the high threshold that must be fulfilled for continuous adequacy determination. Despite a lapse of 18 months from the EU GDPR implementation, the EC has to still approve codes of conduct or certification mechanisms. Further, approval of binding corporate rules is a long-drawn process and can take several years. In such a scenario, organisations have relied on approved standard contract clauses and the data subject's consent as viable alternatives for data export.

## Analysis of the PDP Bill Restrictions and Potential Impact

The PDP Bill's localisation and data export restrictions seem to be motivated by three main ideologies.

1. It is argued that localisation will prevent misuse of valuable and sensitive data in a foreign territory such as foreign government surveillance, unauthorised profiling and unlawful data trade. Foreign surveillance has been a big concern for India due to its geo-political relationships with neighbouring countries. The Indian Government's recent move to permanently ban 59 Chinese apps citing use of data for activities prejudicial to the sovereignty and integrity of India evidences the regulatory mindset towards foreign surveillance, which finds its reflection in the proposed localisation norms.

2. The Government believes that localisation will facilitate the exercise of territorial jurisdiction, which will in turn obligate foreign fiduciaries and processors to provide access to data when required, such as for prevention of crime, investigating breach scenarios and enforcing remedies in India. As early as 2008, the Indian Government in connection with the infamous 2008 Mumbai terror attacks (known as 26/11) engaged in a protracted struggle with

**While cross-border data regulation is a necessary evil, localisation measures are archaic and opposed to the idea of data agility.**

Blackberry. As the perpetrators used Blackberry devices for planning the attacks, the Government compelled Blackberry to locate its servers in India, so that law enforcement agencies could access encrypted data. Thus, data localisation appears to be an obvious choice for the regulator for law enforcement.

3. It is also presented that localisation will facilitate India's trillion-dollar digital economy. The Government believes that the current data-driven economy has a first-mover's advantage and if India is to emerge as a technology leader, data harnessing and harvesting are key, which calls for ramping up local data infrastructure. With mandatory data localisation, the Government hopes to increase foreign direct investment in digital infrastructure including more data centres, communication satellites and network connectivity, which will result in more employment and benefit the economy.

In light of the above justifications, it appears that the PDP Bill's data transfer restrictions are aimed at asserting data sovereignty and it is not solely aimed at protecting a principal's privacy. A by-product of data flow regulation is that it tends to distort trade by creating entry barriers for businesses and new technologies, segregates the Internet on geographical lines, weakens network security management and increases the cost of doing business. The PDP Bill's localisation and data export restrictions in its current form can be counter-productive for the following reasons:

1. There will be a direct cost impact. Since the scope of SPD is wide and can directly or indirectly cover large volumes of PD, the outcome may be that businesses end up storing all data in India. This will have a bearing on data management methods for organisations processing and storing huge volumes of data outside India. Migrating data from an existing location outside India to servers in India is likely to entail substantial costs. Combined with this, the uncertainty around what will qualify as critical PD will constantly require businesses to undertake data inventories on an ongoing basis in order to remain compliant, which again is likely to become a significant cost head.

2. Mandatory localisation can adversely affect privacy management measures. In order to localise, organisations may have to allocate budgets which could be otherwise used for ramping up their network security resources. This will not only result in lesser economies of scale, but also create additional threats for security failure. For instance,

it is a common practice for group entities to leverage intra-group network assets as part of a robust risk mitigation strategy. Where a data breach occurs, affected data is often transferred to a group entity's server irrespective of the physical location to minimise the potential harm. But, with localisation, cross-border data transfer as part of privacy protection measures is out of context and organisations will have to think about other alternatives.

3. There is also increased scepticism that localisation combined with the CG's wide powers under the PDP Bill can be a segue to increased state surveillance jeopaardising privacy. This is in clear derogation of Puttaswamy which requires balancing of an individual's privacy interests and legitimate state concerns. Further, if scepticism becomes a reality, it will be difficult for organisations to import data into India from jurisdictions such as the EU, United Kingdom and Switzerland, as an adequacy finding would be impossible on the grounds of heightened surveillance, lack of rule or law, and insufficient data protection and privacy measures.

4. The PDP Bill provides for very limited circumstances in which cross-border data transfer can be carried out. Unlike the EU GDPR, which provides for additional grounds such as approved codes of conduct, certification mechanisms, performance of a contract, implementation of pre-contractual measures, public interest, initiating and defending legal claims and protection of the data subject's interests, the PDP Bill heavily relies on an adequacy decision, intra-group schemes and standard contracts. From lessons learned under the EU GDPR, it will take quite some time for India to formulate details. Until such time, there will be business uncertainty and it is imperative to permit additional grounds for cross-border transfer to ensure business continuity.

## Conclusion

While cross-border data regulation is a necessary evil, localisation measures are archaic and opposed to the idea of data agility. Instead, the government should focus on strengthening mutual legal assistance treaty mechanisms with other nations to meaningfully implement the PDP Bill in a global set-up. To this effect, the EU GDPR positively obligates the EC and supervisory authorities to take steps for developing international cooperation mechanisms and provide mutual international assistance for enforcement. There is no such provision under the PDP Bill and perhaps a similar provision is a better substitute to a physical localisation mandate. When the final text of the PDP Bill is tabled, it will be interesting to see if India manages to take a step forward for a truly progressive data protection law or retracts two steps to implement regressive localisation norms.

## Notes

[1] Countries like Russia, Indonesia, Vietnam, Kazakhstan and China have localisation requirements and some others like Australia and South Korea have selective localisation requirements for certain kinds of data.
[2] There are specific processing requirements under sectoral laws which have not been analysed in this article.
[3] 2017 (10) S.C.A.L.E 1.
[4] The committee of experts was chaired by former Judge of the Supreme Court, Hon'ble Shri Justice BN Srikrishna.
[5] 'Worldwide turnover' is defined as gross revenue from the sale, supply or distribution of goods and/or services within and outside India. In the context of group entities, the revenue of a fiduciary will be added to the group entity(ies) revenue if it is connected with processing in India.
[6] These include Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay as providing adequate protection and talks are ongoing with South Korea; for details access https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last accessed on 25 January 2021).
[7] In these situations, there is no need to obtain prior permission from the concerned supervisory authority. Adequate safeguards can also be subjected to consent from the supervisory authority under the consistency mechanism, which are not captured in this article.
[8] European Court of Justice (Grand Chamber) ruling in case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems, dated 16 July 2020.

