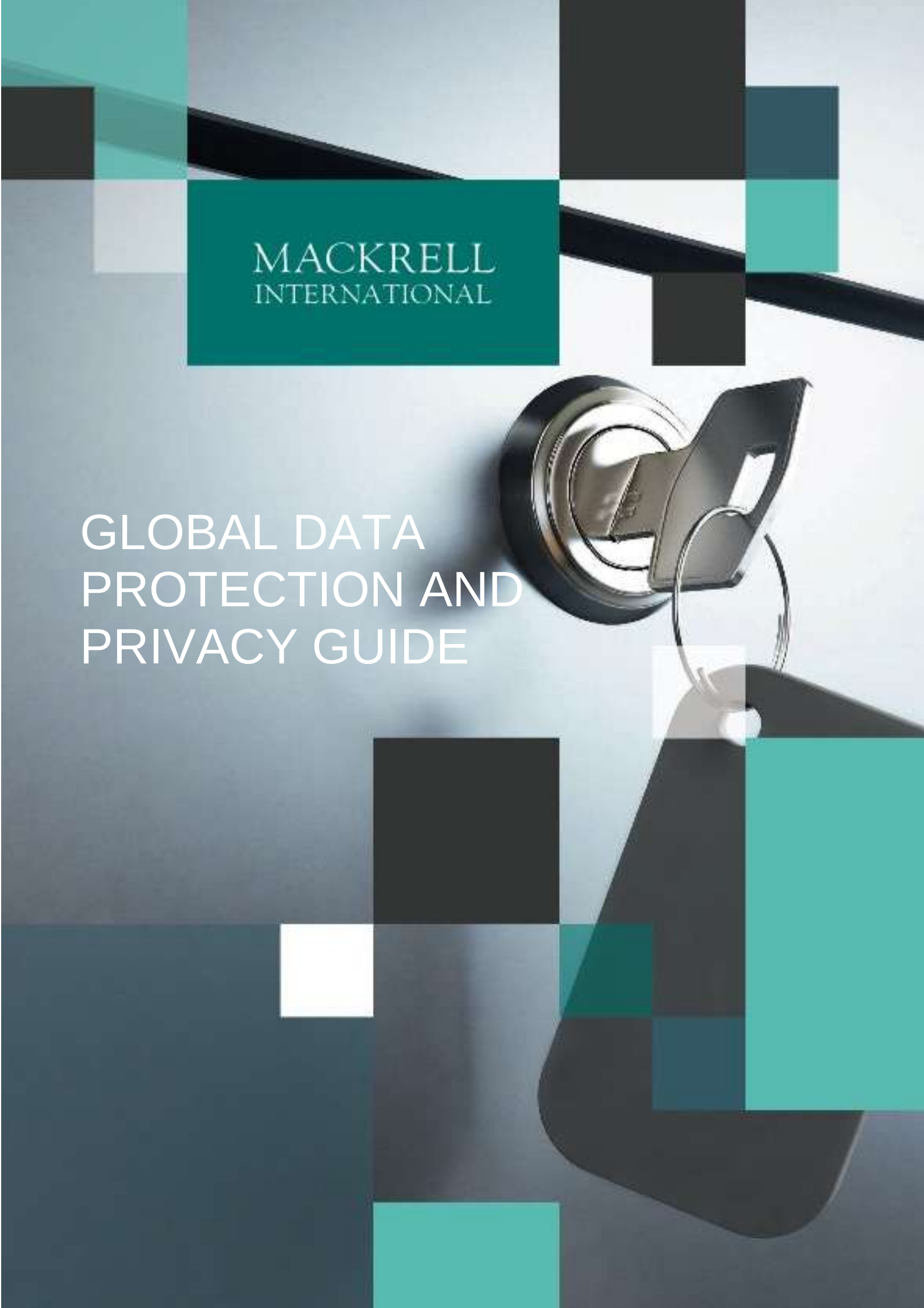
MACKRELL
INTERNATIONAL

GLOBAL DATA PROTECTION AND PRIVACY GUIDE



Mackrell International - Global Data Protection and Privacy Guide

Introduction

The collection, protection and use of personal information is now a heavily regulated area in many jurisdictions around the world.

Rapid advances in technology have fuelled the collection of vast quantities of sensitive personal information by making it possible and commercially viable to collect, share, mine, manage and use information about individuals. Commercial use of personal information is currently a multibillion-dollar industry.

