Data Protection Information Notice for Employees and Candidates

March 2026

Introduction

Waystone are a financial services company operating in Europe, the United States, Canada, Bermuda, the Cayman Islands, the United Arab Emirates and Asia, Waystone have separate legal entities in each location who employ individuals.

This Employee and Candidate Data Protection Information Notice ("**Notice**") sets out details of how Waystone processes your personal data when you apply for a position and/or you are employed by a Waystone legal entity("**Waystone**", "**we**", "**us**", "**our**"), we do this in compliance with our obligations under applicable data protection law. This Notice explains what personal data is collected, the purposes for which it is processed, the third parties to whom it may be disclosed and how individuals can exercise their rights in relation to their personal data.

The identity and contact details of the relevant Waystone Data Controller applicable to you will be provided at the point of application or engagement, or on request.

Waystone has a Global Data Privacy Team, to assist with all data privacy matters. In addition, we have appointed a Data Protection Officer (or equivalent) where we have a legal obligation to do so, in a particular jurisdiction and for certain prescribed processing activities. If you have any questions about the use of your personal data, your data protection rights or if you want to exercise those rights, please contact dataprotection@waystone.com.

Scope

This Notice applies to you, whether you are an applicant, a current (or former) employee, partner, worker, intern, transition year student, secondee, temporary worker, agency worker, consultant, contractor, applicant or director. It also applies to third parties whose information you provide to us in connection with our relationship with you (for example, in respect of emergency contact information). Please ensure that you provide a copy of this Notice to any third parties whose personal data you provide to us.

Where we refer to 'employee personal data' or 'employment' in this Notice, we do so for convenience only, and this should in no way be interpreted as purporting to confer employment status on non-employees to whom this Notice also applies. This Notice does not form part of any contract of employment and does not confer any contractual right on you or place any contractual obligation on us.

It applies to all personal data collected, maintained, transmitted, stored, retained, or otherwise used (i.e. processed) by us regardless of the media on which that personal data is stored.

This Notice reflects the requirements of Article 13 and 14 of Regulation (EU) 2016/679 General Data Protection Regulation (the 'GDPR'), which is our base line for the protection of personal data in Waystone.

However, there may be differences in the way in which this protection is applied in the jurisdiction in which you are located, which, if not explicitly specified here, will be advised to you by the Data Privacy Team and the People & Talent ("P&T") team. You will find in Schedule 1 a list of data protection legislation that applies in our different jurisdictions. In the event of a conflict between the GDPR and the local data protection legislation, the local data protection legislation will prevail.

Personal Data that we Process

'Personal Data' is defined as any data relating to an individual who can be identified directly from that data or indirectly in conjunction with other information. We hold some or all of the types of personal data set out in Appendix 1, in relation to you.

Waystone collects personal data relating to you from you or from public sources in connection with our relationship, and to ensure compliance with our legal obligations. In addition, we may collect personal data relating to you from third party sources, such as specialist databases, or sources for vetting or screening purposes or fitness and probity assessments or from employment or credit reference agencies or previous employers. We collect this personal data to meet our requirements to comply with laws and regulations related to anti-money laundering, taxation, right to work and other applicable legislation. We may also collect special categories of data which will afford a higher level of protection.

Purposes of Processing and Legal Basis

We will process your personal data for the purposes for which it was initially collected, unless it is necessary to process it for another purpose that is compatible with the original purpose. In the event that we intend to process your personal data for a purpose that it is not related to the original purpose, we may obtain your explicit consent, or we will identify and rely upon a legal provision that authorises the new processing. The method and requirements for obtaining consent may vary depending on the jurisdiction in which you are located, and we will ensure compliance with local laws where applicable.