**Arya Tripathy**
**Partner, Priti Suri & Associates (PSA), India**

Arya Tripathy is a Partner of Priti Suri & Associates (PSA), India. She practises in the areas of General Corporate, M&A, Employment and Data Protection laws and has closely worked with various domestic and international clients on diverse aspects of business law. She leads the firm's pro-bono practice and takes a keen interest in working alongside policy think tanks in the niche technology and privacy law space.

# Data Protection — European Road Block or Global Guidance?

With Europe being focused on its General Data Protection Regulation ('GDPR')[1], the US as well as many Asian countries still seem to struggle with the right balance between privacy and opportunities of data exploitation. At the same time, data-driven business models are developing rapidly, oftentimes at a speed that by far outpaces the discussion about the right regulatory approach.

Data stockpiling, artificial intelligence ('AI'), CCTV, facial recognition technology, digital campaigning, machine learning, deep fake, robo-surveillance of CEO earning calls, predictive policing—these buzzwords reflect just a few areas where data is key. With a view to potential economic opportunities, data protection is sometimes perceived as an obstacle, whether in the development of innovative business models or in the fulfilment of state responsibilities such as ensuring public safety or—more recently—combating a pandemic. Nevertheless, from a global perspective, the trend is towards data protection, even though the question often is how.

## Introduction

People reveal data about themselves in almost every situation in life. This may be in the context of an online purchase, the use of a customer card when shopping, an internet search or the mere carrying of a cell phone. Accordingly, the issue of appropriate protection for personal data is ubiquitous. Data protection issues can arise in many forms, on the one hand in the relationship between private individuals/companies and on the other hand in the relationship between state and citizen. In the following, two aspects will be used as examples to show that the question of whether and how to regulate the handling of personal data is answered unanimously in various regions of the world. Finally, some current legislative trends in data protection law will be examined.

## Are Data Protection Regulations a Location Disadvantage?

### The Value of Data

Using customer data, companies can analyse the behaviour of customers, especially for commercial purposes. This has the advantage for companies and

customers alike that customers can be offered suitable products and services in a targeted manner. Not least for this reason, *The Economist* published the following headline on 6 May 2017: 'The world's most valuable resource is no longer oil, but data'.[2] The introduction of the customer card in 1995 allowed the British supermarket operator Tesco to analyse the behaviour of its customers and tailor its offering to the insights gained. Within a year, customers spent 28 per cent more in Tesco supermarkets and 16 per cent less in its competitor Sainsbury's stores.[3] This relatively innocent example shows already that the processing of personal data can have a considerable impact on customer privacy. Technological progress brings new opportunities as well as threats. It is not simply that information is being collected. Nowadays, the resulting data is training complex algorithms, which then may nudge people towards certain behaviours. There are mixed views on how to resolve this conflict between economic interests and the protection of privacy.

**It is sometimes argued that detailed data protection regulations are an obstacle to business.**

### Less Data Protection in Favour of Economic Interests

It is sometimes argued that detailed data protection regulations are an obstacle to business. For example, some German companies complain about a competitive disadvantage on the non-European market compared with companies that are not subject to the scope of the GDPR.[4] There is also criticism regarding the increased administrative burden associated with compliance to the GDPR.[5] In addition, there are higher costs, for example, in connection with employee training.

Industry warns that data protection must not be a roadblock to innovation or a disadvantage in terms of location.[6] Data protection laws that are too strict may put the brakes on innovative, data-driven business models. Within companies, the intelligent evaluation of employee data offers the opportunity to reduce costs and improve employee satisfaction.[7] It is particularly in the development of AI applications and the field of machine learning that data protection can limit technological progress and leadership. Here, large sets of the most accurate data are of the essence.[8] Emmanuel Mogenet, the former head of Google's research in Europe, stated that a neural network would have to be trained with about 100,000 to one million cat pictures until it is able to recognise a cat in a picture that was not yet known to the computer[9]—the more the better. A more complex application such as Google's Gmail SmartReply had to be trained with a dataset consisting of 238 million examples, while Google Translate needed trillions.[10]

It is true that the training data can be anonymised in order to avoid violating the applicable data protection laws. Data anonymisation is a process that aims to modify the training data in such a way that it is no longer possible to draw conclusions about personal conditions from it. This in turn incurs costs and requires appropriate know-how. In insufficiently anonymised databases, data can still be assigned to individual persons by comparing them with other datasets.[11] Moreover, certain industries specifically prosper in regions with a lesser focus on data protection. For example, China has not only become a leader in the global market of facial recognition technology by exploiting data from unrestricted video footage; it is also set to be a major player in the field of emotion recognition—an upcoming technology used for analysing a person's mental state by identifying signs of aggressiveness and nervousness through algorithm supported surveillance of, for example, eye and gait tracking.[12] US companies, also building surveillance tech, are falling behind in these fields, arguably, among other reasons, due to ethical and data protection restrictions.[13]

### More Data Protection in Favour of Privacy and Legal Certainty

Despite the resulting potential limitations of economic opportunities, others, however, consider precise and, if possible, uniform data protection regulations to be indispensable. Several reasons are given for this. In some cases, the high value of privacy is emphasised. The protests by WhatsApp users against planned changes in data protection settings have once again brought the issue of data protection into focus and shown that users do care about the protection of their data. The trust in digitisation, which has been significantly weakened not least by data protection scandals such as the events involving Cambridge-Analytica, the firm that used data improperly obtained from Facebook to build voter profiles, could be strengthened by means of data protection regulations.

Without such limitations, it is almost impossible for ordinary consumers to find out which of their personal data is being collected and processed and whether it is being passed on to third parties—possibly located abroad. In addition, consumers are often dependent on certain services, such as an internet connection, a cell phone contract or an e-mail account, and are therefore in a weak negotiating position *vis-à-vis* the provider of the service, so that they can hardly object to any data processing by the provider. Only strict sanction mechanisms such as those provided for in the GDPR, it is argued, can ensure compliance with data protection standards; the disregard of data protection standards must not pay off financially.