Customer databases and other similar records collected by businesses usually contain personal information, giving rise to important legal issues including:

1. Has personally identifiable information been collected lawfully?
2. What are the permitted uses of the information?
3. Does data portability information be transferred or copied from one country to another?
4. Have measures been put in place to ensure the protection of personal data, such as health information and social security numbers?
5. What happens if there is unauthorized use or disclosure of sensitive personal information?

Compliance with data protection and data privacy laws is essential for modern businesses, both legally and to reputation – particularly in circumstances where a business is responding to a loss of data or security breach. The laws relating to data protection and privacy vary considerably from country to country. Having a clear and up-to-date understanding of the relevant laws and compliance requirements is essential – even more so when entities collect personal information from or about persons in several different countries, because different laws and requirements will apply depending on where individuals reside.

The Mackrell International network (www.mackrell.net) includes more than 4,500 legal professionals in over 90 countries. Data protection and privacy law experts in many of these countries have formed a specialist Practice Area Group and regularly communicate on current and emerging issues.

Several group initiatives, including webinars and presentations on multi-jurisdictional issues, such as cross-border transfers of personal data and the European General Data Protection Regulation (GDPR), have assisted organisations in the proper handling of domestic and international data protection and privacy issues. Mackrell members are experienced in co-ordinating responses to multi-jurisdictional privacy and data security breaches.

The Mackrell International Global Data Protection and Privacy Guide is designed to provide convenient references to the primary data protection laws applicable in multiple countries, and the contact details for highly skilled legal practitioners who can assist in each country. It also gives a snapshot of the breadth of expertise in this field offered by Mackrell International member law firms.

DISCLAIMER
This Guide by its nature cannot be comprehensive and cannot be relied on by any reader as legal advice. Please consult the professional staff of the Mackrell International member firms listed for advice specific to your situation. The content of this Guide is current as at the date of first publication, but may not include subsequent law changes.

This Guide was prepared by Mackrell International member firms in 2021

INDEX

Country	Main laws	Local Summary	Local Expert
EUROPEAN UNION REGULATIONS *(Updated Jun2021)*	EU General Data Protection Regulation	**EU General Data Protection Regulation Summary** The General Data Protection Regulation (**GDPR**) has applied across Europe since 25 May 2018 and brought considerable changes to data protection law. The previous data protection framework in Europe was based on the Data Protection Directive 95/46/EC, which was in place before online services and cloud technology were used and the GDPR updated and clarified the law to attempt to further protect personal data of individuals. The GDPR was introduced to strengthen the protection of personal data of individuals and sets out clear guidance on when personal data can and cannot be used. GDPR seeks to update data protection law in line with modern technology and strengthen the rights of individuals in respect of their consumer data. The GDPR also aims to introduce a harmonised data protection framework across all EU member states, in order for businesses to have a more consistent set of data protection compliance obligations across Europe. The framework is supported by extensive guidance from the European Data Protection Board. "Personal data" is defined under the GDPR as "any information relating to an individual, whether it relates to his or her private, professional or public life". Personal data can include names, contact details, IP addresses, medical information, bank details and social media accounts. The definition of personal data is extremely wide under the GDPR and all information about an individual will be protected so long as they can be identified in some way by it. Essentially, under GDPR more data is caught and the definitions are far broader than was the case under the previous regime. Many of the GDPR's core concepts are similar to the old data protection regime and sufficient compliance with the previous law put businesses in a good position to achieve compliance with GDPR, however the new law also brought some significant changes. The concept of "accountability" is at the heart of the GDPR, meaning organisations must be able to demonstrate that they have analysed the GDPR's requirements in relation to their processing of personal data and have implemented a system that allows them to achieve compliance with this. The GDPR requires businesses to implement "technical and organisational measures" to ensure that the requirements of the new law are met. This can be achieved by businesses taking data protection requirements into account from the inception of any new product or service which involves processing personal data. Key points to note in relation to GDPR compliance include: • The law applies to businesses outside of the EU where their processing activities relate to offering of goods or services (even if free) or monitoring the behaviour of data subjects in the EU. In practice this means that companies outside the EU targeting EU consumers need to comply with the GDPR and may need to appoint a representative in the EU. • In certain circumstances data controllers and processors must appoint a Data Protection	**Refer to member firm within relevant jurisdiction [suggest Germany, France, UK, Sweden]**

