Table of Contents

Volume 1

PART I. INTRODUCTION TO GLOBAL PRIVACY LAWS

CHAPTER 1. INTRODUCTION

§ 1:1 The rise of information security and privacy
§ 1:2 General privacy principles
§ 1:3 The origin of Fair Information Practices
§ 1:4 Organisation for economic co-operation and development guidelines
§ 1:5 Scope of OECD guidelines
§ 1:6 Basic Principles of National Application—Collection Limitation Principle
§ 1:7 —Data Quality Principle
§ 1:8 —Purpose Specification Principle
§ 1:9 —Use Limitation Principle
§ 1:10 —Security Safeguards Principle
§ 1:11 —Openness Principle
§ 1:12 —Individual Participation Principle
§ 1:13 —Accountability Principle
§ 1:14 Basic Principles of International Application—Free Flow and Legitimate Restrictions
§ 1:15 National Implementation
§ 1:16 International Co-Operation and Interoperability
§ 1:17 Principles adopted by the Asia-Pacific Economic Cooperation
§ 1:18 APEC information privacy principles—Preventing Harm
§ 1:19 —Notice
§ 1:20 —Collection Limitation
§ 1:21 —Uses of Personal Information
§ 1:22 —Choice
§ 1:23 —Integrity of Personal Information
§ 1:24 —Security Safeguards
§ 1:25 —Access and Correction
§ 1:26 —Accountability

§ 1:27 The FTC's formulation of FIPs
§ 1:28 Privacy and security: The seven U.S. Safe Harbor privacy principles

CHAPTER 2. EU DIRECTIVES AND REGULATIONS

I. INTRODUCTION

§ 2:1 Introduction to international privacy
§ 2:2 The right to be forgotten
§ 2:3 Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12

II. THE EUROPEAN UNION REGULATIONS AND DIRECTIVES

§ 2:4 Overview

A. CYBER RESILENCY ACT

1. General Provisions

§ 2:5 Subject matter
§ 2:6 Scope
§ 2:7 Free movement
§ 2:8 Requirements for products with digital elements, including critical products
§ 2:9 General product safety
§ 2:10 High-risk AI systems
§ 2:11 Machinery products

2. Obligations of economic operators

§ 2:12 Obligations of manufacturers
§ 2:13 Reporting obligations of manufacturers
§ 2:14 Authorised representatives
§ 2:15 Obligations of importers
§ 2:16 Obligations of distributors
§ 2:17 Cases in which obligations of manufacturers apply to importers and distributors
§ 2:18 Other cases in which obligations of manufacturers apply
§ 2:19 Identification of economic operators

3. Conformity of the product with digital elements

§ 2:20 Presumption of conformity

§ 2:21 Common specifications
§ 2:22 EU declaration of conformity
§ 2:23 General principles of the CE marking
§ 2:24 Rules and conditions for affixing the CE marking
§ 2:25 Technical documentation
§ 2:26 Conformity assessment procedures for products with digital elements

4. Notification of conformity assessment bodies

§ 2:27 Notification
§ 2:28 Notifying authorities
§ 2:29 Requirements relating to notifying authorities
§ 2:30 Information obligation on notifying authorities
§ 2:31 Requirements relating to notified bodies
§ 2:32 Presumption of conformity of notified bodies
§ 2:33 Subsidiaries of and subcontracting by notified bodies
§ 2:34 Application for notification
§ 2:35 Notification procedure
§ 2:36 Identification numbers and lists of notified bodies
§ 2:37 Changes to notifications
§ 2:38 Challenge of the competence of notified bodies
§ 2:39 Operational obligations of notified bodies
§ 2:40 Information obligation on notified bodies
§ 2:41 Exchange of experience
§ 2:42 Coordination of notified bodies

5. Market surveillance and enforcement

§ 2:43 Market surveillance and control of products with digital elements in the Union market
§ 2:44 Access to data and documentation
§ 2:45 Procedure at national level concerning products with digital elements presenting a significant cybersecurity risk
§ 2:46 Union safeguard procedure
§ 2:47 Procedure at EU level concerning products with digital elements presenting a significant cybersecurity risk
§ 2:48 Compliant products with digital elements which present a significant cybersecurity risk
§ 2:49 Formal non-compliance
§ 2:50 Joint activities of market surveillance authorities
§ 2:51 Sweeps

6. Delegated powers and committee procedure

§ 2:52 Exercise of the delegation
§ 2:53 Committee procedure

7. Confidentiality and penalties

§ 2:54 Confidentiality
§ 2:55 Penalties

8. Transitional and final provisions

§ 2:56 Transitional provisions
§ 2:57 Evaluation and review
§ 2:58 Entry into force and application

B. DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 14 DECEMBER 2022 ON MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY ACROSS THE UNION, AMENDING REGULATION (EU) NO 910/2014 AND DIRECTIVE (EU) 2018/1972, AND REPEALING DIRECTIVE (EU) 2016/1148 (NIS 2 DIRECTIVE)

1. General Provisions

§ 2:59 Subject Matter
§ 2:60 Scope
§ 2:61 Essential and important entities
§ 2:62 Sector-specific Union legal acts
§ 2:63 Minimum harmonisation

2. Coordinated cybersecurity frameworks

§ 2:64 National cybersecurity strategy
§ 2:65 Competent authorities and single points of contact
§ 2:66 National cyber crisis management frameworks
§ 2:67 Computer security incident response teams (CSIRTs)
§ 2:68 Requirements, technical capabilities and tasks of CSIRTs
§ 2:69 Coordinated vulnerability disclosure and a European vulnerability database
§ 2:70 Cooperation at national level

3. Cooperation at union and international level

§ 2:71 Cooperation Group
§ 2:72 CSIRTs network
§ 2:73 European cyber crisis liaison organisation network (EU-CyCLONe)
§ 2:74 International cooperation
§ 2:75 Report on the state of cybersecurity in the Union

§ 2:76 Peer reviews

4. Cybersecurity risk-management measures and reporting obligations

§ 2:77 Governance
§ 2:78 Cybersecurity risk-management measures
§ 2:79 Union level coordinated security risk assessments of critical supply chains
§ 2:80 Reporting obligations
§ 2:81 Use of European cybersecurity certification schemes
§ 2:82 Standardisation

5. Jurisdiction and registration

§ 2:83 Jurisdiction and territoriality
§ 2:84 Registry of entities
§ 2:85 Database of domain name registration data

6. Information sharing

§ 2:86 Cybersecurity information-sharing arrangements
§ 2:87 Voluntary notification of relevant information

7. Supervision and enforcement

§ 2:88 General aspects concerning supervision and enforcement
§ 2:89 Supervisory and enforcement measures in relation to essential entities
§ 2:90 Supervisory and enforcement measures in relation to important entities
§ 2:91 General conditions for imposing administrative fines on essential and important entities
§ 2:92 Infringements entailing a personal data breach
§ 2:93 Penalties
§ 2:94 Mutual assistance

8. Delegated and implementing acts

§ 2:95 Exercise of the delegation
§ 2:96 Committee procedure

9. Final provisions

§ 2:97 Review
§ 2:98 Transposition

C. DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS

§ 2:99 Purpose and scope

§ 2:100 Security of processing
§ 2:101 Confidentiality and the "Cookie Directive"
§ 2:102 Traffic data
§ 2:103 Itemized billing
§ 2:104 Caller ID
§ 2:105 Directories
§ 2:106 Unsolicited communications
§ 2:107 Restrictions of directive
§ 2:108 Internal procedures
§ 2:109 Implementation and enforcement

D. PRIVACY IN THE TELECOMMUNICATIONS SECTOR

§ 2:110 Application of directive
§ 2:111 Security
§ 2:112 Confidentiality
§ 2:113 Traffic and billing data
§ 2:114 Subscriber billing rights
§ 2:115 Caller ID
§ 2:116 Directories
§ 2:117 Unsolicited calls
§ 2:118 Restrictions on directive
§ 2:119 Enforcement
§ 2:120 The EU Data Retention Directive
§ 2:121 —Scope of application
§ 2:122 —Data retention obligations
§ 2:123 Select Working Party Opinions
§ 2:124 Opinion 04/2014 on surveillance electronic communications for intelligence and national security purposes, WP 215
§ 2:125 Opinion 05—2014 on anonymization techniques
§ 2:126 Article 29 Working Party Opinion on the notion of legitimate interests of the data controller under Article 7, April 9, 2014
§ 2:127 Opinion 03/2013 on purpose limitation purpose specification and compatible use concepts

CHAPTER 3. GENERAL DATA PROTECTION REGULATION

§ 3:1 An overview

I. GENERAL PROVISIONS

§ 3:2 Subject-matter and objectives

§ 3:3 Material scope
§ 3:4 Territorial scope
§ 3:5 Definitions

II. PRINCIPLES

§ 3:6 Principles relating to processing of personal data
§ 3:7 Lawfulness of processing
§ 3:8 Conditions for consent
§ 3:9 Conditions applicable to child's consent in relation to information society services
§ 3:10 Processing of special categories of personal data
§ 3:11 Processing of personal data relating to criminal convictions and offences
§ 3:12 Processing which does not require identification

III. RIGHTS OF DATA SUBJECT

A. TRANSPARENCY AND MODALITIES

§ 3:13 Transparent information, communication and modalities for the exercise of the rights of the data subject

B. INFORMATION AND ACCESS TO PERSONAL DATA

§ 3:14 Information to be provided where personal data are collected from the data subject
§ 3:15 Information to be provided where personal data have not been obtained from the data subject
§ 3:16 Right of access by the data subject

C. RECTIFICATION AND ERASURE

§ 3:17 Right to rectification
§ 3:18 Right to erasure ('right to be forgotten')
§ 3:19 Right to restriction of processing
§ 3:20 Notification obligation regarding rectification or erasure of personal data or restriction of processing
§ 3:21 Right to data portability

D. RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING

§ 3:22 Right to object
§ 3:23 Automated individual decision-making, including profiling

E. RESTRICTIONS

§ 3:24 Restrictions

IV. CONTROLLER AND PROCESSOR

A. GENERAL OBLIGATIONS

§ 3:25 Responsibility of the controller
§ 3:26 Data protection by design and by default
§ 3:27 Joint controllers
§ 3:28 Representatives of controllers or processors not established in the Union
§ 3:29 Processor
§ 3:30 Processing under the authority of the controller or processor
§ 3:31 Records of processing activities
§ 3:32 Cooperation with the supervisory authority

B. SECURITY OF PERSONAL DATA

§ 3:33 Security of processing
§ 3:34 Notification of a personal data breach to the supervisory authority
§ 3:35 Communication of a personal data breach to the data subject

C. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

§ 3:36 Data protection impact assessment
§ 3:37 Prior consultation

D. DATA PROTECTION OFFICER

§ 3:38 Designation of the data protection officer
§ 3:39 Position of the data protection officer
§ 3:40 Tasks of the data protection officer

E. CODES OF CONDUCT AND CERTIFICATION

§ 3:41 Codes of conduct
§ 3:42 Monitoring of approved codes of conduct
§ 3:43 Certification
§ 3:44 Certification bodies

V. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

§ 3:45 General principle for transfers

§ 3:46 Transfers on the basis of an adequacy decision
§ 3:47 Transfers subject to appropriate safeguards
§ 3:48 Binding corporate rules
§ 3:49 Transfers or disclosures not authorised by Union law
§ 3:50 Derogations for specific situations
§ 3:51 International cooperation for the protection of personal data

VI. INDEPENDENT SUPERVISORY AUTHORITIES

A. INDEPENDENT STATUS

§ 3:52 Supervisory authority
§ 3:53 Independence
§ 3:54 General conditions for the members of the supervisory authority
§ 3:55 Rules on the establishment of the supervisory authority

B. COMPETENCE, TASKS, AND POWERS

§ 3:56 Competence
§ 3:57 Competence of the lead supervisory authority
§ 3:58 Tasks
§ 3:59 Powers
§ 3:60 Activity reports

VII. COOPERATION AND CONSISTENCY

A. COOPERATION

§ 3:61 Cooperation between the lead supervisory authority and other supervisory authorities concerned
§ 3:62 Mutual assistance
§ 3:63 Joint operations of supervisory authorities

B. CONSISTENCY

§ 3:64 Consistency mechanism
§ 3:65 Opinion of the Board
§ 3:66 Dispute resolution by the Board
§ 3:67 Urgency procedure
§ 3:68 Exchange of information

C. EUROPEAN DATA PROTECTION BOARD

§ 3:69 European data protection board
§ 3:70 Independence

§ 3:71 Tasks of the Board
§ 3:72 Reports
§ 3:73 Procedure
§ 3:74 Chair
§ 3:75 Tasks of the Chair
§ 3:76 Secretariat
§ 3:77 Confidentiality

VIII. REMEDIES, LIABILITY AND PENALTIES

§ 3:78 Right to lodge a complaint with a supervisory authority
§ 3:79 Right to an effective judicial remedy against a supervisory authority
§ 3:80 Right to an effective judicial remedy against a controller or processor
§ 3:81 Representation of data subjects
§ 3:82 Suspension of proceedings
§ 3:83 Right to compensation and liability
§ 3:84 General conditions for imposing administrative fines
§ 3:85 Penalties

IX. PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

§ 3:86 Processing and freedom of expression and information
§ 3:87 Processing and public access to official documents
§ 3:88 Processing of the national identification number
§ 3:89 Processing in the context of employment
§ 3:90 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
§ 3:91 Obligations of secrecy
§ 3:92 Existing data protection rules of churches and religious associations

X. ARTICLE 29 WORKING PARTY

§ 3:93 Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679—Introduction
§ 3:94 —Definitions
§ 3:95 —General provisions on profiling and automated decision-making
§ 3:96 —Rights of the data subject
§ 3:97 —Specific provisions regarding solely automated decision-making

§ 3:98 —DPIA
§ 3:99 —DPIA guidelines
§ 3:100 Guidelines on personal data breach notification under regulation 2016/679
§ 3:101 Guidelines on the right to data portability
§ 3:102 Guidelines on consent under regulation 2016/679—Overview
§ 3:103 —Elements of consent
§ 3:104 —Freely given
§ 3:105 — —Imbalance
§ 3:106 — —Conditionality
§ 3:107 — —Granularity
§ 3:108 — —Detriment
§ 3:109 —Specific
§ 3:110 —Informed
§ 3:111 — —Form of providing information
§ 3:112 —Explicit consent
§ 3:113 —Demonstrating consent/length of consent
§ 3:114 —Withdrawal of consent

PART II. EUROPE

CHAPTER 4. ALBANIA

§ 4:1 Albania
§ 4:2 General
§ 4:3 Exceptions
§ 4:4 Methods of personal data processing
§ 4:5 Notice to the data subject
§ 4:6 Requirements for data processors
§ 4:7 Authorization requirement
§ 4:8 Data security
§ 4:9 Rights of the data subject—Preliminary consent requirement
§ 4:10 Access rights by a data subject—Right of access to one's own personal data
§ 4:11 The right to object
§ 4:12 Transfers of data to other countries
§ 4:13 The People's Advocate
§ 4:14 Enforcement

CHAPTER 5. CZECH REPUBLIC

§ 5:1 Privacy Act
§ 5:2 The scope of the Act

§ 5:3 Formation of the Office
§ 5:4 Activities of the Office—Register
§ 5:5 Annual report
§ 5:6 Rights of the controlling persons
§ 5:7 Obligations of controlling persons
§ 5:8 Enforcement
§ 5:9 Additional supervision requirements
§ 5:10 Defenses
§ 5:11 Amendments to other laws
§ 5:12 Rights and obligations in processing of personal data
§ 5:13 Processing not authorized by legal regulation
§ 5:14 Effect of breaches of obligations
§ 5:15 Other restrictions on processing
§ 5:16 Notice obligations
§ 5:17 Termination of processing
§ 5:18 Notice to individuals
§ 5:19 Data security requirements
§ 5:20 Confidentiality requirements
§ 5:21 Investigations
§ 5:22 Exemptions from notification obligation
§ 5:23 Liquidation of personal data
§ 5:24 Access rights
§ 5:25 Protection of data subjects' rights
§ 5:26 Transfer of personal data to other countries
§ 5:27 Sensitive data
§ 5:28 Office for Personal Data Protection
§ 5:29 Czech Republic Interpretation regarding personal or household activity

CHAPTER 6. DENMARK

§ 6:1 Scope of the Act
§ 6:2 Definitions
§ 6:3 Geographic scope of the Act
§ 6:4 Processing of data
§ 6:5 Disclosure to credit information agencies of data on debts to public authorities
§ 6:6 Credit information agencies
§ 6:7 Video surveillance
§ 6:8 Transfer of personal data to third countries
§ 6:9 The data subject's rights—Information to be given to the data subject
§ 6:10 —The data subject's right of access to data
§ 6:11 —Other rights
§ 6:12 Security of processing

§ 6:13 Notification of processing carried out for a public administration
§ 6:14 Notification of processing operations carried out on behalf of a private controller
§ 6:15 Notification of processing operations carried out on behalf of the courts
§ 6:16 Miscellaneous provisions
§ 6:17 The Data Protection Agency
§ 6:18 Supervision of the courts
§ 6:19 Liability in damages and criminal liability
§ 6:20 Final provisions, including commencement provisions

