Global Data and Cyber Handbook - Philippines

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

# What's new?

## Recently Updated Topics

We highlight the new Anti-Financial Scamming Act, which is a key cybersecurity legislation in the Philippines, especially in view of the large number of financial scams being reported in the Philippines.

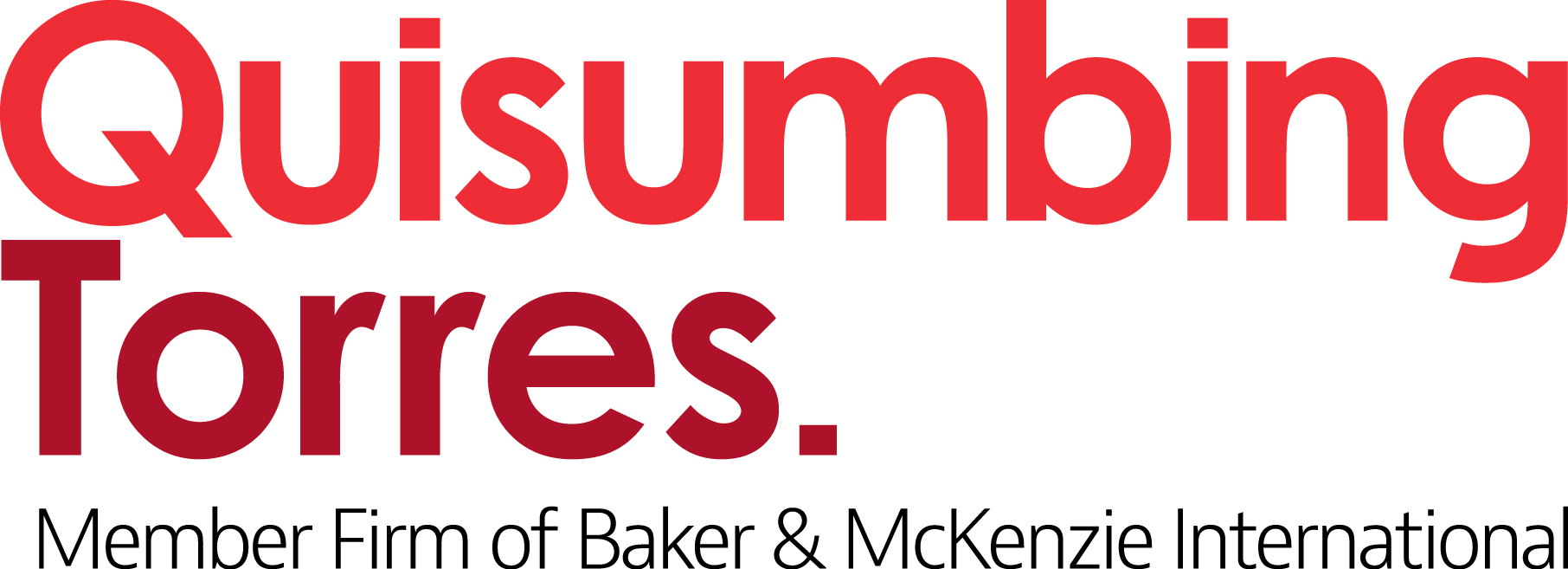
We also discuss the recent issuances of the NPC on security measures, consent, legitimate interest, and child-oriented transparency.

The Artificial Intelligence, Profiling and Automated Decision Making section discusses the new regulations on artificial intelligence by the data privacy regulator and other draft legislations in relation to artificial intelligence regulation.

The Direct Marketing section discusses a recent National Privacy Commission circular, which covers the use of consent and legitimate interest as legal bases to process personal data for direct marketing purposes.

# Key Data & Cyber Contacts

## Contacts



Quisumbing Torres is a member firm of Baker & McKenzie International, a Swiss Verein.

# Key Data & Cybersecurity Laws

## How are data and cybersecurity laws/regulations implemented?

*Last review date: 7 January 2025*

☒         omnibus – all personal data

☒         sector-specific — e.g., financial institutions, governmental bodies

## What are the key data privacy laws and regulations?

*Last review date: 7 January 2025*

[Data Privacy Act](https://www.privacy.gov.ph/data-privacy-act/)

[Implementing Rules and Regulations of the Data Privacy Act](https://www.privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/)

[National Privacy Commission Circulars](https://www.privacy.gov.ph/memorandum-circulars/)

[National Privacy Commission Advisories](https://www.privacy.gov.ph/advisories/)

Decisions of the NPC, Supreme Court, Court of Appeals, and other government bodies

## What are the key cybersecurity laws and regulations?

*Last review date: 7 January 2025*

[Anti-Financial Account Scamming Act](https://lawphil.net/statutes/repacts/ra2024/ra_12010_2024.html) (AFASA)

[Internet Transactions Act](https://www.officialgazette.gov.ph/downloads/2023/12dec/20231205-RA-11967-FRM.pdf)

[Implementing Rules and Regulations of the Internet Transactions Act](https://www.dti.gov.ph/sdm_downloads/implementing-rules-and-regulations-of-the-internet-transactions-act-of-2023/)

[Implementing Rules and Regulations of the Expanded Anti-Trafficking in Persons Act](https://www.officialgazette.gov.ph/2023/03/18/2022-implementing-rules-and-regulations-of-republic-act-r-a-no-9208-the-anti-trafficking-in-persons-act-of-2003-as-amended-by-r-a-no-10364-the-expanded-anti-trafficking-in-persons-act-of/)

[Cybercrime Prevention Act](https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/)

[Implementing Rules and Regulations of the Cybercrime Prevention Act](https://www.officialgazette.gov.ph/2015/08/12/implementing-rules-and-regulations-of-republic-act-no-10175/)

[Rule on Cybercrime Warrants](https://sc.judiciary.gov.ph/1420/)

[Budapest Convention on Cybercrime](https://legacy.senate.gov.ph/17th_congress/resolutions/resno89.pdf)