Personal data may be processed for the following purposes and on the legal grounds set out below:

Purpose	Legal Basis
• processing your application with us and during the recruitment process, to assess your suitability for a role, establishing your identity and determining the terms on which you work with us and to manage an effective recruitment process; • during our relationship for normal P&T management and administration purposes, ensuring that the terms and conditions of your appointment are properly adhered to and managed, to manage the relationship in accordance with relevant policies. • paying you and (where relevant) deducting tax and national insurance and other mandatory or optional contributions; • paying expenses that you have incurred during the course of your work with Waystone. • conducting performance reviews, managing performance and determining performance requirements including decisions about promotions and pay reviews; • to pay trade union premiums or register your status as a protected employee; • making decisions about our relationship, to properly manage the termination of our relationship and ensuring the termination of our relationship is in accordance with relevant policies;	Processing is necessary to take steps at your request prior to entering into a contract; Processing is necessary for the performance of the employment contract;

Purpose	Legal Basis
• maintaining appropriate business records; • ensuring network and information security, including preventing unauthorised access to our computer and electronic communications system and preventing malicious software distribution; • education, training and development requirements; • assessing your fitness to work, providing appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits • providing you with building and IT access • monitoring use of IT and communications in accordance with our information security policies and standards; • keeping attendance records; • organising business travel, accommodation, arranging visas and permits, conference and event management including offsites; • keeping records of gifts and entertainments offered and received; • providing compensation and benefit plans administration services, and assist Waystone and other Group Companies in discharging essential functions regarding its compensation and benefit plans; • providing health insurance for employees and their dependents; and • administering employment/contract termination.	
• for quality control, business and statistical analysis, market research or for tracking fees and costs or for customer service, training and related purposes; • from time to time external service providers (processors) may process limited categories of your personal data, for example your name, job role, work email address, for their own analytics (service-improvement or diagnostic purposes), where this is	Processing is necessary for the purposes of our legitimate interests or the legitimate interests of a third party to whom your personal data is provided. We will not process your personal data for these purposes if our or the third party's legitimate interests should be overridden by your own

Purpose	Legal Basis
expressly permitted under contractual terms and is compatible with applicable data protection law; • sharing within Group Companies for the purposes of global processes, group-wide reporting and human resource management; • administering and monitoring your professional obligations; • using closed-circuit television (CCTV) to assist in the investigation of security incidents and to promote and protect the health and safety of individuals; • using photographs on Waystone websites, Waystone materials and on certain applications such as email and Teams; • for staff welfare, cultural, sports and social programmes and activities; • providing references; • communicating with you pursuant to our constitution or circulating reports or other correspondence to you; responding to, evaluating or dealing with any queries, complaints or legal issues in relation to you; • undertaking internal and external audits, compliance monitoring and, where necessary, investigations; • In the context of a business or group company sale, re-organisation or restructuring or corporate finance activities; • Maintaining emergency contact details; • Accessing your email account during periods of leave or absence for purpose of ensuring that we are aware of all business emails and that our records of business correspondence is complete. This may also include situations where you are unexpectedly out of the office for an extended period; • Using room and desk booking software; • Recording and transcribing Teams calls, when indicated at the start of a meeting, for stated purposes; • Viewing/accessing your work calendar and emails for the purpose of checking availability for work related tasks or for client billing purposes; • Contacting you to advise of major incident.	interests or fundamental rights and freedoms. The legitimate interests pursued by us in this regard include: ○ Conducting our business in a responsible and commercially prudent manner and dealing with any disputes that may arise; ○ Preventing, investigating or detecting theft, fraud or other criminal activity; ○ Promoting Waystone, our services, capabilities, and employees; ○ Pursuing our corporate and social responsibility objectives; ○ Maintaining our client relationships. ○ Operational resiliency in event of an incident.

Purpose	Legal Basis
• to ensure your health and safety at work, • establishing, exercising, defending or gathering evidence, including through discovery processes, in relation to any legal claims, litigation or grievances, or disciplinary hearings; • complying with our legislative and regulatory obligations in connection with our dealings with you, including pension law, revenue law, health and safety law, right to work, taxation, crime-detection, prevention, investigation and prosecution, the prevention of fraud, bribery, anti-corruption, tax evasion, market abuse, conflicts of interest or equivalent, to prevent the provision of financial and other services to those who may be subject to economic or trade sanctions, in response to legal or court requests or requests from regulatory authorities or where it is in the public interest; • to comply with our obligations under data protection laws in the event that we are required to respond to a data subject access request; • to communicate with you by way of notice pursuant to applicable legislation; • where required for tax reporting purposes; • equal opportunities monitoring; • to process your visa application and arrange insurance cover; • to afford natural justice and fair procedures (where relevant); • to submit applications for supervisory approval for certain prescribed roles in financial services; • to comply with our obligation to keep records of telephone conversations and/or electronic communications involving actual or potential investment decisions or client orders, as required by investment adviser legislation e.g. MiFID II, and SEC/FINRA rules.	Processing is necessary to comply with our legal obligations;
• to share personal data in exceptional circumstances e.g. for medical care purposes, and where you are incapable of giving consent.	In exceptional circumstances, where the processing is necessary to protect your vital interests (or someone else's interests).