CHAPTER 7. FINLAND

I. PERSONAL DATA PROCESSING

§ 7:1 Personal Data Act—Objectives
§ 7:2 —Scope of Act
§ 7:3 Application of Finnish law
§ 7:4 Other provisions—Liability for damages
§ 7:5 Criminal liability
§ 7:6 General rules regarding the processing of personal data—Duty of care
§ 7:7 Defined purpose of processing
§ 7:8 Exclusivity of purpose
§ 7:9 Requirements of processing
§ 7:10 Principles related to data quality
§ 7:11 Description of the file
§ 7:12 Processing of credit data
§ 7:13 Information on the processing of data in certain situations
§ 7:14 The right to prohibit processing
§ 7:15 Automated decisions
§ 7:16 Erasure of data in a credit data file
§ 7:17 Data security and storage of personal data—Data security
§ 7:18 Confidentiality obligations
§ 7:19 Archiving of data
§ 7:20 Data subject's rights
§ 7:21 Right of access
§ 7:22 Restrictions on the right of access
§ 7:23 Utilization of the right to access
§ 7:24 Correction of data
§ 7:25 Transfer of personal data to outside the European Union

§ 7:26 Sensitive data
§ 7:27 Processing of a personal identity number
§ 7:28 Personal data and research
§ 7:29 Statistics
§ 7:30 Official plans and reports
§ 7:31 Public registers
§ 7:32 Genealogical research

II. PROTECTION OF PRIVACY IN WORKING LIFE

§ 7:33 Act on the Protection of Privacy in Working Life
§ 7:34 Scope of application
§ 7:35 General requirements for processing personal data
§ 7:36 General requirements for collecting personal data about employees and the employer's duty to provide information
§ 7:37 Processing health information
§ 7:38 Drug test certificates
§ 7:39 Submission of a drug test certificate during the employment relationship
§ 7:40 Personality and aptitude assessments
§ 7:41 Health testing and examinations
§ 7:42 Bar on genetic testing
§ 7:43 Videotaping in the workplace
§ 7:44 E-mail monitoring
§ 7:45 Cooperation in organizing technical monitoring and data network use
§ 7:46 Notice of rights
§ 7:47 Enforcement by Ombudsman
§ 7:48 Criminal enforcement
§ 7:49 Amendment of other acts

III. PRIVACY AND THE MEDIA

§ 7:50 Mass media
§ 7:51 General provisions—Objective
§ 7:52 Scope of application
§ 7:53 Duties of publishers and broadcasters—Responsible editor
§ 7:54 Duty of disclosure
§ 7:55 Recording of a program or a network publication
§ 7:56 Official announcements
§ 7:57 Reply and correction—Right to reply
§ 7:58 Right to correction
§ 7:59 Duty of the responsible editor to publish a reply or correction

§ 7:60 Demand for a reply or correction
§ 7:61 Responsibility for the contents of a published message—Criminal liability of perpetrators and accomplices
§ 7:62 Editorial misconduct
§ 7:63 Civil enforcement
§ 7:64 Right of access to a recording
§ 7:65 Confidentiality of sources and right to anonymous expression
§ 7:66 Coercive measures—Release of identifying information for a network message
§ 7:67 Order to cease the distribution of a network message
§ 7:68 Seizure of a publication
§ 7:69 Sanctions and right to prosecution—Criminal enforcement
§ 7:70 Forfeiture and order to destroy a network message
§ 7:71 Publication of a judgment concerning a violation of honor and privacy

IV. DIRECTION AND GUIDANCE ON THE PROCESSING OF PERSONAL DATA

§ 7:72 Notification to the Data Protection Ombudsman—Duty of notification
§ 7:73 Direction and supervision of the processing of personal data—Data protection authorities
§ 7:74 Data protection authorities' right of access and inspection
§ 7:75 Measures of the Data Protection Ombudsman
§ 7:76 Rights of the Data Protection Ombudsman
§ 7:77 Sectoral codes of conduct
§ 7:78 Power of the Data Protection Board to grant permissions
§ 7:79 Orders of the Data Protection Board
§ 7:80 Appeal
§ 7:81 Fines

V. ELECTRONIC COMMUNICATIONS AND MARKETING

§ 7:82 Act on the Protection of Privacy in Electronic Communications
§ 7:83 Guidance and supervision—General guidance and development
§ 7:84 Duties of the Finnish Communications Regulatory Authority and the Data Protection Ombudsman

§ 7:85 Right of access to information—Guidance and supervision authorities' right of access to information
§ 7:86 Supervision authorities' obligation of secrecy and disclosure of information
§ 7:87 Disclosing information to emergency services authorities
§ 7:88 Certain other authorities' right of access to information
§ 7:89 User's special right of access to information
§ 7:90 Information security fee—Determination of the fee
§ 7:91 Amount of the information security fee
§ 7:92 Miscellaneous provisions—Coercive measures
§ 7:93 Penal provisions
§ 7:94 Appeal
§ 7:95 Protection of privacy and confidentiality of messages—Confidentiality of messages, identification data and location data
§ 7:96 Obligation of secrecy and non-exploitation
§ 7:97 Protecting messages and identification data
§ 7:98 Saving data on the use of a service in the user's terminal device and the use of such data
§ 7:99 Processing of messages and identification data—General processing provisions
§ 7:100 Processing identification data for the purpose of providing and using services
§ 7:101 Processing for billing purposes
§ 7:102 Processing for the purposes of technical development
§ 7:103 Processing in cases of misuse
§ 7:104 Processing for the purpose of detecting a technical fault or error
§ 7:105 Saving information on processing
§ 7:106 Direct marketing
§ 7:107 Processing for marketing purposes
§ 7:108 Information security in communications—Obligation to maintain information security
§ 7:109 Measures taken to implement information security
§ 7:110 Information security notifications
§ 7:111 Telephone services—Subscriber connection identification
§ 7:112 Automatic call transfer
§ 7:113 Call itemization of a bill
§ 7:114 Telephone directories, other subscriber directories and directory inquiries
§ 7:115 Direct marketing—Direct marketing to natural persons

§ 7:116 Direct marketing to legal persons
§ 7:117 Identification of direct marketing
§ 7:118 Preventing the reception of direct marketing
§ 7:119 Location data—Processing and disclosure of location data
§ 7:120 Subscriber's right to prohibit processing of location data
§ 7:121 Service-specific consent of the party to be located

CHAPTER 8. FRANCE

§ 8:1 Principles and definitions
§ 8:2 Application of the Act
§ 8:3 Conditions on the lawfulness of personal data processing
§ 8:4 Specific provisions of certain categories of data
§ 8:5 The Commission Nationale de l'Informatique et des Libertes (CNIL)
§ 8:6 Formalities prior to commencing data processing
§ 8:7 Notification
§ 8:8 Authorization
§ 8:9 Common Provisions
§ 8:10 Obligations incumbent upon data controllers
§ 8:11 Rights of individuals in respect of processing of personal data
§ 8:12 Supervision of the implementation of data processing
§ 8:13 Sanctions pronounced by the Select Committee of the "Commission Nationale de l'Informatique et des Libertés"
§ 8:14 Criminal provisions
§ 8:15 Processing of personal data for the purpose of medical research
§ 8:16 Processing of personal medical data for the purposes of evaluation or analysis of care and prevention practices or activities
§ 8:17 Processing of personal data for the purpose of journalism and literary and artistic expression
§ 8:18 Transfer of personal data to states that are not members of the European Union

CHAPTER 9. GERMANY

§ 9:1 Purpose and scope
§ 9:2 Public and private bodies
§ 9:3 Key definitions
§ 9:4 Data reduction and data economy
§ 9:5 Lawfulness of data collection, processing and use

§ 9:6 Consent
§ 9:7 Transfer of personal data abroad and to supranational or intergovernmental bodies
§ 9:8 Derogations
§ 9:9 Obligation to notify
§ 9:10 Contents of notification
§ 9:11 Data protection official
§ 9:12 Duties of the data protection official
§ 9:13 Confidentiality
§ 9:14 Inalienable rights of the data subject
§ 9:15 Automated individual decisions
§ 9:16 Monitoring of publicly accessible areas with optic-electronic devices
§ 9:17 Mobile storage and processing media for personal data
§ 9:18 Compensation
§ 9:19 Compensation in case of automated data processing by public bodies
§ 9:20 Technical and organizational measures
§ 9:21 Section 9a Data protection audit
§ 9:22 Automated retrieval procedures
§ 9:23 Collection, processing or use of personal data on behalf of others
§ 9:24 Legal basis for data processing
§ 9:25 Data collection
§ 9:26 Recording, alteration and use of data
§ 9:27 Transfer of data to public bodies
§ 9:28 Transfer of data to private bodies
§ 9:29 Section 18 implementation of data protection in the federal administration
§ 9:30 Access to data
§ 9:31 Notification
§ 9:32 Rectification, erasure and blocking of data; right to object
§ 9:33 Appeals to the Federal Commissioner for Data Protection and Freedom of Information
§ 9:34 Legal basis for data processing
§ 9:35 Collection and recording of data for own commercial purposes
§ 9:36 Data transfer to rating agencies
§ 9:37 Scoring
§ 9:38 Commercial data collection and recording for the purpose of transfer
§ 9:39 Commercial data collection and recording for the purpose of transfer in anonymous form
§ 9:40 Commercial data collection and recording for purposes of market or opinion research

§ 9:41 Special restrictions on use
§ 9:42 Data collection, processing and use for employment-related purposes
§ 9:43 Notification of the data subject
§ 9:44 Access to data
§ 9:45 Correction, deletion and blocking of data
§ 9:46 Supervisory authority
§ 9:47 Codes of conduct to facilitate the application of data protection provisions
§ 9:48 Special provisions—Section 39 Restrictions on use of personal data subject to professional or special official secrecy
§ 9:49 —Section 40 Processing and use of personal data by research institutions
§ 9:50 —Collection, processing and use of personal data by the media
§ 9:51 —Obligation to notify in case of unlawful access to data
§ 9:52 Offenses
§ 9:53 Transitional provisions

CHAPTER 10. ITALY

§ 10:1 Right to the Protection of Personal Data
§ 10:2 Purpose of the Code
§ 10:3 Data minimisation principle
§ 10:4 Key definitions
§ 10:5 Subject-matter and scope of application
§ 10:6 Regulations applying to processing operations
§ 10:7 Right to access personal data and other rights
§ 10:8 Exercise of rights
§ 10:9 Mechanisms to exercise rights
§ 10:10 Response to data subjects
§ 10:11 Processing arrangements and data quality
§ 10:12 Codes of conduct and professional practice
§ 10:13 Information to data subjects
§ 10:14 Profiling of data subjects and their personality
§ 10:15 Damage caused on account of the processing
§ 10:16 Termination of processing operations
§ 10:17 Processing operations carrying specific risks
§ 10:18 Principles applying to all processing operations performed by public bodies
§ 10:19 Principles applying to the processing of data other than sensitive and judicial data
§ 10:20 Principles applying to the processing of sensitive data
§ 10:21 Principles applying to the processing of judicial data

§ 10:22 Principles applying to the processing of sensitive data as well as to judicial data
§ 10:23 Consent
§ 10:24 Cases in which no consent is required for processing data
§ 10:25 Bans on communication and dissemination
§ 10:26 Safeguards applying to sensitive data
§ 10:27 Safeguards applying to judicial data
§ 10:28 Data controller
§ 10:29 Data processor
§ 10:30 Persons in charge of the processing
§ 10:31 Security requirements
§ 10:32 Obligations applying to providers of publicly available electronic communications services
§ 10:33 Steps to be taken following a personal data breach
§ 10:34 Minimum security measures
§ 10:35 Processing by electronic means
§ 10:36 Processing without electronic means
§ 10:37 Upgrading
§ 10:38 Notification of the processing
§ 10:39 Notification mechanisms
§ 10:40 Communication obligations
§ 10:41 General authorisations
§ 10:42 Authorisation requests
§ 10:43 Data flows in the EU
§ 10:44 Permitted data transfers to third countries
§ 10:45 Other permitted data transfers
§ 10:46 Prohibited data transfers
§ 10:47 Sector-specific requirements—Processing operations in the judicial sector
§ 10:48 —Processing operations by the police
§ 10:49 —State defence and security
§ 10:50 —Processing operations in the public sector
§ 10:51 —Processing of personal data in the health care sector
§ 10:52 Purposes in the substantial public interest
§ 10:53 Processing for historical, statistical or scientific purposes
§ 10:54 Processing for statistical or scientific purposes

CHAPTER 11. MALTA

§ 11:1 Requirements and criteria for processing
§ 11:2 Restrictions on possessing personal data
§ 11:3 Processing for specific purposes
§ 11:4 Information related to criminal offenses

§ 11:5 Data collection and right of access
§ 11:6 Disclosures at the request of a data subject
§ 11:7 Exemptions, restrictions and other measures
§ 11:8 Automated processing
§ 11:9 Other restrictions
§ 11:10 Data security
§ 11:11 Transfers to other countries
§ 11:12 Notification and other procedures
§ 11:13 Personal data representative
§ 11:14 Prior approval of certain forms of processing
§ 11:15 The Data Protection Commissioner
§ 11:16 Civil actions
§ 11:17 Criminal enforcement
§ 11:18 The powers of the Tribunal
§ 11:19 Regulations

CHAPTER 12. THE NETHERLANDS

§ 12:1 Applicability of Dutch Personal Data Protection Act
§ 12:2 Processing of personal data
§ 12:3 Restrictions on further processing
§ 12:4 Restrictions on processors
§ 12:5 Consent by minors
§ 12:6 Notice to the Data Protection Commission
§ 12:7 Prior investigations
§ 12:8 Automated processing
§ 12:9 Exceptions and restrictions
§ 12:10 Restrictions upon retention of personal data
§ 12:11 Restrictions on processing due to the purpose of collection
§ 12:12 Restrictions upon retention of personal data
§ 12:13 Security requirements
§ 12:14 Disclosures to the data subject
§ 12:15 Notice of security breach
§ 12:16 Corrections to data
§ 12:17 Objections based upon certain forms of processing
§ 12:18 Transfer of data to non-EU countries
§ 12:19 Special personal data
§ 12:20 Restrictions on special personal data
§ 12:21 General exceptions
§ 12:22 Processing of information that relates to a person's religion
§ 12:23 Processing of racial information
§ 12:24 Political information
§ 12:25 Trade unions

§ 12:26 Health information
§ 12:27 Criminal behavior
§ 12:28 Identifying numbers
§ 12:29 Organizational policies
§ 12:30 Civil enforcement
§ 12:31 The Data Protection Commission
§ 12:32 Data protection officers
§ 12:33 Fines
§ 12:34 Criminal enforcement
§ 12:35 Investigation into the combining of personal data by Google the Dutch data protection authority

CHAPTER 13. POLAND

§ 13:1 Rights of persons
§ 13:2 The principles of personal data processing
§ 13:3 Application
§ 13:4 Definitions
§ 13:5 Supervisory authority for personal data protection
§ 13:6 Procedures where data is not directly obtained from the subject
§ 13:7 The rights of the data subject
§ 13:8 Protection of personal data
§ 13:9 Register
§ 13:10 Tracking and maintaining reports under Article 36(2)
§ 13:11 Registration of personal data filing systems and of administrators of information security
§ 13:12 Exceptions to registration of databases
§ 13:13 Transfer of personal data to a third country.
§ 13:14 Sanctions

CHAPTER 14. RUSSIA

§ 14:1 Introduction

I. FEDERAL LAW OF 27 JULY 2006 N 152-FZ ON PERSONAL DATA

§ 14:2 Sphere of regulation
§ 14:3 Purpose of Federal Law
§ 14:4 Key definitions
§ 14:5 Legislative grounds for protection of personal data in the Russian Federation
§ 14:6 Principles of personal data processing
§ 14:7 Conditions of personal data processing
§ 14:8 Confidentiality of personal data
§ 14:9 Public sources of personal data

§ 14:10 Individual's consent to personal data processing
§ 14:11 Special categories of personal data
§ 14:12 Biometric personal data
§ 14:13 Cross-Border transfer of personal data
§ 14:14 Processing of personal data by state agencies and municipal authorities
§ 14:15 Right of access to personal data
§ 14:16 Personal rights during the processing of personal data for promotional or marketing purposes
§ 14:17 Rights of individual in cases when decisions are made based on the automatically processed personal data
§ 14:18 Right to contest operator's actions or failure to act
§ 14:19 Operator's obligations at the time of collection of personal data
§ 14:20 Protective measures while processing personal data
§ 14:21 Operator's obligations to process inquiries of the individual concerned, legal representatives or the authorized body
§ 14:22 Operator's obligations to cure breaches of personal data processing and to correct, block or destroy personal data
§ 14:23 Notice about personal data processing
§ 14:24 Authorized body in the sphere of personal data protection
§ 14:25 Liability for breach of this Federal Law

