Data Protection Policy

Version 4.1

Revised: 1/5/2023

Internal Use Only

This document is confidential and designed for use by Epiq personnel. The contents may be shared with other personnel but may not be copied nor shall the document remain on the premise of any party other than Epiq without a valid Non-disclosure Agreement.

Purpose

The purpose of this Data Protection Policy ("Policy") is to define and communicate Epiq's ("Epiq" or the "Company") commitment to safeguard Confidential and Personal information of the Company and its customers, associates, and third parties in accordance with applicable laws and regulations.

Scope

This Policy applies to all Epiq Associates (as defined below) and Third Parties (as defined below) supporting Epiq operations, including all Epiq subsidiaries and business units. For recent acquisitions to Epiq, this Policy applies only once the integration is complete.

Exceptions

Compliance with this Policy is mandatory. However, the Compliance team will consider requests for exceptions under special circumstances.

If you wish to request an exception to this Policy, please complete the Policy Exception Request form and send to the Compliance team for review. Please refer to Epiq Policy Management Policy for further details around this process, the information you will need to provide as part of the request, and the associated considerations.

Policy Enforcement

Executive management expects every Epiq Associate who use, process, develop, transmit, or store information relevant to Epiq's business to comply with the Policy. Epiq Associates who violate this and/or other policy statements referenced herein may be subject to disciplinary action up to and including termination and/or legal action.

Violation of this Policy by a representative of a Third-Party under contract with Epiq or its subsidiaries may result in the termination of the contract, termination of the assignment, and/or legal action.

Definitions

Associates – Epiq salaried employees, hourly employees, limited duration employees, contingent and/or temporary employees, and/or contractors.

Consent – Any freely given, specific, informed, and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of PII, PHI, or Personal Data relating to him or her.

Controller – the 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.

Customer/Client – Any organization or individual under contractual obligations with Epiq to render payment for products or services received by Epiq.

Data Protection Program – Policies, standards, procedures, plan, notices, controls, and resources in place for the safeguarding of Personal Data processed by, or on behalf of, Epiq.

Data Subject – An identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Confidential / Proprietary Information – All tangible or intangible non-public information, including Intellectual Property, that might be of use to competitors, or harmful to Epiq or others with whom Epiq does business, if disclosed.

Personal Data – Any information relating to a Data Subject and includes PII and PHI.

Personally Identifiable Information (PII) – The following information that alone or in conjunction with one another is processed by, or on behalf of, Epiq, that identifies an individual: (1) name, (2) physical address, (3) email, (4) date of birth, (5) government-issued identification number, (6) biometric data, (7) account number or routing code, and/or (8) credit card number.

Processing / Processed – Any operation or set of operations which is performed on PII or Personal Data or on sets of PII or Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Protected Health Information (PHI) – refer to the "Epiq – HIPAA PHI Reference Guide" for a complete definition of PHI.

Third Parties –Vendors or other non-associate individuals authorized by Epiq to process personal data.

Roles and Responsibilities

Roles	Responsibilities
Data Protection Director (Lori Blackley - Vice President, Risk and Compliance)	▪ Advise the organization on data protection compliance and best practices. ▪ Formally declare a security incident a breach. ▪ Determine whether Epiq is acting as a data controller and/or a data processor with respect to each category of personal data that is subject to a personal data breach. ▪ Determine whether any notification obligations apply. ▪ Where notification obligations apply, the DPD is responsible for notifying the relevant customers, associates, and third parties in accordance with this Policy.
Data Protection Governance Committee	▪ Monitor compliance with data protection laws and regulations, as well as Epiq's Data Protection Program. ▪ Ensure action plans are developed and implemented for the reduction of data privacy residual risk, approving major revisions to this Policy, and enforcing disciplinary actions for any violations of this Policy as necessary.
Compliance Team	▪ Create, maintain, and monitor compliance with this Policy. ▪ Oversee the implementation of data protection controls and measures, such as data protection impact assessments (DPIAs). ▪ Review and approve Policy, annually at minimum. ▪ Inform customers, associates, and third parties of this Policy. ▪ Implement Data Privacy training and awareness programs for employees and contractors. ▪ Provide guidance and training to employees on data protection matters. ▪ Act as a point of contact for data subjects (individuals whose personal data is being processed) and for supervisory authorities.
Information Security	▪ Recommend and enforce standard security controls related to Data Privacy. ▪ Plan against security threats, vulnerabilities, and risks. ▪ Create and maintain Epiq's Incident Response Policy and plan and ensure it includes both requirements and responsibilities for identifying, responding to, investigating documenting, and closing incidents involving potential data breaches. ▪ Report possible Personal Data Breaches to the Data Protection Director.
Event Team	▪ Facilitate all security incident events including Breach Notification. ▪ Conduct recurring calls with key stakeholders until all activities in the Personal Data Breach Notification Plan are completed. ▪ Interview personnel to determine root cause. ▪ Provide a Root Cause Analysis (RCA).
Directors/Managers	▪ Responsible for implementing the Policy and ensuring staff awareness and compliance in their respective departments.

Epiq Associates	▪ Comply with this Policy and all supporting policies, processes, Procedures, and standards. ▪ Send any privacy related questions or concerns to privacy@epiqglobal.com. ▪ Report any attempted or suspected security incidents, breaches or weaknesses in systems to IncidentReporting@epiqglobal.com.

Policy Guidelines

1. DATA PROTECTION GOVERNANCE

1.1. Epiq has formally established a Data Privacy Governance Committee with responsibilities for overseeing the Data Protection Program (see Roles & Responsibilities section above).

1.2. Epiq has formally established a Data Protection Director with responsibility for managing the Data Protection Program (see Roles & Responsibilities section above).

2. LEGAL BASIS FOR PROCESSING

1.1. The legal basis for the processing Personal Data on behalf of a customer is ultimately the responsibility of the customer, and such responsibility shall be indicated in contracts or similar agreements with those customers.

1.2. Personal Data collected from customers must only be obtained and processed for contractually specified and lawful purposes and shall not be further processed or disclosed in any manner incompatible with those purposes.

1.3. All Personal Data processed by Epiq on behalf of a customer must be done so in accordance with the services defined in the customer contract.

3. ACCESS TO PERSONAL DATA

1.1. Requests for access from an individual to his/her Personal Data are managed by the Compliance Team.

1.2. All requests are maintained by Epiq in conjunction with services performed for a customer must be documented and responded to in a timely manner.

1.3. Epiq will promptly notify Data Controller of any request from a Data Subject for information about, access to, correction, amendment, deletion, erasure, portability, or restriction of processing of that Data Subject's Personal Data.

1.4. Epiq shall not respond to such a request except upon written instruction from the Data Controller or as required by applicable law, in which case Vendor shall to the extent permitted by applicable law inform the Data Controller of that legal requirement before Epiq responds to the request.

4. CONSENT

1.1. Epiq does not process, as a Data Controller, Personal Data under the legal basis of "Consent" for an individual, except in the cases of an applicant for employment with Epiq or subscribers to marketing or public relations materials from Epiq.

1.2. Epiq will promptly notify Data Controller of any request from a Data Subject and will wait for instructions from Data Controller on actions to be taken.

5. PRIVACY STATEMENT

1.1. Epiq maintains a Privacy Statement in accordance with applicable laws and regulations at the following site: http://www.epiqglobal.com/en-us/privacy-statement

1.2. The Privacy Statement provides users of the Epiq website notice of what information is processed by Epiq, how the information is used, and contact information for any questions or concerns in connection with Epiq's data processing activities.

6. PRIVACY BY DESIGN & DEFAULT

1.1. Controls for safeguarding, minimizing, and restricting access to personal data must be identified and included in the design of new information systems or enhancements to existing information systems whereby personal data will be processed as a result of the implementation.

1.2. Prior to implementation, information systems must be assessed to verify the adequacy of the controls used to ensure the safeguarding and minimization of personal data.

1.3. Customer Personal Data, and other data designated for deletion upon expiration within the customer's contract with Epiq must be pseudonymized or deleted according to the Epiq Information Lifecycle Management Policy and binding contractual terms and regulatory requirements.

7. CROSS-BORDER DATA TRANSFERS

1.1. Epiq and its wholly owned subsidiaries worldwide that receive Personal Data adhere to applicable law and regulations regarding customer and Associate Personal Data moving across geographical and jurisdictional borders. This includes the use of data transfer agreements and model contractual clauses, where available, between Epiq's corporate entities and Epiq's clients where required. Epiq is relying upon Standard Contractual Clauses (SCCs) to transfer client data from the EU to third countries. Personal data must be secured during transfer according to security control and encryption requirements defined in the Epiq Information Security Policy, and applicable laws and regulations.

8. THIRD PARTY CONTRACTS & DUE DILIGENCE

1.1. Contracts with Third Parties whereby Personal Data will be exchanged or processed must include a binding confidentiality agreement, must specify requirements for compliance with applicable legal, regulatory and/or other third party obligations, and must include requirements for compliance with standards and procedures defined in the Epiq Data Protection Policy and all other policies referenced herein.

1.2. All contracts with Third Parties with responsibilities for processing Personal Data must be reviewed and approved by Epiq Legal prior to entering into agreement with a Third Party.

1.3. Epiq Compliance and/or owners of relationships with Third Parties under contract whereby Personal Data is exchanged or accessed must conduct a review of any independent audits conducted (e.g., SSAE18 SOC1, SOC2 reports, ISO 27001 certification, etc.) to verify a Third Party's security and privacy controls are operating effectively to address Epiq's specific security and privacy requirements defined in the Epiq Data Protection Policy and all other policies referenced herein. If an independent audit has not been performed, Epiq will submit a questionnaire to the Third Party requiring formal responses, conduct an independent audit of the Third Party's security and privacy controls to verify alignment with Epiq's specific security and privacy requirements, or will obtain Executive Management sign-off accepting the risk of not completing the audit.

1.4. Upon termination of a Third-Party contract, the confidentiality arrangements shall be revisited to determine whether confidentiality has to be extended beyond the duration of the contract.

9. DATA SECURITY

1.1. Controls for ensuring the confidentiality, integrity, availability, and resilience of Personal Data are defined in the Epiq Information Security Policy.

10. INCIDENT RESPONSE AND BREACH NOTIFICATION

1.1. The Epiq Incident Response Policy is formally documented and includes both requirements and responsibilities for identifying, responding to, documenting, and closing incidents involving potential data breaches.

1.2. Epiq Breach Notification Plan and Procedures are formally documented and define Epiq's plan and procedures for notifying associates, customers, and/or third parties in the event of a breach of Personal Data.

11. MONITORING

1.1. The Epiq Data Protection Director shall periodically review and identify any new laws and regulations or changes to existing laws and regulations that potentially have an impact on requirements defined in this Data Protection Policy and update the policy as necessary.

12. TRAINING AND AWARENESS

1.1. Mandatory privacy awareness training must be completed by each new employee upon initial hire and annually thereafter.

1.2. Privacy awareness training should educate users on their data privacy responsibilities as well as data privacy risks, safeguards, policies, and procedures. Privacy awareness training should be reviewed and updated upon changes made to this Data Protection Policy and relevant standards and procedures to ensure consistent communication of the most current security and privacy risks, controls, and requirements.

GLOBAL REGULATORY REQUIREMENTS

This section outlines selected data protection requirements that Epiq is subject to that are not explicitly defined in other sections of this Policy.

Contents

APPENDIX A – EU General Data Protection Regulation (GDPR) Regulation (EU) 2016/679

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Applicability

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "to the offering of goods or services" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "the monitoring of their behavior" (Article 3(2)(b)) as far as their behavior takes place within the EU.

Records of Processing

Epiq Data Owners must maintain a complete and accurate inventory of processing activities for EU Personal Data identifying the systems and third parties that support the processing activities and the controls in place for safeguarding the EU Personal Data in compliance with the GDPR.

Data Protection Impact Assessment (DPIA)

Epiq Data Owners must complete and maintain a DPIA, as defined by Article 35 of the GDPR, for processing activities that are likely to result in a high risk to the rights and freedoms of EU Data Subjects.

Data Subject Rights

In instances where an EU Data Subject for which Epiq has not obtained EU Personal Data from requests information regarding the processing of EU Personal Data by Epiq, Epiq will provide the EU Data Subject with the minimum required information as defined by Article 14 of the GDPR.

Epiq will provide an EU Data Subject with confirmation as to whether EU Personal Data concerning him or her is being processed and related information as defined by Article 15 of the GDPR unless this proves impossible or involves disproportionate effort.

Epiq will pseudonymize or delete EU Personal Data in a timely manner upon request by a customer, associate, or third party for an individual EU Data Subject whereby Epiq no longer has a legitimate need or legal basis for retaining or processing the data according to requirements defined in Article 17 of the GDPR, unless this proves impossible or involves disproportionate effort.

Epiq will restrict processing of EU Personal Data upon request by an EU Data Subject who is a customer, associate, or third party according to the requirements defined in Article 18 of the GDPR. Epiq will notify the EU Data Subject of restriction of processing unless this proves impossible or involves disproportionate effort.

Epiq will provide EU Data Subjects requesting portability of their EU Personal Data with the appropriate means for transmitting the data according to the requirements defined in Article 20 of the GDPR, unless this proves impossible or involves disproportionate effort.

Epiq will fulfill an EU Data Subject's right to reject processing of EU Personal Data according to Article 21 of the GDPR unless Epiq is able to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

Epiq does not conduct automated profiling of EU Data Subjects as defined by the GDPR.

Breach Response for EU Personal Data

Upon confirmation of a breach of EU Personal Data, Epiq will notify the appropriate parties as defined by the GDPR within 72 hours of confirmation.

GDPR – United Kingdom

Following the UK's exit from the European Union on 31 January 2020, the UK Government has transposed the General Data Protection Regulation (Regulation (EU) 2016/679) into UK national law (thereby creating the "UK GDPR"). The Data Protection Act 2018 ("DPA") remains in place as a national data protection law and supplements the UK GDPR regime. As well as containing derogations and exemptions from the position under the GDPR in certain permitted areas, the DPA also does the following:

- Part 3 of the DPA transposes the Law Enforcement Directive ((EU) 2016/680) into UK law, creating a data protection regime specifically for law enforcement personal data processing.
- Part 4 of the DPA updates the data protection regime for national security processing; and
- Parts 5 and 6 set out the scope of the Information Commissioner's mandate and her enforcement powers and creates a number of criminal offences relating to personal data processing.