In addition, the protection of personal data from hackers must be ensured by imposing data storage requirements on companies. This aspect is particularly relevant due to recent major hacker attacks. Among others, big tech companies (for example, Yahoo, Facebook, LinkedIn) as well as government institutions were affected in recent years. In 2019, Australian security researcher Troy Hunt drew attention to a collection of 2.2 billion passwords—in plain text or as hash values—to online accounts that came from previously known data leaks ('Collection #1-5').[14] From the point of view of data security, binding guidelines for handling data can represent a locational advantage. Users can thus—within the scope of such regulations—be sure that their data is secured in accordance with the state of the art, which can mean an increase in customers for companies. Finally, data protection rules that are as uniform as possible also lead to greater certainty in legal terms. For companies, this goes hand in hand with greater planning safety.

### Outlook

What remains to be said is that there are weighty arguments in favour of both points of view. Companies, no matter where they are based, will always seek to explore where the creepy line is—the sometimes shady boundary between appropriate protection of individual data and the over paternalistic limitation of economic opportunities. Ultimately, it is up to the respective legislator to balance the conflicting interests and to provide clear guidance with a level playing field for all stakeholders involved.

## Are Data Protection Regulations Obstructing the Fight Against Pandemics?

### Data Privacy Versus the Restriction of Other Fundamental Rights

The issue of data protection in the relationship between state and citizen is not new. More recently, the debate has been reignited as a result of Edward Snowden's revelations surrounding the NSA affair and a series of terrorist attacks in European countries. Now the coronavirus pandemic is shedding light on another facet of the problem. While fundamental rights are also being severely restricted in free democratic countries fighting against COVID-19, the protection of data privacy is sometimes accorded a rather privileged status. Compared to Asian countries that take a more data-invasive approach, western democracies seem to be more reluctant when it comes to using technology that may interfere with the privacy rights of individual citizens.

### The Cautious Approach of Western Democracies Exemplified by the German Corona App

In Germany, for instance, the introduction of a coronavirus app was accompanied by heated discussions about data privacy. One issue was whether contact data should be stored centrally on a server or decentrally on users' devices. A decentralised solution offers greater data protection. However, with a decentralised solution, the scientists have less data available for analysis. The main issue is the decision between a tracking and a tracing solution. Tracing means that the app only registers which other cell phones are in proximity. A tracking app, on the other hand, can be used to determine when a cell phone was at a specific location. By means of a tracking app, the authorities could thus compile movement profiles of users and make them useful in the fight against the pandemic. It can also be used to monitor quarantine regulations. Germany ultimately opted for the most privacy-friendly option, a decentralised tracing app. In line with this, the installation of the app is voluntary. Other European countries, equipped with similar apps, report a restrained use of this technology as well, often due to unspecified data protection concerns.

### The More Invasive Approach of Some Asian Countries

In contrast, data protection considerations play only a subordinate role in the fight against pandemics in countries such as China, South Korea or Taiwan. In South Korea, cell phone data is linked to video surveillance images of streets, houses and squares to track the course of infection. Credit card statements and GPS data from cars are being used as well.[15] In Taiwan, mobile phone data is processed, among other things, to monitor compliance with the quarantine rules. In China, there is a de facto obligation to install the respective province's coronavirus app. Without the app, participation in public life is impossible. If one wants to enter a train station or a restaurant, a QR code must first be scanned with the app. In addition, an infrared camera is used to measure body temperature.[16]

While such measures would have triggered outrage in large parts of the population of the Western world—they would have been considered disproportionate—there is almost unopposed acceptance of them in the above-mentioned countries. Only individual critics have warned against arbitrary digital surveillance. This is not least a reflection of differences in culture. Among many Chinese, for instance, the focus is not on individual data security concerns *vis-à-vis* the state. On the contrary, they predominantly seem to trust the authorities and government institutions and worship the protective role technology solutions play in fighting the pandemic.[17]

### Outlook

Whether and to what extent the increased use of digital surveillance methods has had an impact on the course of the pandemic is still unclear due to the lack of (long-term) scientific studies. Yet it is plausible that such measures helped to prevent the Asian countries from being hit by a second wave of infections, as opposed to the European countries and the US. Nevertheless, it should not be overlooked that these measures are only one aspect of the strategy of these Asian countries, which were comparatively well prepared to deal with a pandemic due to the past SARS epidemic. It is therefore hard to say with certainty whether stricter data protection rules hinder the fight against the pandemic. However, what can be said is that dealing with the question of how data protection is to be structured in the relationship between the state and the citizen has very concrete implications in the context of the COVID-19 crisis. Depending on the value one attaches to privacy, the result of the balancing of interests between privacy and the interests of health and life threatened by the virus will differ. Once again, it is the legislator who ultimately decides in which direction the pendulum swings.

## Conclusion

Since it is ultimately up to the respective legislator to decide how to reconcile the conflicting interests, both in the relationship between private individuals and in the relationship between the state and the citizen, a heterogeneous level of data protection can be found worldwide. The Schrems decisions of the European Court of Justice ('ECJ')[18] have shown the difficulties this can lead to.

However, recently an interesting development has emerged: several countries are currently discussing new data protection laws or have already enacted such laws. Some of these laws are based on the concepts of the GDPR. For example, current data protection laws such as the Brazilian Lei Geral de Proteção de Dados Pessoais ('LPDP') have several striking similarities with the GDPR, such as a right of access to personal data collected about one and a right to be forgotten.[19] Also, on 1 January 2020, California, the home state of tech giants like Google and Facebook, enacted the California Consumer Privacy Act ('CCPA'), a data protection law inspired by the GDPR.[20] Other states such as Nevada, Maine, New York, Massachusetts, Maryland, Hawaii and North Dakota have

also enacted or are considering new privacy laws. Calls are being made for regulation at the federal level in the US.[21] Likewise, its strict rules on the transfer of data to third countries has helped the GDPR become increasingly established as an international standard. In this context, the free trade agreement between Japan and the EU, which came into force on 1 February 2019, should be mentioned. It is based on the European standard and thereby created the world's largest area for secure data traffic.

Overall, the trend is towards more data protection. This strengthens the privacy of citizens and promotes smooth data transfer processes between countries.