II. RUSSIAN FEDERATION FEDERAL ACT ON INFORMATION, INFORMATION TECHNOLOGIES, AND INFORMATION PROTECTION

§ 14:26 Overview
§ 14:27 Competence of the present Federal Act
§ 14:28 Principles of legal regulation of relationships in the sphere of information, information technologies and information protection
§ 14:29 Legislation of the Russian Federation on information, information technologies and information protection
§ 14:30 Information as the object of legal relations
§ 14:31 Possessor of information
§ 14:32 Generally accessible information
§ 14:33 Right to access to information
§ 14:34 Restriction of access to information
§ 14:35 Distribution of information and delivery of information
§ 14:36 Documenting of information

§ 14:37 State regulation in the sphere of application of information technologies
§ 14:38 Information systems
§ 14:39 State information systems
§ 14:40 Usage of information-telecommunication networks
§ 14:41 Amendment
§ 14:42 Procedure for restricting access to information processed in violation of the Russian Federation laws on personal data
§ 14:43 Protection of information
§ 14:44 Responsibility for legal offenses in the sphere of information—Information technologies and information protection
§ 14:45 Repeal of certain legal acts of the Russian Federation

CHAPTER 15. SPAIN

I. INTRODUCTION

§ 15:1 Purpose
§ 15:2 Scope and application
§ 15:3 Key definitions

II. PRINCIPLES OF DATA PROTECTION

§ 15:4 Quality of the data
§ 15:5 Right of information in the collection of data
§ 15:6 Consent of the data subject
§ 15:7 Data with special protection
§ 15:8 Data on health
§ 15:9 Data security
§ 15:10 Duty of secrecy
§ 15:11 Communication of data
§ 15:12 Access to data on behalf of third parties
§ 15:13 Challenging assessments
§ 15:14 Right to consult the General Data Protection Register
§ 15:15 Right of access
§ 15:16 Right of rectification or cancellation
§ 15:17 Objection, access, rectification or cancellation procedure
§ 15:18 Supervision of rights
§ 15:19 Right to damages
§ 15:20 Creation, modification or deletion
§ 15:21 Communication of data between public administrations
§ 15:22 Files of the security forces

§ 15:23 Exceptions to the rights of access, rectification and cancellation
§ 15:24 Other exceptions to the rights of data subjects
§ 15:25 Creation
§ 15:26 Notification and entry in the register
§ 15:27 Communication of transfers of data
§ 15:28 Data included in sources accessible to the public
§ 15:29 Provision of information services on creditworthiness and credit
§ 15:30 Processing for the purpose of publicity and market research
§ 15:31 Publicity register
§ 15:32 Standard codes of conduct
§ 15:33 International movement of data
§ 15:34 Data Protection Agency
§ 15:35 The General Data Protection Register

CHAPTER 16. UNITED KINGDOM

I. GDPR

A. CHAPTER I GENERAL PROVISIONS

§ 16:1 Subject-matter and objectives
§ 16:2 Material scope
§ 16:3 Territorial scope
§ 16:4 Periods of time

B. CHAPTER II PRINCIPLES

§ 16:5 Principles relating to processing of personal data
§ 16:6 Lawfulness of processing
§ 16:7 Conditions for consent
§ 16:8 Conditions applicable to child's consent in relation to information society services
§ 16:9 Purpose limitation: further processing
§ 16:10 Processing of special categories of personal data
§ 16:11 Processing of personal data relating to criminal convictions and offences
§ 16:12 Processing which does not require identification
§ 16:13 Further provision about processing of special categories of personal data

C. CHAPTER III RIGHTS OF THE DATA SUBJECT

1. Transparency and modalities

§ 16:14 Transparent information, communication and

modalities for the exercise of the rights of the data subject

2. Information and access to personal data

§ 16:15 Information to be provided where personal data are collected from the data subject
§ 16:16 Information to be provided where personal data have not been obtained from the data subject
§ 16:17 Right of access by the data subject

3. Rectification and erasure

§ 16:18 Right to rectification
§ 16:19 Right to erasure ('right to be forgotten')
§ 16:20 Right to restriction of processing
§ 16:21 Notification obligation regarding rectification or erasure of personal data or restriction of processing
§ 16:22 Right to data portability

4. Right to object and automated individual decision-making

§ 16:23 Right to object
§ 16:24 Automated individual decision-making, including profiling

4A. Automated individual decision-making

§ 16:25 Automated processing and significant decisions
§ 16:26 Restrictions on automated decision-making
§ 16:27 Safeguards for automated decision-making
§ 16:28 Further provision about automated decision-making

5. Restrictions

§ 16:29 Restrictions

D. CHAPTER IV CONTROLLER AND PROCESSOR

1. General obligations

§ 16:30 Responsibility of the controller
§ 16:31 Data protection by design and by default
§ 16:32 Joint controllers
§ 16:33 Representatives of controllers or processors not established in the United Kingdom
§ 16:34 Processor
§ 16:35 Processing under the authority of the controller or processor
§ 16:36 Records of processing activities

§ 16:37 Cooperation with the Commissioner

2. Security of personal data

§ 16:38 Security of processing
§ 16:39 Notification of a personal data breach to the Commissioner
§ 16:40 Communication of a personal data breach to the data subject

3. Data protection impact assessment and prior consultation

§ 16:41 Data protection impact assessment
§ 16:42 Prior consultation

4. Data protection officer

§ 16:43 Designation of the data protection officer
§ 16:44 Position of the data protection officer
§ 16:45 Tasks of the data protection officer

5. Codes of conduct and certification

§ 16:46 Codes of conduct
§ 16:47 Monitoring of approved codes of conduct
§ 16:48 Certification
§ 16:49 Certification bodies

E. CHAPTER V TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

§ 16:50 General principle for transfers
§ 16:51 Transfers on the basis of an adequacy decision
§ 16:52 Transfers approved by regulations
§ 16:53 The data protection test
§ 16:54 Transfers subject to appropriate safeguards
§ 16:55 Binding corporate rules
§ 16:56 Transfers subject to appropriate safeguards: further provision
§ 16:57 Derogations for specific situations
§ 16:58 Restriction in public interest
§ 16:59 International cooperation for the protection of personal data

F. CHAPTER VI THE COMMISSIONER

1. Independent status

§ 16:60 Monitoring the application of this Regulation

§ 16:61 Independence

2. Tasks and Powers

§ 16:62 Tasks
§ 16:63 Powers

G. CHAPTER VIII REMEDIES, LIABILITY, AND PENALTIES

§ 16:64 Right to lodge a complaint with the Commissioner
§ 16:65 Right to an effective judicial remedy against the Commissioner
§ 16:66 Right to an effective judicial remedy against a controller or processor
§ 16:67 Representation of data subjects
§ 16:68 Right to compensation and liability
§ 16:69 General conditions for imposing administrative fines
§ 16:70 Penalties

H. CHAPTER 8A. SAFEGUARDS FOR PROCESSING FOR RESEARCH, ARCHIVING OR STATISTICAL PURPOSES

§ 16:71 Research, archives and statistics
§ 16:72 Additional requirements when processing for RAS purposes
§ 16:73 Appropriate safeguards
§ 16:74 Appropriate safeguards: further provision

I. CHAPTER IX. PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

§ 16:75 Processing and freedom of expression and information
§ 16:76 Processing and public access to official documents
§ 16:77 Processing and national security and defence
§ 16:78 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

J. CHAPTER 9A. REGULATIONS

§ 16:79 Regulations made by Secretary of State

K. FINAL PROVISIONS

§ 16:80 Repeal of Directive 95/46/EC

§ 16:81 Relationship with domestic law made before IP completion day implementing Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
§ 16:82 Relationship with previously concluded Agreements

II. THE DATA PROTECTION ACT OF 2018

A. PART I PRELIMINARY

§ 16:83 Overview
§ 16:84 Territorial application of this Act
§ 16:85 Protection of personal data

B. PART 2 GENERAL PROCESSING

1. Scope and definitions

§ 16:86 Processing to which this Part applies

2. The UK GDPR

a. Lawfulness of processing

§ 16:87 Lawfulness of processing: public interest etc

b. Relevant international law

§ 16:88 Processing in reliance on relevant international law

c. Special categories of personal data

§ 16:89 Special categories of personal data and criminal convictions etc data
§ 16:90 Special categories of personal data etc: supplementary

d. Rights of the data subject

§ 16:91 Limits on fees that may be charged by controllers
§ 16:92 Obligations of credit reference agencies
§ 16:93 Automated decision-making authorised by law: safeguards

e. Exemptions

§ 16:94 Exemptions
§ 16:95 Power to make further exemptions etc by regulations

f. Certification

§ 16:96 Accreditation of certification providers

g. Transfers of personal data to third countries etc

§ 16:97 Transfers based on adequacy regulations
§ 16:98 Transfers based on adequacy regulations: review etc
§ 16:99 Standard data protection clauses
§ 16:100 Transfers of personal data to third countries etc public interest

h. Specific processing situations

§ 16:101 Processing for archiving, research and statistical purposes: safeguards

3. Chapter 3 Exemptions for manual unstructured processing and for national security and defence purposes

§ 16:102 Manual unstructured data held by FOI public authorities
§ 16:103 Manual unstructured data used in longstanding historical research
§ 16:104 National security and defence exemption
§ 16:105 National security: certificate
§ 16:106 National security and defence: modifications to Articles 9 and 32 of the UK GDPR

C. PART 3 LAW ENFORCEMENT PROCESSING

1. Chapter 1 Scope

§ 16:107 Processing to which this Part applies

2. Chapter 2 Principles

§ 16:108 Overview and general duty of controller
§ 16:109 The first data protection principle
§ 16:110 The second data protection principle
§ 16:111 The third data protection principle
§ 16:112 The fourth data protection principle
§ 16:113 The fifth data protection principle
§ 16:114 The sixth data protection principle
§ 16:115 Safeguards: archiving
§ 16:116 Safeguards: sensitive processing
§ 16:117 Further provision about sensitive processing

3. Chapter 3 Rights of the data subject

a. Overview and scope

§ 16:118 Overview and scope

b. Data subject's rights to information

§ 16:119 Controller's general duties
§ 16:120 Right of access by the data subject
§ 16:121 Exemption from sections 44 and 45: legal professional privilege

c. Data subject's rights to rectification or erasure etc

§ 16:122 Right to rectification
§ 16:123 Right to erasure or restriction of processing
§ 16:124 Rights under section 46 or 47: supplementary

d. Automated individual decision-making

§ 16:125 Right not to be subject to automated decision-making
§ 16:126 Automated decision-making authorised by law: safeguards
§ 16:127 Restrictions on automated decision-making based on sensitive processing
§ 16:128 Safeguards for automated decision-making
§ 16:129 Further provision about automated decision-making

e. Supplementary

§ 16:130 Exercise of rights through the Commissioner
§ 16:131 Form of provision of information etc
§ 16:132 Manifestly unfounded or excessive requests by the data subject
§ 16:133 Meaning of applicable time period

4. Chapter 4 Controller And Processor

a. Overview and scope

§ 16:134 Overview and scope

b. General obligations

§ 16:135 General obligations of the controller
§ 16:136 Data protection by design and default
§ 16:137 Joint controllers
§ 16:138 Processors
§ 16:139 Processing under the authority of the controller or processor
§ 16:140 Records of processing activities
§ 16:141 Logging
§ 16:142 Co-operation with the Commissioner
§ 16:143 Data protection impact assessment

§ 16:144 Prior consultation with the Commissioner

c. Obligations relating to security

§ 16:145 Security of processing

d. Obligations relating to personal data breaches

§ 16:146 Notification of a personal data breach to the Commissioner
§ 16:147 Communication of a personal data breach to the data subject

e. Data protection officers

§ 16:148 Designation of a data protection officer
§ 16:149 Position of data protection officer
§ 16:150 Tasks of data protection officer

f. Codes of conduct

§ 16:151 Codes of conduct

5. Chapter 5 Transfers Of Personal Data To Third Countries Etc

a. Overview and interpretation

§ 16:152 Overview and interpretation

b. General principles for transfers

§ 16:153 General principles for transfers of personal data
§ 16:154 Transfers based on adequacy regulations
§ 16:155 Transfers approved by regulations
§ 16:156 The data protection test
§ 16:157 Transfers on the basis of appropriate safeguards
§ 16:158 Transfers on the basis of special circumstances

c. Transfers to particular recipients

§ 16:159 Transfers of personal data to persons other than relevant authorities

d. Subsequent transfers

§ 16:160 Subsequent transfers

6. Chapter 6 Supplementary

§ 16:161 National security exemption
§ 16:162 National security: certificate
§ 16:163 Special processing restrictions
§ 16:164 Reporting of infringements

D. PART 4 INTELLIGENCE SERVICES PROCESSING

1. Chapter 1 Scope

§ 16:165 Processing to which this Part applies

2. Chapter 2 Principles

a. Overview

§ 16:166 Overview

b. Principles

§ 16:167 The first data protection principle
§ 16:168 The second data protection principle
§ 16:169 The third data protection principle
§ 16:170 The fourth data protection principle
§ 16:171 The fifth data protection principle
§ 16:172 The sixth data protection principle
§ 16:173 Further provision about sensitive processing

3. Chapter 3 Rights of the Data Subject

a. Overview

§ 16:174 Overview

b. Rights

§ 16:175 Right to information
§ 16:176 Right of access
§ 16:177 Right of access: supplementary
§ 16:178 Right not to be subject to automated decision-making
§ 16:179 Right to intervene in automated decision-making
§ 16:180 Right to information about decision-making
§ 16:181 Right to object to processing
§ 16:182 Rights to rectification and erasure

4. Chapter 4 Controller and Processor

a. Overview

§ 16:183 Overview

b. General obligations

§ 16:184 General obligations of the controller
§ 16:185 Data protection by design
§ 16:186 Joint controllers
§ 16:187 Processors

§ 16:188 Processing under the authority of the controller or processor

c. Obligations relating to security

§ 16:189 Security of processing

d. Obligations relating to personal data breaches

§ 16:190 Communication of a personal data breach

5. Chapter 5 Transfers of personal data outside the United Kingdom

§ 16:191 Transfers of personal data outside the United Kingdom

6. Chapter 6 Exemptions

§ 16:192 National security
§ 16:193 National security: certificate
§ 16:194 Other exemptions

E. PART 5 THE INFORMATION COMMISSIONER

1. The Commissioner

§ 16:195 The Information Commissioner and the Information Commission

2. General functions

§ 16:196 General functions under the UK GDPR and safeguards
§ 16:197 Other general functions
§ 16:198 Competence in relation to courts etc

3. International role

§ 16:199 Co-operation between parties to the Data Protection Convention
§ 16:200 Inspection of personal data in accordance with international obligations
§ 16:201 Standard clauses for transfers to third countries etc
§ 16:202 Further international role

4. Duties in carrying out functions

§ 16:203 Principal objective
§ 16:204 Duties in relation to functions under the data protection legislation
§ 16:205 Strategy

§ 16:206 Duty to consult other regulators

5. Codes of practice

§ 16:207 Data-sharing code
§ 16:208 Direct marketing code
§ 16:209 Age-appropriate design code
§ 16:210 Data protection and journalism code
§ 16:211 Other codes of practice
§ 16:212 Panels to consider codes of practice
§ 16:213 Impact assessments for codes of practice
§ 16:214 Approval of codes prepared under sections 121 to 124A
§ 16:215 Publication and review of codes issued under section 125(4)
§ 16:216 Effect of codes issued under section 125(4)

6. Consensual audits

§ 16:217 Consensual audits

7. Records of national security

§ 16:218 Records of national security certificates

8. Information provided to the Commissioner

§ 16:219 Disclosure of information to the Commissioner
§ 16:220 Confidentiality of information
§ 16:221 Guidance about privileged communications

9. Fees

§ 16:222 Fees for services
§ 16:223 Manifestly unfounded or excessive requests by data subjects etc
§ 16:224 Guidance about fees

10. Charges

§ 16:225 Charges payable to the Commissioner by controllers
§ 16:226 Regulations under section 137: supplementary

11. Reports

§ 16:227 Reporting to Parliament
§ 16:228 Analysis of performance

12. Documents and notices

§ 16:229 Publication by the Commissioner
§ 16:230 Notices from the Commissioner

F. PART 6 ENFORCEMENT

1. Information notices

§ 16:231 Information notices
§ 16:232 Information notices: restrictions
§ 16:233 False statements made in response to information notices
§ 16:234 Information orders

2. Assessment notices

§ 16:235 Assessment notices
§ 16:236 Assessment notices: restrictions

3. Information notices and assessment notices: destruction of documents etc

§ 16:237 Destroying or falsifying information and documents etc

4. Enforcement notices

§ 16:238 Enforcement notices
§ 16:239 Enforcement notices: supplementary
§ 16:240 Enforcement notices: rectification and erasure of personal data etc
§ 16:241 Enforcement notices: restrictions
§ 16:242 Enforcement notices: cancellation and variation

5. Powers of entry and inspection

§ 16:243 Powers of entry and inspection

6. Penalties

§ 16:244 Penalty notices
§ 16:245 Penalty notices: restrictions
§ 16:246 Maximum amount of penalty
§ 16:247 Fixed penalties for non-compliance with charges regulations
§ 16:248 Amount of penalties: supplementary