National Data Protection Authority

The Information Commissioner (whose functions are discharged through the Information Commissioner's Office ("ICO")) remains the independent supervisory body regarding the UK's data protection legislation. The UK GDPR also omits Chapter 7 (Cooperation and Consistency) of the EU GDPR, on the basis that the UK will not be part of the EU's cooperation and consistency mechanisms.

The ICO's contact details are:

Wycliffe House
Water Lane
Wilmslow
Cheshire, SK9 5AF
T +0303 123 1113 (or +44 1625 545745 if calling from overseas)
F 01625 524510
www.ico.org.uk

Registration

Controllers have to pay an annual data protection fee to the ICO, unless they are exempt from doing so.

Those controllers who have an unexpired registration under the old system are not required to pay the new fee until their existing registration expires, at which point the ICO will contact them with details of the new fee.

Data Protection Officers

The UK has not opted to extend the requirement to appoint a Data Protection Officer.

Rights of the Data Subject

Article 9(2) of the GDPR provides for a number of exceptions under which special categories of personal data may lawfully be processed. Certain of these exceptions require a basis in Member State law. Parts 1 and 2 of Schedule 1 to the DPA provide a number of such bases, in the form of 'conditions', which in effect provide UK specific gateways to

legalize the processing of certain types of special category data. Many of these conditions are familiar from the previous UK law, whilst other are new. Important examples include:

- Processing required for employment law; health and social care;
- Equal opportunity monitoring; public interest journalism; fraud prevention;
- Preventing / detecting unlawful acts (e.g. money laundering / terrorist financing); insurance; and occupational pensions.

Criminal convictions and offences data (Article 10)

The processing of criminal conviction or offences data is prohibited by Article 10 of the GDPR, except where specifically authorized under relevant member state law. Part 3 of Schedule 1 of the DPA authorizes a controller to process criminal conviction or offences data where the processing is necessary for a purpose which meets one of the conditions in Parts 2 of Schedule 1 (this covers the conditions noted above other than processing for employment law, health and social care), as well as number of other specific conditions:

- Consent
- The protection of a data subject's vital interests
- The establishment, exercising or defense of legal rights, the obtaining of legal advice and the conduct of legal proceedings

Appropriate policy and additional safeguards

In any case where a controller wishes to rely on one of the DPA conditions to lawfully process special category, criminal conviction or offences data, the DPA imposes a separate requirement to have an appropriate policy document in place and apply additional safeguards to justify the processing activity. The purpose of the policy document is to set out how the controller intends to comply with each of the data protection principles in Article 5 of the GDPR in relation to this more sensitive processing data activity.

Child's consent to information society services (Article 8)

Article 8(1) of the GDPR stipulates that a child may only provide their own consent to processing in respect of information society (primarily, online) services, where that child is over 16 years of age, unless member state law applies a lower age. The DPA reduces the age of consent for these purposes to 13 years for the UK.

Automated Decision Making (Article 22)

Article 22(2)(b) of the GDPR allows member states to authorize automated decision making in local law, subject to additional safeguards, for purposes beyond the two permitted gateways already set out in Article 22(2) of the GDPR (i.e., explicit consent, or necessity for entering into or performance of a contract with the data controller).

The DPA takes advantage of this provision to enable automated decision making where the automated decision is accompanied by the sending of a specific notice to the data subject which provides them with a one-month period to request the controller to (i) reconsider the decision, or (ii) take a new decision that is not based solely on automated processing.

Records of Data Processing

As a data processor, Epiq must maintain a database that tracks all the business processes, third parties, products and applications that process personal data and keep it up to date in order to comply with the GDPR and applicable laws. Records of processing activities must include significant information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients. This must be completely made available to authorities upon request.

Epiq will regularly update record of processing activities and conduct reviews of the information processed to ensure our database remains accurate and up to date.

Transfer

On 28 June 2021, the EU approved adequacy decisions for the UK GDPR and the Law Enforcement Directive (LED). This means data can continue to flow freely from the EU to the UK, in the majority of cases. Both decisions are expected to last until 27 June 2025.

Breach Notification

Personal data breaches should be notified to the ICO, as the UK's supervisory authority. Breaches can be reported to the ICO's dedicated breach helpline during office hours (+44 303 123 1113). Outside of these hours (or where a written notification is preferred) a pro forma may be downloaded and emailed to the ICO.

Making a Complaint

Under the GDPR, a Data Subject can file a privacy complaint with Epiq by submitting their request via a dedicated web form on our Privacy Statement page or by using the information below:

Epiq
Attn: Privacy Officer
110 Bishopsgate
Salesforce Tower, 15th Floor
London, EC2N 4AY United Kingdom
privacy@epiqglobal.com

Under the GDPR, data protection authorities are called supervisory authorities. A supervisory authority is defined by the GDPR in GDPR Article 4 (Definitions) as “an independent public authority which is established by a Member State pursuant to Article 51”. Without prejudice to any other administrative or judicial remedy, every Data Subject shall have the right to lodge a complaint with a supervisory authority, in particular in the country of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Whether the complaint is made directly to Epiq or is submitted to a supervisory authority, Epiq will perform a thorough internal investigation in order to resolve the problem. As a data processor under the GDPR, Epiq will investigate each complaint received and record any applicable evidence of the incident. Epiq will strive to remedy the problem as soon as possible.

For privacy complaints lodged against Epiq with supervisory authorities, Epiq will cooperate with the supervisory authorities (such as the ICO) to help them perform their duties when they receive a data privacy complaint against Epiq. To help the applicable supervisory authorities investigate a complaint, Epiq will provide all personal data and information necessary for their enquiries. Epiq will allow access to its the premises should an on-site investigation be needed. Epiq may notify the Data Controller about the complaint, if applicable and let the Controller know that Epiq will cooperate with the applicable supervisory authority, where feasible. Further, if Epiq becomes aware of a personal data breach, Epiq must notify the relevant controller without undue delay and assist the controller in complying with its obligations regarding personal data breaches.

GDPR – Germany

Germany has adjusted the German legal framework to the GDPR by passing the new German Federal Data Protection Act (Bundesdatenschutzgesetz – 'BDSG'). The BDSG was officially published on July 5, 2017 and came into force together with the GDPR on May 25, 2018. The purpose of the BDSG is specially to make use of the numerous opening clauses under the GDPR which enable Member States to specify or even restrict the data processing requirements under the GDPR.

In addition to the BDSG, there exist a number of data protection rules in area-specific laws, for example those regulating financial trade or the energy sector. Many of these laws have been adapted to the GDPR by the Second Data Protection Adaptation and Implementation Act EU (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – '2. DSAnpUG-EU'), which generally entered into force on November 26, 2019. However, some particularly relevant laws have so far remained unchanged, most notably the Telemedia Act (Telemediengesetz – 'TMG'), raising questions about the continued applicability of the data protection rules contained therein.

Data Protection Authority

Germany does not have one central Data Protection Authority but a number of different Authorities for each of the 16 German states (Länder) that are responsible for making sure that data protection laws and regulations are complied with. In addition, the German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für Datenschutz und Informationsfreiheit – 'BfDI') is the Data Protection Authority for telecommunication service providers and represents Germany in the European Data Protection Board. To ensure that all the Authorities have the same approach a committee consisting of members of all Authorities for the public and the private sector has been established – the 'Data Protection Conference' (Datenschutzkonferenz 'DSK'). The coordination mechanism between the German Authorities mirrors the consistency mechanism under the GDPR.

Data Protection Officers

The threshold to designate a Data Protection Officer (DPO) is much lower in the BDSG. The controller and processor have to designate a DPO if they constantly employ as a rule at least 20 persons dealing with the automated processing of personal data, Sec. 38 (1) first sentence BDSG. The meaning of 'automated processing' is interpreted broadly by the German Authorities. It basically covers every employee who works with a computer.

If the threshold of 20 persons is not reached, Sec. 38 (1) second sentence BDSG regulates in addition to Art. 37 GDPR, that a DPO has to be designated in case the controller or processor undertakes processing subject to a data protection impact assessment pursuant to Art. 35 GDPR, or if they commercially process personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research.

Furthermore, a dismissal protection for the DPO is provided in Sec. 38 (2) in conjunction with Sec. 6 (4) BDSG. Where the controller or processor is obliged to appoint a DPO, the dismissal of a DPO who is an employee is only permitted in case there are facts which give the employing entity just cause to terminate without notice. After the activity as DPO has ended, a DPO who is an employee may not be terminated for a year following the end of appointment, unless the employing entity has just cause to terminate without notice.

Additionally, Sec. 38 (2) in conjunction with Sec. 6 (5) and (6) BDSG stipulates that the DPO shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless he

/ she is released from this obligation by the data subject. Also, the DPO has the right to refuse to give evidence under certain conditions.

Moreover, the German Authorities require that the DPO speaks the language of the competent Authorities and data subjects, i.e. German, or at least that instant translation is ensured.

Data Subject Rights

The BDSG has additional rules regarding processing of special categories of personal data. Contrary to Art. 9 (1) GDPR, processing of such data is permitted by public and private bodies in some cases, see Sec. 22 (1), 26 (3) BDSG. Also, Sec. 24 BDSG determines cases in which controllers are permitted to process data for a purpose other than the one for which the data were collected.

Sec. 4 BDSG provides a special rule for video surveillance of publicly accessible areas. According to the German DPAs as well as the German Federal Administrative Court (Bundesverwaltungsgericht – 'BVerwG') and the near unanimous opinion in German legal literature, the provision is not compliant with the GDPR insofar as it regulates surveillance by private bodies (Sec. 4 (1) Nbrs. 2, 3 BDSG). This is based on the argument that the GDPR does not contain any opening clause on which these deviations from Art. 6 (1) GDPR could be based.

Furthermore, the BDSG provides special rules regarding processing for employment-related purposes in Sec. 26 BDSG. The German legislator has made very broad use of the opening clause in Art. 88 (1) GDPR and has basically established a specific employee data protection regime. These new rules reflect the current German employee privacy rules which also has the consequence that a set of case law of the German Federal Labour Court (Bundesarbeitsgericht – 'BAG') will apply. In case the processing is conducted for employment-related purposes it is subject to Sec. 26 BDSG only and a recourse to the general legal grounds set out in Article 6 GDPR is blocked. Personal data of employees can only be processed in the employment context (setting aside some very special cases under the BDSG when it comes to the assessment of the working capacity of the employee and other handling of special categories data as well as exchange of data with the works council) in the following cases:

The processing is necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract (Sec. 26 (1) sentence 1 BDSG) (please note that the BAG interprets the predecessor provision broader than Art. 6 (1) (b) GDPR)

Employees' personal data may be processed to detect criminal offenses only if there is a documented reason to believe the data subject has committed such an offense while employed, the processing of such data is necessary to investigate the offense and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason (Sec. 26 (1) sentence 2 BDSG)

The processing is based on a works council agreement which complies with the requirements set out Art. 88 para. 2 GDPR (Sec. 26 (4) BDSG)

The processing is based on the employee's consent in written or electronic form. A derogation from this form can apply if a different form is appropriate because of special circumstances (but this derogation will rarely apply in practice). Moreover, the utilization of consent as basis for the processing is particularly problematic in Germany as Sec. 26 (2) BDSG stipulates requirements in addition to Art. 7 GDPR. If personal data of employees are processed on the basis of consent, then the employee's level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given. Consent may be freely given in

particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. The German DPAs interpret this provision in a way that employee consent cannot be used for processing of personal data which directly relates to the employment relationship, but only to supplementary services offered by the employer (e.g., private use of company cars or IT equipment, occupational health management or birthday lists).

Notwithstanding, processing of employee personal data for purposes that are not specifically related to employment as such can still be based on Art. 6 (1) GDPR. In particular, controllers that are part of a group of companies may be able to base transfers of data within the group for internal administrative purposes on their legitimate interests in accordance with to Art. 6 (1) f) (as stated by Recital 48 of the GDPR).

Breach Notification

The German BDSG only contains slight changes and additions to the regulations in Art. 33, 34 GDPR.

Sec. 29 (1) BDSG stipulates in addition to the exception in Art. 34 (3) GDPR, the obligation to inform the data subject of a personal data breach according to Art. 34 GDPR shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. By derogation from this, the data subject pursuant to Article 34 GDPR shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

According to Sec. 43 (3) BDSG, a notification pursuant to Art. 33 GDPR or a communication pursuant to Article 34 (1) GDPR may be used in proceedings pursuant to the Act on Regulatory Offences (Gesetz über Ordnungswidrigkeiten – 'OWiG') against the person required to provide a notification or a communication only with the consent of the person obligated to provide a notification or a communication.

Cookie Compliance

Cookie consent is a requirement in Germany. In addition to that, the German data protection authorities have long been of the opinion that the processing of personal data enabled by the cookies used for analysis and tracking tools regularly requires consent, in particular if the tools allow third parties to collect data from website users as (joint) controllers. It remains to be seen whether this position will be upheld by the BGH or another superior German court.

APPENDIX B – Swiss Federal Act on Data Protection 1992 (FDPA)

Applicability

Applies to data processing by individuals, organizations, and federal authorities in Switzerland. According to the FDPA, Personal Data processing must comply with the following general principles:

- Principle of lawfulness – Personal Data can only be processed lawfully
- Principle of proportionality – Personal Data processing must be carried out in good faith and must be proportionate
- Principle of appropriateness – Personal Data can only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law
- Principle of transparency – The collection of Personal Data and the purpose of processing must be evident to the data subject

Data Subject Rights

Right of access to data/copies of data – a person may request information from the Controller of the Data File as to whether data concerning him or her is being processed; the information must normally be provided in writing, in the form of a printout or a photocopy, and is free of charge.

Right to rectification of errors – a data subject may request that incorrect data be corrected.

Right to deletion/right to be forgotten – a data subject may request that incorrect data be deleted, although the right to be forgotten is not explicitly mentioned in the FDPA.

Right to object to processing – a data subject may request (in a civil litigation) that data processing be stopped, that no data be disclosed to third parties, or that the Personal Data be corrected or destroyed, it is important to note that data processing may be blocked by preliminary injunctions.

Right to withdraw consent – a data subject can withdraw consent at any time if their Personal Data is processed against their express wish.

Right to object to marketing – a data subject can object to Personal Data processing for marketing purposes, including mass emails.