## Notes

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 15 February 2021).
[2] 'The World's Most Valuable Resource Is No Longer Oil, but Data', The Economist, available at www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (accessed 15 February 2021).
[3] Ian Westbrook, 'Tesco Clubcard Changes Anger Customers', BBC News, available at www.bbc.com/news/business-42700758 (accessed 15 February 2021).
[4] Barbara Engels/Marc Scheufen, 'Competition Effects of the General Data Protection Regulation – An Analysis Based on a Survey Among German Companies', German Economic Institute, available at www.iwkoeln.de/fileadmin/user_upload/Studien/Report/PDF/2020/IW-Report_2020_DSGVO_und_Wettbewerb.pdf (accessed 15 February 2021).
[5] Kate Fazzini, 'Europe's Sweeping Privacy Rule Was Supposed To Change the Internet, but So Far It's Mostly Created Frustration for Users, Companies, and Regulators, CNBC, available at www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html (accessed 15 February 2021).
[6] Federation of German Industries (BDI), 'Datenschutz darf keinesfalls zum Innovationshemmnis und Standortnachteil werden', available at https://bdi.eu/artikel/news/datenschutz-darf-keinesfalls-zum-innovationshemmnis-und-standortnachteil-werden/ (accessed 15 February 2021).
[7] Ina Lockhart, 'Gute Daten, böse Daten', Frankfurter Allgemeine Zeitung, available at www.faz.net/aktuell/karriere-hochschule/nutzung-und-schutz-von-mitarbeiterdaten-in-unternehmen-17182195.html?printPagedArticle=true#pageIndex_2 (accessed 16 February 2021).
[8] Roslyn Layton, 'The 10 Problems of the GDPR', Statement before the Senate Judiciary Committee, available at www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf (accessed 15 February 2021).
[9] Helmut Martin-Jung, 'So trainiert Google künstliche Intelligenz', Süddeutsche Zeitung, available at www.sueddeutsche.de/digital/algorithmen-so-trainiert-google-kuenstliche-intelligenz-1.3759233 (accessed 15 February 2021).
[10] https://developers.google.com/machine-learning/data-prep/construct/collect/data-size-quality
[11] Yves-Alexandre de Montjoye / César A. Hidalgo / Michel Verleysen / Vincent D. Blondel, 'Unique in the Crowd: The Privacy Bounds of Human Mobility', Nature, available at www.nature.com/articles/srep01376 (accessed 15 February 2021).
[12] Sue-Lin Wong / Qianer Liu, 'Emotion Recognition Is China's New Surveillance Craze', Financal Times, available at www.ft.com/content/68155560-fbd1-11e9-a354-36acbbb0d9b6 (accessed 15 February 2021).
[13] Yuan Yang / Madhumita Murgia, 'Facial Recognition: How China Cornered the Surveillance Market', Financial Times, available at www.ft.com/content/6f1a8f48-1813-11ea-9ee4-11f260415385 (accessed 15 February 2021).
[14] Andy Greenberg, 'Hackers Are Passing Around a Megaleak of 2.2 Billion Records', WIRED, available at www.wired.com/story/collection-leak-usernames-passwords-billions/ (accessed 15 February 2021).
[15] Justin Fendos, 'How Surveillance Technology Powered South Korea's COVID-19 Response', Brookings, available at www.brookings.edu/techstream/how-surveillance-technology-powered-south-koreas-covid-19-response/ (accessed 15 February 2021).
[16] Pratik Jakhar, 'Coronavirus: China's Tech Fights Back', BBC News, available at www.bbc.com/news/technology-51717164 (accessed 15 February 2021).
[17] Yingzhi Yang / Julie Zhu, ‚Coronavirus Brings China's Surveillance State Out of the Shadows', Reuters, available at www.reuters.com/article/us-china-health-surveillance-idUSKBN2011HO (accessed 15 February 2021).
[18] ECJ, Judgment of 16 July 2020 – C-311/18 and ECJ, Judgment of 6 October 2015 – C-362/14.
[19] Jeff Kuo / Scot Ganow, 'So Goes the EU, So Goes the World....Brazil's New Privacy Law Is on the Horizon', Lexology, available at www.lexology.com/library/detail.aspx?g=f6b0a2ec-ecd3-45e3-9caf-69a04a5ebb11 (accessed 15 February 2021).
[20] Navdeep K. Singh, 'What You Need to Know about the CCPA and the European Union's GDPR' American Bar Association, available at www.americanbar.org/groups/litigation/committees/minority-trial-lawyer/practice/2020/what-you-need-to-know-about-the-ccpa-and-the-european-unions-gdpr/ (accessed 15 February 2021).
[21] Carl Schonander, 'The United States Needs a Federal Privacy Law', CIO, available at www.cio.com/article/3379036/the-united-states-needs-a-federal-privacy-law.html (accessed 15 February 2021).

### Dr Björn Otto

**Partner, CMS Germany, Germany**

Dr Björn Otto is a Certified Lawyer for Labour and Employment Law and Co-Head of CMS Germany's cluster of excellence 'Restructuring and Insolvency'. He advises national and international clients on all aspects of both individual and collective labour and employment law. A main focus of his practice is on outsourcing and restructuring as well as privatisation, including conduction of negotiations with unions and other employee representatives on collective bargaining agreements, transfer and reorganisation agreements as well as reconciliation of interests, social plans and voluntary leaver programs. Björn has particular expertise with regards to boardroom co-determination (both nationally and internationally), matrix structures of multinationals, implementation of (cloud-based) HR-, ERP and other IT systems (including data protection), insolvency-specific employment law, European and Societas Europaea Works Council issues and cross-border reorganisation projects.

### David Windhövel

**CMS Germany, Germany**

David Windhövel is a research associate at CMS Germany. He studied law at the Universities of Cologne, Germany, and Paris (Université Paris 1 Panthéon-Sorbonne).

# The Importance of Having a Data Processing Agreement—Drafting Points

A data processing agreement is mandatory under article 28 of the General Data Protection Regulation, the latter having extra-territorial effect beyond the European Union ('EU') member states. Data protection supervisory authorities in the European Union may impose fines for failure to enter into a data processing agreement. Absent any standard agreement adopted by the European Commission, there exist diverse clauses, some of which are considered in this article.

## Requirement to Enter a Data Processing Agreement

The General Data Protection Regulation ('GDPR') Regulation (EU) 2016/679[1] applies since 25 May 2018. The GDPR has extra-territorial effect so that a non-EU company would be subject to the GDPR if the company offers goods or services to data subjects in the EU, pursuant to article 3 of the GDPR, which provides:

> Article 3 – Territorial scope
> …
> 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>  a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union …

To the extent that a company is subject to the GDPR, an obligation to enter into a data processing agreement ('DPA') is imposed on the company, regardless of whether the company would act as controller or processor, pursuant to article 28 of the GDPR:

> Article 28 – Processor
> …
> 3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. …

## Failure to Execute a DPA

A DPA is mandatory under the GDPR. A failure to enter into a DPA may be subject to fines by data protection supervisory authorities pursuant to article 83(4)(a) of the GDPR:

> Article 83 – General conditions for imposing administrative fines
> …
> 4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:
>  a. the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; …

These are the facts of a German case[2] where a data protection authority in Hamburg, Germany (Hmb BfDI)[3], on 17 December 2018, imposed a €5,000 fine on the grounds of failure to execute a DPA. The case concerned a small German company ('Color & Style') advising clients on colour and style and offering to clients certain products used for the purposes of colour analysis, such as colour chart cards, which were sent out via a courier service provider based in Madrid, Spain. By law, a DPA was needed between Color & Style and the courier service provider.