[Electronic Commerce Act](https://lawphil.net/statutes/repacts/ra2000/ra_8792_2000.html)

[Implementing Rules and Regulations of the Electronic Commerce Act](https://www.bfar.da.gov.ph/wp-content/uploads/2021/04/Electronic-Commerce-Act-of-2000-R.A.-8792-Implementing-Rules-and-Regulations.pdf)

[Anti-Online Sexual Abuse or Exploitation of Children and Anti-Child Sexual Abuse or Exploitation Materials Act](https://lawphil.net/statutes/repacts/ra2022/ra_11930_2022.html)

[Access Devices Regulation Act](https://lawphil.net/statutes/repacts/ra1998/ra_8484_1998.html)

[Anti-Photo and Video Voyeurism Act](https://lawphil.net/statutes/repacts/ra2010/ra_9995_2010.html)

[Subscriber Identity Module (SIM) Registration Act](https://www.officialgazette.gov.ph/downloads/2022/10oct/20221010-RA-11934-FRM.pdf)

[Mobile Number Portability Act](https://lawphil.net/statutes/repacts/ra2019/ra_11202_2019.html)

[Philippine Central Bank Circular No. 1019, series of 2018 on Technology and Cyber-Risk Reporting and Notification Requirements](https://www.bsp.gov.ph/Regulations/Issuances/2018/c1019.pdf)

[Philippine Central Bank Circular No. 982, series of 2017 on Enhanced Guidelines on Information Security Management](https://www.bsp.gov.ph/Regulations/Issuances/2017/c982.pdf)

[Philippine Central Bank Circular No. 808, series of 2013 on Guidelines on Information Technology Risk Management for All Banks And Other BSP Supervised Institutions](https://www.bsp.gov.ph/regulations/issuances/2013/c808.pdf)

[Philippine Department of Information and Communications Technology (DICT) Memorandum Circular No. 005 on Prescribing the Policies, Rules and Regulations on the Protection of Critical Infrastructure (CII) Stipulated in the National Cybersecurity Plan (NCSP) 2022](https://dict.gov.ph/wp-content/uploads/2017/09/Memorandum-Circular-005.pdf)

[DICT Memorandum Circular No. 006 on Prescribing the Policies, Rules and Regulations on the Protection of Government Agencies Stipulated in the National Cybersecurity Plan (NCSP) 2022](https://dict.gov.ph/wp-content/uploads/2017/09/Memorandum-Circular-006.pdf)

[DICT Memorandum Circular No. 007 on Prescribing the Policies, Rules and Regulations on the Protection of Individuals Stipulated in the National Cybersecurity Plan (NCSP) 2022](https://dict.gov.ph/wp-content/uploads/2017/09/Memorandum-Circular-007.pdf)

[DICT Department Circular No. 2017-002 on Prescribing the Philippine Government's Cloud First Policy](https://dict.gov.ph/wp-content/uploads/2017/02/Signed_DICT-Circular_2017-002_CloudComp_2017Feb07.pdf)

## What are the key laws and regulations relating to non-personal data?

*Last review date: 7 January 2025*

[Revised Penal Code](https://lawphil.net/statutes/acts/act_3815_1930.html)

[Civil Code of the Philippines](https://lawphil.net/statutes/repacts/ra1949/ra_386_1949.html)

[Intellectual Property Code](https://lawphil.net/statutes/repacts/ra1997/ra_8293_1997.html)

[Philippine Competition Act](https://lawphil.net/statutes/repacts/ra2015/ra_10667_2015.html)

[Implementing Rules and Regulations of the Philippine Competition Act](https://www.phcc.gov.ph/storage/pdf-resources/1683854994_20210528_PCC-Legal-Handbook-RA-10667-IRR.pdf)

[Cybercrime Prevention Act](https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/)

[Implementing Rules and Regulations of the Cybercrime Prevention Act](https://www.officialgazette.gov.ph/2015/08/12/implementing-rules-and-regulations-of-republic-act-no-10175/)

[Electronic Commerce Act](https://lawphil.net/statutes/repacts/ra2000/ra_8792_2000.html)

[Implementing Rules and Regulations of the Electronic Commerce Act](https://www.bfar.da.gov.ph/wp-content/uploads/2021/04/Electronic-Commerce-Act-of-2000-R.A.-8792-Implementing-Rules-and-Regulations.pdf)

[Commission on Elections Resolution No. 11064 on Guidelines on the Use of Social Media, Artificial Intelligence, and Internet Technology, for Digital Election Campaign, and the Prohibition and Punishment of its Misuse for Disinformation, and Misinformation, in Connection with the 2025 National and Local Elections and the BARMM Parliamentary Elections](https://comelec.gov.ph/php-tpls-attachments/2025NLE/Resolutions/com_res_11064.pdf)

[NTC Memorandum Circular No. 02-05-2008 on Value Added Services](https://region7.ntc.gov.ph/wp-content/uploads/2024/01/MC_02-05-2008_VAS.pdf)

[NTC Memorandum Circular No. 03-03-2005-A on Broadcast Messaging](https://region7.ntc.gov.ph/wp-content/uploads/2024/01/MC_03-03-2005A_Amendments_broadcast_messaging.pdf)

[FDA Administrative Order No. 2020-0010 on Regulations on the Conduct of Clinical Trials for Investigational Products](https://www.fda.gov.ph/wp-content/uploads/2020/05/Administrative-Order-2020-0010.pdf)

FDA Circular No. 2020-03 on Guidelines for Pharmaceutical Industry for Pharmacovigilance

## Are new or material changes to those key data and cybersecurity laws anticipated in the near future?

*Last review date: 7 January 2025*

Yes.

There are pending bills before the Philippine Congress that seek to amend the Philippine Data Privacy Act (DPA). Please note that all the pending amendatory bills are currently in the first reading (initial stage) and have not been certified as urgent by the Philippine President to date.

