



ABOUT The *Data Bulletin: Informing the implementation of the Global Compact for Migration* series aims to summarize in an accurate and accessible fashion existing evidence on migration to support the discussion and any follow-up activities.

As part of the project “Support to IOM for the Global Compact for Safe, Orderly and Regular Migration,” funded by the European Union, *Data Bulletin* outlines the strengths and limitations of relevant migration data and highlights innovative data practices that are pertinent to the Global Compact for Migration. This publication reflects the collaborative nature of the Global Compact for Migration process by including relevant contributions from different parts of IOM, as well as other agencies and migration experts.

ADVISORY BOARD

Marla Asis (*Scalabrini Migration Centre (SMC), Manila*)
Alexandra Bilak (*International Displacement Monitoring Centre (IDMC), Geneva*)
Marcello Carammia (*European Asylum and Support Office (EASO), Valetta*)
Tony Luka Elumelu (*Economic Community of West African States (ECOWAS) Commission, Abuja*)
Andrew Geddes (*Migration Policy Centre (MPC), European University Institute, Florence*)
Yosr A.A. Ibrahim (*Central Agency for Public Mobilization and Statistics (CAPMAS), Cairo*)
Diego Iturralde (*Statistics South Africa, Pretoria*)
Juan Manuel Jiménez (*Organization of American States (OAS), Washington, D.C.*)
Manuel Orozco (*Inter-American Dialogue, Washington, D.C.*)
Mustafa Hakki Özel (*International Labour Organization (ILO), Geneva*)
Jorge Martínez Pizarro (*Latin American and Caribbean Demographic Centre (CELADE), Economic Commission for Latin America and the Caribbean, Santiago*)
Sonia Plaza (*World Bank, Washington, D.C.*)
Jon Simmons (*UK Home Office, London*)
Ann Singleton (*University of Bristol / IOM’s Global Migration Data Analysis Centre (GMDAC), Berlin*)
Keiko Osaki Tomita (*Tokyo University of Foreign Studies, Tokyo*)
Alessandra Zampieri (*Joint Research Centre, European Commission, Ispra*)

CHIEF EDITOR

Frank Laczko (*IOM’s GMDAC, Berlin*)

Data protection

The New York Declaration for Refugees and Migrants recognized the importance of improved data collection and the enhancement of international cooperation to this end. States specified that data should “be disaggregated by sex and age and include information on regular and irregular flows, the economic impacts of migration and refugee movements, human trafficking, the needs of refugees, migrants and host communities and other issues”. States added that they will work on this consistent with their “national legislation on data protection, if applicable” and their “international obligations related to privacy, as applicable.”¹

In addition, the Global Compact for Safe, Orderly and Regular Migration (GCM) calls for the collection and dissemination of quality data and that the objectives contained in it relating to data collection, disclosure and use should be implemented “while upholding the right to privacy and protecting personal data.”²

In our era of data revolution, big data and artificial intelligence, it is widely accepted that the collection and dissemination of migration data can yield many benefits. However, privacy and data protection considerations need to be at the centre of all data discussions as the risks associated with data processing may be substantial for the data subjects whose personal data are being processed. It is paramount to respect and ensure human dignity and the right to privacy of individuals, a fundamental human right that is not restricted to a country’s own nationals nor to persons with a specific migratory status.

Data protection is the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the collection, storage, use, disclosure and any other type of processing of personal data. The protection of personal data³ of migrants in particular is of fundamental importance as it is an integral part of protecting the life, integrity and human dignity of migrants.

The regulatory framework

The right to privacy is enshrined in several international human rights conventions, such as the Universal Declaration on Human Rights⁴ and the International Covenant on Civil and Political Rights.⁵ Several regional instruments also mention the right to privacy, such as the European Convention

¹ Resolution adopted by the General Assembly on 19 September 2016, Seventy-first session, *New York Declaration for Refugees and Migrants*, A/RES/71/1, available at www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_71_1.pdf (accessed 18 December 2018).