In May 2018, Color & Style sent an email to the data protection authority in Hessen ('DSK') asking for advice regarding the courier service provider which Color & Style contracted and which processed personal data of the clients of Color & Style, but which courier service provider–despite several reminders–failed to send to Color & Style a DPA. DSK replied that the duty to conclude a DPA lies not only with the processor but also with the controller. Hence, Color & Style was under a duty and had to make real efforts to draft the necessary DPA and to send the DPA to the courier service provider instead of waiting for the courier service provider to do the necessary. DSK pointed out that DPA templates were accessible on the websites of data protection authorities. At that stage, Color & Style engaged the services of a lawyer who informed DSK on behalf of Color & Style that: (1) Color & Style had asked for advice in May as a precaution only; and (2) it was impractical and expensive to draft a DPA accompanied by a translation into Spanish for the courier service provider from Spain. DSK transferred the matter to the data protection authorities in Hamburg ('Hmb BfDI') whereby Hmb BfDI rendered a decision imposing a €5,000 fine.

Hmb BfDI imposed the fine due to infringement of article 28 (3) of the GDPR, stating that on the facts of the case, as they were described by Color & Style in their email to DKS of May 2018 and on the basis of an accompanying data privacy statement, the courier service provider was processing personal data of the clients of Color & Style

as an agent of and upon instructions from Color & Style. Hmb BfDI justified the fine by the fact that, among other things, once Color & Style had received advice from DSK, they should not have contracted the courier service provider without a DPA. Instead, Color & Style, although made aware by DSK of the legal position, decided to act in a non-compliant manner by not taking the DSK advice seriously, avoiding the responsibility and failing to cooperate with the data protection authorities.

## DPA Template

While transfers of European Personal Data into a jurisdiction other than a jurisdiction in the EU, the European Economic Area ('EEA') or the European Commission-approved countries providing 'adequate' data protection are compliant on the basis of Standard Contractual Clauses ('SCC')–Standard Contractual Clauses (Controller to Controller Transfers–Set II) in the Annex to the European Commission Decision of 27 December 2004[4] and Standard Contractual Clauses (Processors) in the Annex to the European Commission Decision of 5 February 2010,[5] which were formally adopted as template agreements by the Commission, no DPA template has been formally adopted so far.

## Incorporation Into Agreement

SCC are generally regarded as independent from the main agreement. A DPA, on the contrary, is deemed incorporated into the main agreement, which approach is supported by the majority of practitioners:

> *Example*:
>
> This DPA is incorporated into the relevant [XZY Ltd.] services agreement attached to or incorporated by reference into the ordering document previously executed by Customer, referred to generically in this DPA as the 'XZY Contract'.[6]
>
> This DPA applies to Personal Data that [ABC Ltd.] processes as a Processor as part of [ABC]'s provision of the Services. This DPA forms part of [ABC Ltd.] and Customer's Agreement.[7]
>
> This Agreement is an integral part of and subject to provisions as set out in the main contract [designation] from [date]. In the event of possible discrepancies between this Agreement and the main contract [designation] from [date], the provisions of this Agreement shall prevail with regard to the Processor and/or Controller data protection obligations.
>
> Any liability arising out of or in connection with a violation of the obligations of this Agreement or under applicable data protection law, shall follow, and be governed by, the liability provisions set forth in, or otherwise applicable to, the main contract [designation] from [date], unless otherwise provided within this Agreement.
>
> The term of this DPA is identical with the term of the Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Agreement.
>
> In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, this DPA shall prevail.
>
> This Data Processing Agreement ('Agreement') forms part of the Contract for Services ('Principal Agreement') between [the Company] and Data Processor.[8]

## Processor as a Group of Companies

The parties to the DPA are generally the same persons as the parties to the main agreement. In practical terms, exception is acceptable as far as a party's affiliates, that is, a legal entity directly or indirectly controlling, controlled by or under common control with a party, are concerned. In other words, data processing or data controlling may be shared within the group. In this case, a controller or a processor will be defined as including the party's affiliates:

> *Example*:
>
> This Data Processing Agreement (the 'DPA'), entered into by the [XYZ Ltd.] customer identified on the applicable [XYZ Ltd] ordering document for [XYZ Ltd] services or [XYZ Ltd] Subscription Agreement (along with its affiliates, 'Customer') and the [XYZ Ltd.] company identified on the

ordering document (along with its affiliates, 'XYZ Ltd.'), […][9]

Any reference to 'Processor' herein shall mean any of the companies of the Processor Group.

## Sub-processors

Where a processor sub-processes data processing, a sub-processing agreement is needed between the processor and sub-processor, which would mirror the obligations of the DPA between a processor and controller pursuant to article 28 of the GDPR:

Article 28 – Processor

…

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. …

…

4. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. …

Hence, any processing outside the group is deemed sub-processing requiring the consent of the controller pursuant to article 28 of the GDPR. The consent requirement shall be complied with if sub-processors are listed in the DPA, including by means of a reference to a web link:

*Example:*

[…] currently available at https://www.linkedin.com/legal/l/customer-subprocessors the use of which Customer approves […]

[XYZ Ltd.] means an English company with its registered office address at […], United Kingdom and its subsidiaries with whom Customer has contracted for the provision of Services, if any (each subsidiary as identified on the signature page), and all subsidiaries which are a party to this DPA.

'Processor' means [XYZ Ltd.] when it processes Personal Data on the Customer's behalf as part of the Services

'Sub-processor' means a third party that [XYZ Ltd.] engages to process any Personal Data that [XYZ Ltd.] processes under this DPA, as a processor on [XYZ Ltd.]'s behalf.