Some of the notable changes sought to be introduced by these amendatory bills include:

Excluding from the scope of the DPA any processing of personal data that is necessary to address a health crisis upon a declaration of a national health emergency or pandemic

Including biometric data for the purpose of uniquely identifying a natural person in the definition of sensitive personal information

Defining the digital age of consent to process personal information to more than 15 years old, which will be applicable where information society services are provided and offered directly to a child (as children more than 15 years old under Philippine laws may already act with discernment).

In addition, the Philippine government, specifically the Department of Information and Communications Technology, is currently pushing the Philippine Congress to pass a comprehensive law on cybersecurity.

Finally, we anticipate that the Philippine government will release the implementing rules and regulations of the AFASA within the year.

# Regulators, Enforcement Priorities and Penalties

## Who are the main data privacy, non-personal data and/or cybersecurity regulator(s) in the jurisdiction?

*Last review date: 7 January 2025*

[The Philippine National Privacy Commission (NPC)](https://www.privacy.gov.ph/advisories/)

[Department of Information and Communications Technology](https://dict.gov.ph/)

[National Cybersecurity Inter-Agency Committee](https://lawphil.net/executive/execord/eo2019/pdf/eo_95_2019.pdf)

[Department of Justice – Office of Cybercrime](https://cybercrime.doj.gov.ph/)

[Cybercrime Investigation and Coordinating Center](https://cicc.gov.ph/), which coordinates cooperation among the following agencies:

[Bureau of Immigration](https://immigration.gov.ph/)

[Philippine Drug Enforcement Agency](https://pdea.gov.ph/)

[Bureau of Customs](https://customs.gov.ph/)

[National Prosecution Service](https://www.doj.gov.ph/national-prosecution-service.html)

[Anti-Money Laundering Council](http://www.amlc.gov.ph/)

[Securities and Exchange Commission](https://www.sec.gov.ph/)

[National Telecommunications Commission](https://ntc.gov.ph/)

## How active is each of the regulator(s)?

*Last review date: 7 January 2025*

☒ Very active

## What are each of the regulator's anticipated enforcement priorities for the next 12 months?

*Last review date: 7 January 2025*

The key priorities of the National Privacy Commission are:

Conduct both online and on-site compliance checks

Investigation of targeted smishing attacks and other financial-related scams

Coordination with local telecommunications companies concerning the implementation of the SIM Registration Act

Takedown of online lending apps that violate Philippine data privacy regulations

## What trends are you seeing in regulatory investigations relating to data & cyber?

*Last review date: 7 January 2025*

Regulatory investigations or direct enforcement activity by data or cyber regulators are:

☒         Common

Class actions/group actions under data or cyber regulation are:

☒         Rare

## What are the potential penalties/remedies for non-compliance with the key data and cybersecurity laws in the jurisdiction?

*Last review date: 7 January 2025*

There are:

☒         administrative remedies / civil penalties applied by regulators and law enforcement

The NPC shall perform all acts as may be necessary to effectively implement the DPA, its IRR, and its other issuances and to enforce its Orders, Resolutions or Decisions, including the imposition of administrative sanctions, fines, or penalties. This includes:

Issuing compliance or enforcement orders

Awarding indemnity on matters affecting any personal data, or rights of data subjects

Issuing cease and desist orders or imposing a temporary or permanent ban on the processing of personal data upon finding that the processing will be detrimental to national security or public interest, or if it is necessary to preserve and protect the rights of data subjects

Recommending to the Department of Justice (DOJ) the prosecution of crimes and imposition of penalties specified in the Act

Compelling or petitioning any entity, government agency, or instrumentality, to abide by its orders or take action on a matter affecting data privacy

Imposing administrative fines for violations of the DPA, its IRR, and other issuances of the NPC

Additionally, the NPC recently issued Circular No. 2022-01 on the imposition of administrative fines. In light of said circular, the NPC may now impose administrative fines ranging from 0.5% to 3% of the annual gross income of the PIC or PIP in case of grave infractions and 0.25% to 2% of the annual gross income of the PIC or PIP in case of major infractions.

A grave infraction is committed when:

There is an infraction of any of the general privacy principles in the processing of personal data pursuant to Section 11 of the DPA, where the total number of affected data subjects exceeds 1,001 or more.

There is an infraction of any of the data subject rights pursuant to Section 16 of the DPA, where the total number of affected data subjects exceeds 1,001 or more.

There is a repetition of the same infraction penalized under the circular, regardless of whether the first infraction was classified as a major or other infraction.

A major infraction is committed when:

There is an infraction of any of the general privacy principles in the processing of personal data pursuant to Section 11 of the DPA, where the total number of affected data subjects is 1,000 or below (1-1,000).

There is an infraction of any of the data subject rights pursuant to Section 16 of the DPA, where the total number of affected data subjects is 1,000 or below (1- 1,000).

There is a failure on the part of the PIC to implement reasonable and appropriate measures to protect the security of personal information pursuant to Section 20 (a), (b), (c), or (e) of the DPA.

There is a failure on the part of the PIC to ensure that third parties processing personal information on its behalf shall implement security measures pursuant to Section 20 (c) or (d) of the DPA.

There is a failure on the part of the PIC to notify the NPC and affected data subjects of personal data breaches pursuant to Section 20 (f) of the DPA, unless otherwise punishable by Section 30 of the DPA.

In both cases, the computation shall be based on the PIC's or PIP's annual gross income of the immediately preceding year when the infraction occurred. Note that for purposes of said computation, the NPC may require the PIC or PIP to submit its audited financial statement filed with the appropriate tax authorities for the immediately preceding year when the infraction occurred, its last regularly prepared balance sheet or annual statement of income and expenses, and such other financial documents as the NPC may deem relevant and appropriate. However, where the PIC or PIP has not been operating for more than one year, the basis for the NPC's computation will be its gross income at the time the infraction was committed.