² *Global Compact for Safe, Orderly and Regular Migration*, A/CONF.231/3, Marrakech, Morocco, 10 and 11 December 2018 Item 10 of the provisional agenda, available at <https://undocs.org/A/CONF.231/3> (accessed 18 December 2018).

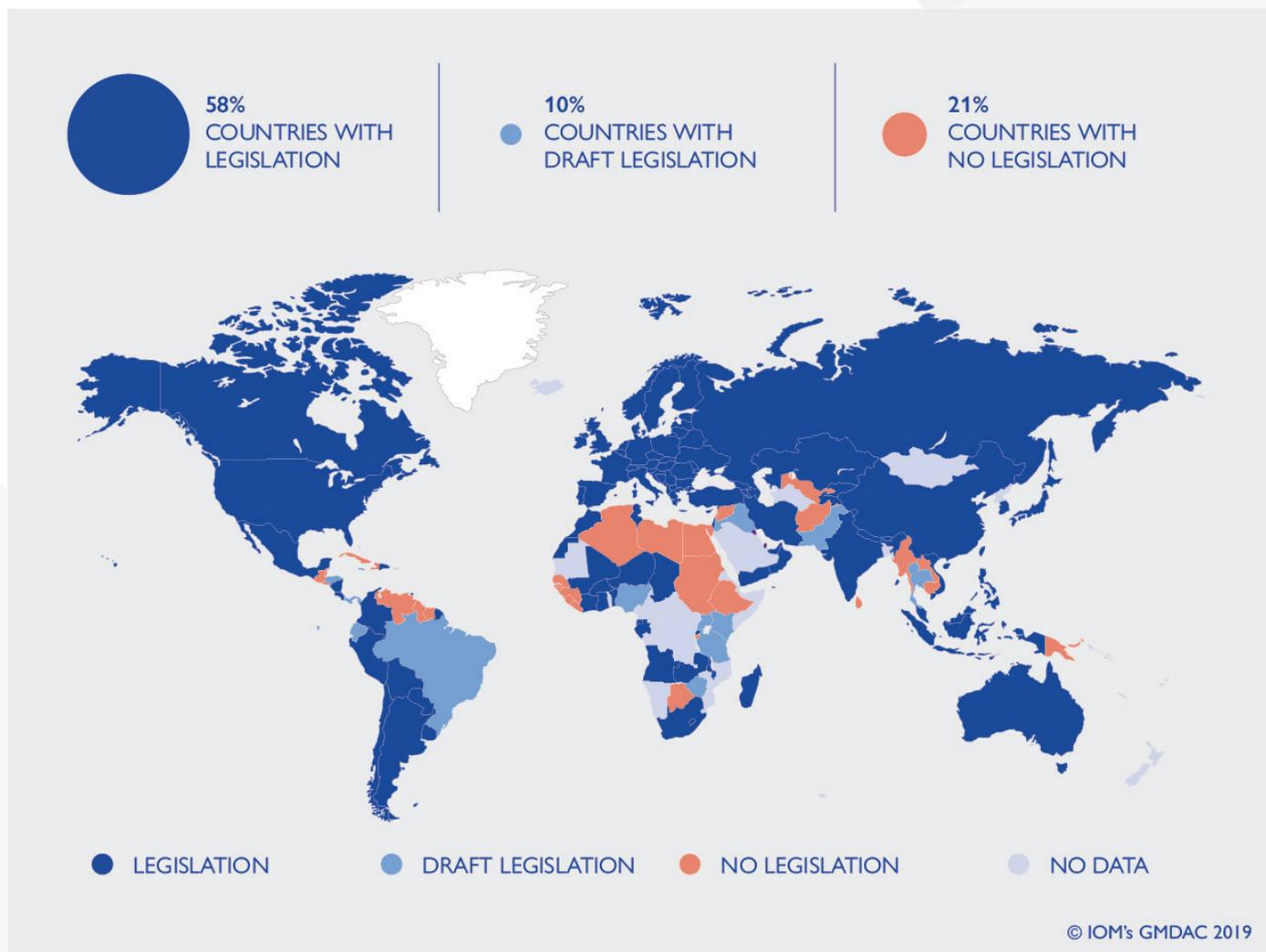
³ Adapted from the *IOM Data Protection Manual*, International Organization for Migration, 2010, available at http://publications.iom.int/system/files/pdf/iomdataprotection_web.pdf (accessed 18 December 2018).