Right to complain to the relevant data protection authority(ies) – the Federal Data Protection and Information Commissioner (FDPIC) may investigate cases in more detail on their own initiative or at the request of a third party.

Breach Notification

The FDPA is currently being revised to include a data breach notification obligation that is comparable with the breach notification obligation under the EU General Data Protection Regulation (GDPR), but with different and higher thresholds.

Cookies

Cookies can only be used if the data subject is informed of such use and is given the choice to deactivate cookies through appropriate opt-out mechanisms.

The revised FDPA is expected to go into effect in 2023.

APPENDIX C – US California Consumer Privacy Act (CCPA)

The US has several sector-specific and medium-specific national privacy or data security laws, including laws and regulations that apply to financial institutions, telecommunications companies, personal health information, credit report information, children's information, telemarketing and direct marketing.

The US also has hundreds of privacy and data security among its 50 states and territories, such as requirements for safeguarding data, disposal of data, privacy policies, appropriate use of Social Security numbers and data breach notification. California alone has more than 25 state privacy and data security laws, including the recently enacted California Consumer Privacy Act of 2018 (CCPA), effective January 1, 2020. The CCPA applies cross-sector and introduces sweeping definitions and broad individual rights, and imposes substantial requirements and restrictions on the collection, use and disclosure of personal information, which is very broadly defined as explained later in this chapter. A number of other US states are also currently proposing and considering state-level privacy legislation; in general, such legislation is similar to the CCPA in some ways, but also includes some additional or materially different requirements. Thus, it is highly possible that additional state-level privacy laws will be enacted in the US that impose requirements that go beyond or are materially different from those of the CCPA.

Personal Information

The CCPA defines personal information as any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. The definition specifically includes name, alias, contact information, government IDs, biometrics, genetic data, location data, account numbers, education history, purchase history, online and device IDs, and search and browsing history and other online activities, if such information is linked or linkable with a particular consumer or household. Under the law, consumer is broadly defined as any resident of California.

Collection and Processing

CCPA requires that a business obtain explicit consent prior to the sale of any personal information about a consumer that the business has "actual knowledge" is less than 16 years old. (As discussed further below, the definition of "sale" under the CCPA is very broad and may include online advertising and retargeting activities, for example.)

Under the CCPA (which applies to individual and household data about California residents, businesses must, among other things:

- At or before collection, notify individuals of the categories of personal information to be collected and the purposes of use of such information
- Post a privacy policy that discloses
- the categories of personal information collected, categories of personal information disclosed for a business purpose, and categories of personal information "sold" by the business in the prior 12 months,
- the purposes for which the business collects, uses and sells personal information, the categories of sources from which the business collects personal information,
- the categories of third parties to whom the business discloses personal information, and
- the rights consumers have regarding their personal information and how to exercise those rights
- A “do-not-sell my information” link on the business's website and page where consumers can opt-out of the sale of their personal information (if applicable).
- Generally, provide at least two methods for consumers to submit CCPA requests to the business, including an online method (e.g., submission of an online form) and a toll-free number.

Transfer

No geographic transfer restrictions apply in the US, except with regard to storing some government information.

The US is a major point of storage of personal data. The US is presently considered an "adequate" destination for transfers of personal from the EU and Switzerland to recipients in the US who are certified to the EU-US and Swiss-US Privacy Shield principles and program, respectively. However, the legality of the EU-US Privacy Shield program is being challenged in a case that will eventually be heard by the Court of Justice of the European Union.

Records of Data Processing

Epiq Data Owners must maintain a database that tracks all the business processes, third parties, products and applications that process California residents' personal data and keep it up to date in order to comply with the CCPA. Epiq's data inventory must record the categories of personal data, whether the data was only collected more than 12 months ago and indicate which data categories are covered by pre-emptive federal legislation such as HIPAA, GLBA and FCRA.

Data Protection Impact Assessment (DPIA)

Epiq Data Owners must complete and maintain a DPIA for activities related to the collection and use of personal data that are likely to result in a high risk to the rights and freedoms of California residents.

Data Subject Rights (DSR)

Right of data access. Epiq will disclose to California consumers the categories and specific pieces of personal data that Epiq has collected when requested by these consumers.

Right of data erasure. Epiq will comply with California consumers' request to delete any personal data about the consumer which Epiq has collected from the consumer.

Right to stop data selling and disclosure. Epiq does not sell or disclose California consumer's personal data to third parties.

Epiq will disclose and deliver the required information to a California consumer free of charge within 45 days of receiving a verifiable request from the consumer.

Epiq does not conduct automated profiling of California consumers, as defined by the CCPA.

Breach Response for Personal Data

Upon confirmation of a breach of California residents' personal data, Epiq will notify the appropriate parties within 72 hours of confirmation.

APPENDIX D – US California Privacy Rights Act (CPRA)

The California Privacy Rights Act (CPRA), also known as Proposition 24, is a ballot measure that was approved by California voters on Nov. 3, 2020. It significantly amends and expands the California Consumer Privacy Act of 2018 (CCPA), and it is sometimes referred to as "CCPA 2.0." The CPRA becomes fully operative in 2023.

CPRA Rights and Obligations

Purpose Limitation & Data Minimization: Businesses must limit their collection, use, retention, and disclosure of personal information to that which is "reasonably necessary" and "proportionate" to achieve its intended purpose.

New Right to Correction: Businesses must provide consumers with the ability to correct inaccurate personal information.

New Obligations Related to "Sharing": Businesses that "share" personal information are required to provide consumers with notice of this practice and the ability to opt out. "Sharing" is defined as transferring or otherwise communicating a consumer's personal information to a third party for cross-context behavioral advertising (similar to targeted advertising or interest-based advertising).

New Obligations Related to Sensitive Personal Information: Businesses that collect "sensitive personal information" must disclose how they collect, use, and disclose this information and provide consumers with the ability to limit the use and disclosure of this information. "Sensitive personal information" includes, but is not limited to, account log-in credentials, precise geolocation information, biometric information, genetic and health data, social security number or other government-issued identification card number, and information related to race, ethnicity, religion, or sexual orientation.

Broader Timeframe for Access Right: Businesses must provide information to consumers beyond the CCPA-mandated 12-month period preceding the request, unless doing so would be impossible or involve a disproportionate effort.

New Disclosure Requirements: Businesses must disclose the length of time they retain each category of personal information collected or the criteria that will be used to determine such period. Businesses must also disclose the new consumer rights afforded under the CPRA, including the right to correction, the right to opt out of sharing, and the right to limit the use and disclosure of sensitive personal information.

Changes to Deletion Requirements: Businesses that receive verifiable consumer requests to delete personal information must notify service providers and contractors to delete the personal information from their records.

Downstream Contractual Restrictions: Businesses must impose specific contractual obligations on service providers, contractors, and third parties before selling, sharing or disclosing personal information to them.

B2B and Employee Personal Information: While B2B and employee personal information have largely been exempted from the CCPA, the CPRA extends consumer rights and protections to this information.

Enforcement and Penalties

The CPRA creates and transfers all rulemaking and enforcement authority from the California attorney general to the new state agency, the California Privacy Protection Agency. The CPRA tightens enforcement, removing the mandatory 30-day cure period that businesses currently enjoy under the CCPA and tripling penalties for violations that involve minors under the age of 16. The law also expands the types of data breaches that are considered within the scope of the

data breach private right of action to include breaches of a username or email address, in combination with a password or security question and answer that would permit access to an online account.

The CPRA may be enforced beginning on July 1, 2023, and only as to violations that occur on or after that date.

APPENDIX E – US Colorado Privacy Act (CPA)

The Colorado Privacy Act is set to take effect on July 1, 2023. The Colorado Privacy Act applies to "Personal Data," which is defined as "information that is linked or reasonably linkable to an identified or identifiable individual." Personal Data does not include information that is de-identified or that is publicly available. The Colorado Privacy Act's definition of consumer does not include individuals acting in commercial or employment contexts.

The Colorado Privacy Act identifies and imposes obligations on "controllers" and "processors."

A controller is defined as a person that "determines the purposes for and means of processing personal data." Under the Colorado Privacy Act, controllers are required to:

- Provide consumers with a "reasonably accessible, clear, and meaningful privacy notice, "that outlines i) categories of personal data collected or processed by the controller or processors; ii) the purposes for processing; iii) how consumers can exercise the rights granted by the Colorado Privacy Act; iv) categories of personal data shared with third parties; v) categories of third parties with whom personal data is shared
- Disclose in a conspicuous manner any sale of consumer data and the manner in which a consumer may opt-out of the sale or processing of personal data
- Limit collection of personal data to what is adequate, relevant, and "reasonably necessary in relation to the specified purposes for which the data are processed"
- Take reasonable measures to secure personal data compatible with the scope, volume, and nature of the data
- Obtain consumer consent before processing sensitive personal data by a clear affirmative act signifying that consent is freely given, specific, informed, and unambiguous. Notably, the Colorado Privacy Act specifies that such consent shall not be obtained through general or broad terms of use or through dark patterns designed to subvert consumer decision-making.

A processor is a person that processes personal data on behalf of the controller. The Colorado Privacy Act requires processors to adhere to the controller's instructions and assist and cooperate with the controller to comply with its obligations under the act. The Colorado Privacy Act also requires that all processing be governed by a contract between the controller and processor that outlines relevant consumer privacy provisions.

Data Subject Rights

The CPA provides five main rights for the consumer.

Right of access. Consumers have "the right to confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data."

Right to correction. Consumers have "the right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data."

Right to delete. Consumers have "the right to delete personal data concerning the consumer."

Right to data portability. Consumers have "the right to obtain a personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance."

Right to opt out. Consumers have "the right to opt out of the processing of personal data concerning the consumer for purposes of:

- targeted advertising
- the sale of personal data
- profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer."

Right to appeal. The CPA provides consumers the right to appeal a business's denial to take action within a reasonable time period. Under the CPA, a business must respond to a consumer request within 45 days of receipt and may subsequently extend that deadline by an additional 45 days when reasonably necessary. When a business elects to extend that deadline, it must notify the consumers within the initial 45-day response period.

Obligations

Duty of transparency. The CPA mandates a controller provide consumers with a "reasonably accessible, clear, and meaningful privacy notice." This notice must include:

Categories collected or processed by controller or processor.

- Purpose(s) of processing the data
- How to exercise rights and appeal
- Categories of personal information shared
- Categories of third parties data is shared with

If sold to a third party or processed for targeted advertising, the controller shall "clearly and conspicuously disclose the sale or processing" as well as the opt-out mechanism.

Duty of purpose specification. When collecting personal data, a controller is required to "specify the express purposes for which personal data are collected and processed."

Duty of data minimization. Colorado institutes a policy of data minimization where "a controller's collection of personal data must be adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed."

Duty to avoid secondary use. Absent consent, the CPA dictates a controller shall not process personal data for "purposes that are not reasonably necessary to or compatible with the specified purposes for which the personal data are processed."

Duty of care. The CPA requires controllers take security precautions during storage and use of data by imposing a duty of care. Precautionary measures must be "appropriate to the volume, scope, and nature of the personal data processed."

Duty to avoid unlawful discrimination. The law prohibits a controller from processing personal data "in violation of state or federal laws that prohibit unlawful discrimination against consumers."

Duty regarding sensitive data. Controllers are likewise prohibited from processing sensitive data without consent. Consent must be "freely given, specific, informed, and unambiguous."

Data protection assessments. Controllers may not process activity "that presents a heightened risk of harm to a consumer without conducting and documenting a data protection assessment of each of its processing activities," and includes multiple examples.

Data processing contracts. The CPA requires processing by a processor must "be governed by a contract between the controller and the processor."

Enforcement

Enforcement falls not only to the attorney general but also district attorneys. As it stands now, once the attorney general or district attorney decides to initiate an action, the office must then provide notice to the controller. The controller then has 60 days to cure the violation.

APPENDIX F – US Connecticut Data Privacy Act (CTDPA)

The Connecticut Data Privacy Act (CTDPA) establishes rights including a right to access, deletion, as well as portability for consumers, and provides the right to opt-out of targeted advertising, sale of personal data, and automated profiling. The CTDPA also establishes various controller and processor obligations, privacy notice requirements, and grants the Connecticut Attorney General ('AG') exclusive authority to enforce its provisions. The CTDPA will enter into effect on 1 July 2023.

Consumer rights under the CTDPA are:

Right to access. Consumers have the right to "confirm whether or not a controller is processing the consumer's personal data and access such personal data."

Right to correct. Consumers have the right to "correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data."

Right to delete. Consumers have the right to "delete personal data provided by, or obtained about, the consumer."

Right to data portability. When exercising their access rights, consumers have the right to "obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided such controller shall not be required to reveal any trade secret."

Right to opt out. Consumers have the right to "opt out of the processing of the personal data for the purposes of:

- targeted advertising,
- the sale of personal data,
- profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer."

Obligations

Limits on collection. Controllers are required to "limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer."

Limits on use. Unless an exception applies, such as obtaining consent, controllers are prohibited from processing personal data for "purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed."

Data security. Controllers must also "establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data at issue."

Consent requirements. Absent consent, the law prohibits controllers from processing sensitive data. "Sensitive data" includes personal data collected from an individual the controller knows is under 13 years old, in which case the data must be processed in accordance with the Children's Online Privacy Protection Act.

Nondiscrimination. If a consumer decides to exercise any of their rights provided by the law, controllers are prohibited from discriminating against them by "denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer."

Transparency. Connecticut's law requires controllers to provide consumers with a "reasonably accessible, clear and meaningful privacy notice." Privacy notices must include:

- The categories of personal data processed by the controller.
- The purpose for processing personal data.
- How consumers may exercise their rights and appeal.
- The categories of personal data the controller shares with third parties, if any.
- The categories of third parties, if any, with which the controller shares personal data.
- An active email address or other online mechanism for consumers to contact the controller.

Responding to consumer requests. Controllers are obligated to respond to a consumer's request "without undue delay," but within 45 days after receiving the request, which may be extended an additional 45 days when reasonably necessary.

Data processing contracts. The law requires there be a contract between a controller and processor to govern the data processing performed by the processor on behalf of the controller. Such contracts must "clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties".