The NPC is also empowered to impose administrative fines for other infractions, including the failure to register the true identity or contact details of the PIC, the data processing system, or information on automated decision-making which can reach up to either PHP 200,000 (approximately USD 4,000) or PHP 50,000 (approximately USD 1,000), depending on the violation committed.

Notwithstanding the foregoing, please note that the total imposable administrative fine for a single act or omission of a PIC or PIP, whether resulting in a single or multiple infractions, shall not exceed PHP 5 million (approximately USD 100,000).

☒         criminal penalties from regulators and law enforcement

The following are the criminal penalties:

**Unauthorized Processing of Personal Information and Sensitive Personal Information**

The unauthorized processing of personal information shall be penalized by imprisonment ranging from one to three years and a fine of PHP 500,000 to PHP 2,000,000 shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under the DPA or any existing law.

The unauthorized processing of personal sensitive information shall be penalized by imprisonment ranging from three to six years and a fine of PHP 500,000 to PHP 4,000,000 shall be imposed on persons who process personal information without the consent of the data subject, or without being authorized under the DPA or any existing law.

**Accessing Personal Information and Sensitive Personal Information Due to Negligence**

Accessing personal information due to negligence shall be penalized by imprisonment ranging from one to three years and a fine of PHP 500,000 to PHP 2,000,000 shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under the DPA or any existing law.

Accessing sensitive personal information due to negligence shall be penalized by imprisonment ranging from three to six years and a fine of PHP 500,000 to PHP 4,000,000 shall be imposed on persons who, due to negligence, provided access to personal information without being authorized under the DPA or any existing law.

**Improper Disposal of Personal Information and Sensitive Personal Information**

The improper disposal of personal information shall be penalized by imprisonment ranging from six months to two years and a fine of PHP 100,000 to PHP 500,000 shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

The improper disposal of sensitive personal information shall be penalized by imprisonment ranging from one to three years and a fine of PHP 100,000 to PHP 1,000,000 shall be imposed on persons who knowingly or negligently dispose, discard or abandon the personal information of an individual in an area accessible to the public or has otherwise placed the personal information of an individual in its container for trash collection.

**Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes**

The processing of personal information for unauthorized purposes shall be penalized by imprisonment ranging from one year and six months to five years and a fine of PHP 500,000 to PHP 1,000,000 shall be imposed on persons processing personal information for purposes not authorized by the data subject, or otherwise authorized under the DPA or under existing laws.

The processing of sensitive personal information for unauthorized purposes shall be penalized by imprisonment ranging from two to seven years and a fine of PHP 500,000 to PHP 2,000,000 shall be imposed on persons processing sensitive personal information for purposes not authorized by the data subject, or otherwise authorized under the DPA or under existing laws.

**Unauthorized Access or Intentional Breach**

The penalty of imprisonment ranging from one to three years and a fine of PHP 500,000 to PHP 2,000,000 shall be imposed on persons who knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information is stored.

**Concealment of Security Breaches Involving Sensitive Personal Information**

The penalty of imprisonment of one year and six months to five years and a fine of PHP 500,000 to PHP 1,000,000 shall be imposed on persons who, after having knowledge of a security breach and of the obligation to notify the NPC, intentionally or by omission conceals the fact of such security breach.

**Malicious Disclosure**

Any personal information controller or personal information processor or any of its officials, employees or agents, who, with malice or in bad faith, discloses unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her, shall be subject to imprisonment ranging from one year and six months to five years and a fine of PHP 500,000 to PHP 1,000,000.

**Unauthorized Disclosure**

Any personal information controller or personal information processor or any of its officials, employees or agents, who disclose to a third party personal information not covered by the immediately preceding section without the consent of the data subject, shall he subject to imprisonment ranging from one to three years and a fine of PHP 500,000 to PHP 1,000,000.

Any PIC or PIP or any of its officials, employees or agents, who disclose to a third party sensitive personal information not covered by the immediately preceding section without the consent of the data subject, shall be subject to imprisonment ranging from three to five years and a fine of PHP 500,000 to PHP 2,000,000.

**Combination or Series of Acts**

Any combination or series of acts as defined in Sections 25 to 32 will subject the person to imprisonment ranging from three to six years and a fine of PHP 1,000,000 to PHP 5,000,000.

☒         private remedies

The NPC, *sua sponte*, or persons who are the subject of a privacy violation or personal data breach, or who are otherwise personally affected by a violation of the Data Privacy Act, may file complaints for violations of the DPA. The person who is the subject of the privacy violation or personal data breach, or their duly authorized representative may file the complaint, provided that the circumstances of the authority must be established.

Any person who is not personally affected by the privacy violation or personal data breach may: (a) request for an advisory opinion on matters affecting the protection of personal data; or (b) inform the NPC of the data protection concern, which may in its discretion, conduct monitoring activities on the organization or take such further action as may be necessary.

## If data subjects have private remedies, what form can these remedies take?

*Last review date: 7 January 2025*

☒         individual personal actions

☒         representative actions (e.g., brought by a consumer / data privacy body or the supervisory authority)

☒         class actions

# Key Definitions

## Personal data

*Last review date: 7 January 2025*

"Personal data" refers to all types of personal information, which, in turn, refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

## Sensitive/special personal data (including personal data subject to additional protections/ restrictions/breach notification obligations)

*Last review date: 7 January 2025*

Sensitive data includes:

☒         personal data revealing racial or ethnic origin

☒         personal data revealing political opinions

☒         personal data revealing religious or philosophical belief

☒         genetic data

☒         biometric data for the purpose of uniquely identifying a natural person or biometric templates

☒         data concerning health/medical information

☒         data concerning a natural person's sex life or sexual orientation

☒         government identity card or number information

☒         personal data regarding an individual's criminal convictions or record

## Controller vs Processor

*Last review date: 7 January 2025*

Do the privacy laws distinguish between controllers/owners and processors/agents? Whereby:

The controller/owner is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

The processor/agent is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**Answer:** Yes.