⁴ Article 12 of the *Universal Declaration of Human Rights*, UN General Assembly, 10 December 1948, 217 A (III), available at www.un.org/en/universal-declaration-human-rights/ (accessed 18 December 2018).

⁵ Article 17 of the *International Covenant on Civil and Political Rights*, UN General Assembly, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx (accessed 18 December 2018).



Figure 1: Data protection and privacy legislation worldwide



Source: UNCTAD, Data Protection and Privacy Legislation Worldwide. Available from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

on Human Rights,⁶ the American Convention on Human Rights⁷ and the African Charter on the Rights of the Child.⁸ The EU Charter on Fundamental Rights refers not only to the right to privacy but also to the right to the protection of personal data.⁹

⁶ Article 8 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms*, as amended by Protocols Nos. 11 and 14, Council of Europe, 4 November 1950, ETS 5, available at www.echr.coe.int/Documents/Convention_ENG.pdf (accessed 18 December 2018).

⁷ Article 11 of the *American Convention on Human Rights, "Pact of San Jose"*, Organization of American States (OAS), Costa Rica, 22 November 1969, available at www.cidh.oas.org/basicos/english/basic3.american%20convention.htm (last accessed 18 December 2018).

⁸ Article 10 of the *African Charter on the Rights and Welfare of the Child*, Organization of African Unity (OAU), 11 July 1990, CAB/LEG/24.9/49 (1990), available at: www.achpr.org/instruments/child/ (accessed 18 December 2018).

⁹ Protection of personal data: 1. *Everyone has the right to the protection of personal data concerning him or her; 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; 3. Compliance with these rules shall be subject to control by an independent authority*". Article 8 of European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN> (accessed 18 December 2018).

The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data¹⁰ set the first high-level non-binding international standards on data protection and they were followed by the binding standards of 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (Convention 108).¹¹ The text of Convention 108 has now been modernized and the relevant Protocol¹² has been open for signature since 10 October 2018. The modernization of Convention 108 aims to address innovations in the area of information and communication technology and strengthening its effective implementation. It also has the potential of becoming a binding international standard on data protection as it is open to all countries of the world which meet the required standards.

¹⁰ Organisation for Economic Cooperation and Development (OECD), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September 1980, updated in 2013, available at www.oecd.org/internet/ieconomy/oecdguidelinesontheprivacyandtransborderflowsof-personaldata.htm

¹¹ Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, 28 January 1981, ETS 108, available at www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 (accessed 18 December 2018).

¹² Council of Europe, *Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, available online at <https://rm.coe.int/16808ac918> (accessed 18 December 2018).

The EU General Protection Regulation (GDPR) is considered to be “the most comprehensive and progressive piece of data protection legislation in the world, updated to deal with the implications of the digital age”.¹³ The changes brought to the EU data protection legislation by the GDPR include increased territorial scope, strengthened notion of consent, obligations for data processors, higher penalties for non-compliance, enhanced data subject rights and the inclusion of the concept of privacy by design. The GDPR is the only binding set of norms at the regional level. Although it is a regional instrument its scope stretches beyond Europe as it may be applicable directly or indirectly to entities outside the EU territory.

In addition to the above, more than 100 countries in the world¹⁴ have adopted national data protection legislation, however, privacy and data protection issues are not regulated to the same extent by all of them. Many countries also have an independent data protection authority in place overseeing the implementation of the relevant data protection legislation. Several countries are currently in the process of adopting such legislation.¹⁵

The International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families¹⁶ specifically refers to the right to privacy of all migrant workers and members of their families. Yet, as already mentioned, it is important to keep in mind that irrespective of this reference, the right to privacy is a universal human right to be enjoyed by all human beings, regardless of their migratory status.