Country	Main laws	Local Summary	Local Expert
		Officer, a formal role required by the new law. • Data processors such as agents or suppliers (organisations who are engaged by a controller to process personal data on their behalf) now have direct compliance obligations under the GDPR, including the obligation to maintain written records of processing activities, designating a Data Protection Officer in certain circumstances and notifying the data controller of breaches. Practically this is changing the risk profile for businesses, as suppliers need to comply with GDPR and face the threat of sanctions for failing to comply. • Consent from data subjects for the processing of their personal data is harder for organisations to obtain and rely on given the standard for obtaining consent has become more onerous. Consent must be fully unbundled from other terms and conditions and is not valid unless freely given, specific, informed and unambiguous. • There are new requirements in respect of keeping data processing records and documentation. • Data subjects have been afforded enhanced rights by the GDPR. • Data controllers must (unless exceptions apply) notify data breaches to their relevant supervisory authority without undue delay and, where feasible, within 72 hours of awareness. • Data Protection Impact Assessments are mandatory in certain circumstances, specifically in situations where data processing is likely to result in high risk to individuals. • GDPR introduced tougher sanctions for business, including very high revenue based fines. Supervisory authorities are also afforded a wide range of investigative and corrective powers. The GDPR has adopted a tiered approach to penalties for breaches of the law and significantly increased fines for breaches. In the most serious cases fines can be made of up to the higher of 4% of annual worldwide turnover and EUR20 million. The significant increases in maximum fines mean that businesses are re-evaluating the risks of non-compliance and adopting a more rigorous approach to compliance with data protection law. There is overall a much higher bar for compliance with GDPR and harsher sanctions businesses can face. There have been a number of key enforcement actions taken by supervisory authorities since the GDPR was introduced. As such, it is important for businesses to take advice and constantly work towards compliance in order to minimise their risk of enforcement action under the current data protection regime in Europe.	
ARGENTINA *(Updated May 2021)*	National Constitution as amended in 1994 (Article 43 and article 75 subsection 12) Data Protection Law	**Collection:** Data Controllers are responsible for compliance with core principles when collecting and processing personal data from data subjects. They must (i) obtain the data subject's informed and unambiguous consent as well as granting a right of access, modification, update and/or deletion of their personal data when requested; (ii) collect and process data for specific and legitimate purposes only; (iii) ensure that the data is collected and processed fairly and lawfully; and (iv) ensure	**Zang, Bergel & Viñes Abogados** Alejandro Estivariz Senior Associate Francisco J. Roggero

Country	Main laws	Local Summary	Local Expert
	25,326 of 2000 and Regulatory Decree 1558/01 of 2001	the safety and the confidentiality of personal data so as to avoid unauthorized access, adulteration or loss of the personal data collected. **Registration**: Individuals and entities collecting personal data must (i) register as *Responsables de Datos Personales* before the *Agencia de Acceso a la Información Pública ("*AAIP*")* and (ii) register all databases containing personal data before the National Registry of Personal Databases of the AIIP. **Data transfer to third countries**: International data transfers are authorized only to third countries considered with adequate levels of protection by the AAIP. The AAIP has also established the guidelines regarding Binding Corporate Rules for international data transfers within companies of the same economic group through the issuance of Resolution 159/2018 of 2018. **Officer**: Data controllers have no legal obligation to appoint a Data Protection Officer. **Privacy Breach/Loss**: The Data Protection Act does not stipulate a specific procedure to notify a data breach to the AAIP. Notwithstanding the foregoing, the AIIP has issued Resolution 47/2018 of 2018 in which it provides for recommended security measures for Data Controllers collecting personal data. In such resolution, the AAIP recommends Data Controllers to have specific procedures to notify the AAIP of the occurrence of any data breach. **Electronic Direct Marketing:** The Data Protection Act requires previous consent from data subjects to receive messages regarding electronic marketing (opt-in). Notwithstanding the foregoing, Regulatory Decree 1558/2001 has allowed the assignment of personal data to third parties without prior consent of data subjects when such personal data is used to categorize groups of people according to their behaviours or preferences strictly for the purposes of delivering commercial offers. In all cases the Data Protection Act provides that users must have the option to unsubscribe from electronic marketing (opt-out).	Partner and Mackrell main contact a.estivariz@zbv.com.ar f.roggero@zbv.com.ar Tel: +54 11 43234000 Florida 537, 18th Floor, Buenos Aires, Argentina www.zbv.com.ar
AUSTRIA *(Updated Jun2021)*	EU General Data Protection Regulation (DSGVO - Datenschutzgrundverordnung) Data Protection Act (Datenschutzgesetz)	**Collection:** Processing of personal data is rather strictly regulated. "Data processing" includes in particular collection, storage and modification of data. The processing of personal data is permitted only (i) with the consent of the the data subject, (ii) if the processing is necessary in fulfilment of contractual obligations or (iii) for the reasons stated in Art. 6 GDPR. Furthermore, data processing may only be carried out in compliance with the principles of Art. 5 GDPR such as lawfulness, fairness and transparency, data minimisation etc. **Registration:** There is no registration requirement for entities that collect, store or use personal data. However, the GDPR obliges to keep internal records on the processing of data. This obligation applies to both the controller and the processor. **Officer:** An obligation to appoint a data protection officer is only provided for companies whose core activity consists of carrying out processing operations, which due to their nature, scope and purposes, require extensive regular and systematic monitoring of data subjects (e.g. banks, insurance companies, credit reference agencies and professional investigators) or if the core activity of the company consists of extensive processing of sensitive data	**Winischhofer Rechtsanwälte** Dr. Felix Winischhofer Partner, Schuppich, Sporn & Winischhofer Rechtsanwälte felix.winischhofer@falke.at Tel: +43 1 512 47 99 Falkestraße 6, 1010 Wien, Austria www.falke.at