# Territorial Scope

## What is the territorial reach of the data privacy and cybersecurity laws?

*Last review date: 7 January 2025*

☒         applies to organizations located in the jurisdiction

☒         no express territorial scope, but would require some nexus to the jurisdiction

# Legal Bases for Processing of Personal Data

## Is an identified legal basis required in order to collect or process non-sensitive personal data?

*Last review date: 7 January 2025*

Yes.

The following are potential legal bases for processing personal data:

☒         the data subject has provided consent to the processing for the identified purposes

☒         the personal data is necessary to perform a contract with the data subject

☒         the personal data is necessary to comply with a legal obligation

☒         the personal data is necessary to protect the vital interests of a natural person

☒         the personal data is necessary for a public interest

☒         the personal data is necessary to fulfil a legitimate interest of the controller or third party (provided that the interest is not overridden by the data subject's privacy interests and the data subject has not made use of his/her right to object)

## Is an identified legal basis required in order to collect or process sensitive personal data?

*Last review date: 7 January 2025*

☒ Yes

The Privacy Act does not make specific reference to "sensitive personal data." The same matters that apply to "non-sensitive data" will apply.

The following are potential legal bases for processing special categories of personal data:

☒         the data subject has given consent to the processing, where consent is measured to a higher standard than for non-sensitive personal data (for example, additional requirement for consent to be "explicit")

☒         processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

☒         processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and further conditions

☒         processing is necessary for the establishment, exercise or defense of legal claims

☒         processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

## Are there special requirements that apply to the collection or processing of personal data from minors?

*Last review date: 7 January 2025*

Yes. If a Personal Information Controller (PIC) processes a minor’s personal data on the basis of consent, the PIC must obtain parental consent, as a minor is legally incapable of providing valid consent under Philippine data privacy regulations.

## In what circumstances do these special requirements apply?

The requirement of parental consent only applies in case the PIC will rely on consent as its legal basis to process the minor’s personal data.

*Last review date: 7 January 2025*

☒         generally

☒         other

Minors are considered vulnerable data subjects. The processing of their information is considered likely to pose a risk to their rights and freedoms. Consequently, PICs that process the sensitive personal information or information that may enable identity fraud of minors are likely to be covered by personal data breach notification obligations in case of confidentiality breaches of such data.

## What are the special requirements that apply to collecting or processing personal data from minors?

*Last review date: 7 January 2025*

☒         consent must be given or authorized by the parent/ guardian of the minor

☒         other

In case of a personal data breach involving minors, notification must be made to both the minor and their parents or guardians.

# Information Requirements, Data Subject Rights, Accountability and Governance

## What information needs to be included in a privacy notice to data subjects?

*Last review date: 7 January 2025*

☒         the identity and the contact details of the controller and, where applicable, of the controller's representative

☒         the contact details of the data protection officer, where applicable

☒         the purposes of the processing for which the personal data is intended

☒         the legal basis for the processing

☒         the categories of personal data concerned

☒         the recipients or categories of recipients of the personal data, if any

☒         information regarding data transfers to third countries, where applicable, and reference to appropriate or suitable safeguards and the means by which by to obtain a copy of them or where they have been made available

☒         the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

☒         the existence of data subjects' rights, such as the right to access, rectification, erasure, data portability, etc.

☒         how the data is held

☒         the security provided to the data

☒         the right to lodge a complaint with a supervisory authority

☒         if applicable, information regarding automated decision making, including profiling

## Do data subjects have specific privacy rights that must be operationalized?

*Last review date: 7 January 2025*

Yes.

Data subjects have the following data privacy rights, although the specifics of the scope and conditions for each of these vary depending on the circumstances and local law:

☒         right to access the data subject's own personal data

☒         right to rectify/correct the data subject's own personal data where inaccurate or incomplete

☒         right to erasure of personal data

☒         right to data portability

☒         right to object to the processing of personal data

☒         right to withdraw consent

☒         other

e.g., right to indemnity, right to file a complaint with the National Privacy Commission

## Are there accountability and governance requirements?

*Last review date: 7 January 2025*

Yes.

There are accountability and governance requirements to:

☒         take privacy by default and design measures for all processing of personal data

This should take into account [NPC Advisory No. 2023-01](https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Advisory-No.-2023-01-Guidelines-on-Deceptive-Design-Patterns_7Nov23.pdf) on Guidelines on Deceptive Design Patterns.

☒         perform and document data protection impact assessments (DPIAs) for high-risk processing:

[NPC Circular No. 2023-06](https://privacy.gov.ph/wp-content/uploads/2024/03/NPC-Circular-Repeal-16-01-Signed.pdf?fbclid=IwAR2ikCb192s8AFsM5Ep88BGbn9y4tTydkaKAOt5O2XMXI8K7e6mKHPsYq10) requires controllers and processors to conduct a privacy impact assessment (PIA) for every processing system that involves the processing of personal data, regardless of the risk.

☒         maintain a record of processing activities

☒         implement appropriate measures to comply with data privacy and cybersecurity

☒         demonstrate compliance with data privacy and cybersecurity

☒         identify a specific individual as the data privacy contact for data subject or data protection authority inquiries

☒         provide training to employees

☒         audit or supervise data processors

# DPOs and Notification Requirements

## Is the concept of data protection officer (DPO) recognized in the jurisdiction?

*Last review date: 7 January 2025*

Yes.

## Are there circumstances in which it is mandatory to appoint a DPO or similar position?

*Last review date: 7 January 2025*

Yes.

If yes, under what circumstances?

☒         other

It is mandatory for a Personal Information Controller (PIC) or Personal Information Processor (PIP) to designate an individual or individuals who shall function as a Data Privacy Officer (DPO).

## Where a DPO is appointed, does the DPO have to meet specific requirements?

*Last review date: 7 January 2025*

Yes.

If yes, what are these requirements?