Data protection assessments. For each processing activity "that presents a heightened risk of harm" to consumers, controllers must conduct and document a data protection assessment. The types of activities that must be assessed include:

- Processing data for the purposes of targeted advertising.
- Selling personal data.
- Processing personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of substantial injury to consumers.
- Processing sensitive data.

Enforcement

Enforcement falls solely to the attorney general. Prior to initiating an action, the attorney general must notify the controller of its violation. The CTDPA gives a controller 60 days to cure the violation. Entities may face civil penalties up to $5,000 per willful violation.

APPENDIX G – US Illinois Biometric Information Privacy Act (BIPA)

The Illinois Biometric Information Privacy Act (BIPA) was enacted in 2008, and it governs all biometrics collection. Biometrics include fingerprints, DNA, gestures, gait, typing rhythm, voice prints, palm vein patterns, and facial features. BIPA establishes standards for how companies must handle Illinois consumers' biometric information. In addition to its notice and consent requirement, the law prohibits any company from selling or otherwise profiting from consumers' biometric information.

The BIPA's comprehensive set of rules for companies collecting biometric data of state residents has five key features:

- Requires informed consent prior to collection
- Permits a limited right to disclosure
- Mandates protection obligations and retention guidelines
- Prohibits profiting from biometric data
- Creates a private right of action for individuals harmed by BIPA violations
- Provides statutory damages up to $1,000 for each negligent violation, and up to $5,000 for each intentional or reckless violation.

Obligations

BIPA imposes five requirements upon private entities which handle biometric data:

1. Notification/Destruction. The notification provision requires that private entities who possess biometric data must develop and make publicly available a written policy that details how long the entity will retain the biometric data and a schedule for the permanent destruction of such biometric data. The published policy must provide for destruction of biometric data (i) once the initial purpose for collecting the data has been fulfilled, or (ii) within three years of the individual's last interaction with the private entity, whichever occurs first.

2. Consent. The consent provision consists of three requirements that must be fulfilled for a private entity to be allowed to handle biometric data of an individual: the entity must (i) inform the individual in writing that their biometric data is being collected; (ii) inform the individual in writing of the purpose of the biometric collection and the length for which the biometric data will be collected, stored, and used; and (iii) receive a written release for the biometric collection that is executed by the individual whose biometric data is being collected.

3. Ban on Profit. The ban on profit provision prohibits any private entity from selling, leasing, trading, or profiting from an individual's biometric data.

4. Ban on Disclosure. The disclosure ban provision forbids a private entity from the disclosure of an individual's biometric data except where the individual has consented to the disclosure, or where the disclosure completes a financial transaction that the individual has requested or authorized. BIPA also allows for disclosure where required by federal, state, or local law or by valid warrant or subpoena.

5. Storage and Security Requirements. BIPA's storage and security requirements provision requires that private entities (i) use "the reasonable standard of care within the private entity's industry" when storing, transmitting, and protecting from disclosure of biometric data in their possession, and (ii) do so in "a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information."

Enforcement

BIPA provides for statutory damages of $5,000 for each willful and/or reckless violation of BIPA or, in the alternative, statutory damages of $1,000 for each negligent violation.

APPENDIX H – US Utah Consumer Privacy Act (UCPA)

Utah enacted the Utah Consumer Privacy Act (the "UCPA"), which will go into effect on December 31, 2023. The UCPA applies to any entity that (1) conducts business in Utah or produces products or services that are targeted to Utah residents; (2) has annual revenue of $25 million or more; and (3) annually controls or processes the personal data of at least 100,000 Utah residents, or controls or processes the personal data of at least 25,000 Utah residents and derives over 50% of its gross revenue from the sale of personal data.

Consumer rights

The UCPA grants Utah residents acting in an individual or household context ("consumers") six categories of rights:

- **The Right to Know**: Consumers have the right "to confirm whether a controller is processing the consumer's personal data".
- **The Right to Access**: Consumers have the right to access their personal data.
- **The Right to Deletion**: Consumers have the right to "delete the consumer's personal data" that they provided to a controller.
- **The Right to a Copy**: Consumers have the right to "obtain a copy of the consumer's personal data that the consumer previously provided to the controller" in a portable and readily usable (if technically feasible) format.
- **The Right to Opt Out**: Consumers have the right to "opt out of the processing of personal data" for the purposes of targeted advertising and the sale of their personal data.
- **The Right to Avoid Discrimination**: Controllers "may not discriminate against a consumer for exercising a right" provided by the UCPA.

Obligations

Transparency. The UCPA requires a controller to provide consumers with a "reasonably accessible and clear privacy notice."

Consent to process children's personal data. Controllers processing the personal data of consumers known to be under the age of 13 are required to obtain verifiable parental consent and process such data in accordance with the Children's Online Privacy Protection Act.

Security. Controllers must "establish, implement, and maintain reasonable administrative, technical, and physical data security practices designed to protect the confidentiality and integrity of personal data."

Responding to consumer requests. Unless an exception applies, controllers are obligated to respond to a consumer's request within 45 days. The UCPA prohibits controllers from charging a fee for responding to a request. A controller may, however, charge a reasonable fee if:

- The request is a consumer's "second or subsequent request during the same 12-month period."
- The request is "excessive, repetitive, technically infeasible, or manifestly unfounded."
- The controller "reasonably believes the primary purpose in submitting the request was something other than exercising a right."
- The request "harasses, disrupts, or imposes undue burden on the resources of the controller's business."

Data processing contracts. Processing activities performed by a processor on behalf of a controller must be governed by contract. The UCPA does not require controllers to conduct data protection assessments to evaluate the risks associated with data processing activities.

Exceptions
The UCPA does not apply to certain categories of data, including information protected by HIPAA, patient-identifying information, information relating to human research subjects, information used by a consumer reporting agency, personal data covered by particular federal laws, and data that are processed and maintained about a controller's job applicants, employees, agents, or independent contractors that are used in relation to such individuals' respective roles.

Enforcement
Controllers and processors have 30 days to cure a violation and provide the attorney general with an "express written statement that the violation has been cured and no further violation of the cured violation will occur." The attorney general may initiate an enforcement action and impose penalties — actual damages and fines up to $7,500 per violation — if a controller or processor fails to cure the violation or continues to violate the law after providing a written statement otherwise.

APPENDIX I – US Virginia Consumer Data Protection Act (VCDPA)

The Commonwealth of Virginia passed the Virginia Consumer Data Protection Act ("VCDPA") into law in March 2021 and the law goes into effect on January 1, 2023. The VCDPA builds on frameworks used in California's early legislation and the European Union's General Data Protection Regulation (GDPR). Within the context of the law, "personal data" means any information that is linked or reasonably associated to an identified or identifiable natural person who is a resident of the Commonwealth of Virginia. "Personal data" excludes any deidentified data or publicly available information.

The VCDPA provides consumers with six main rights.

Right to access. Consumers have the right "to confirm whether or not a controller is processing the consumer's personal data and to access such personal data."

Right to correct. Consumers have the right to correct inaccuracies in their personal data, considering the nature of the personal data and the purposes of the processing of the consumer's personal data.

Right to delete. Consumers have the right to delete personal data provided by or obtained about the consumer.

Right to data portability. Consumers have the right to obtain a copy of the consumer's personal data that the consumer previously provided to the controller in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means.

Right to opt out. To opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data and profiling in advancing decisions that produce legal or similarly significant effects concerning the consumer.

Right to appeal. The final right the VCDPA provides to consumers is the right to appeal a business's denial to act within a reasonable time. Under the law, a business must respond to a consumer request within 45 days of receipt of the request. Where reasonably necessary, the business may then extend the response deadline by an additional 45 days as long as they notify the consumer within the initial response window. If a business fails to do this, the VCDPA mandates that a "controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable time after the consumer's receipt of the decision." If the appeal is denied, the controller needs to inform the consumer how they can submit a complaint to the attorney general.

Data protection assessments

The VCDPA requires controllers to conduct "data protection assessments" that evaluate the risks associated with processing activities.

Data processing agreements

The VCDPA requires that processing activities undertaken by a processor on behalf of a controller be governed by a data processing agreement. Such agreements must "clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the rights and obligations of both parties." The provision provides a set of enumerated terms that must be included in the agreement.

Enforcement

Under the VCDPA, enforcement falls solely to the attorney general. Once the attorney general decides to take action, the office must notify the controller. The controller then has 30 days to cure the violation and provide the attorney general with an "express written statement that the alleged violations have been cured and that no further violations shall occur."

APPENDIX J – Canada Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, C. 5.

Applicability

PIPEDA applies to the collection, use or disclosure of personal data in the course of a commercial activity. A commercial activity is defined as any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fund-raising lists. PIPEDA does not apply to provinces that have their own privacy laws that have been declared "substantially similar" to PIPEDA.

With respect to employee data, PIPEDA only applies to those organizations that are federally regulated, so-called "federal works, undertakings and businesses." With the exception of British Columbia, Alberta, and Quebec, provincial employers are not subject to statutory privacy laws with respect to employee data.

Personal Data

Section 2(1) of PIPEDA states that "personal information" means "information about an identifiable individual."

Section 4(1) provides that PIPEDA applies to every organization in respect of personal information that the organization "collects, uses or discloses in the course of commercial activities" or "is about an employee of, or an applicant for employment with, the organization and that the organization collects, uses or discloses in connection with the operation of a federal work, undertaking or business."

Business and Professional Context

PIPEDA does not apply to an organization in respect of the business contact information of an individual that the organization collects, uses or discloses solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession.

An individual's cell phone records from their work cell phone may be the personal data of the individual. Information about a company is generally not personal data. However, an individual's personal information may be so inextricably linked to information about his or her company (e.g. an owner/operator of a small business) that information about that company can constitute personal data about the individual. Each situation must be assessed on a case-by-case basis.

Other personal data in the Business and Professional context include: an individual's Notice of Assessment (NOA) and Social Insurance Number (SIN); email addresses and messages; consumer purchases, services, and transactions; customer membership and account information in the context of frequent flyer or consumer loyalty programs; and customer complaint information.

Employment Context

An individual's views or opinions about an employee (e.g. performance appraisals, internal investigation files, medical diagnoses or assessments, or complaints against an employee) may constitute the personal data of that employee.

Other examples of personal data of employees of federal works, undertakings or businesses include: employee number; employee voices; swipe cards and video footage or live- feed; salary, benefits and performance ratings; and employee personnel files.

Financial Context

Examples of financial information which may constitute personal data of an individual include: bank account numbers, summaries or balances; transaction histories; debt-related information; mortgage applications/renewals, tax returns and net worth; credit reports and credit scores.

Technological Context

Examples of personal data in the technological context include forms of biometric information, such as fingerprints and voiceprints. A voiceprint is personal data even though it may not necessarily tell much about an individual. How much more it reveals about an individual will depend on how the voiceprint is used.

Video surveillance that captures an individual's physical image or movement may also constitute his or her personal data even if it is not taped, since the definition of personal information in PIPEDA does not require that the information be recorded.

Tracking information collected from a Global Positioning System (GPS) placed in company vehicles is personal data since the information can be linked to specific employees driving the vehicles. The employees are identifiable even if they are not identified at all times to all users of the system.

Information collected through the use of radio frequency identification (RFID) tags to track and locate baggage, retail products, and individual purchases may constitute the personal data of any identifiable individual associated with those items.

An Internet Protocol (IP) address can be considered personal data if it can be associated with an identifiable individual.

Consent and Exceptions

Valid, informed consent is required for the disclosure of personal data, except in the following instances:

- To a lawyer representing the organization
- To comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction
- Where it is produced by individuals in the course of their employment, business or profession–as long as the disclosure is consistent with the purpose for which the information was produced
- To another organization in instances where it is reasonable for the purposes of: investigating a breach of an agreement or contravention of a federal or provincial law that has been, is being or is about to be committed; or detecting or suppressing or preventing fraud that is likely to be committed; and
- When it is contained in a witness statement, and the disclosure is necessary to assess, process, or settle an insurance claim.

APPENDIX K – Canada. Québec's Bill 64

On June 12, 2020, Bill 64 was introduced in Québec to modernize its private and public sector privacy laws. Bill 64 was adopted by the National Assembly on September 21, 2021. Québec takes the view that its privacy legislation applies to all collection of personal information in Québec, irrespective of the organization's general regulatory framework. Some key provisions of Bill 64 include:

Increased fines: The Bill introduces new penal offences with significant fines (upwards of 4% of annual revenue) and allows Québec's privacy regulator, the Commission d'accès à l'information (CAI), to impose on businesses, administrative penalties of up to the greater of (i) CAD 10,000,000, and (ii) the amount corresponding to 2% of worldwide turnover in the preceding year.

Stricter privacy requirements: This includes, among other requirements, mandatory PIAs, assessments for communications of personal information outside of Québec to ensure adequate protection, "separate" and "granular" consent and new individual rights such as data portability.

Mandatory Privacy Impact Assessments (PIA)

Québec law will now require PIAs with respect to: i) any project of acquisition, development and redesign of an information system project or electronic service delivery project involving personal information, ii) the transfer of personal information outside of Québec and iii) the communication of personal information without consent for study, research or statistics.

Enhanced Consent and Transparency Obligations

Bill 64 refines existing transparency requirements and introduces new ones to support valid consent from individuals. Consent must be specific to each use of personal information and implied consent is only accepted where some conditions are met. For example, implied consent may not be relied upon for the processing of sensitive personal information, as "opt-in" or express consent is required. As part of the amendments, "medical, biometric or otherwise intimate information" is now specifically considered as sensitive by nature, while the contextual analysis to determine whether any other type of information is sensitive in the circumstances, remains.

Regulation For De-Identified and Anonymized Information

Bill 64 regulates the use of de-identified and anonymized information. In the Bill, "de-identified information" means information that "no longer allows the person concerned to be directly identified", the operative term being "directly". Anonymized information, according to the Bill, means that "it is at all times reasonable to expect in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly", the operative terms being "irreversibly" and "directly or indirectly".

Once the organization achieves the purposes for which the personal information was collected, the Bill proposes two options: first, it can destroy it, or alternatively, it may anonymize it "for a serious and legitimate purpose" according to "generally accepted best practices."

Regulated Automated Decision-Making

Bill 64 introduces requirements related to the use of automated decision-making involving personal information. The terms refer particularly to decisions based exclusively on automated processes, which are understood to refer to decision made without the intervention of a human being.

Right to Data Portability

Bill 64 affords organizations a transition period of three years after the date of assent to develop and install the mechanisms necessary to transfer personal information "in a structured, commonly used technological format".