Purpose	Legal Basis
• to process dependent visa applications; • office access control using biometrics; • driver collection and drop off using home address; • receiving birthday greetings; • get well/celebratory greetings using home address.	In certain limited circumstances, your consent.

Where legitimate interests are not recognised as a lawful basis under applicable local law, processing will instead be carried out on the basis of contractual necessity, legal obligation, or other lawful grounds permitted in that jurisdiction.

How we use special categories of personal data

Waystone will not process special category personal data, unless one of the following circumstances is met:

- Where it is necessary for the purposes of complying with our obligations and exercising our specific rights, or yours, in the field of employment and social security and social protection law; where it is necessary to protect your vital interests or that of someone else where the data subject is physically or legally incapable of giving consent;
- Where it is needed in the public interest, or is requested by a law authority;
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards;
- Where it is necessary for the purpose of or in connection with any legal claims and proceedings, or to obtain legal advice.
- Where you have already made the information public;
- Where Waystone is subject to a due diligence process and provides professional experience details of senior management or key individuals in the business; and
- In certain circumstances with your explicit written consent.

Security and Storage of Personal Data

We securely store your personal data in a centralised database, with controlled access to that database. Access to personal data (including special category personal data) in both electronic and paper form is restricted to members of the P&T Team and employees who have a legitimate and justifiable reason to view such data.

Recipients of your Personal Data

Your personal data may be disclosed to various recipients in connection with the above purposes, including:

- Your reporting Manager, other members of the Executive Team, the P&T teams within the different Waystone entities, across all our jurisdictions;
- Other Waystone entities who are either the provider or recipient of intragroup services;
- The Board of a Waystone legal entity and (in circumstances where there is legitimate interest, performance of a contract or legal obligation) other employees, in relation to the P&T activities of Waystone;
- Clients who may request your personal data as part of their due diligence on Waystone;
- Third parties who may assist us with recruitment;
- Third parties to assist in the administration, processing and management of certain activities pertaining to past, current and prospective employees e.g. employee share option schemes, payroll providers, pension and health insurance providers, pensions trustee;
- Individuals or companies employed by Waystone in respect of business travel, accommodation and event organisation;
- Health Insurance providers;
- Providers of employee benefit schemes such as cycle to work scheme in the United Kingdom;
- Auditors;
- Trade Unions (if applicable in your jurisdiction);
- Tax authorities in your jurisdiction as required by applicable law;
- Financial regulators in your jurisdiction including but not limited to the Central Bank of Ireland, Cayman Islands Monetary Authority, the Financial Conduct Authority, National Futures Association, Commission de Surveillance du Secteur Financier, Dubai Financial Services Authority (DIFC), the Malta Financial Services Authority, the Financial Services Regulatory Authority (ADGM) in the UAE, Monetary Authority of Singapore and Securities & Futures Commission;
- Industrial relation bodies or tribunals, Courts, mediation bodies, pension authorities in your jurisdiction and Court-appointed persons;
- Relevant and applicable Government departments and agencies in your jurisdiction;
- Other third parties who we engage to provide services to us, such as building landlords, professional advisers, independent investigators, insurers, occupational health specialists, legal advisers, auditors, IT consultants, IT providers, and IT software as a service (SaaS) providers;
- Screening and other reference agencies in order to carry out identity and money laundering checks to comply with legal and regulatory obligations;
- Other third parties in order to obtain pre-employment references from other employers and where we are requested to provide references to future employers;

- Learning and development providers e.g. professional bodies, external training, conferences organisers;

- Relatives or legal representatives of past, current and prospective employees; and

- Potential purchasers or bidders of Waystone.