☒         other professional qualifications / experience

☒         other

Familiarity with the personal data processes and policies of the PIC or PIP of which they are the DPOs.

## Are there obligations to notify, submit filings to, register with or obtain approval from local data protection authorities to collect and/or process personal data generally?

*Last review date: 7 January 2025*

Yes.

PICS and PIPs that have personal data processing systems operating in the country and (a) have at least 250 employees; (b) involve accessing or requiring sensitive personal information of at least 1,000 individuals, or (c) belong to any of the industries or business sectors listed by the NPC (government agencies, financial institutions, medical and educational institutions, business process outsourcing companies, etc.) as subject to the [registration requirement](https://privacy.gov.ph/wp-content/uploads/2023/05/Circular-2022-04-2.pdf), are required to register their DPO with the NPC. Data Processing Systems (DPS) that process personal or sensitive personal information involving automated decision-making or profiling must also be registered with the NPC. The registration is subject to the approval of the NPC.

# Data Processors

## Are there obligations for controllers to establish controls with respect to data processors?

*Last review date: 7 January 2025*

Yes.

The obligations are as follows:

☒         controllers must conduct due conduct diligence on the processor to ensure it will provide appropriate security and processing of the personal data

☒         controllers must only use processors subject to a written agreement that complies with specific requirements

## Are there any direct regulatory or statutory requirements on processors?

*Last review date: 7 January 2025*

Yes.

Personal information processors are likewise required to implement the organizational, physical, and technical security measures enumerated under Sections 25, 26, 27, 28 of the Implementing Rules and Regulations (IRR) of the DPA for the confidentiality, integrity, and availability of the personal information they process on behalf of personal information controllers. Under Section 29 of the IRR, the NPC will monitor compliance by the PICs and PIPs with the required security measures.

# International Data Transfer

## Are there restrictions on the transfer of personal data to third countries?

*Last review date: 7 January 2025*

Yes.

The Data Privacy Act does not define the word "third country." Rather, it uses the term "cross border" in discussing the transfer of personal data to other countries.

Transfers of personal data to third countries are only permissible if there is a legal basis for the processing/transfer and one of the following applies:

☒         approved standard contractual clauses

☒         binding corporate rules

***Please see separate question for information on data localization provisions that are not restricted to personal data.***

# Cookies, Online Tracking and Direct Marketing

## Are there specific requirements for the use of cookies and other online tracking technologies?

*Last review date: 7 January 2025*

No.

## Are there specific requirements related to the use of personal data for direct marketing activities?

*Last review date: 7 January 2025*

Yes.

**☒         email marketing**

☒         prior opt-in consent

☒prior existing business relationship (and subject to other requirements) with opt-out consent

**☒         telephone marketing**

☒         prior opt-in consent

☒         prior existing business relationship (and subject to other requirements) with opt-out consent

**☒         SMS/text message marketing**

☒         prior opt-in consent

☒         prior existing business relationship (and subject to other requirements) with opt-out consent

**☒         postal marketing**

☒         prior opt-in consent

☒         prior existing business relationship (and subject to other requirements) with opt-out consent

**☒**         **online behavioral advertising targeting/social media targeting/ad personalization marketing**

☒         prior opt-in consent

☒         prior existing business relationship (and subject to other requirements) with opt-out consent

[NPC Circular No. 2023-04](https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Circular-No.-2023-04_Guidelines-on-Consent_07Nov2023.pdf) states that when processing non-sensitive personal information, a controller may consider direct marketing as a legitimate interest, which would not require the consent of the data subject, provided that the controller conducts a legitimate interest assessment (LIA). If the LIA reveals that legitimate interest cannot be made the basis for processing, the controller may still process the personal data on the basis of consent. In case consent is relied upon by the controller as its legal basis for processing and such consent is withdrawn by the data subject, the controller cannot claim legitimate interest to continue the processing activity.

Additionally, in an [office advisory](https://privacy.gov.ph/wp-content/uploads/2023/11/Advisory-Opinion-No.-2023-016.pdf) issued by the NPC, the NPC reiterated that the DPA does not consider a soft opt-in approach as valid consent, and hence PICs and PIPs have to rely on the other lawful criteria for processing: (1) the legitimate interest is established; (2) the processing is necessary to fulfill the legitimate interest that is established; and (3) the interest is legitimate or lawful and it does not override fundamental rights and freedoms of data subjects.

# Data Processing in the Employment Context

## Is an identified legal basis required in order to collect or process personal data or sensitive personal data in the employment context?

*Last review date: 7 January 2025*

Yes.

## Can consent be validly obtained in the employment context?

*Last review date: 7 January 2025*

☒         Yes, same as for data subjects outside the employment context.

Yes, consent may be validly obtained in the employment context for as long as the employee's consent is freely given, specific, informed, and recorded. The consent should also be time-bound, and in case of processing of sensitive personal information, it should also specify the purposes of processing to which the employee consents.

## Has the data privacy regulator issued guidance on use of artificial intelligence, automated decision making or profiling in an employment context – for example, relating to use in employee monitoring or hiring?

☒         Yes

If yes, please provide a link.