## Case Studies

### Adaptive Remote Learning

The 'Platform' is a platform for personalised and adaptive remote learning. The Platform's adaptive learning algorithms mimic the way viruses behave in nature: evolving moment-by-moment using trial and error as their environment changes. The Platform's algorithms allow the learner to make mistakes and pursue misconceptions, closely mimicking real-world cognitive situations, and providing an effective and engaging experience.[10]

A company ('Company') develops the content of a training course ('Content') which the Company offers to its customers via the Platform. The Company acts as processor towards its customers. Customers are data subjects and controllers. The Platform acts as a sub-processor towards the Company. The Platform and the Company enter into a data sub-processing agreement. In these circumstances personal data flows from a customer to the Company and from the Company to the Platform.

*Example*:

As a processor, the Principal processes personal data on behalf a controller in accordance with Article 28 GDPR. In this context, the Principal may engage the Agent as another processor with specific or general written authorisation of the controller (Article 28(2), Article 28(3)(d) GDPR). For the Agent to be allowed to carry out specific processing activities – as set out in this agreement – on behalf of the controller, it is required to impose on the Agent the same data

**It is customary and practical to submit a DPA to the same law as the main agreement.**

protection obligations, as set out in the contract or other legal act between the controller and the processor by way of a contract between Principal and Agent (Article 28(3)(d), Article 28(4) GDPR). This agreement serves this purpose.

**Mobile Phone Apps**

A sub-processing agreement may not be appropriate in the circumstances where, for example, a mobile phone producer ('Producer') sells–directly or via resellers –mobile apps developed by a software company ('Company') to the Producer's customers. Customer personal data flows directly from a customer to the Company. A customer acts as the controller and the Company as the processor. The Producer enters into a DPA with the Company on behalf of a customer:

*Example*:

The provision of the Services may involve the processing of personal data of which Customers are the Controllers. In particular, in the context of the tasks set out under the Agreement, the Company shall process–as Processor–the personal data described in Agreement.

To this end, the Company hereby acknowledges and agrees that each End User shall grant to the Producer, directly or indirectly via resellers, pursuant to Articles [article] and [article] of the [jurisdiction] Civil Code, a mandate in order to appoint the Company as Processor on its behalf, or alternatively, the Controller may directly appoint Company as Processor of the processing data, solely for the purpose of providing the service covered by this agreement, so that the treatment meets the requirements Art. GDPR 28.

Consequently, the Company (hereinafter also the 'Processor') is appointed by the Producer, on behalf of Customers (hereinafter 'Controller'), as Processor for the personal data processing on behalf of the Controller exclusively for the purposes set forth in Agreement.

**Internet of Things (IoT)**

An IoT company providing services in the field of IoT is a global player with offices across the world and having the need to share/export client personal data within the group while analysing and resolving support incidents reported in software products of a client. The IoT company, as processor, and the client, as controller, may agree to bundle sub-processors who are members of the IoT company group by a listing of the processors in an Appendix to the DPA:

*Example:*

The bundling of processors is only undertaken for efficiency purposes i.e., to avoid a multitude of different contract documents) and shall result in legally separate DPAs between the Controller and each Processor as designated in the Appendix and shall not create any legal or other relationship whatsoever between the bundled Processors other than between the Controller and each Processor separately. The Supplier [IoT company] is acting in its own name and acting in the name and on behalf of the Processors listed in the Appendix.

The Supplier has been given a power of attorney by the listed organisations to conclude the EU Standard Contractual Clauses with the Customer on their behalf.

**Lead Generation**

A marketing company grants access to its database of prospective clients ('leads') to customers by way of subscription. A customer having obtained personal data of leads to be used for its own marketing purposes must

ensure that the leads have given valid consent for the marketing company to share their personal data with certain third parties:

*Example:*

1. The Service Provider guarantees that all data subjects the personal data of which it provides to the Company have given their consent to the use of such data to direct marketing purposes and to transfer of their personal data to the Company.

2. The Service Provider guarantees that all data subjects/participants to the events subject to the Services are informed of the personal data processing by the Company.

3. In accordance with Article 46 of the GDPR the Company guarantees to have provided that all the appropriate safeguards and that enforceable data subjects rights and effective legal remedies for data subjects are available. Standard data protection clauses have been signed with all potential recipients (Article 46.2.c)

Article 46 of the GDPR provides:

Article 46 – Transfers subject to appropriate safeguards

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
   ...
   c. standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);

## Applicable Law

It is customary and practical to submit a DPA to the same law as the main agreement. Optionally, if the controller or processor have a data protection representative within the EU and if the main agreement is subject to a non-EU law, the DPA may be subject to the law of the jurisdiction where the representative is located:

*Example:*

This DPA shall be governed by the same law as the Agreement.

The Agreement shall be governed by the by the law of the state in which the data controllers representative is established, namely [jurisdiction].

## Warranties

A processor processes personal data, provided by the controller, only on instructions from the controller, pursuant to article 29 of the GDPR:

Article 29 – Processing under the authority of the controller or processor

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

Although GDPR protection is sufficient, in addition, warranties may be included in the DPA:

*Example*:

The Controller warrants and represents that:

- all Controller Personal Data provided by the Controller to the Processor is necessary, accurate and up-to-date;

- all Processing Instructions shall at all times be in accordance with Data Protection Legislation.

## Indemnity

Controller(s) and processor(s) are subject to joint and several liability with respect to data subjects irrespective

of their proportionate fault, and then it remains up to controller(s) and processor(s) to sort out liability and payment or cross claims among or between themselves pursuant to article 82 of the GDPR:

> Article 82 – Right to compensation and liability
> …
> 5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

Nevertheless, the DPA may include an indemnity provision:

> *Example*:
>
> The Controller shall indemnify and keep indemnified the Processor in respect of all losses suffered or incurred by, awarded against or agreed to be paid by, the Processor and any Sub-Processor arising from or in connection with any:
>
> - non-compliance by the Controller with Data Protection Legislation;
> - processing carried out by the Processor or any Sub-Processor pursuant to any Processing Instruction that infringes Data Protection Legislation; or
> - breach by the Controller of any of its obligations under this DPA,
>
> except to the extent that the Agency is liable under the clause [below].
>
> The Processor shall indemnify the Controller for losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with this DPA:
>
> - only to the extent caused by the processing of Controller Personal Data under this DPA and directly resulting from the Processor's breach of this DPA; and
> - in no circumstances to the extent that any losses (or the circumstances giving rise to them) are contributed to or caused by any breach of this DPA by the Controller.