Transfers Abroad

In connection with the above purposes your personal data may be transferred, stored and processed outside of the jurisdiction where you have applied or where you are employed.

This may be to a jurisdiction which is not recognised by the European Commission or other data protection supervisory authorities outside the EU, as providing for an equivalent level of protection for personal data as that in the GDPR or their local legislation.

Waystone operates globally and these jurisdictions may include the United States of America, the Cayman Islands, Bermuda, the United Arab Emirates and Asia. If and to the extent that we do transfer data to these locations, we will ensure that appropriate measures are in place to protect the privacy and integrity of such personal data and in particular will comply with our obligations under GDPR or other local data protection legislation, governing such transfers, which may include the "standard contractual clauses" approved for this purpose by the European Commission or other local data protection supervisory authorities.

Retention

We will retain your personal data for the duration of our relationship and for such a period of time as required to satisfy the purpose for which the data was collected and used, unless a longer period is necessary to comply with our obligations under applicable law and, if relevant, to deal with any claim or dispute that might arise. This means that for employees we will retain your data for a period of at least seven years post-termination of your employment contract, and for unsuccessful candidates for twelve months from the date the position was filled (or longer if there is a claim of legal action), in accordance with our record retention policy.

Automated decision-making

Automated decision-making refers to the process where decisions are made by systems or algorithms without direct human intervention.

You will not be subject to any decisions with a significant impact on you that are based solely on automated decision-making processes unless we have a lawful basis for such actions and have provided you with appropriate notice. At this time, we do not anticipate that any decisions regarding you will be made using automated means. However, should this position change, we will notify you accordingly.

Your Rights

You have the following rights, in certain circumstances and subject to applicable exemptions, in relation to your personal data:

- the right to information about our processing of your personal data;

- the right to access the personal data processed;

- the right to rectify any inaccuracies in your personal data;

- the right to have any incomplete personal data completed;
- the right to erase your personal data (in certain specific circumstances);
- the right to request that your personal data is no longer processed for particular purposes (in certain specific circumstances);
- where the legal basis for processing is consent, the right to withdraw your consent at any time;
- the right to object to the use of your personal data or the way in which it is processed where we have determined it to be necessary for the purposes of our legitimate interests;
- the right to data portability (in certain specific circumstances);
- the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you (in certain specific circumstances);
- to lodge a complaint with a supervisory authority, in particular in the European Member State of your habitual residence, place of work or place of the alleged infringement if you consider that the processing of personal data relating to you infringes the GDPR, or your local data protection legislation. A list of the relevant supervisory authorities and their contact information is included in Appendix 2.

These are the main Data Subject Rights set out under the GDPR, some of which are also recognised outside the EU/EEA. Additional rights exist in these jurisdictions, and the key ones are listed below in the relevant jurisdictional sections in Appendix 2.

However, not all of these rights are absolute and may be restricted in certain circumstances prescribed by the GDPR and/or the applicable data protection legislation in your jurisdiction. We will advise you if such circumstances arise in relation to your request to exercise your rights.

If you wish to exercise any of your rights in this regard, please contact dataprotection@waystone.com. We will acknowledge your request and endeavour to respond to your request within one month. That period may be extended by two further months where necessary, taking into extent the complexity and number of requests. If this is the case, you will be informed. We may request proof of identification to verify your request, if necessary.

What happens if you do not provide us with your information

If we believe that we require relevant information to effectively and properly manage our relationship, we may not be able to continue our relationship with you, e.g. process your job application or (in certain circumstances) to pay you or administer your pension, if you decline to provide us with that personal data. We will tell you when we ask for information which is a statutory or contractual requirement or needed to comply with our legal obligations.

Changes to this Notice

We reserve the right to update this Notice at any time. We will provide an updated Notice to employees through the usual internal channels which are in use at the time of said update. For those who were

candidates but not employees or those who are no longer employees we will provide a copy of the Notice on reasonable request to the P&T Team.