Challenges

Firstly, many challenges in the field of privacy and data protection derive from the rapid pace of technological advancements. Technology nowadays is facilitating people’s everyday life, but it also leads to large amounts of personal data being collected and processed in a small amount of time. For example, developments in the Internet of Things technology allow individuals today to monitor and track their physical activity with wearable fitness monitors, turn on the heating or electricity before they arrive home or even remotely unlock their door for visitors if they are not at home. At the same time, devices would be, for example, collecting information about an individual’s heart rate, distance walked in a day, hours of sleep, exact time of leaving and returning home, energy consumption at home and much more. Many migrants are nowadays also using new technologies, especially smartphones with a variety of applications for messaging, video communication, map tracking and social networking. All of these applications collect a vast amount of data and metadata about their users. Laws about how such data are collected, used, shared, or otherwise processed do not always guarantee adequate protection of the right to privacy.

This leads to a second group of challenges which is linked to technology moving at a quicker pace than the law. Even though many States have data protection legislation in place, some of it is not sufficiently updated to take technological advancements

into account. Creating legislation for new technologies is by no means an easy task. Legal gaps are evident, for example, in the case of self-driving cars as most laws are silent on whether it is necessary for a human being to be driving a car. On top of this, self-driving cars raise privacy concerns due to the amount of personal data collected (such as location tracking and sensor data that might include voice recognition devices)¹⁷ and the frequent absence of regulations on how this data should be processed. In a similar vein, the use of unmanned aerial vehicles (UAVs) may interfere with an individual’s privacy. They process more personal data than planes or CCTV and may have a “chilling effect on freedom of expression”.¹⁸ Some States are already using or considering using UAVs in border patrol and surveillance,¹⁹ however several issues remain unclear: How will the data subjects be informed about the processing of their personal data? How will the data collected be shared across borders? Are the principles of necessity and proportionality respected when using UAVs for border control?²⁰ Have privacy by design and by default been incorporated into the process? It is important for States to clarify these and similar issues relating to privacy and data protection prior to using new technologies, such as UAVs.

Thirdly, additional challenges derive from data ethics, which go beyond legal compliance. In today’s digital data-driven world, adherence to the law is not considered to be enough; the ethical dimension of data processing needs to be considered.²¹ Ethical problems concerning data would include, for example, algorithmic biases that might lead to discrimination and perpetuate pre-existing social and cultural biases. Automated decision making is nowadays part of many national immigration systems, predictive policing mechanisms are put in place for security reasons and several biometric recognition software are used at border crossing points. From an ethical point of view, it is crucial that all such initiatives are not only based on robust legal regimes but that they are fair, transparent and impartial. It has been written that there are seven “shifts” that define the new landscape for digital ethics, namely: “from the individual to the digital subject; from analogue to digital life; from governance by institutions to governmentality through data; from a risk society to a scored society; from human autonomy to the convergence of humans and machines; from individual responsibility to distributed responsibility; and from

¹³ Data protection page of the European Data Protection Supervisor (EDPS), available at https://edps.europa.eu/data-protection_en (accessed 18 December 2018).

¹⁴ United Nations Conference on Trade and Development (UNCTAD), Data Protection and Privacy Legislation Worldwide, available at https://unctad.org/en/Pages/DTL/STI_and ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (last accessed 18 December 2018) and Commission nationale de l’informatique et des libertés (CNIL), *Data Protection around the world*, available at www.cnil.fr/en/data-protection-around-the-world (accessed 18 December 2018)

¹⁵ Ibid.

¹⁶ Article 14 of the *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families*, UN General Assembly, 18 December 1990, A/RES/45/158, available at <https://www.ohchr.org/en/professionalinterest/pages/cmaw.aspx> (accessed 18 December 2018)

¹⁷ M. et K. Fenwick, A. Wulf and E., P.M. Vermeulen, *Regulation Tomorrow: What Happens When Technology Is Faster Than the Law?* (2017), American University Business Law Review, Vol. 6, No. 3, 561; U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-20, available at SSRN: <https://ssrn.com/abstract=3204119> (accessed 18 December 2018) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3204119 and <https://www.dataprotectionreport.com/2017/07/the-privacy-implications-of-autonomous-vehicles/>

¹⁸ European Data Protection Supervisor (EDPS), Opinion 4/2015, Towards a new digital ethics, 11 September 2015, page 8 available online at https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf (last accessed 18 December 2018) and Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on “A new era for aviation - Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner”, 26 November 2014, available online at https://edps.europa.eu/sites/edp/files/publication/14-11-26_opinion_rpas_en.pdf (accessed 18 December 2018).