## The Importance of Obtaining Legal Advice

The German company Color & Style who had been penalised (referred to under 'Failure to Execute a DPA') posted comments on their website[11] saying, in particular, that it was unrealistic for them to engage an expensive IT lawyer to draft a DPA.[12] However, that case illustrates the importance of at least obtaining legal advice.

## Notes

[1] See https://eur-lex.europa.eu/legal-content/EN/AUTO/?uri=CELEX:02016R0679-20160504&qid=1532348683434.
[2] Reported at https://www.heise.de/newsticker/meldung/DSGVO-5000-Euro-Bussgeld-fuer-fehlenden-Auftragsverarbeitungsvertrag-4282737.html.
[3] https://datenschutz-hamburg.de/.
[4] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0915&from=EN.
[5] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&from=EN.
[6] See e.g. www.linkedin.com/legal/l/dpa?
[7] See e.g. www.brandwatch.com/wp-content/themes/brandwatch/src/legal/documents/BW-C2P-DPA-V004b-09062020-(DRM).pdf.
[8] See e.g. https://gdpr.eu/data-processing-agreement/.
[9] See e.g. www.linkedin.com/legal/l/dpa?
[10] https://area9lyceum.com/adaptive-learning/how-it-works/.
[11] https://kolibri-image.com/causa-datenschutz/.
[12] '… Es sei auch nicht realistisch, einen teuren IT-Anwalt zu beauftragen, das Ergebnis anschließend auf eigene Kosten ins Spanische übersetzen zu lassen und dies dann an den Hauptsitz des Auftragsdienstleisters in Madrid zu senden, mit der Aufforderung, doch gefälligst zu unterschreiben.'

**Ekaterina Biruleva**
**In-House Counsel, Kaspersky, Russia**

Ekaterina Biruleva is currently Counsel with a global IT company based in Europe, responsible for software licensing and digital advertising agreements. Previously she was an international arbitration attorney with a private practice. Ekaterina's alma mater is the School of Oriental and African Studies in London. She has a BA in Law and Economics with specialisation on economic development and the legal system of Japan. She has been admitted to the Bar in New York and England & Wales.

# Up Close and Personal: Miyuki Ishiguro

**Tell us about your years growing up, such as interests, hobbies and causes that you are passionate about. What are some of the childhood experiences that shaped you?**

I was born in Kagoshima, the southern area of Kyusyu Island, Japan, in 1964. I have one brother, six years younger than me, who is very kind and gentle. Kagoshima has been a relatively traditional area in connection with the roles of men and women, in other words, it is a male-dominated society. My father was the eldest son of a traditional samurai family in Kagoshima and males had priority in everything. On the other hand, my mother was raised by her mother, who came from outside of Kagoshima and she did not care about the priority of males. In my childhood, I was sometimes told by other male persons, except for my father, that it was meaningless to be good at studying. They may have thought that men were wiser than women, although I did not think so. This kind of message did not discourage me at all but rather encouraged me more.

During my childhood, I always played outside my home with my friends (girls and boys) from my neighborhood until dusk and sometimes my mother would angrily shut me out of our home and my father would secretly let me come inside. He loved me a lot and was always kind to me. I was never scolded or discouraged by him.

I like exercising rather than reading books and in my primary school days I enjoyed swimming and basketball after school. In my junior high school, high school and college days, I was a member of the soft tennis teams. I became darkly tanned so that it was said that my legs were like beer bottles! I spend a lot of time playing soft tennis and those days gave me a strong base of good health.

**Who has inspired your life and why?**

My mother inspired and encouraged me every day. She did not praise me even if I achieved a good score in my studies, but has never stopped me from doing anything because I am a female. As I explained above, Kagoshima is a male-dominated society and girls are not generally encouraged, but my mother did not follow these strictures at all. She was very reasonable and always told me to just do what I wanted to. It is very easy to find hundreds of excuses as to why you can't do something, but that does not make sense and you should look for ways to help you to do it. This is the message that my mother always said to me. These magic words always gave me power and encouraged me.

**What did you do before you joined IPBA? Why and how the IPBA? What do you think other people should know about the IPBA?**

Before I joined the IPBA, I worked at the same firm as a capital market lawyer (this is the same until now) and raised two children. The reason why I joined the IPBA was very simple. Hara-san, the ex-Japan JCM and our firm's managing partner, introduced the IPBA to me and I thought that the IPBA must be a nice organisation because Hara-san, whom I highly respected,

recommended the IPBA to me. Soon after I joined, I realised that the IPBA is a very unique organisation with a lot of interesting and friendly and powerful members, especially women. If a business lawyer would like to make friends outside of his or her home country, I definitely recommend the IPBA.

## What is the biggest challenge you have faced to date and how did you overcome it?

The biggest challenge I have faced may be raising children while continuing practice as a capital market lawyer which is time-consuming and filled with many thick documents and great time pressure. I cannot remember how I coped during the days with small children, but everyone helped me, my husband (a good cook), my parents-in-law who lived next door to us (who took care of the children at night), the small kindergarten within three minutes walk (which offered the Montessori method to children), my parents in Kagoshima (who took care of the children at Kagoshima in the spring or summer breaks) and housekeeping service providers. I should thank all of them from the bottom of my heart.

## Have you faced gender-related challenges in your career? If so, what have they been and how have you overcome the adversities?

No, not at all. Fortunately, I have enjoyed my career with wonderful senior and junior colleagues and clients and have never faced any problem related to gender. But in order to avoid such situations, when I became a lawyer, I carefully selected the field and the firm.

## What advice or tips you can provide, on managing a work/life balance, especially for women in law?

We have just 24 hours a day and just one body, so it is better to rely on support from others in terms of work, housekeeping and raising children. It is very important to keep in good health and mental condition to enjoy our busy life. If I do everything only by myself, I could not maintain this. In this connection, I also believe that a feeling of gratitude to others who help us is also important.

## The pandemic changed the world as we know it—everyone working from home and a general heightened state of anxiety. How has this disrupted your work/life balance and how have you overcome those challenges?

I do not think the pandemic disrupted my work because I could continue working at the same level even at home with the full assistance of IT. Before the pandemic, we could not work at home efficiently because of a lack of many functions, but after the pandemic, many legal and other services which enable us to work at home developed rapidly. The pandemic forced us to look for ways to help us do things, rather than to look for excuses as to why we can't do something.