Further Information

If you require any further clarification regarding this Notice, please contact either a member of your local P&T Team or contact dataprotection@waystone.com.

Appendix 1

General Personal Data

Personal – Recruitment related data and information on your personnel file - these include your name, signature, postal address, email address, mobile and land line numbers, fax number, date and place of birth, nationality, equal opportunities, credit history, references, work and educational history, right to work documentation, passport number, utility bills (for proof of address), photographic identification and verification such as copies of your passport, passport number, gender, drivers licence , photographs, emergency contact details, marital status, next of kin and family details.

Professional – Curriculum Vitae and/or application form, cover letter, previous employment background, references from previous employers, background reference check including credit check, directorships, shareholdings, , record of interview/interview notes, selection and verification records, psychometric tests, educational details, professional and/or academic transcripts, professional certifications, special skills , information about disciplinary and grievance process, language skills, memberships of committees or other bodies.

Employment – work contact details (corporate email address and telephone number), identification number, photograph, videos, business cards, details regarding the job function, primary work location, start date, working hours, employment status, your terms and conditions of employment or engagement, contract of employment, trade union membership and deductions, notice period, signed confidentiality agreement, immigration status, visa, relocation assistance including taxation, work permit details, job description, history and details of current position, employee survey data.

Premises and IT access – information required to access company systems and applications such as email account and system passwords, login and access records, download and print records, call recordings, records of email and internet usage in accordance with our email and internet policy, CCTV images captured through the legitimate use of CCTV within Waystone, car type and registration plate.

Fees, remuneration and benefits – fees/payment and benefits package, base salary, bonus, compensation type, long term incentives, employee share option schemes, long service, pension scheme, PRSA, health insurance scheme (and any third-party beneficiaries), company credit card data, salary reviews, payment of expenses.

Travel – Organising business travel, accommodation, arranging visas and permits; passports, dates of travel, flights, car and taxi hire, hotels, meal, dietary requirements, entertainment, credit cards and out of pocket expenses.

Leave – including documentation which may be provided in connection with any statutory leave, sick leave, holiday and family related leave records such as maternity, carer's, parental and adoptive, garden leave, and any other type of leave such as study leave, force majeure.

Payroll information – these include your national insurance number, bank account details, salary arrangements, bonus entitlements and tax allowances.

Performance, grievance and disciplinary details – these include performance and grievance review forms, notes from performance review and grievance investigation meetings, performance improvement and grievance plan documentation, witness statements, complaints.

Training and development – such as data relating to training and development needs, or training received.

General correspondence/meetings – relating to grievance and/or disciplinary processes, misconduct or performance issues, data arising in connection with litigation and complaints, involvement in incident reporting and disclosures.

Health & safety – nature of incident, injuries and remediation.

Incapacity - any accommodations or adjustments in connection with any incapacity.

Legal & regulatory –

- securities trading information including information relating to family members and other accounts under employees' control, details of any shares of common stock or directorships;
- Information about outside activities for employees and family members;
- Information about gifts received/given for the employee and family members; and
- Information about potential conflicts with your family members that impact on your role or with Waystone in general;
- Provision of current staff data to whistleblower service provider;
- Documentation containing information relating to Politically Exposed Persons, Financial checks, Bankruptcy, Sanction Lists screening, and Directorship History;
- Letter of Authority;
- Criminal record details, where required for regulatory fitness and probity requirements.

Information obtained through electronic means – these include emails stored in your work email inbox, data relating to your internet browsing history, your use of devices and Apps installed on these devices, your IP address.

Pension details – these include Pension Benefit Contract and Employee plan numbers.

Termination of our relationship – these include resignation letters, exit interviews and reference letters.

Call recordings – We may collect and process personal data relating to you in connection with our relationship, such as via correspondence and calls. Telephone and videoconference calls with you may be recorded for the purposes of record keeping, security and training.

Special Categories of Personal Data

Medical/health information– these include sick certificates, sick leave records, sick pay records, occupational health assessments and health insurance membership applications which may include health information of employees and dependencies.