7. Guidance and report

§ 16:249 Guidance about regulatory action
§ 16:250 Approval of first guidance about regulatory action
§ 16:251 Annual report on regulatory action

8. Appeals

§ 16:252 Rights of appeal
§ 16:253 Determination of appeals

§ 16:254 Applications in respect of urgent notices

9. Complaints

§ 16:255 Complaints by data subjects to controllers
§ 16:256 Controllers to notify the Commissioner of the number of complaints
§ 16:257 Complaints by data subjects
§ 16:258 Orders to progress complaints

10. Remedies in the court

§ 16:259 Compliance orders
§ 16:260 Compensation for contravention of the UK GDPR
§ 16:261 Compensation for contravention of other data protection legislation

11. Offences relating to personal data

§ 16:262 Unlawful obtaining etc of personal data
§ 16:263 Re-identification of de-identified personal data
§ 16:264 Re-identification: effectiveness testing conditions
§ 16:265 Alteration etc of personal data to prevent disclosure to data subject

12. The special purposes

§ 16:266 The special services
§ 16:267 Provision of assistance in special purposes proceedings
§ 16:268 Staying special purposes proceedings
§ 16:269 Guidance about how to seek redress against media organisations
§ 16:270 Review of processing of personal data for the purposes of journalism
§ 16:271 Effectiveness of the media's dispute resolution procedures

13. Jurisdiction and court procedure

§ 16:272 Jurisdiction
§ 16:273 Procedure in connection with subject access requests

G. PART 7 SUPPLEMENTARY AND FINAL PROVISION

1. Regulations under this Act

§ 16:274 Regulations and consultation

2. Changes to the Data Protection Convention

§ 16:275 Power to reflect changes to the Data Protection Convention

3. Prohibitions and restrictions on processing

§ 16:276 Protection of prohibitions and restrictions etc on processing: relevant enactments

§ 16:277 Protection of prohibitions and restrictions etc on processing: other enactments

4. Rights of the data subject

§ 16:278 Prohibition of requirement to produce relevant records

§ 16:279 Avoidance of certain contractual terms relating to health records

§ 16:280 Protection of data subject's rights

§ 16:281 Protection of data subject's rights: further provision

5. Representation of data subjects

§ 16:282 Representation of data subjects with their authority

§ 16:283 Representation of data subjects with their authority: collective proceedings

§ 16:284 Duty to review provision for representation of data subjects

§ 16:285 Post-review powers to make provision about representation of data subjects

6. Framework for Data Processing by Government

§ 16:286 Framework for Data Processing by Government

§ 16:287 Approval of the Framework

§ 16:288 Publication and review of the Framework

§ 16:289 Effect of the Framework

7. Offences

§ 16:290 Penalties for offences

§ 16:291 Prosecution

§ 16:292 Liability of directors

8. The Tribunal

§ 16:293 Disclosure of information to the Tribunal

§ 16:294 Proceedings in the First-tier Tribunal: contempt

§ 16:295 Tribunal Procedure Rules

PART III. ASIA AND PACIFIC

CHAPTER 17. AUSTRALIA

§ 17:1 Privacy Act 1988
§ 17:2 Australian Privacy Principle 1—Open and transparent management of personal information
§ 17:3 Australian Privacy Principle 2—Anonymity and pseudonymity
§ 17:4 Australian Privacy Principle 3—Collection of solicited personal information
§ 17:5 Australian Privacy Principle 4—Dealing with unsolicited personal information
§ 17:6 Australian Privacy Principle 5—Notification of the collection of personal information
§ 17:7 Australian Privacy Principle 6—Use or disclosure of personal information
§ 17:8 Australian Privacy Principle 7—Direct marketing
§ 17:9 Australian Privacy Principle 8—Cross-border disclosure of personal information
§ 17:10 Australian Privacy Principle 9—Adoption, use or disclosure of government related identifiers
§ 17:11 Australian Privacy Principle 10—Quality of personal information
§ 17:12 Australian Privacy Principle 11—Security of personal information
§ 17:13 Australian Privacy Principle 12—Access to personal information
§ 17:14 Australian Privacy Principle 13—Correction of personal information
§ 17:15 Credit reporting
§ 17:16 Regulations
§ 17:17 Privacy regulatory action policy
§ 17:18 Australian guide to securing personal information

CHAPTER 17A. CHINA

I. PERSONAL INFORMATION PROTECTION LAW (PIPL)

A. CHAPTER I GENERAL PROVISIONS

§ 17A:1 Generally

B. CHAPTER II PERSONAL INFORMATION PROCESSING RULES

§ 17A:2 General rules

§ 17A:3 Processing based upon consent
§ 17A:4 Notices
§ 17A:5 Retention/deletion
§ 17A:6 Joint controllers
§ 17A:7 Processors
§ 17A:8 Certain data transfers
§ 17A:9 Subprocessors/other processors
§ 17A:10 Automated decisions
§ 17A:11 Image capture/public collection
§ 17A:12 Rules on processing sensitive personal information
§ 17A:13 Minors
§ 17A:14 Special provisions on the processing of personal information by state organs

C. CHAPTER III RULES ON PROVISION OF PERSONAL INFORMATION ACROSS BORDER

§ 17A:15 Cross-border transfers

D. CHAPTER IV INDIVIDUALS' RIGHTS IN PERSONAL INFORMATION PROCESSING ACTIVITIES

§ 17A:16 Individuals' rights in personal information processing activities
§ 17A:17 Erasure
§ 17A:18 Deceased individuals
§ 17A:19 Mechanism for exercise of rights

E. CHAPTER V OBLIGATIONS OF PERSONAL INFORMATION PROCESSORS

§ 17A:20 Obligations of personal information processors
§ 17A:21 Compliance audits
§ 17A:22 DPIAs
§ 17A:23 Breaches
§ 17A:24 Internet platform providers
§ 17A:25 Security

F. CHAPTER VI DEPARTMENTS WITH PERSONAL INFORMATION PROTECTION DUTIES

§ 17A:26 Departments with personal information protection duties

G. CHAPTER VII LEGAL LIABILITY

§ 17A:27 Legal liability

H. CHAPTER VIII SUPPLEMENTARY PROVISIONS

§ 17A:28 Supplementary provisions

II. CYBERSECURITY LAW

A. CHAPTER I GENERAL PROVISIONS

§ 17A:29 General provisions

B. CHAPTER II SUPPORT AND PROMOTION OF NETWORK SECURITY

§ 17A:30 Support and promotion of network security

C. CHAPTER III NETWORK OPERATIONS SECURITY

§ 17A:31 Ordinary provisions
§ 17A:32 Operations security for critical information infrastructure
§ 17A:33 Localization
§ 17A:34 Assessments
§ 17A:35 Security requirements for critical infrastructure

D. CHAPTER IV NETWORK INFORMATION SECURITY

§ 17A:36 Network information security
§ 17A:37 Deletion of data
§ 17A:38 Illegal access/methods
§ 17A:39 Restrictions on disclosure
§ 17A:40 Public reporting for security events
§ 17A:41 Inspection

E. CHAPTER V MONITORING, EARLY WARNINGS, AND EMERGENCY RESPONSES

§ 17A:42 Monitoring, early warnings, and emergency responses

F. CHAPTER VI LEGAL RESPONSIBILITY

§ 17A:43 Legal responsibility

G. CHAPTER VII SUPPLEMENTARY PROVISIONS

§ 17A:44 Supplementary provisions

III. DATA SECURITY LAW

A. CHAPTER I GENERAL PROVISIONS

§ 17A:45 General provisions

B. CHAPTER II DATA SECURITY AND DEVELOPMENT

§ 17A:46 Data security and development

C. CHAPTER III DATA SECURITY SYSTEMS

§ 17A:47 Data security systems

D. CHAPTER IV DATA SECURITY PROTECTION OBLIGATIONS

§ 17A:48 Data security protection obligations

E. CHAPTER V SECURITY AND OPENNESS OF GOVERNMENT DATA

§ 17A:49 Security and openness of government data

F. CHAPTER VI LEGAL LIABILITY

§ 17A:50 Legal liability

G. CHAPTER VII SUPPLEMENTARY PROVISIONS

§ 17A:51 Supplementary provisions

CHAPTER 18. HONG KONG

§ 18:1 Ordinance
§ 18:2 Miscellaneous definitions—Consent
§ 18:3 —Contravention of Act
§ 18:4 —Complaints
§ 18:5 —Miscellaneous provisions
§ 18:6 Application
§ 18:7 Data protection principles
§ 18:8 Establishment of Privacy Commissioner for Personal Data
§ 18:9 Functions and powers of Commissioner
§ 18:10 Staff of Commissioner

§ 18:11 Delegations by Commissioner
§ 18:12 Establishment of Personal Data (Privacy) Advisory Committee
§ 18:13 Immunity
§ 18:14 Approval of codes of practice by Commissioner
§ 18:15 Data user returns
§ 18:16 Verification of data user returns
§ 18:17 Register of data users
§ 18:18 Inspection of register
§ 18:19 Register shall not limit operation of this Ordinance
§ 18:20 Interpretation of Part 5
§ 18:21 Data access request
§ 18:22 Compliance with data access request
§ 18:23 Circumstances in which data user shall or may refuse to comply with data access request
§ 18:24 Notification of refusal to comply with data access request
§ 18:25 Data correction request
§ 18:26 Compliance with data correction request
§ 18:27 Circumstances in which data user shall or may refuse to comply with data correction request
§ 18:28 Notification of refusal to comply with data correction request
§ 18:29 Erasure of personal data no longer required
§ 18:30 Log book to be kept by data user
§ 18:31 Imposition of fees by data user
§ 18:32 Service and language of certain notices
§ 18:33 Matching procedure not to be carried out except with consent of data subject
§ 18:34 Matching procedure request
§ 18:35 Determination of matching procedure request
§ 18:36 Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances
§ 18:37 Repeated collections of personal data in same circumstances
§ 18:38 Interpretation of Part 6A
§ 18:39 Application
§ 18:40 Data user to take specified action before using personal data in direct marketing
§ 18:41 Circumstances under which section 35C does not apply
§ 18:42 Data user must not use personal data in direct marketing without data subject's consent
§ 18:43 Data user must notify data subject when using personal data in direct marketing for first time

§ 18:44 Data subject may require data user to cease to use personal data in direct marketing
§ 18:45 Prescribed consent for using personal data in direct marketing under data protection principle 3
§ 18:46 Application
§ 18:47 Data user to take specified action before providing personal data
§ 18:48 Data user must not provide personal data for use in direct marketing without data subject's consent
§ 18:49 Data subject may require data user to cease to provide personal data for use in direct marketing
§ 18:50 Prescribed consent for providing personal data for use in direct marketing under data protection principle 3
§ 18:51 Inspections of personal data systems
§ 18:52 Complaints
§ 18:53 Investigations by Commissioner
§ 18:54 Restrictions on investigations initiated by complaints
§ 18:55 Commissioner may carry out or continue investigation initiated by complaint notwithstanding withdrawal of complaint
§ 18:56 Commissioner to inform relevant data user of inspection or investigation
§ 18:57 Power of entry on premises for the purposes of an inspection or investigation
§ 18:58 Proceedings of Commissioner
§ 18:59 Evidence
§ 18:60 Protection of witnesses
§ 18:61 Commissioner to maintain secrecy
§ 18:62 Persons to be informed of result of inspection or investigation
§ 18:63 Reports by Commissioner
§ 18:64 Cases in which sections 47 and 48 shall not apply
§ 18:65 Enforcement notices
§ 18:66 Offences relating to enforcement notices
§ 18:67 Offences relating to failure to comply with requirements of Commissioner
§ 18:68 Interpretation
§ 18:69 Performance of judicial functions
§ 18:70 Domestic purposes
§ 18:71 Employment—Staff planning
§ 18:72 —Transitional provisions
§ 18:73 Relevant process
§ 18:74 Personal references
§ 18:75 Security in respect of Hong Kong

§ 18:76 Use of data related to criminal issues
§ 18:77 Protected product and relevant records under Interception of Communications and Surveillance Ordinance
§ 18:78 Health
§ 18:79 Care and guardianship of minors
§ 18:80 Legal professional privilege
§ 18:81 Self-incrimination
§ 18:82 Legal proceedings
§ 18:83 News
§ 18:84 Statistics and research
§ 18:85 Exemption from section 18(1)(a)
§ 18:86 Human embryos
§ 18:87 Due diligence exercise
§ 18:88 Emergency situations
§ 18:89 Transfer of records to Government Records Service
§ 18:90 Offences for disclosing personal data obtained without consent from data users
§ 18:91 Miscellaneous offences
§ 18:92 Time limit for laying of information
§ 18:93 Liability of employers and principals
§ 18:94 Compensation
§ 18:95 Help for aggrieved persons in obtaining information
§ 18:96 Commissioner may grant assistance in respect of proceedings
§ 18:97 Power of Commissioner to specify forms
§ 18:98 Service of notices
§ 18:99 Regulations—fees
§ 18:100 Amendment of Schedules 2, 4 and 6
§ 18:101 Data Protection Principles
§ 18:102 DPP1—Data Collection Principle
§ 18:103 DPP2—Accuracy & Retention Principle
§ 18:104 DPP3—Data Use Principle
§ 18:105 DPP4—Data Security Principle
§ 18:106 DPP5—Openness Principle
§ 18:107 DPP6—Data Access & Correction Principle

Volume 2

CHAPTER 19. INDIA

I. INFORMATION TECHNOLOGY ACT, 2000

A. PRELIMINARY

§ 19:1 Overview

B. DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE

§ 19:2 Authentication of electronic records
§ 19:3 Electronic signature

C. ELECTRONIC GOVERNANCE

§ 19:4 Legal recognition of electronic records
§ 19:5 Legal recognition of electronic signatures
§ 19:6 Use of electronic records and electronic signatures in Government and its agencies
§ 19:7 Delivery of services by service provider
§ 19:8 Retention of electronic records
§ 19:9 Audit of documents maintained in electronic form
§ 19:10 Publication in Electronic Gazette
§ 19:11 No right to insist on a document being accepted in electronic form
§ 19:12 Power to make rules by Central Government in respect of an electronic signature
§ 19:13 Validity of contracts formed through electronic means

D. ATTRIBUTION, ACKNOWLEDGMENT AND DESPATCH OF ELECTRONIC RECORDS

§ 19:14 Attribution of electronic records
§ 19:15 Acknowledgment of receipt
§ 19:16 Time and place of dispatch and receipt of electronic record

E. SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES

§ 19:17 Secure electronic record
§ 19:18 Secure electronic signature
§ 19:19 Security procedures and practices

F. REGULATION OF CERTIFYING AUTHORITIES

§ 19:20 Appointment of Controller and other officers
§ 19:21 Functions of Controller
§ 19:22 Recognition of foreign Certifying Authorities
§ 19:23 License to issue electronic signature Certificates
§ 19:24 Application for license
§ 19:25 Renewal of license
§ 19:26 Procedure for grant or rejection of license
§ 19:27 Suspension of license
§ 19:28 Notice of suspension or revocation of license
§ 19:29 Power to delegate
§ 19:30 Power to investigate contraventions
§ 19:31 Access to computers and data
§ 19:32 Certifying Authority to follow certain procedures
§ 19:33 Certifying Authority to ensure compliance of the Act
§ 19:34 Display of license
§ 19:35 Surrender of license
§ 19:36 Disclosure

G. ELECTRONIC SIGNATURE CERTIFICATES

§ 19:37 Certifying authority to issue electronic signature Certificate
§ 19:38 Representations upon issuance of Digital Signature Certificate
§ 19:39 Suspension of Digital Signature Certificate
§ 19:40 Revocation of Digital Signature Certificate
§ 19:41 Notice of suspension or revocation

H. DUTIES OF SUBSCRIBERS

§ 19:42 Generating key pair
§ 19:43 Duties of subscriber of Electronic Signature Certificate
§ 19:44 Acceptance of Digital Signature Certificate
§ 19:45 Control of private key

I. PENALTIES, COMPENSATION AND ADJUDICATION

§ 19:46 Penalty and compensation for damage to computer, computer system, etc
§ 19:47 Compensation for failure to protect data
§ 19:48 Penalty for failure to furnish information, return, etc
§ 19:49 Residuary penalty
§ 19:50 Power to adjudicate

§ 19:51 Factors to be taken into account by the adjudicating officer

J. THE APPELLATE TRIBUNAL

§ 19:52 Appellate Tribunal
§ 19:53 Decision by majority
§ 19:54 Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings
§ 19:55 Appeal to Appellate Tribunal
§ 19:56 Procedure and powers of the Appellate Tribunal
§ 19:57 Right to legal representation
§ 19:58 Limitation
§ 19:59 Civil court does not have jurisdiction
§ 19:60 Appeal to High Court
§ 19:61 Compounding of contraventions
§ 19:62 Recovery of penalty or compensation