[NPC Advisory No. 2024-04 on Guidelines on the Application of the Data Privacy Act, its Implementing Rules and Regulations, and the Issuances of the National Privacy Commission to Artificial Intelligence Systems Processing Personal Data](https://privacy.gov.ph/wp-content/uploads/2024/12/Advisory-2024.12.19-Guidelines-on-Artificial-Intelligence-w-SGD.pdf)

[NPC Circular No. 2023-04 on Guidelines on Consent](https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Circular-No.-2023-04_Guidelines-on-Consent_07Nov2023.pdf), particularly Section 18 on Profiling and Automated Processing

[NPC Advisory Opinion No. 2024-005 on Use of Artificial Intelligence in Call Analysis and Monitoring of Call Center Employees](https://privacy.gov.ph/wp-content/uploads/2024/05/Advisory-Opinion-No.-2024-005.pdf)

[NPC Advisory Opinion No. 2024-002 on Request for Comments/Insights Regarding the Use of Artificial Intelligence in the Civil Service Commission’s Correspondence](https://privacy.gov.ph/wp-content/uploads/2024/01/Advisory-Opinion-No.-2024-002.pdf)

[NPC Advisory Opinion No. 2017-041 on Profiling of Individuals and Collection of Personal Information Based on Publicly Available Data](https://privacy.gov.ph/wp-content/uploads/2022/01/NPC_AdvisoryOpinionNo._2017-041.pdf)

[NPC Advisory Opinion No. 2017-008 on Clarifications on the Data Privacy Act and Its Implementing Rules and Regulations](https://privacy.gov.ph/wp-content/uploads/2022/01/NPC_AdvisoryOpinionNo._2017-008.pdf)

# Artificial Intelligence, Profiling and Automated Decision Making

## Are there any restrictions or requirements related to creating profiles of data subjects or utilizing automated decision-making for decisions related to data subjects, including with respect to artificial intelligence?

*Last review date: 7 January 2025*

Yes.

The restrictions or requirements are as follows:

☒         qualified right not to be subject to a decision based solely on automated decision making, including profiling – for example, only applicable if the decision produces legal effects concerning them or similarly significantly affects them

☒         right to information / transparency requirement

☒         right to request human review of the automated decision making

☒         other

Data subjects have a right to be informed about whether their personal data is being processed, or will be processed, including any automated decision-making and profiling activities.

Likewise, the data subject has the right to object and withhold consent for the processing of their data for direct marketing, automated processing, or profiling purposes.

Furthermore, PICs are required to implement mechanisms that allow data subjects to question and contest automated decisions, especially when such decisions pose a significant risk to their rights and freedoms.

## If such restrictions or requirements exist, are they subject to any exceptions?

*Last review date: 7 January 2025*

Yes.

The following are the exceptions:

The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract

When necessary for compliance with a legal obligation applicable to the PIC

When the data subject provides consent

## Has the data privacy regulator issued guidance on data privacy and artificial intelligence, automated decision-making or profiling?

*Last review date: 7 January 2025*

☒         Enforcement activity under existing privacy law

## Has the data privacy regulator taken enforcement action in relation to artificial intelligence, including automated decision-making or profiling?

*Last review date: 7 January 2025*

Yes

***If yes, please provide brief details and a link.***

The NPC recently issued [Advisory No. 2024-04](https://privacy.gov.ph/wp-content/uploads/2024/12/Advisory-2024.12.19-Guidelines-on-Artificial-Intelligence-w-SGD.pdf), which provides guidance on the responsible development and deployment of AI systems that process personal data.

The NPC likewise issued [Circular No. 2022-04](https://privacy.gov.ph/wp-content/uploads/2023/05/Circular-2022-04-2.pdf), requiring the registration of personal data processing systems including the notification regarding automated decision-making or profiling.

Further, the NPC issued [Circular No. 2023-04](https://privacy.gov.ph/wp-content/uploads/2023/11/NPC-Circular-No.-2023-04_Guidelines-on-Consent_07Nov2023.pdf) on the guidelines of consent, requiring the PICs engaged in profiling and automated processing to inform the data subject of these activities and provide specific details before or at the next practical opportunity. PICs should obtain the consent of the data subject when automated processing is the sole basis for a decision that has legal effects or may significantly affect the data subject. They must also ensure safeguards against the harms of extensive profiling, such as discriminatory outcomes and infringement on the right to fair treatment.

## Do other (non-personal data or cybersecurity) laws or regulations impose restrictions on use of artificial intelligence, automated decision-making or profiling?

*Last review date: 7 January 2025*

☒         Draft legislation in progress

☒         Non-binding guidance or principles issued or in progress

***If yes, please provide brief details and a link.***

As mentioned above, the NPC recently issued [Advisory No. 2024-04](https://privacy.gov.ph/wp-content/uploads/2024/12/Advisory-2024.12.19-Guidelines-on-Artificial-Intelligence-w-SGD.pdf), which provides guidance on the responsible development and deployment of AI systems that process personal data.

Further, there are certain draft legislations in Congress aimed at ensuring that personal data collected through Artificial Intelligence is protected in accordance with the DPA. Pending bills include:

[House Bill No. 7396 or the Artificial Intelligence Development and Regulation Act of the Philippines](https://hrep-website.s3.ap-southeast-1.amazonaws.com/legisdocs/basic_19/HB07396.pdf)

[House Bill No. 7913 or the Artificial Intelligence (AI) Regulation Act](https://hrep-website.s3.ap-southeast-1.amazonaws.com/legisdocs/basic_19/HB07913.pdf)

[House Bill No. 9448 or the Protection of Labor Against Artificial Intelligence (AI) Automation Act.](https://hrep-website.s3.ap-southeast-1.amazonaws.com/legisdocs/basic_19/HB09448.pdf)

# Data privacy and cybersecurity in a transactional context

## Has the data privacy authority issued any guidance on data privacy compliance in the context of transactional activity (including, but not limited to, share sales, asset sales, reorganizations or spinouts)?

*Last review date: 7 January 2025*

☒         No

## In the context of an asset sale (the sale of a separate business unit as a going concern), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the assets that are the subject of the asset sale)?

*Last review date: 7 January 2025*

☒         It depends (for example, on the way the asset sale is structured, and/or the assets being acquired)

In its [Office Advisory Opinion No. 2022-010](https://privacy.gov.ph/wp-content/uploads/2022/08/Advisory-Opinion-No.-2022-010-Final-sgd_Redacted.pdf), the NPC advised that the transfer of the personal information of the data subjects to the purchaser is subject to the scope, method, purpose, and extent of the processing as contained in the terms and conditions, privacy policies, and policies on the processing of information provided by the seller to their data subjects at the time the consent was given remains the same, the consent given by the data remains to be valid as well.