Introducing the "Right to Be Forgotten"

Under Bill 64, individuals may require organizations to cease disseminating personal information or to "de-index" a hyperlink attached to their name, that provides access to information by technological means, provided that certain conditions are met.

In addition to the "right to be forgotten", the individual has the right to require that an organization rectify information if the information is "inaccurate, incomplete or equivocal" or if collecting, communicating or keeping it are not authorized by law. If this information is obsolete or not justified by the purpose of the file, the individual may request that this information be deleted.

Transfer To Foreign Jurisdiction

Bill 64 sets out rules integrating the adequacy principle to the transfer of personal information to a foreign jurisdiction. Before communicating personal information outside Québec, businesses are required to conduct a privacy impact assessment in order to ensure that the personal information would receive protection equivalent to that afforded under the Private Sector Act. The same applies to situations where a business outsources the task of collecting, using, communicating or keeping personal information to an entity in a foreign jurisdiction.

Data Breach Notification

It is mandatory to report a confidentiality incident where a business has cause to believe that such an incident has occurred and that such incident presents a risk of serious injury. In that event, the business must promptly notify the Commission d'accès à l'information du Québec (CAI) and any person whose personal information is concerned.

Enforcement

Bill 64 allows the CAI to impose heavy monetary administrative penalties for violations of the Act.

APPENDIX L – Hong Kong. The Personal Data (Privacy) Ordinance (Cap. 486).

Applicability

The Ordinance applies to "everyone who is responsible for handling data (Data User) should follow the six Data Protection Principles ("DPPs") which represent the core of the Ordinance covering the life cycle of a piece of personal data."

Data Collection Principles

Data Collection Principle, Accuracy & Retention Principle, Data Use Principle, Data Security Principle, Data Openness Principle, and Data Access & Correction Principle.

Personal Data

Personal data is any data:

- Relating directly or indirectly to a living individual;
- From which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- In a form in which access to or processing of the data is practicable.

Examples of personal data protected by the ordinance include names, phone numbers, addresses, identity card numbers, photos, medical records and employment records.

Data Subject

In relation to personal data, data subject means the individual who is the subject of the data.

Data Controller ("Data User")

"Data User": In relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

Data Processor

A Data Processor:

- Processes personal data on behalf of another person; and
- Does not process the data for any of the person's own purposes.

Third Party: in relation to personal data, means any person other than:

- The data subject;
- A relevant person in the case of the data subject;
- The data user; or
- A person authorized in writing by the data user to collect, hold, process or use the data (i) under the direct control of the data user; or (ii) on behalf of the data user.

Cross-Border Transfers

No requirements on transfer of personal data to cross-border.

Access and Correction

A data subject must be given access to his/her personal data and allowed to make corrections if it is inaccurate.

Penalties

Noncompliance with Data Protection Principles does not constitute a criminal offense directly.

The commissioner may serve an Enforcement Notice to direct the data user to remedy the contravention and/or instigate the prosecution action. Contravention of an enforcement notice is an offense which could result in a maximum fine of HK$50,000 and imprisonment for two years.

An individual who suffers damage, including injured feelings, by reason of a contravention of the ordinance in relation to his or her personal data may seek compensation from the data user concerned.

The ordinance also criminalizes misuse or inappropriate use of personal data in direct marketing activities (Part VI); noncompliance with Data Access Request (section 19); unauthorized disclosure of personal data obtained without data user's consent (section 64).

APPENDIX M – Japan. Act on Protection of Personal Information.

Applicability

Applies to the use of a personal information for business. The APPI has a very broad and open concept of data processing.

Personal Data

"Personal Information" means the following two categories of information.

- Information about a living individual which can identify a specific individual by the description contained in the information, such as name, date of birth or other description (including voice or behavior information), including information which can easily be combined with other information so as to enable the identification of that individual; and
- Information that contains Personal Identifier Codes. "Personal Identifier Codes" means either
    - letters, numbers, marks or other codes for use with computers converted from a person's bodily information which may identify the person, or
    - letters, numbers, marks or other codes on cards or other documents which are unique to the user or purchaser and may identify the person. Apart from "Personal Information", "Personal Data" is separately defined to cover information stored in a business operator's database.

Personal Data is defined as Personal Information constituting the business operator's "Personal Information Database". A "Personal Information Database" in turn is defined as: (i) an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer; or (ii) an assembly of information in accordance with certain rules, and that has a table of contents, index or other means to facilitate the retrieval. Accordingly, once "Personal Information" is stored into a "Personal Information Database", such Personal Information becomes "Personal Data" under the APPI. There are some provisions in the APPI that specifically deal with Personal Data.

Sensitive Personal Data

Personal Information that needs special care ("Sensitive Data") is defined to include race, religion, social status medical history, criminal history and the fact that the person suffered damages by a crime.

Data Controller

There is no concept of a "Data Controller" under Japanese law. However, the APPI uses the term "business operator," which essentially refers to the entity responsible for the proper handling of all "Personal Information." This is similar to the concept of data controller under EU law.

Data Processor

There is no concept of a "Data Processor" under Japanese law. As such, handling of personal data under the APPI should pertain to how a "business operator" treats and manages the personal information or personal data in its possession.

Purpose Limitation

A business operator handling personal information shall not handle personal information beyond the scope necessary for achieving the purpose of use unless the business operator has obtained prior consent of data subjects. Purpose of use must promptly be notified to data subjects or publicly announced once a business operator acquires Personal Data, unless the purpose of use has already publicly announced.

Accuracy

A business operator handling personal information must endeavor to keep the content of Personal Data accurate and up to date, within the scope necessary for achieving the purpose of use.

Accountability

Japan does not recognize the concept of a data processor. Accountability lies with the business operator, which is similar to a data controller under EU law.

Access and Correction

The data subject may request the business operator to disclose, correct, add or delete the retained Personal Data.

Transfer of Personal Data to another Country

The APPI provides that Personal Data may not be transferred to a foreign country unless:

- The data subject has given specific advance consent to the transfer of the data subject's Personal Data to the entity in a foreign country;
- The country in which the recipient is located has a legal system that is deemed equivalent to the Japanese personal data protection system, designated by the Japanese data protection authority; or
- The recipient undertakes adequate precautionary measures for the protection of Personal Data, as specified by the Japanese data protection authority.

APPENDIX N – Singapore. Personal Data Protection Act.

Applicability

The PDPA has limited scope and does not apply to all Personal Data processing activities, most notably, it does not apply to the activities of the public sector or any organization acting as an agent of a public agency in processing Personal Data. Further, business contact information has effectively been excluded entirely from the operation of the PDPA. Also excluded from much of the PDPA obligations are data intermediaries, although data intermediaries do need to abide by the provisions on the protection of Personal Data and the deletion of Personal Data when the purposes are no longer served in their retention.

Personal Data

Personal Data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organization has or is likely to have access.

Sensitive Personal Data

The PDPA does not provide extra protection or special handling for sensitive Personal Data, such as health data, race, ethnicity and religion.

Consent

Section 13 of the PDPA requires consent to be given before Personal Data is collected, used, or disclosed. It explicitly provides in Section 14 that consent that is obtained without first notifying the individual of the purpose(s) is not valid consent, nor is the consent valid if false, misleading, or deceptive practices have been utilized. Further, the PDPA prohibits an organization from requiring an individual to consent to the collection, use or disclosure of Personal Data about the individual beyond what is reasonable to provide the product or service to that individual.

Exceptions to Consent

Consent can be deemed from an individual if the individual, without giving consent, voluntarily provides the Personal Data to the organization for that purpose, and it is reasonable that the individual would voluntarily provide the data.

Access, Correction and Erasure

Section 21 of the PDPA allows an individual to request access to Personal Data held by an organization and to information concerning its use or disclosure in the preceding one year. This right to request access is, however, subject to many exceptions. Similarly, Section 22 of the PDPA grants a right to request corrections in the Personal Data held by an organization that is due to error or omission. However, organizations can, on reasonable grounds, choose not to correct the data. If organizations decide against correction, then the Personal Data should be annotated with the correction that was requested but not made. There are also numerous exceptions to this right.

Any notion of a right to erasure in the PDPA might come from Section 25 concerning the requirement to destroy or de-identify Personal Data when there are no longer any legal or business and any other purpose for the retention of the Personal Data. This, however, is extremely limited in scope and could not be relied upon to compel the erasure of publicly available Personal Data on websites.

Accuracy and Completeness

Section 23 of the PDPA requires organizations to make a reasonable effort to ensure that Personal Data collected by or on behalf of the organization is accurate and complete.

Protection of Personal Data

Section 24 of the PDPA requires organizations to protect Personal Data in its possession or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.

Transfer Limitation

The PDPA has a provision limiting the transfer of Personal Data outside Singapore. The operation of this provision is set out in the Personal Data Protection Regulations 2014, and it is a codification of the most effective and workable aspects of the solutions currently found in international practice for protecting Personal Data that is transferred overseas.

APPENDIX O – People's Republic of China. Cybersecurity Law of the People's Republic of China.

Applicability

Limited to the territory of the People's Republic of China. The Law generally imposes obligations on three types of entities: (1) network operators; (2) "critical information infrastructure" operators; and (3) providers of network products and services.

Network Operators

Network operators are owners and administrators of networks and network service providers. A "network" is defined as any system comprising computers or other information terminals and related equipment for collection, storage, transmission, exchange, and processing of information.

On its face, the term network operator could broadly be interpreted to encompass any company that uses a network to do business in China despite not having a physical presence in China.

Critical Information Infrastructure Operators

Critical information infrastructure operators are defined as entities providing services that, if lost or destroyed, would endanger China's national security, economy, or public interest. The PRC Cybersecurity Law lists public communication and information services, energy, finance, transportation, water conservation, public services, and e-government as examples of CII operators.

Personal Data

Any information relating to an identified or identifiable Natural person.

Includes: all kinds of information, recorded electronically or otherwise, that can be used independently or combined with other information to identify a natural person.

Consent

If a network operator wishes to conduct a cross-border transfer that includes Personal Data, it must explain to the data subjects the cross-border transfer's purpose, scope, type, and country or region in which the recipient is located. The network operator must also obtain data subjects' consent except in emergencies (i.e., when the life or property of a data subject is in danger). The measures provide that consent can be inferred in certain scenarios, including where the data subject makes international phone calls related to the network operator, sends emails or instant messages to individuals or organizations overseas, and conducts cross-border e-commerce transactions, as well as other activities initiated by data subjects.

Cross-Border Transfers

If a network operator wishes to transfer Local Data outside of China, it must undergo a security assessment. Self-assessments generally suffice for this requirement and must consider, among other factors:

- The legality, legitimacy, and necessity of the cross-border transfer.
- The amount, scope, type, and sensitivity of the data.
- If the transfer involves Personal Data, whether data subjects have consented to the transfer.
- The data recipient's security capability, measures, and environment.

- The risks associated with the data being leaked, damaged, tampered with, or misused after the data transfer or subsequent re-transfer.
- The risks to national security, societal and public interests, and the individual lawful rights and interests after the cross-border transfer.

Cross-border transfers of Local Data are prohibited in the following circumstances:

- The transfer does not comply with state laws, administrative regulations, or departmental rules.
- Data subjects do not consent to a transfer involving personal information.
- The transfer poses risks to China's national security or public interests.
- The transfer could endanger China's security of national politics, territory, military, economy, culture, society, technology, information, ecological environment, resources, and nuclear facilities.
- Other circumstances where the Chinese government determines that the data involved in the transfer is prohibited from being transferred offshore.

Security

Network operators

Network operators must (1) develop internal security management systems and procedures, (2) appoint personnel responsible for network security, and (3) implement network security protection responsibility. In addition, they must:

- Adopt measures to prevent viruses, network attacks, network intrusions, and other threats to network security.
- Monitor and record network activity and security incidents, and store network logs for at least six months.
- Implement measures to classify, back up, and encrypt data.

Critical Information Infrastructure (CII) Operators

CII operators must adhere to the same requirements as that of network operators.

Providers of Network Products and Services

Providers of network products and services must comply with relevant national and industry standards and ensure the security of their products. Products determined to be "Critical Network Equipment and Network Security Products" are required to go through testing by accredited evaluation centers prior to being marketed in China.

Penalties

Penalties for violation of the CSL include (1) a fine, the limit of which is up to 10 times the illegal gains resulting from the violation, with a limit of approximately $145,000 per violation; (2) equitably remedies, such as a website shutdown or a temporary or definitive suspension of the business license; and/or (3) criminal penalties, such as detention of the person responsible for the violation (in the case of serious circumstances).

APPENDIX P – People's Republic of China. Personal Information Protection Law (PIPL)

On August 20, 2021, the National People's Congress (NPC) of China adopted the Personal Information Protection Law (PIPL) with an effective date of November 1, 2021. The PIPL aims to "protect the rights and interests of individuals," "regulate personal information processing activities," and "facilitate reasonable use of personal information" (Article 1).

The definition of "personal information" and "processing of personal information" are defined similarly under both of the PIPL and the GDPR. Sensitive personal information is defined under the PIPL as "personal information that, once leaked, or illegally used, may easily infringe the dignity of a natural person or cause harm to personal safety and property security, such as biometric identification information, religious beliefs, specially-designated status, medical health information, financial accounts, information on individuals' whereabouts, as well as personal information of minors under the age of 14" (Article 28). The PIPL uses the term "personal information processing entity" to refer to "organization or individual that independently determines the purposes and means for processing of personal information" (Article 73). This appears to be the Chinese law equivalent of the "data controller" concept under the GDPR. Further, the PIPL uses "entrusted party" to refer to "data processor" as defined under the GDPR.

Exceptions

There are few, if any, exceptions to PIPL for types of information or categories of organizations. One exception is similar to GDPR in that PIPL "does not apply to natural persons handling personal information for personal or family affairs" (Art. 72). There is also an exception to PIPL for government agencies for statistical and archival purposes, but only where those activities should follow the applicable law.

Sensitive Personal Information

Data Handlers or Data Controllers managing sensitive personal information carry additional obligations. Sensitive personal information may only be processed for a specific purpose and need, with strict protective measures (Art. 28). "Sensitive personal information" means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons, grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.