K. OFFENCES

§ 19:63 Tampering with computer source documents
§ 19:64 Computer related offences
§ 19:65 Punishment for sending offensive messages through communication service
§ 19:66 Punishment for dishonestly receiving stolen computer resource or communication device
§ 19:67 Punishment for identity theft
§ 19:68 Punishment for cheating by personation by using computer resource
§ 19:69 Punishment for violation of privacy
§ 19:70 Punishment for cyber terrorism
§ 19:71 Punishment for publishing or transmitting obscene material in electronic form
§ 19:72 Punishment for publishing or transmitting of material containing sexually explicit act, in electronic form
§ 19:73 Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form
§ 19:74 Preservation and retention of information by intermediaries
§ 19:75 Power of Controller to give directions
§ 19:76 Power to issue directions for interception or monitoring or decryption of any information through any computer resource
§ 19:77 Power to issue directions for blocking for public

access of any information through any computer resource
§ 19:78 Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security
§ 19:79 Protected system
§ 19:80 National nodal agency
§ 19:81 Indian Computer Emergency Response Team to serve as national agency for incident response
§ 19:82 Penalty for misrepresentation
§ 19:83 Penalty for Breach of confidentiality and privacy
§ 19:84 Punishment for disclosure of information in breach of lawful contract
§ 19:85 Penalty for publishing electronic signature Certificate false in certain particulars
§ 19:86 Publication for fraudulent purpose
§ 19:87 Act to apply for offence or contravention committed outside India
§ 19:88 Confiscation
§ 19:89 Compensation, penalties or confiscation not to interfere with other punishment
§ 19:90 Compounding of offences
§ 19:91 Offences with three years imprisonment to be bailable
§ 19:92 Power to investigate offences

L. INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES

§ 19:93 Exemption from liability of intermediary in certain cases

M. EXAMINER OF ELECTRONIC EVIDENCE

§ 19:94 Central Government to notify Examiner of Electronic Evidence

N. MISCELLANEOUS

§ 19:95 Power of police officer and other officers to enter, search, etc
§ 19:96 Act to have overriding effect
§ 19:97 Application of the Act to electronic cheque and truncated cheque
§ 19:98 Controller, Deputy Controller and Assistant Controller to be public servants
§ 19:99 Power to give directions

§ 19:100 Protection of action taken in good faith
§ 19:101 Modes or methods for encryption
§ 19:102 Punishment for abetment of offences
§ 19:103 Punishment for attempt to commit offences
§ 19:104 Offences by companies
§ 19:105 Removal of difficulties
§ 19:106 Power of Central Government to make rules
§ 19:107 Constitution of Advisory Committee
§ 19:108 Power of Controller to make regulations
§ 19:109 Power of State Government to make rules

II. NO. 20(3)/2022-CERT-IN GOVERNMENT OF INDIA MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY (MEITY) INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-IN)

§ 19:110 Overview

CHAPTER 20. JAPAN

§ 20:1 Introduction to Japanese law

I. ACT ON THE PROTECTION OF PERSONAL INFORMATION (ACT NO. 57 OF 2003)

§ 20:2 Key definitions
§ 20:3 Specification of the Purpose of Utilization
§ 20:4 Transfer of business operations and personal information
§ 20:5 Restrictions on acquisition of information
§ 20:6 Notice generally
§ 20:7 Notice of changes of the Purpose of Utilization
§ 20:8 Exceptions to notice generally and notice of changes of the Purpose of Utilization
§ 20:9 Data accuracy
§ 20:10 Data security
§ 20:11 Supervision of employees and trustees
§ 20:12 Restrictions on transfers to third-parties
§ 20:13 Public announcements versus notice
§ 20:14 Notice of Purpose of Utilization
§ 20:15 Right of access
§ 20:16 Right of correction
§ 20:17 Deletion of information
§ 20:18 Procedural requirements for disclosures and charges
§ 20:19 Processing of complaints and collection of reports

§ 20:20 Collection of reports
§ 20:21 Exemption from certain requirements
§ 20:22 Enforcement

II. JAPAN — GUIDELINES FOR PERSONAL INFORMATION PROTECTION IN THE FINANCIAL FIELD

§ 20:23 Purpose (relevant to Article 1 of the Law)
§ 20:24 Definitions, etc. (Article 2 of the Law, Article 1 to 4 of the Order for Enforcement)
§ 20:25 Specification of the Purpose of Use (relevant to Article 15 of the Law)
§ 20:26 Regarding the format of consent (relevant to Article 16 and 23 of the Law)
§ 20:27 Restriction by the Purpose of Use (relevant to Article 16 of the Law)
§ 20:28 Regarding sensitive information
§ 20:29 Proper acquisition (relevant to Article 17 of the Law)
§ 20:30 Notice of the Purpose of Use at the time of acquisition (relevant to Article 18 of the Law)
§ 20:31 Maintenance of the accuracy of data (relevant to Article 19 of the Law)
§ 20:32 Security control measures (relevant to Article 20 of the Law and the Basic Policy)
§ 20:33 Supervision of employees (relevant to Article 21 of the Law and the Basic Policy)
§ 20:34 Supervision of trustees (relevant to Article 22 of the Law and the Basic Policy)
§ 20:35 Restriction of provision to third parties (relevant to Article 23 of the Law)
§ 20:36 Announcement of matters concerning retained personal data, etc. (relevant to Article 24 of the Law and Article 5, Order for enforcement)
§ 20:37 Disclosure (relevant to Article 25 of the Law)
§ 20:38 Correction (relevant to Article 26 of the Law and Article 6, Order for enforcement)
§ 20:39 Stopping the use (relevant to Article 27 of the Law)
§ 20:40 Explanation of reasons (relevant to Article 28 of the Law)
§ 20:41 Procedures to meet requests for disclosure and others (relevant to Article 29 of the Law and Article 7, 8, Order for enforcement)
§ 20:42 Charges (relevant to Article 30 of the Law)
§ 20:43 Handling of complaints by entities handling personal information (relevant to Article 31 of the Law)

§ 20:44 Responding to leakages (relevant to the Basic Policy)—Notice of security breach
§ 20:45 Formulation of pronouncement concerning protection of personal information (relevant to Article 18, 24 of the Law, and the Basic Policy)
§ 20:46 Ministry of Economy, Trade and Industry October 9, 2009 guidance

CHAPTER 21. MALAYSIA

§ 21:1 The Personal Data Protection Act
§ 21:2 Data Protection Authority
§ 21:3 Scope and key definitions
§ 21:4 Other definitions
§ 21:5 Appointment of representative
§ 21:6 The personal data protection principles
§ 21:7 The general principle
§ 21:8 The notice and choice principle
§ 21:9 Restrictions on direct marketing
§ 21:10 The disclosure principle
§ 21:11 The security principle
§ 21:12 The data integrity principle
§ 21:13 The data retention principle
§ 21:14 The access principle
§ 21:15 Cross-border transfers
§ 21:16 Database registration
§ 21:17 Breach notification
§ 21:18 Enforcement
§ 21:19 Exemptions

CHAPTER 22. PHILIPPINES

§ 22:1 Data Privacy Act
§ 22:2 Declaration of policy
§ 22:3 Definition of terms
§ 22:4 Scope
§ 22:5 Protection afforded to journalists and their sources
§ 22:6 Extraterritorial application
§ 22:7 Functions of the National Privacy Commission
§ 22:8 Confidentiality
§ 22:9 Organizational Structure of the Commission
§ 22:10 General data privacy principles
§ 22:11 Criteria for lawful processing of personal information
§ 22:12 Sensitive personal information and privileged information
§ 22:13 Subcontract of personal information

§ 22:14 Extension of privileged communication
§ 22:15 Rights of the data subject
§ 22:16 Transmissibility of rights of the data subject
§ 22:17 Right to data portability
§ 22:18 Non-applicability
§ 22:19 Security of personal information
§ 22:20 Principle of accountability
§ 22:21 Responsibility of heads of agencies
§ 22:22 Requirements relating to access by agency personnel to sensitive personal information
§ 22:23 Off-site access
§ 22:24 Applicability to government contractors
§ 22:25 Unauthorized processing of personal information and sensitive personal information
§ 22:26 Accessing personal information and sensitive personal information due to negligence
§ 22:27 Improper disposal of personal information and sensitive personal information
§ 22:28 Processing of personal information and sensitive personal information for unauthorized purposes
§ 22:29 Unauthorized access or intentional breach
§ 22:30 Concealment of security breaches involving sensitive personal information
§ 22:31 Malicious disclosure
§ 22:32 Unauthorized disclosure
§ 22:33 Combination or series of acts
§ 22:34 Extent of liability
§ 22:35 Large-scale
§ 22:36 Offense committed by public officer
§ 22:37 Restitution
§ 22:38 Interpretation
§ 22:39 Implementing Rules and Regulations (IRR)
§ 22:40 Reports and Information

CHAPTER 23. SINGAPORE

I. THE PERSONAL DATA PROTECTION ACT 2012

§ 23:1 Key definitions
§ 23:2 Purpose
§ 23:3 Application of Act
§ 23:4 Personal Data Protection Commission
§ 23:5 Functions of Commission
§ 23:6 Advisory committees
§ 23:7 Delegation

§ 23:8 Administration Body
§ 23:9 Co-operation agreements
§ 23:10 Compliance with Act
§ 23:11 Policies and practices
§ 23:12 Consent required
§ 23:13 Provision of consent
§ 23:14 Deemed consent
§ 23:15 Withdrawal of consent
§ 23:16 Collection, use and disclosure without consent
§ 23:17 Limitation of purpose and extent
§ 23:18 Personal data collected before appointed day
§ 23:19 Notification of purpose
§ 23:20 Access to personal data
§ 23:21 Correction of personal data
§ 23:22 Accuracy of personal data
§ 23:23 Protection of personal data
§ 23:24 Retention of personal data
§ 23:25 Transfer of personal data outside Singapore
§ 23:26 Alternative dispute resolution
§ 23:27 Power to review
§ 23:28 Power to give directions
§ 23:29 Enforcement of directions of Commission in District Court
§ 23:30 Reconsideration of directions or decisions
§ 23:31 Right of private action
§ 23:32 Data Protection Appeal Panel and Data Protection Appeal Committees
§ 23:33 Appeal from direction or decision of Commission
§ 23:34 Appeals to High Court and Court of Appeal
§ 23:35 Key definitions
§ 23:36 Meaning of "specified message"
§ 23:37 Application of the law
§ 23:38 Register
§ 23:39 Applications
§ 23:40 Evidence
§ 23:41 Information on terminated Singapore telephone number
§ 23:42 Duty to check register
§ 23:43 Contact information
§ 23:44 Calling line identity not to be concealed
§ 23:45 Consent
§ 23:46 Withdrawal of consent
§ 23:47 Defence for employee
§ 23:48 Advisory guidelines
§ 23:49 Powers of investigation

§ 23:50 Offences and penalties
§ 23:51 Offences by bodies corporate, etc.
§ 23:52 Liability of employers for acts of employees
§ 23:53 Jurisdiction of court
§ 23:54 Composition of offences
§ 23:55 General penalties
§ 23:56 Public servants
§ 23:57 Evidence in proceedings
§ 23:58 Preservation of secrecy
§ 23:59 Protection from personal liability
§ 23:60 Symbol of Commission
§ 23:61 Power to exempt
§ 23:62 Certificate as to national interest
§ 23:63 Amendment of schedules
§ 23:64 Power to make regulations
§ 23:65 Rules of Court

II. PERSONAL DATA PROTECTION (DO NOT CALL REGISTRY) REGULATIONS 2013

§ 23:66 Key Definitions
§ 23:67 Application by subscriber to add or remove Singapore telephone number
§ 23:68 Effective date of addition or removal
§ 23:69 Application by subscriber to confirm listing in register
§ 23:70 Application by or on behalf of subscriber
§ 23:71 Correction or alteration of register
§ 23:72 Registration before applying to check register
§ 23:73 Application to check Do Not Call Registers
§ 23:74 Fees
§ 23:75 Application on behalf of person
§ 23:76 Registration of telecommunications service providers
§ 23:77 Submission of report on terminated Singapore telephone numbers
§ 23:78 Prescribed fee
§ 23:79 Schedules

CHAPTER 24. SOUTH KOREA

I. PERSONAL INFORMATION PROTECTION ACT

§ 24:1 Overview
§ 24:2 Principles
§ 24:3 Rights of data subjects

§ 24:4 State obligations
§ 24:5 Relationship to other acts
§ 24:6 Creation of a Data Protection Commission
§ 24:7 Collection and use of personal information
§ 24:8 Limitations on the collection of personal information
§ 24:9 Sharing of personal information
§ 24:10 Limitations on the use and sharing of personal information
§ 24:11 Public institutions
§ 24:12 Out-of purpose use of personal information or control of provision thereof to a third party
§ 24:13 Exceptions
§ 24:14 Limitations on third-party use of personal information
§ 24:15 Right to request information regarding third-party data sources
§ 24:16 Data destruction
§ 24:17 Methods to obtain consent
§ 24:18 Consent from minors
§ 24:19 Limitations on processing personal information—Limitations on processing sensitive data
§ 24:20 Limitations on processing unique identifiers
§ 24:21 Limitations to processing resident registration number
§ 24:22 Limitations on video surveillance
§ 24:23 Limitations on outsourcing
§ 24:24 Limitations on the transfer of personal information on mergers
§ 24:25 Supervision of "handlers" of personal information
§ 24:26 Safeguards
§ 24:27 Privacy policies
§ 24:28 Designation of privacy officer
§ 24:29 Certification of personal information protection
§ 24:30 Data breach notification
§ 24:31 Access rights
§ 24:32 The right of rectification and deletion
§ 24:33 Suspension of the processing of personal information
§ 24:34 Method and procedure for exercise of rights
§ 24:35 Responsibility for damages
§ 24:36 Personal Information Dispute Mediation Committee—Establishment and composition of committee
§ 24:37 Application for mediation of dispute
§ 24:38 Time limitation of mediation procedure
§ 24:39 Dispute mediation
§ 24:40 Rejection and suspension of mediation

§ 24:41 Collective dispute mediation
§ 24:42 Collective suits
§ 24:43 Application for approval of lawsuits
§ 24:44 Requirement for approval of the lawsuit
§ 24:45 Effects of conclusive judgment
§ 24:46 Application of Civil Procedure Act
§ 24:47 Select exceptions
§ 24:48 Prohibited activities
§ 24:49 Confidentiality
§ 24:50 Suggestions and advice for improvement
§ 24:51 Reporting of violations
§ 24:52 Request for materials and inspection
§ 24:53 Corrective measures
§ 24:54 Accusation and recommendation of disciplinary action
§ 24:55 Result disclosure
§ 24:56 Annual report
§ 24:57 Delegation of authority
§ 24:58 Government processing of unique identifiers
§ 24:59 Penal provisions
§ 24:60 Fine for negligence

II. PERSONAL INFORMATION SAFEGUARD AND SECURITY STANDARD

§ 24:61 Additional security regulations
§ 24:62 Internal management plan
§ 24:63 Access management
§ 24:64 Access controls
§ 24:65 Encryption
§ 24:66 Connection records and audits
§ 24:67 Anti-Malware
§ 24:68 Physical security
§ 24:69 Destruction

III. OTHER LAWS

§ 24:70 Sector specific laws

CHAPTER 25. TAIWAN

§ 25:1 Personal Data Protection Act
§ 25:2 Key definitions
§ 25:3 Rights of an individual
§ 25:4 Collection and processing of information—Scope of processing
§ 25:5 Collection and processing of sensitive information

§ 25:6 Written consent
§ 25:7 Collection, processing and utilization of personal data by government agencies
§ 25:8 Collection, processing and utilization of personal data by non-government agencies
§ 25:9 Exemptions
§ 25:10 Enforcement
§ 25:11 Taiwan enforcement rules of the Personal Information Protection Act
§ 25:12 Key definitions
§ 25:13 Outsourcing
§ 25:14 Notice of security breach

PART IV. CANADA

CHAPTER 26. CANADA AND SELECT PROVINCES

§ 26:1 The Patriot Act and international compliance issues

I. GENERAL CONSIDERATIONS

§ 26:2 Purpose of PIPEDA
§ 26:3 Overview of PIPEDA
§ 26:4 Key definitions
§ 26:5 Application of PIPEDA

II. PRINCIPLES OF PIPEDA

§ 26:6 Accountability
§ 26:7 Identifying purposes
§ 26:8 Consent
§ 26:9 —Use without knowledge or consent
§ 26:10 —Disclosures without knowledge or consent
§ 26:11 —Form of consent
§ 26:12 Implied consent in a dispute resolution process
§ 26:13 Consent—Withdrawal of consent
§ 26:14 Limiting collection
§ 26:15 Limiting use, disclosure and retention
§ 26:16 Accuracy
§ 26:17 Safeguards
§ 26:18 Openness
§ 26:19 —Regional disclosures
§ 26:20 Individual access
§ 26:21 —Information related to paragraphs 7(3)(c), (c.1) or (d)

§ 26:22 —Refusal of access
§ 26:23 Notice of refusal of access
§ 26:24 Challenging compliance

III. ENFORCEMENT AND EXCEPTIONS

§ 26:25 Enforcement
§ 26:26 —Powers of commissioner
§ 26:27 —Reporting by the commissioner
§ 26:28 Civil enforcement
§ 26:29 Exceptions to PIPEDA