## If so, how would any regulatory fines be calculated?

*Last review date: 7 January 2025*

☒         Unclear

## In the context of a share sale (where the acquiring entity acquires 100% of the shares of a target company), does the acquiring entity inherit liability for pre-acquisition data privacy or cybersecurity breaches (connected with the target company)?

*Last review date: 7 January 2025*

☒         It depends (for example, on the way the share sale is structured)

The juridical entity of the target company, being separate from that of owners of its shareholdings, will retain the liability for any data privacy and cybersecurity breaches regardless of transfers of its shareholdings.

## If so, how would any regulatory fines be calculated?

*Last review date: 7 January 2025*

☒         Based on a metric other than those outlined above

# Security Requirements and Breach Notification

## Do data privacy laws or regulations impose obligations to maintain information security controls to protect personal data from unauthorized access or processing?

*Last review date: 7 January 2025*

Yes.

☒         general obligation to take appropriate / reasonable technical, physical and/or organizational security measures

☒         obligation to take specific security measures e.g., encryption

☒         requirement to undertake third party due diligence (security assessment of third party providers)

Please note that [NPC Circular No. 2023-06](https://privacy.gov.ph/wp-content/uploads/2024/03/NPC-Circular-Repeal-16-01-Signed.pdf?fbclid=IwAR2ikCb192s8AFsM5Ep88BGbn9y4tTydkaKAOt5O2XMXI8K7e6mKHPsYq10) sets out the minimum security requirements to protect personal data. The circular applies to both private and public sector entities.

## Do other laws or regulations impose obligations to protect systems from cyberattack?

*Last review date: 7 January 2025*

☒         financial services requirements

☒         providers of critical infrastructure

## Has there been regulatory activity – including enforcement action, investigations, regulatory guidance or other public statements by the regulator – relating to cybersecurity by the following regulators in the last 12 months?

☒         Data privacy

☒         Securities or public company

☒         network information security

☒         health

☒         financial services

☒         telecommunications

☒         critical infrastructure

☒         other

## Does data privacy or cybersecurity law impose obligations to make notifications about personal data security breaches?

*Last review date: 7 January 2025*

Yes.

"Personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

The obligation to notify the NPC and affected data subjects of a personal data breach arises if all of the following conditions are met:

The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" includes: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like PhilHealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

There is reason to believe that the information may have been acquired by an unauthorized person.

The personal information controller or the NPC believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

## Controllers/Owners have to notify:

*Last review date: 7 January 2025*

☒         data protection authorities

The PIC should notify the NPC within 72 hours of having knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred.

Moreover, the PIC should notify the NPC by submitting a report, whether written or electronic, containing the required contents of notification within 72 hours of the detection of the breach. The report should also include the name of a designated representative of the PIC, and their contact details.

☒         affected individuals

The PIC should notify the affected data subject within 72 hours of having knowledge of, or when there is reasonable belief by the PIC or PIP that, a personal data breach requiring notification has occurred.

In cases where the affected data subjects are minors, the PIC should notify both the children and their parents or guardians.

## Processors/Agents have to notify:

*Last review date: 7 January 2025*

☒         controller/ owner

To facilitate the timely reporting of a personal data breach, the PIC should use contractual or other reasonable means to require the PIP to report any knowledge or reasonable belief that a personal data breach has occurred. The PIP should promptly report this to enable the PIC to comply with its obligation to notify the data protection authorities and affected individuals within 72 hours of detection of the breach.

## Are there any additional sector-specific or non-personal data security breach notification requirements?

*Last review date: 7 January 2025*

Yes.

☒         financial services requirements

**Obligations of institutions supervised by Bangko Sentral ng Pilipinas (BSIs)**

The Bangko Sentral ng Pilipinas supervises the operations of banks and exercises regulatory powers over finance companies and non-bank financial institutions performing quasi-banking functions, in accordance with the New Central Bank Act and other pertinent laws.

**Details regarding the identified data security breach notification requirements**

An information security incident or security breach refers to security events that have a significant probability of compromising business operations and threatening the confidentiality, integrity, or availability of a BSI's information system(s). All BSIs should report any cybersecurity issues to the Bangko Sentral ng Pilipinas within two hours of first detection and submit an updated report within 24 hours.

# Data localization and regulation of non-personal data

## Are there data localization/data residency or other types of laws that may require the retention and storage of data in the local jurisdiction, or prohibit the transfer of data out of the jurisdiction?

*Last review date: 7 January 2025*

There are currently no data localization requirements under Philippine data privacy regulations (except for certain types of government data), but there are restrictions to cross-border data transfers.

## Does law or regulation impose mandatory requirements to share or make accessible non-personal data?

*Last review date: 7 January 2025*

☒         Obligation for private organizations to share or make accessible other non-personal data

***If so, please provide brief details of the relevant law or regulation.***

Under the Implementing Rules and Regulations of the Cybercrime Prevention Act, Philippine law enforcement authorities, upon securing a court warrant, can require any person or service provider to disclose or submit, within 72 hours from receipt of an order, subscriber’s information, traffic data, or relevant data in its possession or control, in relation to a valid complaint officially docketed and assigned for investigation by law enforcement authorities, and the disclosure of which is necessary and relevant for the purpose of investigation.

## What specific obligations do these data-sharing rules impose on private organizations?

*Last review date: 7 January 2025*

☒         Obligation to share data on request

Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership:** This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising:** This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction:** Reproduction of reasonable portions of the Content is permitted provided that (i) such reproductions are made available free of charge and for non-commercial purposes, (ii) such reproductions are properly attributed to Baker McKenzie, (iii) the portion of the Content being reproduced is not altered or made available in a manner that modifies the Content or presents the Content being reproduced in a false light and (iv) notice is made to the disclaimers included on the Content. The permission to re-copy does not allow for incorporation of any substantial portion of the Content in any work or publication, whether in hard copy, electronic or any other form or for commercial purposes.