Principles

Personal information must be handled (processed) under certain principles, and cannot be processed in "misleading, swindling, coercive, or other such ways" (Art. 5). These principles include:

- Legality
- Propriety
- Necessity
- Sincerity
- Transparency (Art. 7)
- Quality & Accuracy (Art. 8)

Data Subject Rights

PIPL provides individuals with certain rights (Chapter IV), which must be addressed in a timely manner. Except where applicable laws say otherwise, these rights include the following:

- Transparency and notice (Art. 17)
- Know if an entity is processing their personal information (Art. 44)
- Decide if and how their personal information is processed (Art. 44)
- Limit or refuse data processing (Art. 44)
- View and copy (exceptions are provided, mainly if restricted by other laws) (Art. 45)
- Portability (Art. 45)
- Correction and amendment (Art. 46)
- Deletion (Art. 46)
- To know (and have explained) the personal information handling rules, if there are any (Art. 48)
- Non-discrimination for exercising rights (Art. 16)
- Know automated decision-making activities (Art. 24)
- Refuse automated decision-making for significant activities
- Refuse targeted ads done by automation
- Consent to cross-border transfers (Art. 39)

Consent

Consent under the PIPL must be informed, freely given, demonstrated by a clear action of the individual, and may later be withdrawn (Articles 14 & 15). However, the PIPL requires a separate consent for certain processing activities, namely if a processing entity (i) shares personal information with other processing entities; (ii) publicly discloses personal information; (iii) processes sensitive personal information; or (iv) transfers personal information overseas (Articles 23, 25, 29 and 39). If any changes occur, such as a new purpose for the data, a new way of handling the data, or collecting new categories of data, the individual must be informed and must agree to such new or different data processing - in advance. If Handlers process the personal information of minors under the age of 14, they shall obtain the consent of the parent or other guardian of the minor (Art. 31). Along with consent, though, comes the revocation of consent (Art. 15). Individuals must be able to revoke consent in a convenient manner.

Automated Decision-making

“Automated decision-making” refers to the activity of using computer programs to automatically analyze or access personal behaviors, habits, interest, or hobby, or financial, health, credit, or other status, and make decisions (based thereon). Handlers must be transparent about the decision-making automated process and guarantee the fairness and justice of the result. Handlers are prohibited from engaging in unreasonable differential treatment of individuals in trading conditions, such as with a trade price, etc. (Art. 24).

De-identification vs Anonymization

“De-identification” refers to the process of personal information undergoing handling to ensure it is impossible to identify specific natural persons without the support of additional information whereas “anonymization” refers to the process of personal information undergoing handling to make it impossible to distinguish specific natural persons and impossible to restore. The former makes it hard to identify people, only possible with additional information. The latter means they cannot be identified any longer.

Surveillance

PIPL prohibits the installation of image collection or personal identity recognition equipment in public venues, unless for public security only, when abiding by relevant State regulations, and if clear signs are posted indicating surveillance is in place. Collected personal images and personal distinguishing identity characteristic information can only be used for the

purpose of safeguarding public security; it may not be used for other purposes, except where individuals' separate consent is obtained.

Responding to Individual Requests

The requirement is to respond "in a timely manner" with no mention of a delayed response scenario. However, if entities reject individuals' requests to exercise their rights, individuals may file a lawsuit.

Transparency (privacy notice)

Before processing personal information, Data Handlers shall explicitly provide an accurate (truthful), clear, and understandable privacy notice (Art. 17) that includes:

- The name or personal name and contact method of the personal information handler
- The purpose of personal information handling and the handling methods, the categories of handled personal information, and the retention period
- Methods and procedures for individuals to exercise the rights including how to reach the DPO
- Other items that laws or administrative regulations provide shall be notified
- For sensitive personal information, Handlers must also disclose the necessity and the influence on individuals' rights and interest except where permitted not to do so (Art. 30)
- Cross-border transfers, currently or proposed in future, with separate consent

Cookies

Under the general provisions of the law, it is safe to assume that the placement of cookies and trackers on the equipment of a user that is based in China, constitutes data processing that is covered by PIPL. The handling of cookie and tracker data requires a legal basis under Article 13 PIPL and opt-in consent is required. Essential cookies can be placed without the individual's consent, based on an exception in Article 16 PIPL, that allows data processing "necessary for the provision of products or services."

Security and Data Breach

Handlers must immediately remediate personal information leaks, distortions, or loss (potential or actual) and notify the designated authorities and the individuals. The notification shall include the following items:

- The information categories, causes, and possible harm caused by the leak, distortion, or loss that occurred or might have occurred
- The remedial measures taken by the Handler and measures individuals can adopt to mitigate harm
- Contact method of the Handler.

Handlers are not required to notify individuals if there was no harm, however, where authorities believe harm may have been created, they may require individuals to be notified. There is no timeframe provided, nor are there references to notifications by entrusted persons.

Data Transfers

Data Transfers due to Mergers, etc.
Handlers can transfer personal information, where necessary, due to mergers, separations, dissolution, declaration of bankruptcy, and other such reasons, but must notify individuals about the receiving party's name or personal name and contact method. The receiving party shall continue to fulfill the personal information handler's duties.

Sharing Personal Information – Vendors/Data Processors (Entrusted Persons)
Where Handlers share personal information outside the entity, the recipients are considered "entrusted persons" (Art. 59) and must only process the information according to PIPL and other applicable laws, safeguard the information, and assist Handlers in their obligations under PIPL. Handlers must notify individuals about any data sharing outside the entity. Where this is to another Handler (controller to controller), Handlers shall provide the name or personal name of the recipient, contact method, purpose for sharing, data categories, and obtain separate consent from the individual (Art. 23). Recipients must honor the approved processing - the purposes, methods, categories of data, etc. If recipients change any of this, they must obtain new consent from the individuals.

Cross-Border Transfers
Where Handlers "truly need" to transfer personal information outside the borders of China or business or other requirements, they have to meet the following conditions (Art. 38):

- Passing a security assessment organized by the State cybersecurity and information Department according to Article 40
- Undergoing personal information protection certification conducted by a specialized body according to Provisions by the State
- Including a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and information Department, agreeing upon the rights and responsibilities of both sides
- Other conditions provided in laws or administrative regulations or by the State cybersecurity and information department.

Enforcement

Under PIPL, enforcement options include both civil and criminal penalties (Art. 66), and may include:

- Compliance orders
- Processing bans
- Confiscation of unlawful income
- Fines

APPENDIX Q – People's Republic of China. Data Security Law (the DSL)

On June 10, 2021, China's national legislature – the Standing Committee of the National People's Congress passed the Data Security Law (the "DSL"). The DSL took effect on September 1, 2021, and marks China's first comprehensive data regulatory regime, one of three key frameworks that will buttress the country's data and cybersecurity governance. The DSL works in tandem with China's 2017 Cybersecurity Law (the "CSL"), which requires firms to improve the security of their data networks and the Personal Information Protection Law (the "PIPL"), which took effect on November 1, 2021.

1. Scope of Application and Extraterritorial Reach

The DSL governs not only data processing (which includes the collection, storage, use, processing, transmission, provision, and disclosure of data) and management activities conducted within China, but also those outside of China that have the potential to harm China's national security or public interest or damage the legal interests of any Chinese citizen or organization. The DSL empowers multiple Chinese governmental authorities to oversee data security matters:

- The Central National Leadership Organ is responsible for issuing and overseeing national data security strategies and major policies. It is required to establish a national data security working and coordination mechanism with bureaus responsible for data security supervision and management.
- Local governments and regulatory authorities are also responsible for data security in their respective regions and industries and are empowered to formulate specific catalogues of important data.

2. Data Categorization

The DSL grants authority to China's Central Government to establish a hierarchical data categorization system in accordance with the importance of the data to China's economy, national security, livelihood of Chinese citizens, and public and private interests. This system will result in data deemed more important to China's national interest being more heavily regulated. To this point, the DSL focuses on two categories of data subject to a heightened level of regulation and protection: "important data" and "national core data." We discuss each in turn below:

Important Data

The concept of "important data" was introduced in the CSL, requiring elevated protection, a localization requirement, and a prior security assessment for cross-border transfer of important data by critical information infrastructure operators ("CIIOs"). CIIOs are generally entities operating in the communications, information technology, finance, transportation, and energy sectors. While the CSL only required CIIOs to comply with heightened regulation for important data, the DSL expands this requirement to all businesses that process important data. Under the DSL, processors of important data must:

i. Identify the responsible person and management body for data security and allocate data security protection responsibilities; and
ii. Conduct regular risk assessments on data processing activities and submit risk assessment reports to competent authorities.

While the CSL and DSL do not define "important data," the DSL states that a consortium of national-level agencies will develop catalogue(s) of "important data" and mandates that local governments and regulatory agencies develop more detailed catalogues to identify the scope of "important data" based on their respective region and sectors. Thus, international companies have to comply with both the broader national requirements, as well as the region and industry-specific catalogue(s) for important data.

National Core Data
The DSL also introduces the concept of "national core data," a class of data subject to stricter regulations due to its relation to national security, the national economy, citizen's livelihoods, and important public interests. While there will likely be further rules and regulations detailing the scope of national core data and guidelines for its protection, violations of the national core data management system may be subject to fines of up to 10 million yuan (~$1.56 million USD), revocation of business licenses, suspension of business, or possible criminal penalties. The law also imposes penalties on entities that fail to cooperate with data requests from Chinese authorities for law enforcement or national security matters.

3. General Data Security Obligations of Data Processors
The DSL specifies numerous obligations that data processors must fulfil, including:

- Establishing a data security management system, adopting necessary technical measures for data security, and conducting data security training.
- Collecting and using data by lawful and proper means, including in accordance with any restrictions imposed by laws and regulations that speak to the purpose and scope of data collection and use.
- Monitoring potential risks and, in the event of discovering a security incident or defect, promptly notifying users and adopting remedial measures.
- Under the DSL, entities that process "important data" must designate a data security officer, establish a data security management department, conduct periodic assessments to monitor potential risks, and report those results to applicable government agencies.

4. Cross-Border Data Transfers
For cross-border transfers of "important data," the DSL establishes a separate framework for CIIOs and non-CIIOs. CIIOs must comply with rules under the CSL, which requires local storage for important data that is collected in China. If a CIIO must transfer data out of China for a necessary business purpose, a security assessment in accordance with the procedures of the Cyberspace Administration of China (CAC) is required.

Importantly for litigation and international legal proceedings, the DSL states that without approval from Chinese authorities, no organizations or individuals in China may transfer data stored within China to any foreign judicial or enforcement authorities. Neither the specific authorities nor the details of the approval processes are specified in the DSL, but entities that violate this requirement face fines of up to 1 million yuan (~$156,000 USD), with additional fines for responsible individuals. Entities whose violations result in "serious consequences" may face fines of up to 10 million yuan (~1,560,000 USD) and the potential suspension of the business and revocation of its business license.

5. Penalties for Violations
Entities that violate their obligations under the Data Security Law face severe penalties. In addition to those penalties mentioned above, Chinese authorities may impose fines of up to 500,000 yuan (~$77,000 USD) on noncompliant entities, issue additional fines to responsible individuals, and mandate remedial measures. If an entity fails to adopt remedial measures after receiving a warning, or if a security incident results in serious consequences (such as a large-scale data breach or leak), the entity may face fines of up to 2 million yuan (~$310,000 USD), as well as the potential suspension of business processes and revocation of the business license.

Additionally, the DSL empowers China's Central Government to respond in kind against any foreign state that purportedly discriminates against Chinese interests regarding investment and trade related to data technologies.

APPENDIX R – Australia. Privacy Act 1988

Applicability

The Australian Privacy Principles (APPs) apply to "APP entities" — that is, Australian, Australian Capital Territory, and Norfolk Island government agencies and private sector businesses.

Individuals and "small business operators" — businesses with an annual turnover of less than AUD $3 million, are exempt from the operation of the act. The Privacy Act does not distinguish between data controllers and data processors — any APP entity that holds Personal Data must comply with the APPs.

Australian Privacy Principles (APPs)

The APPs include: APP 1: Open and transparent management of personal information; APP 2: Anonymity and pseudonymity; APP 3: Collection of solicited personal information; APP 4: Dealing with unsolicited personal information; APP 5: Notification of the collection of personal information; APP 6: Use or disclosure of personal information; APP 7: Direct marketing; APP 8: Cross-border disclosure of personal information; APP 9: Adoption, use or disclosure of government related identifiers; and APP 10: Quality of personal information.

Personal Data

The Privacy Act governs the handling of Personal Data, defined as “information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.”

Data Subject

"Individual" is defined as “a natural person”.

Controller and Processor

The Privacy Act does not distinguish between controllers and processors. Instead, the APPs apply to any APP entity that collects Personal Data. The definition of "APP entity" includes:

- Most Australian Government agencies,
- All private sector and not-for-profit organizations with an annual turnover of more than AUS $3 million,
- All private health service providers, and
- Some small businesses (i.e., that trade in personal information for a benefit, are a contracted service provider to the Australian Government, or are a credit reporting body.

Consent

“Consent” is defined as “express consent or implied consent.” Regulator guidance indicates that the four key elements of consent are:

- The individual is adequately informed before giving consent.
- The individual gives consent voluntarily;
- The consent is current and specific; and
- The individual has the capacity to understand and communicate consent.

Sensitive Personal Information

- "Sensitive information" is a subset of Personal Data and is defined as: Information or an opinion (that is also personal information) about an individual's: (1) Racial or ethnic origin; (2) Political opinions; (3) Membership of a political association; (4) Religious beliefs or affiliations; (5) Philosophical beliefs; (6) Membership of a professional or trade association; (7) Membership of a trade union; (8) Sexual orientation or practices, or (9) Criminal record.
- Health information about an individual.
- Genetic information (that is not otherwise health information);
- Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- Biometric templates.

APP 3 provides that sensitive information about an individual must not be collected unless the individual consents and the collection is reasonably necessary for an APP entity's functions or activity, or a listed exception applies.

Cross-Border Transfers

APP provides that, before disclosing personal information outside of Australia, a business must take reasonable steps to ensure that the recipient does not breach the APPs in relation to the information unless a listed exception applies. An APP entity that discloses personal information to an overseas recipient is accountable for a breach of the APPs by the recipient in relation to the information.

Breach Notification

APP entities that experience "eligible data breaches" (that generate a "likely risk of serious harm" to affected individuals) must give a statement in a prescribed format to the Information Commissioner as soon as practicable, and to affected individuals.