¹⁹ R. Koslowski, and M. Schulzke, Drones Along Borders: Border Security UAVs in the United States and the European Union, *International Studies Perspectives*, Volume 19, Issue 4, 1 November 2018, Pages 305–324.

²⁰ *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*, Article 29 Working Party, adopted on 16 June 2015, available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf (accessed 18 December 2018).

²¹ European Data Protection Supervisor (EDPS), Opinion 4/2015, Towards a new digital ethics, 11 September 2015, page 4, available online at https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf (accessed 18 December 2018).

criminal justice to pre-emptive justice”.²² All these shifts pose ethical challenges in the digital age. The “digital representation” of migrants, for example, may expose them to new forms of vulnerability and harm, especially when highly sensitive personal data of migrants are processed by actors who may not have good intentions.

Conclusion

Despite the increase in regulatory efforts around the world, a lot remains to be done. States are encouraged to ratify Convention 108, if they have not already done so, as a first step towards demonstrating their commitment to strong standards of privacy and data protection. The adoption of comprehensive national data protection legislation together with the creation of an independent data protection authority overseeing the implementation of that legislation is also crucial to ensuring the protection of personal data of all people, including migrants present in the State’s territory.

Efforts to ensure that data protection considerations are taken into account in the development of new technologies need to be strengthened so that intrusion into individuals’ privacy is minimized. The concepts of privacy by design and by default are a step towards that direction. Yet, such concepts are not always included in relevant legislation, and, in cases where they are, they are not always accompanied by clear guidance on how to apply them in practice. Similarly, ethical considerations are not always part of relevant legislation and they end up being part of discussions about policies and guidelines while falling through legal gaps.

In the end, it should be highlighted that at the heart of data protection and privacy is the migrant’s human dignity and these are intricately linked with migrants’ right to a private life, being autonomous and in control of their personal data. Safeguarding the privacy and data protection of migrants is not a problem in that respect but part of the solution.

²² Ethics Advisory Group (EAG) report, European Data Protection Supervisor (EDPS), *Towards a digital ethics*, January 2018, available online at https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf (accessed 18 December 2018).

IOM’s GMDAC

In response to growing calls for better data on migration, and for better use and presentation of migration data, IOM has created the Global Migration Data Analysis Centre (GMDAC).

Located in Berlin, Germany, the Centre aims to provide authoritative and timely analyses of data on global migration issues as a global hub for data and statistics on migration.

For more information, please contact:
IOM’s Global Migration Data Analysis Centre (GMDAC)
Taubenstr. 20–22 | 10117 Berlin, Germany
Tel.: +49 30 278 778 21

GMDAC website: <https://gmdac.iom.int>
Migration Data Portal: <https://migrationdataportal.org>

Author

Christina Vasala Kokkinaki
International Organization for
Migration (IOM) Geneva
cvasala@iom.int

Contact

Marzia Rango
IOM’s GMDAC
mrango@iom.int

Emma Borgnäs
IOM’s GMDAC
eborgnas@iom.int

Mailan Thai
IOM Geneva
mthai@iom.int

The opinions expressed in this data bulletin are those of the author and do not necessarily reflect the views of the International Organization for Migration (IOM). The designations employed and the presentation of material throughout the publication do not imply the expression of any opinion whatsoever on the part of IOM concerning the legal status of any country, territory, city or area, or of its authorities, or concerning its frontiers and boundaries.

This publication has been produced with the assistance of the European Union. The contents of this publication are the sole responsibility of its author(s) and can in no way be taken to reflect the views of the European Union.