IV. ELECTRONIC MAIL

§ 26:30 Anti-spam law
§ 26:31 Purpose
§ 26:32 Defining a recipient
§ 26:33 Conflict of provisions
§ 26:34 Effect on government corporations
§ 26:35 Application
§ 26:36 Requirements and prohibitions
§ 26:37 Administrative monetary penalties—Designation
§ 26:38 —Preservation demand
§ 26:39 —Notice to produce
§ 26:40 —Warrants
§ 26:41 —Violations
§ 26:42 —Undertakings
§ 26:43 —Notices of violation
§ 26:44 —Determination of responsibility
§ 26:45 —Appeal to Federal Court of Appeal
§ 26:46 —Recovery of penalties and other amounts
§ 26:47 —Rules about violations
§ 26:48 —General provisions
§ 26:49 Injunction
§ 26:50 Offences
§ 26:51 Private right of action
§ 26:52 —Hearing
§ 26:53 —Rules about contraventions and reviewable conduct
§ 26:54 Consultation and disclosure of information
§ 26:55 General
§ 26:56 Transitional provisions
§ 26:57 Regulations

V. OTHER CONSIDERATIONS

§ 26:58 Data sharing with U.S. parent

§ 26:59 Loss of laptop computers in Canada

VI. ALBERTA

§ 26:60 Alberta
§ 26:61 Purpose of the Act
§ 26:62 Application
§ 26:63 Information collected prior to January 1, 2004
§ 26:64 Inconsistencies
§ 26:65 Waiver
§ 26:66 Compliance with the Act
§ 26:67 Policies and practices
§ 26:68 Consent
§ 26:69 Form of consent
§ 26:70 Withdrawal or variation of consent
§ 26:71 Consent obtained by deception
§ 26:72 Limitations on collection of personal information
§ 26:73 Limitation on sources for collection
§ 26:74 Notification required for collection
§ 26:75 Collection without consent
§ 26:76 Collection of personal employee information
§ 26:77 Use of personal information—Limitations on use
§ 26:78 Use without consent
§ 26:79 Use of personal employee information
§ 26:80 Disclosure of personal information—Limitations on disclosure
§ 26:81 Disclosure without consent
§ 26:82 Disclosure of personal employee information
§ 26:83 Disclosure regarding an acquisition of a business
§ 26:84 Access and correction to personal information
§ 26:85 Right to request correction
§ 26:86 Making a request for access or correction
§ 26:87 Duty to assist
§ 26:88 Time limit for responding
§ 26:89 Contents of response
§ 26:90 Method of giving access
§ 26:91 Extending the time limit for responding
§ 26:92 Fees
§ 26:93 Accuracy of information
§ 26:94 Protection of information
§ 26:95 Retention of information
§ 26:96 General powers of the Commissioner
§ 26:97 Power to authorize an organization to disregard requests

§ 26:98 Powers of the Commissioner regarding investigations or inquiries
§ 26:99 Statements not admissible in evidence
§ 26:100 Privileged information
§ 26:101 Restrictions on disclosure of information
§ 26:102 Protection of the Commissioner and staff
§ 26:103 Delegation by the Commissioner
§ 26:104 Extra-provincial commissioner
§ 26:105 Annual report of the Commissioner
§ 26:106 Right to ask for a review or initiate a complaint
§ 26:107 Initiating review or a complaint
§ 26:108 Notifying others of review or complaint
§ 26:109 Mediation with the Commissioner
§ 26:110 Inquiry by the Commissioner
§ 26:111 Burden of proof
§ 26:112 The Commissioner's orders
§ 26:113 No appeal
§ 26:114 Duty to comply with orders
§ 26:115 Professional regulatory organizations
§ 26:116 Exercise of rights by other persons
§ 26:117 General regulations
§ 26:118 Non-profit organizations
§ 26:119 Protection of organization from legal actions
§ 26:120 Protection of employees
§ 26:121 Offences and penalties
§ 26:122 Damages for breach of this Act
§ 26:123 Review of Act

VII. BRITISH COLUMBIA

A. PERSONAL INFORMATION PROTECTION ACT

§ 26:124 Purpose
§ 26:125 Application of Act
§ 26:126 Compliance with Act
§ 26:127 Policies and practices
§ 26:128 Role of consent
§ 26:129 Form of consent
§ 26:130 Restrictions on requests for consent
§ 26:131 Other uses of information
§ 26:132 Withdrawal of consent
§ 26:133 Notice
§ 26:134 Collection of employee personal information
§ 26:135 Limitations on use of information
§ 26:136 Use of personal information without consent

§ 26:137 Limitations on disclosure of personal information
§ 26:138 Disclosure of personal information without consent
§ 26:139 Disclosure of employee personal information
§ 26:140 Transfer of personal information in the sale of an organization or its business assets
§ 26:141 Disclosure for research or statistical purposes
§ 26:142 Disclosure for archival or historical purposes
§ 26:143 Access to personal information
§ 26:144 Right to request correction of personal information
§ 26:145 Circumstances in which request may be made
§ 26:146 Time for response
§ 26:147 Form of response
§ 26:148 Fees
§ 26:149 Accuracy of personal information
§ 26:150 Protection of personal information
§ 26:151 Retention and destruction of personal information
§ 26:152 The Commissioner—General powers
§ 26:153 Powers of commissioner in conducting investigations, audits or inquiries
§ 26:154 Procedural requirements at hearings
§ 26:155 Testimonial limitations
§ 26:156 Immunity for libel or slander actions
§ 26:157 Restrictions on disclosure of information by commissioner and staff
§ 26:158 Immunity for commissioner and staff
§ 26:159 Delegation by commissioner
§ 26:160 Annual report of commissioner
§ 26:161 Reviews and complaints
§ 26:162 Timing of review
§ 26:163 Burden of proof
§ 26:164 Commissioner's orders
§ 26:165 Duty to comply with orders
§ 26:166 Protection
§ 26:167 Non-retaliation
§ 26:168 Offences and penalties
§ 26:169 Damages for breach of Act
§ 26:170 Power to make regulations

PART V. LATIN AMERICA

CHAPTER 27. ARGENTINA

§ 27:1 Personal Data Protection Act—Purpose and scope of regulation
§ 27:2 —Data files and lawfulness

§ 27:3 —Quality of the data
§ 27:4 —Consent
§ 27:5 —Information
§ 27:6 —Sensitive data
§ 27:7 —Health-related data
§ 27:8 —Data security
§ 27:9 —Confidentiality duty
§ 27:10 —Communication of data
§ 27:11 —International transfer
§ 27:12 —Right to information
§ 27:13 —Right of access
§ 27:14 —Information contents
§ 27:15 —Correction, updating and suppression rights
§ 27:16 —Exceptions
§ 27:17 —Legislative committees
§ 27:18 —Objection to personal assessments
§ 27:19 —Registers of data files
§ 27:20 —Public data banks, files or registers
§ 27:21 —Special cases
§ 27:22 —Private data files, registers, databases or databanks
§ 27:23 —Provision of computerized services involving personal data
§ 27:24 —Credit information services
§ 27:25 —Data files, registers or banks with advertising purposes
§ 27:26 —Data files, registers, databases or databanks relating to opinion polls
§ 27:27 —Controlling agency
§ 27:28 —Codes of conduct
§ 27:29 —Administrative sanctions
§ 27:30 —Criminal acts
§ 27:31 —Action for protection of personal data—Legal basis for complaint
§ 27:32 — —Persons entitled to bring action
§ 27:33 — —Parties against whom action may be brought
§ 27:34 — —Procedures
§ 27:35 — —Requirements of complaint
§ 27:36 — —Submission of data
§ 27:37 — —Confidentiality of information

CHAPTER 28. COLOMBIA

§ 28:1 Overview

I. STATUTORY REQUIREMENTS

§ 28:2 Key definitions

§ 28:3 Key principles
§ 28:4 Purpose
§ 28:5 Scope of application/Territorial application
§ 28:6 Special categories of data—processing of sensitive data
§ 28:7 —Rights of children and adolescents
§ 28:8 Rights of the data subjects
§ 28:9 Authorization of the data subject
§ 28:10 Cases when authorization is not necessary
§ 28:11 Supply of the information
§ 28:12 Duty to inform the data subject
§ 28:13 Persons to whom the information may be supplied
§ 28:14 Consultations
§ 28:15 Complaints
§ 28:16 Admissibility Requisite
§ 28:17 Duties of Data Controllers
§ 28:18 Duties of Data Processors
§ 28:19 Data Protection Authority
§ 28:20 Functions
§ 28:21 Process
§ 28:22 Sanctions
§ 28:23 Criteria to adjust the sanctions
§ 28:24 Registration requirements
§ 28:25 Prohibition on cross-border data transfer
§ 28:26 Binding Corporate Rules

II. REGULATIONS

§ 28:27 Purpose of the regulations
§ 28:28 Exemption for data processing in the personal or household realm
§ 28:29 Key definitions
§ 28:30 Authorization and the collection of personal data
§ 28:31 Sensitive data
§ 28:32 Method to obtain the authorization
§ 28:33 Proof of authorization
§ 28:34 Revoking the authorization and/or removal of the data
§ 28:35 Data collected prior to the date on which this decree is issued
§ 28:36 Time limits to personal data processing
§ 28:37 Special requirements for the processing of personal data of children and adolescents.
§ 28:38 Information processing policies
§ 28:39 Privacy notice

§ 28:40 Minimum content of the privacy notice
§ 28:41 Duty to prove the availability of the privacy notice and the information processing policies
§ 28:42 Methods to disclose the privacy notice and the information processing policies
§ 28:43 Procedures for the proper processing of personal data
§ 28:44 Safety measures
§ 28:45 Standing to exercise the rights of the data subject
§ 28:46 The right of access
§ 28:47 The right to update, rectify and remove
§ 28:48 Means to exercise the rights
§ 28:49 International transfers and transmissions of personal data
§ 28:50 Personal data transmission agreement
§ 28:51 Establishing compliance
§ 28:52 Term and repeals

CHAPTER 29. COSTA RICA

I. STATUTE

§ 29:1 Objective and purpose
§ 29:2 Scope of application
§ 29:3 Definitions
§ 29:4 Self determination in information
§ 29:5 Principle of informed consent—Obligation to inform
§ 29:6 —Granting consent
§ 29:7 Principle of quality of the information
§ 29:8 Current character
§ 29:9 Truthfulness/accuracy
§ 29:10 Exactness
§ 29:11 Suitability for the purpose
§ 29:12 Rights of the person
§ 29:13 Access to information
§ 29:14 The right of rectification
§ 29:15 Exceptions to the self-determination and information of the citizen
§ 29:16 Special data categories—Sensitive data
§ 29:17 —Restricted access personal data
§ 29:18 —Unrestricted access personal data
§ 29:19 —Data concerning credit behavior
§ 29:20 Data security
§ 29:21 Confidentiality duty
§ 29:22 Action protocols
§ 29:23 Effective guarantees

§ 29:24 Transfer of personal data—General rule
§ 29:25 Agency for the Protection of the Data of the Inhabitants
§ 29:26 Functions
§ 29:27 Complaint
§ 29:28 Processing of complaints
§ 29:29 Effects of the resolution in favor of the complainant
§ 29:30 Sanctioning procedure
§ 29:31 Sanctions

II. REGULATIONS

§ 29:32 Purpose of regulations
§ 29:33 Key definitions
§ 29:34 Scope of application
§ 29:35 Requirements regarding consent
§ 29:36 Formalities of consent
§ 29:37 Revocation of consent
§ 29:38 Processing of revocation
§ 29:39 Deadline for confirming revocation of consent
§ 29:40 Refusal to revoke
§ 29:41 Right to be forgotten
§ 29:42 The rights of data owners—Informational self-determination
§ 29:43 Exercise of rights
§ 29:44 Restrictions on the exercise of rights
§ 29:45 Persons authorized to exercise the rights
§ 29:46 Ways and means of exercising rights
§ 29:47 Method of receiving notice from the owner
§ 29:48 Applications of the owner to the responsible party
§ 29:49 Requests for additional information
§ 29:50 Response by the responsible party
§ 29:51 Right of access to information
§ 29:52 Refusal by the responsible party
§ 29:53 Right of rectification
§ 29:54 Right of deletion or removal
§ 29:55 Exercise of the right of deletion or removal
§ 29:56 Security—procedures for the treatment of personal data
§ 29:57 Conditions of the treatment
§ 29:58 Outsourcing
§ 29:59 Processing of data by the responsible party
§ 29:60 Obligations of the responsible party
§ 29:61 Minimum protocols of action
§ 29:62 Method of verification

§ 29:63 Security measures in the treatment of personal data
§ 29:64 Factors to determine safety measures
§ 29:65 Actions for the safety of personal data
§ 29:66 Updates to security measures
§ 29:67 Security vulnerabilities
§ 29:68 Minimum Information
§ 29:69 The transfer of personal data—conditions of transfer
§ 29:70 —compliance with the minimum standards
§ 29:71 —Burden of proof
§ 29:72 —Contracts for the transfer of personal data
§ 29:73 Registration of databases—FAQ
§ 29:74 Superuser
§ 29:75 Finding of possible infractions
§ 29:76 Manual databases
§ 29:77 Registration procedure
§ 29:78 Substantiation of defense and filing of the request
§ 29:79 Payment
§ 29:80 Resolution of the registration
§ 29:81 Content of the resolution of registration
§ 29:82 Resolution of inadmissibility
§ 29:83 Update and modification of the registration
§ 29:84 Cancellation of the registration
§ 29:85 Appeals
§ 29:86 Deadline for resolving
§ 29:87 Protection of rights before the agency—The beginning of the procedure of protection of rights
§ 29:88 —Requirements of the complaint
§ 29:89 —Accreditation documentation
§ 29:90 —Troubleshooting, admissibility, and files
§ 29:91 —Admissibility
§ 29:92 —Precautionary measures
§ 29:93 —Appeal of the decision
§ 29:94 —Budgets for precautionary measures
§ 29:95 —Transfer of charges
§ 29:96 —Final actions
§ 29:97 —Fixing of fines/sanctions
§ 29:98 —Appeals
§ 29:99 Collection procedure—Fines/Payment Arrangements/ Final act of the recovery procedure
§ 29:100 Annual Fee for the regulation and administration of databases
§ 29:101 Deadline for payment
§ 29:102 Proportional Payment
§ 29:103 Canon by sale of data from the file
§ 29:104 Global contracts

§ 29:105 Canon and penalty interest
§ 29:106 Failure to pay
§ 29:107 The Agency-Employment regime/status
§ 29:108 Types of competition
§ 29:109 Manual of jobs and responsibilities
§ 29:110 Recruitment and selection

CHAPTER 30. MEXICO

I. FEDERAL LAW ON PERSONAL DATA PROTECTION OF PRIVATE OWNERSHIP

§ 30:1 General provisions
§ 30:2 Principles for the protection of personal data
§ 30:3 Processing with consent
§ 30:4 Consent not needed
§ 30:5 Databases
§ 30:6 Privacy notice
§ 30:7 Information security
§ 30:8 Notice of security breach
§ 30:9 Duty of confidentiality
§ 30:10 Rights of holders of personal data
§ 30:11 Rights of access, rectification, cancellation and opposition
§ 30:12 Data protection official
§ 30:13 Denial of access to information by the data protection official
§ 30:14 Data transfer
§ 30:15 Formation of the Institute
§ 30:16 Regulatory authorities
§ 30:17 Functions of the Ministry
§ 30:18 Self regulation
§ 30:19 Enforcement
§ 30:20 Other investigations
§ 30:21 Procedure for imposing sanctions
§ 30:22 Violations of the Act
§ 30:23 Criminal enforcement
§ 30:24 Transition provisions

II. REGULATIONS OF THE FEDERAL LAW ON THE PROTECTION OF PERSONAL DATA HELD BY PRIVATE PARTIES

§ 30:25 Purpose
§ 30:26 Scope of application

§ 30:27 Territorial application
§ 30:28 Information from individuals with business and data representation and contact
§ 30:29 Publicly available sources
§ 30:30 Groups without legal personality
§ 30:31 Data protection principles
§ 30:32 Principle of legality
§ 30:33 Principle of consent
§ 30:34 Features of consent
§ 30:35 Implied consent
§ 30:36 Application of implied consent
§ 30:37 Express consent
§ 30:38 Application for consent
§ 30:39 Exceptions to the principle of consent
§ 30:40 Verbal consent
§ 30:41 Written consent
§ 30:42 Test to show obtaining consent
§ 30:43 Withdrawal of consent
§ 30:44 Proceedings before the refusal to cease treatment
§ 30:45 Principle of information
§ 30:46 Features of the privacy notice
§ 30:47 Media
§ 30:48 Elements of the privacy notice
§ 30:49 Privacy notice for the direct taking of personal data
§ 30:50 Privacy notice for indirect collection of personal data
§ 30:51 Treatment for marketers, advertising or commercial research
§ 30:52 Countervailing measures
§ 30:53 Request for approval of compensation measures
§ 30:54 Procedure for authorizing countervailing
§ 30:55 Quality principle
§ 30:56 Limits for the storage of personal data
§ 30:57 Procedures for conservation, blocking and deletion of personal data
§ 30:58 Proof of compliance with the storage times
§ 30:59 Principle of finality
§ 30:60 Opposition treatment for different purposes
§ 30:61 Treatment for different purposes
§ 30:62 Principle of loyalty
§ 30:63 Principle of proportionality
§ 30:64 Minimization criterion
§ 30:65 Principle of responsibility
§ 30:66 Measures for the principle of accountability
§ 30:67 Manager