Special categories of more sensitive personal information – information about your race or ethnicity, religious beliefs, sexual orientation and political opinions, membership of a trade union or equivalent industrial relations body, information about criminal convictions and offences, genetic information and biometric data.

Appendix 2

List of jurisdictions where Waystone has a presence and the applicable data protection legislation and supervisory authorities

Ireland

Legislation

Data Protection Act 2018

the GDPR

Supervisory Authority

Data Protection Commission

Luxembourg

Legislation

Act of 1 August 2018 on the Organisation of the National Commission for Data Protection and Implementing the GDPR (the Act)

the GDPR

Supervisory Authority

National Commission for Data Protection (CNPD)

Bermuda

Legislation

Personal Information Protection Act 2016 (PIPA)

Supervisory Authority

Office of the Privacy Commissioner for Bermuda (PrivCom)

Key Differences from GDPR

- The term 'Personal Information' is used instead of 'Personal Data'.
- 'Data Subject', 'Data Controller' and 'Data Processor' are not defined terms in PIPA. Instead, 'organisation' and 'individual' are used.
- No explicit right to data portability.
- No explicit right not to be subject to automated decision-making including profiling.

- PIPA prohibits an organisation from using sensitive information without lawful authority to discriminate against any person contrary to Part II of the Bermuda Human Rights Act 1981.

Canada

Legislation

Personal Information Protection and Electronic Documents Act 2000 (PIPEDA)

Privacy Act 1985 ('the Privacy Act')

Supervisory Authority

Office of the Privacy Commissioner of Canada (OPC)

Key Differences from GDPR

- The term 'Personal Information' is used instead of 'Personal Data'.
- 'Data Subject', 'Data Controller', and 'Data Processor' are not defined terms in PIPEDA. Instead 'organisation' and 'individual'.
- No explicit right to erasure but organisations are required to erase personal information when the purpose for the processing has been completed.
- No explicit right to restrict processing.
- No explicit right to object, however PIPEDA provides for the right for individuals to withdraw consent at any time subject to legal or contractual restriction and reasonable notice (Schedule 1, Clause 4.3.8).
- No explicit right to data portability.
- No explicit right to not to be subject to automated decision making.

Cayman Islands

Legislation

Data Protection Act (2021 Revision) (the Act)

Data Protection Regulations 2018 (SL 17 of 2019) (the Regulations)

Supervisory Authority

Cayman Islands Ombudsman | Cayman Islands Ombudsman

Key Differences from GDPR

- No explicit right to data portability.

Hong Kong

Legislation

Personal Data (Privacy) Ordinance (Cap. 486) as amended in 2021

Supervisory Authority

The Office of the Privacy Commissioner for Personal Data

For information on the collection of Personal Information and your rights, please refer to this Notice.

United Arab Emirates – Federal

Legislation

Federal Decree-Law No.45 of 2021 Concerning the Protection of Personal Data

Supervisory Authority

UAE Data Office

Key Differences from GDPR

- Legitimate interests is not a valid legal basis.
- Does not make available rights concerning automated decision-making protections and right to restriction of processing.

United Arab Emirates – ADGM

Legislation

Data Protection Regulations 2021

Supervisory Authority

Office of Data Protection (ODP)

United Arab Emirates – DIFC

Legislation

DIFC Data Protection Law No.5 of 2020 (as amended) (the Law)

DIFC Data Protection Regulations

Supervisory Authority

Commissioner of Data Protection

United Kingdom

Legislation

UK GDPR (retained EU law, now domestic UK law)

Data Protection Act 2018

Data (Use and Access) Act 2025 (DUAA)

Supervisory Authority

Information Commissioner's Office

Key Differences from GDPR:

- Introduces “recognised legitimate interests” (e.g. crime prevention, safeguarding, emergency response), which do not require a balancing test.

- Data Subject has right to complain to the organisation processing their personal data, which must be acknowledged within 30 days and responded to without undue delay. (effective June 2026).

USA – New Jersey

Legislation

Act concerning commercial internet websites, online services, consumers, and personal identifiable information (NJDPA)

Supervisory Authority

New Jersey Office of the Attorney General

Key Differences from GDPR

- ‘Data Subject’ is not defined in NJDPA. Instead, ‘Consumer’ is defined as an identified person who is a resident of New Jersey acting only in an individual or household context. It does not include a person acting in a commercial or employment context.