If it is unclear whether a breach is eligible, APP entities must conduct an assessment within 30 days of becoming aware of the breach.

Penalties

A breach of the APPs is an "interference with privacy. Serious or repeated interferences with privacy may be subject to a civil penalty of up to AUD $2.3 million for companies."

APPENDIX S – U.S. HIPAA (Health Insurance Portability and Accountability Act).

Applicability

Epiq maintains a HIPAA Compliance Program which addresses the company's program governance compliance requirements under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). HIPAA provides certain standards for creating, storing, managing, transmitting, and disclosing Protected Health Information ("PHI") designed to protect the confidentiality and security of the PHI.

HIPAA applies directly to a Covered Entity (defined as a health plan, a health care clearinghouse, or a health care provider), and Business Associate, i.e., a subcontractor that creates, receives, maintains, or transits protected health information on behalf of a Covered Entity. Epiq provides services as a Business Associate and thus must comply with HIPAA standards.

HIPAA applies to covered entities and business associates within the United States, including non-United States citizens or residents.

Business Associate Agreement

Epiq will not accept PHI from a Covered Entity unless a Business Associate Agreement (BAA) that meets the requirements of HIPAA has been entered into with the Covered Entity. This policy applies whenever PHI is disclosed by a Covered Entity to Epiq, including the period before and after an engagement begins.

Use and Disclosure of PHI

Epiq will use and disclose a client's PHI only as permitted by its Business Associate Agreement, as permitted or required by law, and in accordance with the HIPAA Compliance Program. Epiq will limit its uses, disclosures, or requests for PHI, to the extent practicable, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request.

Return or Destruction of PHI

Where feasible, at the termination of a project, Epiq will return or will destroy PHI received from a Covered Entity or created or received on behalf of such an entity. PHI contained in reports or other files from a project will be deleted at the end of an engagement, including backup copies from a client's system. Paper copies containing PHI will be shredded with Epiq's or the client's shred vendor, unless such information can be retained pursuant to the BAA or in accordance with applicable law.

Requests for Information

Requests for access to information by the Secretary of Health and Human Services for access, amendment, or accounting purposes by individuals, or by the Covered Entity, should be directed to the HIPAA Security & Privacy Officer, who will respond to such request in accordance with the applicable BAA and Sections 164.524, 164.526, and 164.528 of the HIPAA Privacy Rule and in coordination with the client.

HIPAA Security Requirements

Epiq is responsible for ensuring the security, confidentiality, integrity, and availability of its information systems containing ePHI by implementing appropriate and reasonable policies, procedures, and controls to prevent, detect, contain, and correct issues or concerns. Epiq will develop and maintain written policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission and/or disposal of electronic protected health information.

Disciplinary Actions

In accordance with the provisions of the Epiq Code of Business Conduct and Ethics, Epiq Personnel found to have violated the HIPAA Compliance Program will be disciplined in an appropriate, measured, and consistent fashion. Violations, including the failure to report the misconduct of other Epiq Personnel, may result in disciplinary actions, including termination.

Communication and Reporting

Epiq Personnel are required, within twenty-four (24) hours of identifying an issue, to notify any issue or violation of the Program to such individual's Manager, who will immediately notify the appropriate HIPAA Program Owner, in order to report any violations of law, suspected breaches of PHI, suspected security incidents involving PHI, as well as any actual or suspected Program violations for which they are responsible or become aware.

Communications received by any Epiq Personnel from government agencies or Epiq clients on any of the matters addressed in this Program shall be forwarded to the HIPAA Program Owner immediately for discussion with the HIPAA Security & Privacy Officer.

PHI Breach Determination and Notification Process

A breach may have occurred if (a) unsecured PHI is accessed, used or disclosed in a way that is not allowed under the HIPAA Privacy Rules and (b) such access, use or disclosure compromises the security or privacy of the PHI by posing a significant risk of financial, reputational, or other harm to the potentially affected individual.

If the Covered Entity or a Business Associate discovers a breach of unsecured PHI, organizations may be required to notify affected individuals, federal and state government agencies, and in some cases, the media. Notification is not required if there is a breach and PHI is "secured".

APPENDIX T – Brazil. General Data Protection Law (LGPD)

Applicability

The LGPD applies to any processing operation carried out by a natural person or a legal entity, of public or private law, irrespective of the means used for the processing, the country in which its headquarter is located or the country where the data are located, provided that:

- The processing operation is carried out in Brazil
- The purpose of the processing activity is to offer or provide goods or services, or the processing of data of individuals located in Brazil, or
- The personal data was collected in Brazil

On the other hand, the law does not apply to the processing of personal data which is:

- Carried out by a natural person exclusively for private and non-economic purposes
- Performed for journalistic, artistic or academic purposes
- Carried out for purposes of public safety, national security and defense or activities of investigation and prosecution of criminal offenses (which will be the subject of a specific law), or
- Originated outside the Brazilian territory and are not the object of communication
- Shared data use with Brazilian processing agents or the object of international transfer of data with another country that is not the country of origin, provided that the country of origin offers a level of personal data protection adequate to that established in the Brazilian law

Personal Data

The LGPD defines personal data as any information related to an identified or identifiable natural person.

Anonymized data is not to be considered personal data, except when the process of anonymization has been reversed or if it can be reversed applying reasonable efforts.

Sensitive personal data is defined as any personal data concerning:

- Racial or ethnic origin
- Religious belief
- Political opinion
- Trade union
- Religious, philosophical or political organization membership
- Health or sex life
- Genetic or biometric data

Collection and Processing

Under LGPD collection and processing is referred to as data treatment, and defined as all operations carried out with personal data.

Treatment of personal Data

The treatment of personal data may only be carried out based on one of the following legal bases, which largely align to the GDPR:

- With data subject consent
- To comply with a legal or regulatory obligation by the controller
- By the public administration, for the processing and shared use of data which are necessary for the execution of public policies provided in laws or regulations or contracts, agreements, or similar instruments
- For carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data
- For the execution of a contract or preliminary procedures related to a contract of which the data subject is a party
- For the regular exercise of rights in judicial, administrative or arbitration procedures
- As necessary for the protection of life or physical safety of the data subject or a third party
- For the protection of health, in a procedure carried out by health care, health services or sanitary authority professionals
- To fulfill the legitimate interests of the controller or a third party, except in the case of prevailing the fundamental rights and freedoms of the data subject, and
- For the protection of credit

As for the processing of sensitive personal data, the treatment can only occur when the data subject or her or his legal representative consents specifically and in highlight, for specific purposes; or, without consent, under the following situations:

- As necessary for the controller's compliance with a legal or regulatory obligation
- Shared data processed as necessary for the execution of public policies provided in laws or regulations by the public administration
- For carrying out studies by research entities, ensuring, whenever possible, the anonymization of personal data
- For the regular exercise of rights, including in a contract or in a judicial, administrative and arbitration procedure
- Where necessary to for the protection of life or physical safety of the data subject or a third party
- The protection of health, exclusively, in a procedure performed by health care, health services or sanitary authority professionals, or
- ensuring the prevention of fraud and the safety of the data subject
- The controller and operator must keep records of the data treatment operations they carry out, mainly when the processing is based on a legitimate interest.

The controller and operator must keep records of the data treatment operations they carry out, mainly when the processing is based on a legitimate interest.

Cross-Border Transfer

The transfer of personal data to other jurisdictions is allowed only subject to compliance with the requirements of the LGPD. Also, prior consent is needed for such transfer, unless:

- The transfer is to countries or international organizations with an adequate level of protection of personal data
- There are adequate guarantees of compliance with the principles and rights of data subject provided by LGPD, in the form of
    - Specific contractual clauses for a given transfer Standard contractual clauses
    - Global corporate norms, or
    - Regularly issued stamps, certificates, and codes of conduct
- The transfer is necessary for international legal cooperation between public intelligence, investigative and prosecutorial agencies
- The transfer is necessary to protect life or physical safety of the data subject or of third-party Authorization has been provided by the ANPD
- The transfer is subject to a commitment undertaken through international cooperation
- The transfer is necessary for the execution of a public policy or legal attribution of public service
- The transfer is necessary for compliance with a legal or regulatory obligation, execution of a contract or preliminary procedures related to a contract, or the regular exercise of rights in judicial, administrative or arbitration procedures

Breach Notification

The controller must report to ANDP and the data subject in a reasonable time-period (to be further defined by the ANDP) if the breach is likely to result in risk or harm to data subjects.

The notice must contain, at least, the following:

- Description of the nature of the affected personal data
- Information regarding the data subjects involved
- Indication of the security measures used
- The risks generated by the incident
- The reasons for delay of communication (if any)
- The measures that were or will be adopted

Additionally, the ANDP shall verify the seriousness of the incident and may, if necessary to safeguard the data subject's rights, order the controller to adopt measures, such as the broad disclosure of the event in communications media, as well as measures to reverse or mitigate the effects of the incident.

Appendix U – India. Information Technology Act, 2000

At present, the Information Technology Act, 2000 (the Act) and rules notified thereunder largely govern data protection in India.

On August 24, 2017, a Constitutional Bench of nine judges of the Supreme Court of India in Justice K.S.Puttaswamy (Retd.) v. Union of India [Writ Petition No. 494/ 2012] upheld that privacy is a fundamental right, which is entrenched in Article 21 [Right to Life & Liberty] of the Constitution. This led to the formulation of a comprehensive Personal Data Protection Bill 2019 (the PDP Bill)1. The enactment of the PDP Bill will overhaul the personal data protection and regulatory regime in India. Until such time, the Act and rules provided therein govern data privacy in India. The PDP Bill is currently pending consideration of the Indian Parliament
and may undergo significant changes to its current form, based on a report submitted by a Joint Parliamentary Committee formed to analyze the PDP Bill. The PDP Bill is expected to come into effect towards the end of 2021.

India's IT Ministry adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Privacy Rules), notified under the Act. The Privacy Rules, which took effect in 2011, require corporate entities collecting, processing and storing personal information, including sensitive personal information, to comply with certain procedures. It distinguishes both 'personal information' and 'sensitive personal information', as defined below.

In August 2011, India's Ministry of Communications and Information issued a 'Press Note' Technology (Clarification on the Privacy Rules), which provided that any Indian outsourcing service provider/organization providing services relating to the collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligation with any legal entity located within or outside India is not subject to collection and disclosure of information requirements, including the consent requirements discussed below, provided that they do not have direct contact with the data subjects (providers of information) when providing their services.

As stated above, India is in the process of overhauling its personal data protection regime. However, there is a possibility of a new regulatory framework for non-personal data in India. The Ministry of Electronics & Information Technology in the year 2019 formed a committee to make recommendations for the consideration of the Central Government on the regulation of non-personal data (NPD) and released its report on non-personal data governance framework (the NPD Report). The NPD Report defines NPD as data which is not personal data as defined under the PDP Bill or data without any personally identifiable information. The NPD Report, among others, recommends that appropriate standards of anonymization of NPD be defined to prevent/minimize the risks of re-identification. It remains to be seen if NPD will also be regulated under the PDP Bill and how it will impact various stakeholders.

Personal Data

The Privacy Rules define "personal information" as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is

capable of identifying such person.

Sensitive Personal Data

The Privacy Rules define "sensitive personal data or information" to include the following information relating to:

- Passwords
- Financial Information
- Physical, physiological and mental health conditions
- Sexual orientation
- Medial records and history
- Biometric information
- Any detail relating to the above clauses as provided to a corporate entity for providing services
- Any of the information received under the above clauses for storing or processing under lawful contract or otherwise

Biometrics means the technologies that measure and analyze human body characteristics, such as fingerprints, eye retinas and irises, voice patterns, facial patterns, hand measurements and DNA for authentication purposes.

However, any information that is freely available in the public domain is exempt from the above definition.

Data Protection Officers

Every corporate entity collecting sensitive personal information must appoint a Grievance Officer to address complaints relating to the processing of such information, and to respond to data subject access and correction requests in an expeditious manner but within one month from the date of receipt of the request or grievance.

There is no specific requirement that the data protection officer must be a citizen of or resident of India, nor are there any specific enforcement actions or penalties associated with not appointing a data protection officer correctly. However, appointment of a data protection officer is part of the statutory due diligence process and it is thus imperative that such an officer should be appointed.

Collection and processing

Under the Act, if a corporate entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining compliance with the Privacy Rules, and its negligence causes wrongful loss or wrongful gain to any person, the corporate entity shall be liable for damages to the person(s) affected.

Cross Border Transfer

The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal

information to any other corporate entity or person in India, or to any other country that ensures the same level of data protection as provided for under the Privacy Rules. However, consent is not necessary for the transfer if it is required for the performance of a lawful contract between the corporate entity (or any person acting on its behalf) and the provider of information or as otherwise specified in the Act.

A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required by the Act.

The contract regulating the data transfer should contain adequate indemnity provisions for a third-party breach, should clearly specify the end purposes of the data processing (including who has access to such data) and should specify a mode of transfer that is adequately secured and safe.

Further, under the Act, it is an offense for any person who has pursuant to a contract gained access to any material containing personal information to disclose that information without the consent of the person concerned, and with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.

Breach Notification

The government of India has established and authorized the Indian Computer Emergency Response Team ("Cert-In") to collect, analyze and disseminate information on cyber incidents, provide forecasts and alerts of cybersecurity incidents, provide emergency measures for handling cybersecurity incidents and coordinate cyber incident response activities.

The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 ("Cert-In Rules") impose mandatory notification requirements on service providers, intermediaries, data centers and corporate entities, upon the occurrence of certain cybersecurity incidents.

Companies are required to notify the Cert-In within reasonable time, so as to leave scope for appropriate action by the authorities. However, it is important to follow breach notice obligations, which would depend upon the "place of occurrence of such breaches" and whether or not Indian customers have been targeted.

Appendix V – New Zealand. The Privacy Act 2020 (Act) and its Information Privacy Principles (IPPs)

The Privacy Act 2020 (Act) and its Information Privacy Principles (IPPs) govern how agencies collect, use, disclose, store, retain and give access to personal information. The Act gives the Privacy Commissioner the power to issue codes of practice that modify the operation of the Act in relation to specific industries, agencies, activities, or types of personal information. The following codes are currently in place:

- Credit Reporting Privacy Code Health Information Privacy Code Justice Sector Unique Identifier Code
- Superannuation Schemes Unique Identifier Code Telecommunications Information Privacy Code
- Civil Defence National Emergencies (Information Sharing) Code

Enforcement is through the Privacy Commissioner. The Privacy Commissioner has the power to investigate any action which appears to interfere with the privacy of an individual and can do so either on a complaint made to the Commissioner or on the Commissioner's own initiative. The Privacy Commissioner can also issue compliance notices requiring agencies to do or refrain from doing something in order to comply with the Act.