§ 30:68 Relationship between the controller and the processor
§ 30:69 Processing of personal data in cloud computing
§ 30:70 Remissions policy
§ 30:71 Outsourcing of services
§ 30:72 Authorization of outsourcing
§ 30:73 Assumptions for the creation of databases of sensitive personal data
§ 30:74 Scope
§ 30:75 Attenuation of sanctions
§ 30:76 Security features
§ 30:77 Factors to determine the security measures
§ 30:78 Actions for personal data security
§ 30:79 Updating security measures
§ 30:80 Security breaches
§ 30:81 Notification of security breaches
§ 30:82 Corrective measures in case of security breaches
§ 30:83 Conditions for transfer
§ 30:84 Receiver of personal data
§ 30:85 Specific conditions for international transfers
§ 30:86 Coordination mechanisms
§ 30:87 Object of autoregulation
§ 30:88 Specific objectives of self-regulation
§ 30:89 Incentives for self-regulation
§ 30:90 Minimum content of the self-regulatory schemes
§ 30:91 Certification data protection
§ 30:92 Individuals or corporations accredited
§ 30:93 Parameters autoregulation
§ 30:94 Self-regulatory schemes registry
§ 30:95 Exercise of rights
§ 30:96 Restrictions on the exercise of rights
§ 30:97 Persons entitled to exercise rights
§ 30:98 Means for the exercise of rights
§ 30:99 Services to the public
§ 30:100 Specific procedures for the exercise of ARCO
§ 30:101 Costs
§ 30:102 Domicile
§ 30:103 Registration requests
§ 30:104 Request for additional information
§ 30:105 Extension of deadlines
§ 30:106 Response from the responsible party
§ 30:107 Access to personal data on site
§ 30:108 Refusal by the responsible party
§ 30:109 Access rights
§ 30:110 Means to fulfill the right of access

§ 30:111 Right of rectification
§ 30:112 Requirements for exercising the right of reply
§ 30:113 Right to cancel
§ 30:114 Exercise of the right of cancellation
§ 30:115 Blocking
§ 30:116 Purposes of blocking
§ 30:117 Right to object
§ 30:118 Exclusion listings
§ 30:119 Public register of consumers and users public registry
§ 30:120 Processing of personal data without human intervention in making evaluation
§ 30:121 Initiation
§ 30:122 Methods of protecting rights
§ 30:123 Events of origin
§ 30:124 Application requirements rights protection
§ 30:125 Agreement admission
§ 30:126 Offer of proof
§ 30:127 Reconciliation
§ 30:128 Audience
§ 30:129 Presentation of allegations
§ 30:130 Third party
§ 30:131 Lack of response
§ 30:132 Resolutions
§ 30:133 Renewal of procedure
§ 30:134 Initiation
§ 30:135 Events of origin
§ 30:136 Public faith
§ 30:137 Requirements complaint
§ 30:138 Verification development
§ 30:139 Verification visits
§ 30:140 Staff ID verifier
§ 30:141 Acta verification
§ 30:142 Content of records check
§ 30:143 Resolution
§ 30:144 Renewal of procedure
§ 30:145 Initiation
§ 30:146 Offer and presentation of evidence

PART VI. AFRICA AND THE MIDDLE EAST

CHAPTER 31. ISRAEL

§ 31:1 Israel

§ 31:2 Restrictions on "infringement" of privacy
§ 31:3 Registration and use of a data base
§ 31:4 Applications for registration
§ 31:5 Powers of registrar
§ 31:6 Privacy protection report
§ 31:7 Notices with requests for information
§ 31:8 Register of data bases
§ 31:9 Inspection rights
§ 31:10 Amendment of information
§ 31:11 Appeal to courts
§ 31:12 Secrecy of information
§ 31:13 Duty to protect information
§ 31:14 Security officer
§ 31:15 Direct mail
§ 31:16 Application of Article II
§ 31:17 Delivery of information by public bodies
§ 31:18 Surplus information
§ 31:19 Permitted disclosures
§ 31:20 Regulations
§ 31:21 Application of other laws
§ 31:22 Enforcement
§ 31:23 Defenses
§ 31:24 Vicarious liability for newspaper publication
§ 31:25 Other vicarious liability
§ 31:26 Additional criminal penalties
§ 31:27 Inadmissibility of evidence
§ 31:28 Burden of proof
§ 31:29 Regulations
§ 31:30 Fees
§ 31:31 Basic Law: Human Dignity and Liberty

CHAPTER 32. QATAR

I. DATA PROTECTION REGULATIONS 2005

§ 32:1 Key definitions
§ 32:2 General requirements
§ 32:3 Requirements for legitimate processing
§ 32:4 Processing of sensitive personal data
§ 32:5 Transfers to jurisdictions with adequate levels of protection
§ 32:6 Transfers to jurisdictions without adequate level of protection
§ 32:7 Providing information where data obtained from the data subject

§ 32:8 Providing information where data not obtained from the data subject
§ 32:9 Confidentiality
§ 32:10 Security of processing

II. PART 3: RIGHTS OF DATA SUBJECTS

§ 32:11 Right to access, rectification, erasure and blocking of personal data
§ 32:12 Right to object to processing
§ 32:13 Requirement to record operations and notify the QFC Authority
§ 32:14 Register of notifications
§ 32:15 General powers of the QFC Authority
§ 32:16 Production of information
§ 32:17 Power to make rules
§ 32:18 General exemptions
§ 32:19 Enforcement—Directions
§ 32:20 —Claims

CHAPTER 33. REPUBLIC OF SOUTH AFRICA

§ 33:1 Introduction
§ 33:2 Purpose
§ 33:3 Application provisions—Application and interpretation
§ 33:4 Lawful processing of personal information
§ 33:5 Rights of data subjects
§ 33:6 General exclusions
§ 33:7 Exclusions for journalistic, literary, or artistic purposes
§ 33:8 Conditions for lawful processing of personal information—Accountability
§ 33:9 —Processing limitation
§ 33:10 —Purpose specification
§ 33:11 —Further processing limitations
§ 33:12 —Quality of information
§ 33:13 —Documentation
§ 33:14 —Notification
§ 33:15 —Security safeguards
§ 33:16 —Information processed by operators or authorized persons
§ 33:17 —Security measures for information processed by the operator
§ 33:18 —Notification of security compromises

§ 33:19 Data subject participation—Access to personal information
§ 33:20 —Correction of personal information
§ 33:21 Manner of access
§ 33:22 Processing of special personal information—Prohibition
§ 33:23 Authorization: Data subject's religious or philosophical beliefs
§ 33:24 Authorization: Data subject's race or ethnic origin
§ 33:25 Authorization: Data subject's trade union membership
§ 33:26 Authorization: Data subject's political persuasion
§ 33:27 Authorization: Data subject's health or sex life
§ 33:28 Authorization: Data subject's criminal behavior or biometric information
§ 33:29 Processing children's personal information—Prohibition and general authorization
§ 33:30 Exemption from conditions for processing personal information
§ 33:31 Exemption for certain functions
§ 33:32 Information regulator—Establishment and powers, duties and functions
§ 33:33 Appointment, term of office, and removal
§ 33:34 Vacancies
§ 33:35 Powers, duties, and functions of chairpersons and other members
§ 33:36 Regards to certain matters
§ 33:37 Conflict of interest
§ 33:38 Remuneration, allowances, benefits and privileges
§ 33:39 Staff
§ 33:40 Power, duties, and functions of the chief executive officer
§ 33:41 Committees of regulator
§ 33:42 Establishment of enforcement committee
§ 33:43 Meetings of the regulator
§ 33:44 Funds
§ 33:45 Protection of regulator
§ 33:46 Duty of confidentiality
§ 33:47 Information officer—Duties and responsibilities
§ 33:48 Designation and delegation of deputy information officers
§ 33:49 Prior authorization—Processing subject to prior authorization
§ 33:50 Responsible party must notify regulator if processing is subject to prior authorization

§ 33:51 Failure to notify processing subject to prior authorization
§ 33:52 Codes of conduct—Issuing codes of conduct
§ 33:53 Process for issuing codes of conduct
§ 33:54 Notification, availability, and commencement of code of conduct
§ 33:55 Dealing with complaints
§ 33:56 Amendment and revocation of codes of conduct
§ 33:57 Guidelines about codes of conduct
§ 33:58 Register of approved codes of conduct
§ 33:59 Review of operation of approved code of conduct
§ 33:60 Effect of failure to comply with code of conduct
§ 33:61 Data subjects' rights regarding direct marketing by unsolicited electronic communication
§ 33:62 Data subjects' rights regarding directories
§ 33:63 Data subjects' rights regarding automated decision making
§ 33:64 Transborder information flows—Transferring personal information outside the Republic of South Africa
§ 33:65 Enforcement—Interference with protection of a data subject's personal information
§ 33:66 Complaints
§ 33:67 Action on receipt of complaint
§ 33:68 Regulator can decide to take no action on complaints
§ 33:69 Pre-investigation proceedings
§ 33:70 Investigations proceedings
§ 33:71 Issuing of warrants
§ 33:72 Requirements for issuing a warrant
§ 33:73 Warrant execution
§ 33:74 Communication between legal adviser and client exemption
§ 33:75 Objections to search and seizure
§ 33:76 Assessment
§ 33:77 Information notice
§ 33:78 Parties to be informed of result of assessment
§ 33:79 Matters referred to enforcement committee
§ 33:80 Functions of the enforcement committee
§ 33:81 Parties to be informed of developments during and result of investigation
§ 33:82 Enforcement notice
§ 33:83 Cancellation of enforcement notice
§ 33:84 Right of appeal
§ 33:85 Consideration of appeal
§ 33:86 Civil remedies
§ 33:87 Offenses, penalties, and administrative fines

§ 33:88 Witnesses
§ 33:89 Parties in connection with account numbers
§ 33:90 Penalties
§ 33:91 Administrative fines
§ 33:92 General provisions—Amendment
§ 33:93 Regulations
§ 33:94 Procedures for making regulations
§ 33:95 Transitional arrangements

CHAPTER 34. UAE/DUBAI

§ 34:1 Data Protection Law 2007
§ 34:2 Key definitions
§ 34:3 General requirements
§ 34:4 Requirements for legitimate processing
§ 34:5 Processing of sensitive personal data
§ 34:6 Transfers out of the DIFC—Adequate level of protection
§ 34:7 Transfers out of the DIFC in the absence of an adequate level of protection
§ 34:8 Providing information where personal data has been obtained from the data subject
§ 34:9 Providing information where personal data has not been obtained from the data subject
§ 34:10 Confidentiality
§ 34:11 Security of processing
§ 34:12 Notice of security breach
§ 34:13 Right to access to and rectification, rrasure or blocking of personal data
§ 34:14 Right to object to processing
§ 34:15 Requirement to notify the commissioner of data protection
§ 34:16 Register of notifications
§ 34:17 Duty to notify of changes
§ 34:18 Appointment and powers of the Commissioner of Data Protection
§ 34:19 Production of information
§ 34:20 Directions
§ 34:21 UAE rules
§ 34:22 References to writings
§ 34:23 Applications for permits—Sensitive data
§ 34:24 Permits for processing sensitive data
§ 34:25 Permits for transfer out of the DIFC
§ 34:26 Records and notification
§ 34:27 Notices
§ 34:28 Time for filing notices

§ 34:29 Fines and mediation

PART VII. OTHER

CHAPTER 35. BERMUDA

I. PERSONAL INFORMATION PROTECTION ACT 2016—INTERPRETATION AND SCOPE

§ 35:1 Interpretation
§ 35:2 Application
§ 35:3 Exclusions

II. PERSONAL INFORMATION PROTECTION ACT 2016—GENERAL PRINCIPLES AND RULES

§ 35:4 Responsibility and compliance
§ 35:5 Conditions for using personal information
§ 35:6 Sensitive personal information
§ 35:7 Fairness
§ 35:8 Privacy notices
§ 35:9 Purpose limitation
§ 35:10 Proportionality
§ 35:11 Integrity of personal information
§ 35:12 Security safeguards
§ 35:13 Notice of breach of security
§ 35:14 Transfer of personal information to an overseas third party
§ 35:15 Personal information about children in the information society

III. PERSONAL INFORMATION PROTECTION ACT 2016—RIGHTS OF INDIVIDUALS

§ 35:16 Access to personal information
§ 35:17 Access to medical records
§ 35:18 Rectification, blocking, erasure and destruction
§ 35:19 Procedure for making a request under section 17, 18 or 19
§ 35:20 Compensation for financial loss or distress

IV. PERSONAL INFORMATION PROTECTION ACT 2016—EXEMPTIONS

§ 35:21 National security exemption

§ 35:22 Communication provider exemption
§ 35:23 Regulatory activity and honours exemption
§ 35:24 General exemption

V. PERSONAL INFORMATION PROTECTION ACT 2016—GENERAL PROVISIONS

§ 35:25 Disclosure for purposes of business transaction
§ 35:26 Offences and penalties
§ 35:27 Power to make regulations
§ 35:28 Review of the Act
§ 35:29 Crown application
§ 35:30 Power to make consequential amendments
§ 35:31 Privacy Commissioner

CHAPTER 36. U.S. STATE GENERAL PRIVACY LAWS

I. CALIFORNIA CONSUMER PRIVACY ACT OF 2018 (THE "CCPA")

§ 36:1 General rights
§ 36:2 Consumer rights
§ 36:3 Employee Exemption
§ 36:4 Response to consumer request
§ 36:5 Business disclosure to service provider exemption
§ 36:6 Collection or retention of personal information not otherwise collected or retained in ordinary course of business
§ 36:7 Rights and freedoms of other consumers
§ 36:8 B-to-B exemption
§ 36:9 Civil Action—Remedies
§ 36:10 —Requirements to bring action
§ 36:11 Attorney General guidance; civil action brought by Attorney General; amount and allocation of penalties
§ 36:12 Adoption of regulations; public participation; subject matter; enforcement actions
§ 36:13 Void and unenforceable provisions of contract or agreement
§ 36:14 Liberal construction of title
§ 36:15 Construction with federal law, United States Constitution, and California Constitution
§ 36:16 Operative date
§ 36:17 Severability

§ 36:18 CCPA regulations—Title and scope
§ 36:19 —Overview of required notices
§ 36:20 —Notice at collection of personal information
§ 36:21 —Notice of right to opt-out of sale of personal information
§ 36:22 —Notice of financial incentive
§ 36:23 —Privacy policy
§ 36:24 —Methods for submitting requests to know and requests to delete
§ 36:25 —Responding to requests to know and requests to delete
§ 36:26 —Responding to requests to know
§ 36:27 —Responding to requests to delete
§ 36:28 —Service providers
§ 36:29 —Requests to opt-out
§ 36:30 —Requests to opt-in after opting out of the sale of personal information
§ 36:31 —Training; record-keeping
§ 36:32 —Requests to access or delete household information
§ 36:33 —General rules regarding verification
§ 36:34 —Verification for password-protected accounts
§ 36:35 —Verification for non-accountholders
§ 36:36 —Authorized agent
§ 36:37 —Minors under 13 years of age—process for opting-in to sale of personal information
§ 36:38 —Minors 13 to 16 years of age
§ 36:39 —Notices to minors under 16 years of age
§ 36:40 —Discriminatory practices
§ 36:41 —Calculating the value of consumer data
§ 36:42 —Severability

II. CALIFORNIA PRIVACY RIGHTS AND ENFORCEMENT ACT OF 2020 (THE "CPRA")

§ 36:43 Overview

III. COLORADO CONSUMER PROTECTION ACT

§ 36:44 Applicability
§ 36:45 Obligations
§ 36:46 Consumer personal data rights
§ 36:47 —The right to opt out
§ 36:48 —Right of access
§ 36:49 —Right to correction
§ 36:50 —Right to deletion
§ 36:51 —Right to data portability

§ 36:52 —Responding to consumer requests
§ 36:53 Processing de-identified data
§ 36:54 Duties of controllers—Duty of transparency
§ 36:55 —Duty of purpose specification
§ 36:56 —Duty of data minimization
§ 36:57 —Duty to avoid secondary use
§ 36:58 —Duty of care
§ 36:59 —Duty to avoid unlawful discrimination
§ 36:60 —Duty regarding sensitive data
§ 36:61 Data protection assessments—Attorney general access and evaluation—Definition
§ 36:62 Liability
§ 36:63 Enforcement—Penalties
§ 36:64 Rules
§ 36:65 Effective date

IV. VIRGINIA CONSUMER DATA PROTECTION ACT

§ 36:66 Scope
§ 36:67 Personal data rights; consumers
§ 36:68 Data controller responsibilities; transparency
§ 36:69 Responsibility according to role; controller and processor
§ 36:70 Data protection assessments
§ 36:71 Processing de-identified data; exemptions
§ 36:72 Limitations
§ 36:73 Violations of chapter; civil penalties
§ 36:74 Enforcement; civil penalty
§ 36:75 Consumer Privacy Fund
§ 36:76 Effective date

CHAPTER 37. APPLICATION OF NON-PRIVACY AND SECURITY-BASED LAWS TO CYBERSECURITY, PRIVACY, AND OTHER DATA ISSUES: SEC AND DELAWARE OBLIGATIONS

I. OVERVIEW

§ 37:1 Introduction
§ 37:2 An overview

II. UNDERSTANDING SEC AND DELAWARE OBLIGATIONS

§ 37:3 Why do for-profit companies exist?