- No explicit right to restrict processing.

- No explicit right to not be subject to automated decision-making, but the NJDPA provides consumers with a right to opt out of processing personal data for the purposes of profiling (Section 7(5) of the NJDPA).

USA – New York

Legislation

Article 5 of the Civil Rights Law regulates civil right to privacy. The Stop Hacks and Improve Electronic Data Security Act 2019, SHIELD Act regulates data breach and data security matters in New York, including data breach requirements, obligations regarding developing security programs, and

enforcement capabilities. The General Business Law of the Consolidated Laws of New York was recently amended in terms of timings of data breach notifications and bodies that must be notified.

Supervisory Authority

New York State AG

Key Differences from GDPR

- A living person's name, portrait, picture, likeness or voice cannot be used for advertising or trade purposes without their consent.
- New York law does not currently provide a mechanism for data access requests.

USA – Illinois

Legislation

Personal Information Protection Act (PIPA)

Biometric Information Protection Act (BIPA)

Supervisory Authority

Office of the Illinois Attorney General

Key Differences from GDPR

- 'Data Subject', 'Data Controller', and 'Data Processor' are not defined terms in PIPA and BIPA. Instead 'data collectors' and 'individuals' or 'consumers'.
- No explicit right to access.
- No explicit right to rectification.
- No explicit right to object, however under the BIPA, individuals have the right to refuse the collection of their biometric data.
- No explicit right to erasure.
- No explicit right to restrict processing.
- No explicit right to data portability.
- No explicit right to not be subject to automated decision making.

India

Legislation

The Digital Personal Data Protection Act 2023 (the Act)

The Digital Data Protection Rules 2025 (the Rules)

Supervisory Authority

Data Protection Board of India (to be established by the Government of India)

Key Differences from GDPR

- Data Principal is the individual to whom the personal data relates to.
- Data Controller: Referred to as a "Data Fiduciary", a person who, alone or in conjunction with other persons, determine the purpose and means of processing of personal data.
- No explicit right to erasure under The SPDI Rules currently, however, the DPDP Act will provide for this right when in effect.
- No explicit right to restrict processing.
- No explicit right to data portability.
- No explicit right to not be subject to automated decision making.
- There are specific limitations to the access rights granted to employees. Employers are not obliged to disclose details about data shared with other data fiduciaries or data processors where such sharing is legally authorised, for example, when data is shared with government authorities for investigations or to comply with legal requirements.

The Philippines

Legislation

The Data Privacy Act of 2012 (Republic Act No. 10173)

Implementing Rules and Regulations of Republic Act No. 10173

Supervisory Authority

National Privacy Commission

Key Differences from GDPR

- Personal information is the term used to refer to personal data.
- Data Controller: Referred to as "Personal Information Controller", a person or organisation who controls the collection, holding, processing, or use of personal information, including a person or organisation who instructs another person or organisation to collect, hold, process, use, transfer, or disclose personal information on their behalf.
- Data processor: Referred to as 'Personal Information Processor', any natural or juridical person qualified to act as such under the Act, and to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
- Right of Access: A data subject may only request access to their own personal data, and this would exclude any analysis made by the controller with respect to the data subject's personal data (i.e. inferred, derived, modelled, or business-generated data).
- No explicit right to restrict processing.

Singapore

Legislation

Personal Data Protection Act 2012 (PDPA)

Personal Data Protection (Amendment) Act 2020

Personal Data Protection Regulations 2021

Supervisory Authorities

Personal Data Protection Commission

For information on the collection of Personal Information and your rights, please refer to this Notice.

Switzerland

Legislation

Federal Act on Data Protection 2020 (FADP)

Ordinance to the Federal Act on Data Protection of 31 August 2022 (the Ordinance)

Swiss Civil Code (the Civil Code)

Supervisory Authority

Federal Data Protection and Information Commissioner (FDPIC)

Key Differences from GDPR

- No explicit right to erasure.
- No explicit right to restrict processing.
- No explicit right to object.