## If you were the leader of a country of your choice, what would you do?

Tough question. I have never thought of this type of question but, if anything, I would like to eliminate every kind of discrimination.

## Finally, some quick questions…
## What is a motto you live by?

Where there is a will, there is a way.

## What would you say to your 20-year old self?

Work hard, play hard.

## Cats or dogs?

I may be a cat. But I like both cats and dogs.

## If I could be a superhero, I would be...

I would be a gorgeous super model like Cindy Crawford!

# IPBA New Members November 2020 to February 2021

We are pleased to introduce our new IPBA members who joined our association from November 2020 to February 2021. Please welcome them to our organisation and kindly introduce yourself at the next IPBA conference.

| | |
|---|---|
| **Argentina**, Fernando Liu<br>*Marval, O'Farrell & Mairal* | **France**, Anais Bove<br>*BOVE LAW OFFICE, Inc.* |
| **Belgium**, XiufangTu<br>*Monard Law* | **France**, Wissam Mghazli<br>*W.M Avocats* |
| **Canada**, Ruzbeh Hosseini<br>*Cambridge LLP* | **Hong Kong**, Richard Lyons<br>*Hill Dickinson Hong Kong* |
| **Canada**, Barbara Miller<br>*Fasken Martineau DuMoulin LLP* | **Hong Kong**, Alex May<br>*Hill Dickinson Hong Kong* |
| **Canada**, David Ward<br>*Miller Thomson LLP* | **India**, Gautam Bhatikar<br>*Phoenix Legal* |
| **China**,Wang Hongmei<br>*Hebei Sanhe Shidai Law Firm* | **India**, Ritika Ganju<br>*Phoenix Legal* |
| **China**, Wencong Li<br>*Jin Mao Partners* | **India**, Satish Triplicane Damodaran<br>*Sarvada Legal* |
| **China**, Zhe Liu<br>*Grandall Law Firm (Shijiazhuang Office)* | **Italy**, Maria Francesca Lanzio<br>*Studio Lanzio Pelargonio* |
| **China**, Kangwei Pei<br>*Jin Mao Partners* | **Italy**, Giovanni Lovisetti<br>*Dezan Shira & Associates* |
| **China**, Yu Bin Qin<br>*Hebei Jimin Law Firm* | **Italy**, Andrea Rudelli<br>*Studio avv. Andrea Rudelli* |
| **China**, Jingyan Wang<br>*Grandall Law Firm (Shijiazhuang)* | **Japan**, Masahiro Nakatsukasa<br>*Chuo Sogo Law Office, P.C.* |
| **China**,Jing Xu<br>*Beijing Yingke (Shijiazhuang) Law Firm* | **Japan**, Asa Shinkawa<br>*Nishimura & Asahi* |
| **China**, Xiang Xu<br>*Zhe Jiang Z&J Law Firm* | **Japan**, Yo Yamagishi<br>*Miyakezaka Sogo Law Offices* |
| **China**, Wenjun Xu<br>*ANHUI CHENGYI LAW FIRM WUHU OFFICE* | **Netherlands**, Minos van Joolingen<br>*Banning N.V.* |
| **China**, ZianYang<br>*Jin Mao Partners* | **Philippines**, Editha R. Hechanova<br>*Hechanova Bugay Vilchez & Andaya-Racadio* |
| **China**, Yangmin Zhong<br>*Shanghai Kunlun Law Firm* | **Philippines**, Kristine Tupaz-Torres<br>*Gorriceta Africa Cauton & Saavedra Law* |

| | |
|---|---|
| **Russia**, Ekaterina Biruleva Butler<br>*Kaspersky* | **Switzerland**, Fabienne Limacher<br>*Walder Wyss AG* |
| **Russia**, Mikhail Krasilnikov<br>*Law Office Mikhail Krasilnikov &Co.* | **Turkey**, Ismet Mumtaz<br>*Yayan Yayans Law* |
| **Russia**, Andrew Lomas<br>*EPAM Law Offices* | **United Kingdom**, Anastasia Kantzelis<br>*6 Pump Court Chambers* |
| **Singapore**, Wilson Lim<br>*ASIAN ASSETS ALLIANZ PTE LTD, SINGAPORE* | **United Kingdom**, Simon Kerry<br>*Hardwicke Chambers* |
| **Singapore**, Benedict Teo<br>*Drew & Napier LLC* | **United Kingdom**, Carl Wall<br>*4 Pump Court* |
| **Singapore**, Shintaro Uno<br>*Nishimura & Asahi (Singapore) LLP* | **United States**, Thomas Allen<br>*Greenberg Traurig, LLP* |

# Save the dates for the IPBA Virtual Conference

## "Innovative Resilience in an Altered Legal Landscape"
## June 15-19, 2021

Join us for our usual great conference in an exciting virtual environment!

June 15: Opening Ceremony and Plenary Session, followed by a Reception
June 16-18: Three time blocks with 3-4 concurrent sessions, followed by discussion and networking
June 19: IPBA Council Meetings and Annual General Meeting

Plus: Registration for IPBA Tokyo 2022; exhibition booths; and fun activities to keep us entertained and alert

Contact the IPBA Secretariat if you are interested in sponsorship opportunities: ipba@ipba.org

Check the IPBA web site for the latest information: https://ipba.org

# Raise your profile

**Content marketing**

**Advertisement design**

**Event signage**

**Copywriting**

**Corporate newsletters**

**Professional magazines**

ninehills media

T: +852 3796 3060

E: enquiries@ninehillsmedia.com

W: www.ninehillsmedia.com

# Master your career

with the LLM (Applied Law) majoring in ASEAN+6 Cross-Border Legal Practice and Graduate Certificate in Cross-border Transactions.

Key areas of study

- Negotiating and Drafting Cross-border Contracts
- Cross-border Mergers and Acquisitions
- Banking and Finance Practice
- Intellectual Property Practice
- ASEAN+6 Arbitration and Dispute Resolution Practice
- Trade and Investment in Asia
- ASEAN+6 Capital Markets Practice

**Next Intake begins 17 May 2021**

Find out more about the LLM (Applied Law) and the Graduate Certificate here: llm.collaw.edu.au/ASEAN

IPBA INTER-PACIFIC BAR ASSOCIATION

The program has been developed by The College of Law in collaboration with the Inter-Pacific Bar Association.

## Enquire about how to enrol today

Contact us at **colasia@collaw.edu.au**

**Postgraduate Specialisation**
The College of Law