§ 37:4 SEC obligations summarized
§ 37:5 Delaware law summarized—Why does Delaware law matter?
§ 37:6 —The internal affairs doctrine
§ 37:7 —Operations versus oversight
§ 37:8 —The duty of care and the duty of loyalty
§ 37:9 Key take-aways regarding SEC and Delaware law

III. GOVERNANCE

§ 37:10 Overview
§ 37:11 Differing governance obligations
§ 37:12 Corporate governance
§ 37:13 Nested governance
§ 37:14 The materiality fallacy—An over-emphasis on legal risk
§ 37:15 Putting technology, data, and AI risk in context
§ 37:16 Combining Delaware corporate principles and technology, data, and AI risk
§ 37:17 Examples of resiliency and legal compliance impacts
§ 37:18 Creating Technology, Data, and AI Risk Governance
§ 37:19 Redefining requests
§ 37:20 Conclusions and take-aways

CHAPTER 38. EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT

§ 38:1 Introduction
§ 38:2 Subject matter
§ 38:3 Scope
§ 38:4 Amendments to Annex I
§ 38:5 Prohibited AI practices
§ 38:6 High-risk AI practices—Classification of AI systesm as high-risk—Classification rules for high-risk AI systems
§ 38:7 — —Amendments to Annex III
§ 38:8 —Requirements for high-risk AI systems—Compliance with the requirements
§ 38:9 — —Risk management system
§ 38:10 — —Data and data governance
§ 38:11 — —Technical documentation
§ 38:12 — —Record-keeping
§ 38:13 — —Transparency and provision of information to users
§ 38:14 — —Human oversight
§ 38:15 — —Accuracy, robustness and cybersecurity

§ 38:16 —Obligations of providers and users of high-risk AI systems and other parties—Obligations of providers
§ 38:17 — —Quality management system
§ 38:18 — —Obligation to draw up technical documentation
§ 38:19 — —Conformity assessment
§ 38:20 — —Automatically generated logs
§ 38:21 — —Corrective actions
§ 38:22 — —Duty of information
§ 38:23 — —Cooperation with competent authorities
§ 38:24 —Obligations of providers and users of high-risk AI systems and other parties—Obligations of product manufacturers
§ 38:25 —Obligations of providers and users of high-risk AI systems and other parties—Authorised representatives
§ 38:26 — —Obligations of importers
§ 38:27 — —Obligations of distributors
§ 38:28 — —Obligations of distributors, importers, users or any other third-party
§ 38:29 — —Obligations of users of high-risk AI systems
§ 38:30 —Notifiying authorities and notified bodies—Notifying authorities
§ 38:31 — —Application of a conformity assessment body for notification
§ 38:32 — —Notification procedure
§ 38:33 Requirements for high-risk AI systems—Notifiying authorities and notified bodies—Notified bodies
§ 38:34 High-risk AI practices—Notifiying authorities and notified bodies—Subsidiaries of and subcontracting by notified bodies
§ 38:35 — —Identification numbers and lists of notified bodies designated under this regulation
§ 38:36 — —Changes to notifications
§ 38:37 — —Challenge to the competence of notified bodies
§ 38:38 — —Coordination of notified bodies
§ 38:39 — —Conformity assessment bodies of third countries
§ 38:40 —Standards, conformity assessment, certificates, registration—Harmonised standards
§ 38:41 — —Common specifications
§ 38:42 — —Presumption of conformity with certain requirements
§ 38:43 — —Conformity assessment
§ 38:44 — —Certificates
§ 38:45 — —Appeal against decisions of notified bodies
§ 38:46 — —Information obligations of notified bodies

§ 38:47 — —Derogation from conformity assessment procedure
§ 38:48 — —EU declaration of conformity
§ 38:49 — —CE marking of conformity
§ 38:50 — —Document retention
§ 38:51 — —Registration
§ 38:52 Transparency obligations for certain AI systems
§ 38:53 Measures in favor of innovation—AI regulatory sandboxes
§ 38:54 —Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox
§ 38:55 —Measures for small-scale providers and users
§ 38:56 Governence—European Artificial Intelligence Board—Establishment of the European Artificial Intelligence Board
§ 38:57 — —Structure of the Board
§ 38:58 — —Tasks of the Board
§ 38:59 —National competent authorities—Designation of national competent authorities
§ 38:60 EU database for stand-alone high-risk AI systems
§ 38:61 Post-market monitoring, information sharing, market surveillence—Post-market monitoring—Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems
§ 38:62 — —Sharing of information on incidents and malfunctioning—Reporting of serious incidents and of malfunctioning
§ 38:63 —Enforcement—Market surveillance and control of AI systems in the Union market
§ 38:64 — —Access to data and documentation
§ 38:65 — —Procedure for dealing with AI systems presenting a risk at national level
§ 38:66 — —Union safeguard procedure
§ 38:67 — —Compliant AI systems which present a risk
§ 38:68 — —Formal non-compliance
§ 38:69 Codes of conduct
§ 38:70 Confidentiality and penalties—Confidentiality
§ 38:71 —Penalties
§ 38:72 —Administrative fines on Union institutions, agencies and bodies
§ 38:73 Delegation of power and committee procedure—Exercise of the delegation
§ 38:74 —Committee procedure
§ 38:75 Amendments
§ 38:76 Evaluation and review

§ 38:77 Entry into force and application

CHAPTER 39. AGE-APPROPRIATE DESIGN CODE LAWS

I. AGE-APPROPRIATE DESIGN CODES

§ 39:1 Introduction

A. CALIFORNIA

1. California Age-Appropriate Design Code Act

§ 39:2 Law enjoined
§ 39:3 Legislative findings and declarations
§ 39:4 Business that provides an online service, product, or feature likely to be accessed by children; required actions; prohibited actions
§ 39:5 California Children's Data Protection Working Group
§ 39:6 Completion of Data Protection Impact Assessment; exception
§ 39:7 Violations and penalties; business in substantial compliance
§ 39:8 Application of title

B. MARYLAND

1. Maryland Age-Appropriate Design Code Act

§ 39:9 Effective date
§ 39:10 Application of subtitle
§ 39:11 Legislative intent
§ 39:12 Data protection impact assessments
§ 39:13 Duties of entities required to complete data protection impact assessments
§ 39:14 Processing data of children; profiling children; monitoring by parents or guardians
§ 39:15 Disclosure of data protection impact assessments to the Division
§ 39:16 Violations
§ 39:17 Notice of filing action; opportunities to cure violations
§ 39:18 Interpretation and construction of subtitle
§ 39:19 Confidentiality of data protection impact assessments
§ 39:20 Construction with other laws

C. NEBRASKA

1. The Age-Appropriate Online Design Code Act

§ 39:21 Generally

§ 39:22 Covered online service; provide safeguards for minors
§ 39:23 Covered online service; personal data; collection and use
§ 39:24 Covered online service; parental tools; notification of covered minor
§ 39:25 Covered online service; reporting mechanisms
§ 39:26 Covered online service; acts; prohibited
§ 39:27 Act, violation; deceptive trade practice; compliance officer; civil penalty

D. SOUTH CAROLINA

1. Age-Appropriate Code Design

§ 39:28 Effective date
§ 39:29 Requirements
§ 39:30 Enforcement
§ 39:31 Conflict

E. VERMONT

1. Age Appropriate Design Code Act

§ 39:32 Effective dates
§ 39:33 Exclusions
§ 39:34 Minimum duty of care
§ 39:35 Required default privacy settings and tools
§ 39:36 Transparency
§ 39:37 Prohibited data and design practices
§ 39:38 Privacy protections for age assurance data
§ 39:39 Enforcement
§ 39:40 Limitations
§ 39:41 Rights and freedoms of covered minors

II. GENERAL AGE VERIFICATION AND OTHER ONLINE PROTECTIONS

§ 39:42 Introduction

A. CALIFORNIA

1. Privacy Rights for California Minors in the Digital Age

§ 39:43 Introduction
§ 39:44 Restrictions on advertising
§ 39:45 Restrictions on use, disclosure, or compiling of information regarding minors

§ 39:46 No requirement to collect or retain information
§ 39:47 Advertising service compliance
§ 39:48 Exceptions
§ 39:49 Deletion of information by minors
§ 39:50 Deemed compliance
§ 39:51 No requirement to collect age information
§ 39:52 Effective date

2. Pupil Online Personal Information Protection Act

§ 39:53 Internet and student marketing law
§ 39:54 Exceptions

3. Privacy of pupil records

§ 39:55 Information obtained from social media

B. DELAWARE

1. Student Data Privacy Protection Act

§ 39:56 Operator duties
§ 39:57 Operator prohibited activities
§ 39:58 Exclusions
§ 39:59 Effective date
§ 39:60 Enforcement

C. DELAWARE

1. Online and Personal Privacy Protection Act

§ 39:61 Effective date
§ 39:62 Prohibitions on online marketing or advertising to a child
§ 39:63 Posting of privacy policy by operators of commercial online sites and services
§ 39:64 Enforcement

D. FLORIDA

1. Age Verification for Online Access to Materials Harmful to Minors

§ 39:65 Requirements
§ 39:66 Anonymous age verification

E. GEORGIA

1. Minors—Online Internet Safety

§ 39:67 Effective date

§ 39:68 Product or service to block specific websites to minors
§ 39:69 Liability of providers and interactive computer service
§ 39:70 Report of violations of child pornography laws; misdemeanor or misdemeanor of high and aggravated nature
§ 39:71 Public websites; definitions; age verification methods; liability
§ 39:72 Provider required to verify minor's age and obtain express consent of minor's parent or guardian
§ 39:73 Provider prohibitions
§ 39:74 Enforcement
§ 39:75 Application of chapter

2. Department of Education—Online Internet Safety

§ 39:76 Model programs

F. LOUISIANA

1. Secure Online Child Interaction and Age Limitation Act

§ 39:77 Law enjoined
§ 39:78 Age requirements for use of social media platform; parental consent
§ 39:79 Prohibition on data collection for certain accounts and advertising
§ 39:80 Parental access to social media account settings; parental supervision
§ 39:81 Investigative powers of the division
§ 39:82 Enforcement powers of the division
§ 39:83 Annual report
§ 39:84 Waiver prohibited

III. MINOR'S INFORMATION—REGULATION OF SOCIAL MEDIA PLATFORMS AND APP STORES

A. ARKANSAS

§ 39:85 Minor's information

1. Regulation of Social Media

§ 39:86 Social media platforms—Reasonable age verification methods—Parental consent required [Effective until April 21, 2026]

§ 39:87 — —Parental consent required [Effective April 21, 2026]
§ 39:88 Liability for social media companies
§ 39:89 Liability for commercial entity or third-party vendor
§ 39:90 Protection against circumvention

2. Arkansas Children and Teens' Online Privacy Protection Act

§ 39:91 Prohibited activity by social media platform
§ 39:92 Liability of social media platform

B. FLORIDA

1. Protection of children in online spaces

§ 39:93 Protection of children in online spaces; public records exemption
§ 39:94 Enforcement and implementation by the department
§ 39:95 Jurisdiction
§ 39:96 Public records exemption
§ 39:97 Social media use for minors

C. LOUISIANA

1. Online Protections for Minors

§ 39:98 Legislative findings
§ 39:99 Prohibitions; data collection; targeted advertising
§ 39:100 Enforcement

2. Protection of Children on Applications

§ 39:101 Application stores
§ 39:102 Developer requirements
§ 39:103 Protections
§ 39:104 Enforcement; penalties

D. NEBRASKA

1. Parental Rights in Social Media Act

§ 39:105 Effective date
§ 39:106 Social media company; social media platform; account holder; minors; restrictions; age verification; parental consent
§ 39:107 Civil action; damages

E. NEW YORK

1. Prohibition of Addictive Feeds

§ 39:108 Effective date

§ 39:109 Prohibition of addictive feeds
§ 39:110 Overnight notifications
§ 39:111 Parental control
§ 39:112 Nondiscrimination
§ 39:113 Rulemaking authority
§ 39:114 Language access
§ 39:115 Scope
§ 39:116 Remedies

F. TEXAS

1. App Store Accountability Act

§ 39:117 Effective date
§ 39:118 Duties of app stores—Duty to verify age of user; age categories
§ 39:119 —Parental consent required
§ 39:120 —Display of age rating for software application
§ 39:121 —Information for software application developers
§ 39:122 —Protection of personal data
§ 39:123 —Violation
§ 39:124 —Construction of subchapter
§ 39:125 Duties of software developers—Applicability of subchapter
§ 39:126 —Designation of age rating
§ 39:127 —Changes to software applications
§ 39:128 —Age verification
§ 39:129 —Use of personal data
§ 39:130 —Violation
§ 39:131 Enforcement—Deceptive trade practices
§ 39:132 —Cumulative remedies

G. UTAH

1. Minor Protection in Social Media Act

§ 39:133 Law enjoined
§ 39:134 Legislative findings
§ 39:135 Age assurance required
§ 39:136 Requirements for Utah minor account holders
§ 39:137 Supervisory tools
§ 39:138 Parental consent—Data privacy for Utah minor accounts
§ 39:139 Enforcement powers
§ 39:140 Age Assurance and verifiable parental consent safe harbor
§ 39:141 Severability

2. Harm to Minors by Algorithmically Curated Social Media Service

§ 39:142 Legislative findings
§ 39:143 Private right of action
§ 39:144 Affirmative defense
§ 39:145 Waiver prohibited
§ 39:146 Severability

H. VIRGINIA

1. Social Media Platforms; Responsibilities and Prohibitions Related to Minors

§ 39:147 Effective date
§ 39:148 Responsibilities and prohibitions related to minors

IV. STUDENT DATA

A. ARIZONA

1. Student Accountability Information System

§ 39:149 Establishment
§ 39:150 Data submission requirements
§ 39:151 Confidentiality
§ 39:152 Allowable disclosure
§ 39:153 Data security and privacy policies
§ 39:154 Exclusions

B. DELAWARE

1. Student Data Privacy Protection Act

§ 39:155 Effective date
§ 39:156 Enforcement
§ 39:157 Operator duties
§ 39:158 Operator prohibited activities
§ 39:159 Exclusions

C. GEORGIA

1. Student Data Privacy, Accessibility, and Transparency Act

§ 39:160 Short title
§ 39:161 Legislative findings and intent
§ 39:162 Findings
§ 39:163 Chief privacy officer

§ 39:164 State data system
§ 39:165 Student data not to be reported
§ 39:166 Prohibited activities
§ 39:167 Rights of parents and guardians
§ 39:168 Rules and regulations

D. NEW HAMPSHIRE

1. Student and Teacher Information Protection and Privacy Law

§ 39:169 Data inventory and policies publication
§ 39:170 Limits on disclosure of information
§ 39:171 Student privacy
§ 39:172 Student online personal information
§ 39:173 Severability

E. NORTH CAROLINA

1. Protective Provisions and Maintenance of Student Records

§ 39:174 School personnel to report child abuse
§ 39:175 School counseling inadmissible evidence
§ 39:176 Prohibition on the disclosure of information about students
§ 39:177 Student online privacy protection—Effective date
§ 39:178 —Prohibitions for operators
§ 39:179 —Requirements for operators
§ 39:180 —Permissible uses and disclosures
§ 39:181 —Enforcement
§ 39:182 Student records; maintenance; contents; confidentiality—Official student records
§ 39:183 —Expungement of suspension or expulsion records
§ 39:184 —Confidentiality and public records status
§ 39:185 Student data system security—Accessibility, transparency, and accountability
§ 39:186 —Restrictions on student data collection

F. VERMONT

1. Student Privacy Law

§ 39:187 Effective date
§ 39:188 Operator prohibitions
§ 39:189 Operator duties
§ 39:190 Permissive use or disclosure

§ 39:191 Operator actions that are not prohibited
§ 39:192 Applicability
§ 39:193 Enforcement

V. OTHER MINOR'S LAWS

A. ARKANSAS

1. Child Content Creation Protection Act

§ 39:194 Law enjoined
§ 39:195 Compensation for content creation featuring minor—Records—Trust account required—Right to civil action
§ 39:196 Privacy removal requests
§ 39:197 Intentional sexualization of a minor

B. ILLINOIS

1. Artificial Intelligence

§ 39:198 Use of artificial intelligence in elementary and secondary education

C. TENNESSEE

1. The Data Accessibility, Transparency and Accountability Act

§ 39:199 Student data; board duties
§ 39:200 Student records; review; copies; model student records policy
§ 39:201 Individual student data; collection
§ 39:202 Student biometric and other health and physical attribute data; collection
§ 39:203 New student data collection

Index