Under the Act, an agency can be any person or body of persons, whether corporate or unincorporated, and whether in the public sector or in the private sector.

The Act has extraterritorial scope – it applies to any actions taken by an overseas organization in the course of carrying on business in New Zealand, regardless of where the information was collected or held and where the person to whom the information relates is located. An organization would be treated as carrying on business in New Zealand whether or not it has a physical place of business in New Zealand, charges any monetary payment for goods or services, or makes a profit from its business in New Zealand.

Personal Data

Personal information under the Act is defined as information about an identifiable individual and includes information relating to a death that is maintained by the Registrar General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act.

National Data Protection Authority

The Privacy Commissioner’s Office
Level 8
109.111 Featherston Street
Wellington 6143
New Zealand
T +64 474 7590
enquires@privacy.org.nz

www.privacy.org.nz

Data Protection Officers

The Act requires each agency to appoint one or more individuals to be a privacy officer. The privacy officer may be within or external to the agency (i.e. the privacy officer role may be outsourced to a third party) and does not need to be a New Zealand citizen or reside in New Zealand.

The privacy officer's responsibilities include the following:

- The encouragement of compliance with the personal information privacy principles contained in the Act Dealing with requests made to the agency pursuant to the Act
- Working with the Privacy Commissioner in relation to investigations relating to the agency Ensuring compliance with the provisions of the Act

Collection and Processing

Subject to specific exceptions, agencies may collect, store and process personal information in accordance with the 13 information privacy principles (IPP) summarized below.

IPP 1 - Purpose of collection of personal information
An agency must not collect personal information other than for a lawful connected to the agency's functions, and only if the collection of the information is necessary for that purpose.

IPP 2 - Source of personal information
An agency must collect information directly from the relevant individual, unless one of the specified exceptions applies, which include if collection from the individual is not practical in the circumstances, if collection from a third party would not prejudice the interests of the individual, or if the information is publicly available.

IPP 3 - Collection of personal information from subject
Before collecting personal information, an agency has to make the relevant individual aware of certain things, such as the fact that information is being collected, the purposes for which it will be used, and the right to access and request correction of personal information. This is typically done by way of a privacy policy. There are several exceptions where the person collecting information would not need to comply with IPP 3, including where compliance is not reasonably practicable in the circumstances.

IPP 4 - Manner of collection of personal information
Agencies cannot collect personal information by unlawful or unfair means, or in a manner that intrudes to an unreasonable extent upon the personal affairs of the individual concerned. Particular care must be taken when collecting personal information from children or young persons.

IPP 5 - Storage and security of personal information

Agencies must ensure personal information is protected by reasonable security safeguards against loss and unauthorized access, use, modification or disclosure or other misuse. If it is necessary to give personal information to another person (e.g. a service provider), an agency must do everything reasonably within its power to prevent unauthorized use or disclosure of that information.

IPP 6 - Access to personal information

Where an agency holds personal information about an individual, subject to certain exceptions, if requested by the individual, the agency must confirm whether it holds the information and grant the individual access to it. The exceptions include where the information is not readily retrievable or:

- The refusal is for the protection of the health, safety or similar of an individual
- In an employment context, the information is evaluative (eg, compiled for the purpose of determining the suitability of an individual for employment) and disclosure would breach an implied promise that was made to the person who supplied the information
- The information needs protecting because it would involve disclosure of a trade secret or be likely to unreasonably prejudice the commercial position of the person who supplied the information, unless the public interest in disclosure outweighs the withholding of the information
- The information does not exist or cannot be found
- The disclosure would involve the unwarranted disclosure of the affairs of another individual the disclosure would breach legal professional privilege, or
- The request is frivolous or vexatious, or the information requested is trivial

IPP 7 - Correction of personal information

An individual can request an agency to correct information the agency holds about the individual or attach a statement of a correction sought but not made. If an agency has corrected personal information or attached a statement of a correction sought but not made, if reasonably practicable, it will inform each person or entity to whom it has disclosed that information of that correction or statement. The agency must inform the individual of any action taken as a result of the individual's request.

IPP 8 - Accuracy of personal information to be checked before use or disclosure

Agencies must take reasonable steps to ensure personal information they hold is accurate, up to date, complete, relevant, and not misleading.

IPP 9 - Agency not to keep personal information for longer than necessary

Agencies must not keep personal information for longer than is required for the purposes for which the information may lawfully be used.

IPP 10 - Limits on use of personal information

Agencies must not use personal information obtained in connection with one purpose for any other purpose

unless the agency reasonably believes:

- The source of the information is publicly available, and it would not be unfair or unreasonable to use that information the use of the information for the other purpose is authorized by the relevant individual
- Non-compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency: for the enforcement of a law imposing a pecuniary penalty; for the protection of public revenue; or for the conduct of proceedings before a court or tribunal
- The use of the information for the other purpose is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of an individual
- The other purpose is directly related to the purpose for which the information was obtained, or
- The information is used in a form where the individual is not identified, or is used for statistical or research purposes and will not be published in a form where the individual could reasonably be expected to be identified

IPP 11 - Limits on disclosure of personal information

Agencies must not disclose personal information for any purpose other than the purpose for which it was collected, or a purpose directly related to the purpose for which it was collected unless the agency reasonably believes:

- The source of the information is publicly available, and it would not be unfair or unreasonable to disclose that information the disclosure is to the relevant individual
- The disclosure is authorized by the relevant individual
- Non-compliance is necessary: to avoid prejudice to the maintenance of the law by any public sector agency; for the enforcement of a law imposing a pecuniary penalty; for the protection of public revenue; or for the conduct of proceedings before a court or tribunal
- The disclosure of the information is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of an individual
- The disclosure is necessary to enable an intelligence and security agency to perform any of its functions the disclosure is necessary to facilitate the sale or other disposition of a business as a going concern, or
- The information is to be used in a form where the individual is not identified, or is used for statistical or research purposes and will not be published in a form where the individual could reasonably be expected to be identified

IPP 12 - Disclosure to an overseas person

Agencies must not disclose personal information to a foreign person or entity unless the agency reasonably believes:

- the relevant individual authorizes the disclosure after being informed by the agency that the foreign person or entity may not be required to protect the information in a way that provides comparable safeguards to those in the Act
- The foreign person or entity is carrying on business in New Zealand and the agency reasonably believes

that, in relation to the information being disclosed, the foreign person or entity is subject to the Act

- The foreign person or entity is subject to privacy laws that provide comparable safeguards to those in the Act the foreign person or entity is a participant in a prescribed binding scheme
- The foreign person or entity is subject to privacy laws of a prescribed country, or
- The foreign person or entity is required to protect the information in a way that provides comparable safeguards to those in the Act (for example, pursuant to contractual clauses). New Zealand's Privacy Commissioner has released model contractual clauses that can be used to satisfy these exceptions, but it is not mandatory to use these exact provisions.

IPP 13 - Unique identifiers

Agencies can only assign 'unique identifiers' to an individual if it is necessary to enable the agency to carry out one or more of its functions efficiently. The agency must not assign an individual a unique identifier that it knows has been assigned to that individual by another agency unless the unique identifier is being used for statistical or research purposes only. Additionally, the agency must take reasonable steps to ensure that unique identifiers are only assigned to individuals whose identities are clearly established and that the risk of the unique identifiers being misused is minimized. An agency must not require an individual to disclose any unique identifier assigned to them unless the disclosure is one of the purposes, or directly related to one of the purposes, for which that unique identifier was assigned.

Transfer

Generally, an agency should not disclose personal information to another entity unless the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained. Care must be taken that all safety and security precautions are met to ensure the safeguarding of that personal information to make certain that it is not misused or disclosed to any other party.

Additionally, the Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country (State) by issuing a transfer prohibition notice (Notice) if it is satisfied that information has been received in New Zealand from one State and will be transferred by an agency to a third State which does not provide comparable safeguards to the Act and the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the Organisation for Economic Co-operation and Development (OECD) Guidelines.

In considering whether to issue a Notice, the Privacy Commissioner must have regard to whether the proposed transfer of personal information affects, or would be likely to affect any individual, the desirability of facilitating the free flow of information between New Zealand and other States, and any existing or developing international guidelines relevant to trans-border data flows.

On December 19, 2012 the European Commission issued a decision formally declaring that New Zealand law provides a

standard of data protection that is adequate for the purposes of EU law. This decision means that personal data can flow from the 27 EU member states to New Zealand for processing without any further safeguards being necessary.

Breach Notification

Under the Act, any 'privacy breach' which it is reasonable to believe has caused or is likely to cause serious harm to an individual must be notified to the Privacy Commissioner and to the affected individuals.

A 'privacy breach' is any unauthorized or accidental access to, or disclosure, alteration, loss, or destruction of, personal information, or any action that prevents the agency from accessing the information on either a temporary or permanent basis.

When assessing whether a privacy breach is likely to cause serious harm, agencies must consider:

- any action taken by the agency to reduce the risk of harm following the breach whether the personal information is sensitive in nature
- the nature of the harm that may be caused to affected individuals
- the person or body that has obtained or may obtain personal information as a result of the breach (if known) whether the personal information is protected by a security measure, and
- any other relevant matters

Agencies must notify the Privacy Commissioner and affected individuals as soon as practicable after becoming aware of a notifiable privacy breach. If it is not reasonably practicable to notify an affected individual or each member of a group of affected individuals, an agency can give a public notice of the breach.

Notification to affected individuals is not required or can be delayed in certain circumstances. For example, notification to affected individuals can be delayed if the agency believes that a delay is necessary because notification or public notice may pose risks for the security of personal information held by the agency and those risks outweigh the benefits of informing affected individuals (for example, if notification of the breach would expose an unremedied security vulnerability).

Anyone who outsources services that involve data processing should be aware that the Act includes an express provision that anything relating to a notifiable privacy breach that is known by an agent is to be treated as being known by the principal agency. This is because the legislators consider that the principal agency should be responsible for informing individuals about a notifiable breach.

Appendix W – South Korea. Personal Information Protection Act ("PIPA")

The Korean legislative system for personal information protection is composed of the Personal Information Protection Act ("PIPA"), a general, comprehensive statute and the Credit Information Use and Protection Act which regulates personal credit information.

The Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. ("Network Act") once functioned as a special statute that regulated the processing of users' personal information by online service providers. However, after the substantial amendments to the PIPA and the Network Act on January 9, 2020, all provisions related to the processing and protection of personal information applicable to online service providers under the Network Act have been either removed or consolidated into the amended PIPA. The amendments to the PIPA and the Network Act went into force on August 5, 2020, and now the processing of personal information while providing online services is subject to the PIPA under a separate section exclusively dedicated to regulating online service providers ("Special Section") further explained below. Note that other parts of the PIPA will also apply to "Online Service Providers" (defined as 'telecommunications service providers' as prescribed in Article 2, Item 8 of the Telecommunications Business Act and other persons who provide information or act as an intermediary for the provision of information for the purpose of earning profit, by utilizing the services rendered by telecommunications service providers) if the Special Section is silent on a given issue.

Personal Data

Under PIPA, "personal information" means information relating to a living individual that constitutes any of the following:

- Information that identifies a particular individual by his/her full name, resident registration number, image, etc.
- Information which, even if by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual (in this case, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured)
- Information under items (a) or (b) above that is pseudonymised in accordance with the relevant provisions and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state (referred to as "pseudonymised information").

Sensitive Personal Data

Under the PIPA, "sensitive information" is defined as personal information concerning an individual's ideology, faith, labor union membership, political views or membership in a political party, health or medical treatment information, sexual orientation, genetic

Data Protection Officer

Under PIPA, every personal data controller (which means any person, any government entity, company, individual or other person that, directly or through a third party, controls and/or processes personal information in order to operate personal information files as part of its activities) must designate a chief privacy officer ("CPO") who must be an employee or executive of the company.

Collection and Processing

Under the PIPA, there must be a specific legitimate basis for processing personal information, with the most representative basis being the data subject's consent. As a result, in principle, the explicit consent of data subjects must be obtained before processing their personal information. However, the data subjects' consent is not required in cases where the processing of personal information is prescribed by a statute or where it is necessary for an entity to process personal information to comply with its legal obligations.

Transfer

As a general rule, a personal data controller may not provide personal information to a third party without obtaining the prior opt in consent of the data subject.

Exceptions to the general rule above apply in the following cases:

- where there exist special provisions in any Act or it is necessary to fulfil an obligation imposed by or under any Act and subordinate statute
- where it is necessary for a public institution to perform its affairs provided for in any Act and subordinate statute, etc., and where it is deemed obviously necessary for the physical safety and property interests of a data subject or a third person when the data subject or his/her legal representative cannot give prior consent because he/she is unable to express his/her intention or by reason of his/her unidentified address, etc.

Breach Notification

Under the PIPA, if a breach of personal information occurs the personal data controller must notify the data subjects without delay of the details and circumstances, and the remedial steps planned. If the number of affected data subjects is 1,000 or more, the personal data controller shall immediately report the notification to data subjects and the result of measures taken to PIPC or the Korea Internet & Security Agency ("KISA").

Document Control

Version	Date Published	Author	Description/Approval
1.0	01/29/2018	Protiviti	Initial Draft
1.1	04/09/2018	Lori Blackley	Minor Edits
1.1	04/09/2018	Masai Male	Review and Approve
1.1	04/09/2018	Alison Wisniewski	Review and Approve
1.2	07/01/2019	Edna Oburu	Minor Edits
2.0	8/27/2019	Ketty Wilson	Content update (CCPA)
3.0	12/21/2020	Ketty Wilson	Template and content update
3.1	01/27/2021	Lori Blackley	Added additional country specific regulation
3.2	11/2/2021	Ketty Wilson	Content update and added additional country specific regulation
3.3	11/11/2021	Lori Blackley	Review and Approve
4.0	11/16/2022	Ketty Wilson	Content update and added additional country specific regulation
4.1	01/05/2023	Lori Blackley	Review and Approve