Country	Main laws	Local Summary	Local Expert
		or data relating to criminal convictions or offences (e.g. hospitals). **Data transfers to third countries**: Any transfer of personal data to a third country or an international organisation is only permissible if the controller and the processor comply with the conditions laid down in Art. 44 et seq GDPR and also with the other provisions of this Regulation. **Privacy Breach/Data Loss:** There is a legal obligation to report data breaches to the data protection Agency (Art. 33 GDPR). Where the personal data breach is likely to result in a high risk to the personal rights and freedoms of natural persons, the controller shall notify the data subject of the breach without undue delay (Art. 34 GDPR). **Electronic Direct Marketing:** Regulated by the Telecommunication Act (Telekommunikationsgesetz) 2003, Media Act (Mediengesetz), and Data Protection Act.	
BELGIUM *(Updated June 2021)*	General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) The Law of 3 December 2017 ("Data Protection Authority Act") The Law of 30 July 2018 ("Privacy Act") The Law of 5 September 2018 ("Information Security Committee Act") The Law of 21 March 2018 ("Camera Act") The Law of 13 June 2005 transposing the e-Privacy Directive The "Arrêté Royal" of 4 April 2003	**Collection**: legal entity is responsible for compliance with GDPR core principles when collecting and processing personal data. They must (i) obtain the data subject's informed, voluntary and unambiguous consent, grant a right of information, access, modification, restriction of processing, data portability, objection and deletion; (ii) collect and process data for specific, explicit and legitimate purposes only; (iii) ensure that the data are collected and processed fairly, transparency and lawfully; (iv) ensure that the data collected are adequate, relevant and not excessive; (v) ensure the safety and the confidentiality of the collected data and (vi) ensure that the storage of personal data is limited. **Registration**: The general requirement of registration has disappeared with the GDPR. The controller must be able to demonstrate, at any time, his compliance with the GDPR requirements. The authorisation of the Belgian "APD" has been maintained when: (i) there are more than 250 workers, (ii) there is a risk of breach of confidentiality, (iii) there is regular processing of personal data, (iv) there is a particular use of data. **Officer:** DPO must be designated by a controller or a processor if they: (i) are a public authority or body; (ii) carry out large scale, regular and systematic monitoring of individuals; or (iii) carry out large scale processing of special categories of data or data relating to criminal convictions and offences. **Data Transfers from EU**: A data controller can only transfer personal data from the EU to a non-EU member state if (i) the transfer is based on appropriate safeguards (ii) the controller relies on one of the exceptions of Article 49 GDPR. **Privacy Breach/Data Loss**: Controllers must notify a breach to the Belgian "APD" without undue delay and where feasible, no later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). When the breach is likely to result in a high risk to the data subject, the controller is also required to inform the affected data subject without undue delay. **Electronic Direct Marketing**: Regulated by the GDPR and the e-Privacy Directive (transposed in the "Code de droit	**Van Cutsem, Wittamer Marnef & Partners** Nicolas Magrez Partner nmz@vancutsem.be Tel: +32 2 543 02 00 Avenue Louise 235 1050-Brussels Belgium https://www.vancutsem.be

Country	Main laws	Local Summary	Local Expert
		économique", art.XII.13 and the "Arrêté Royal" dated 4 April 2003). Direct Marketing activities (emails) are prohibited without the prior, free, specific and informed consent of the recipient of the message.	
BOSNIA & HERZEGOVINA *(updated Jun 2021)*	Personal Data Protection Law BiH	**Data Processing**: Personal Data Protection Law (hereinafter: ''PDP Law'') applies to personal data processed by all public bodies, natural and legal persons, unless otherwise provided by other law. The PDP Law provides the principles of the data processing. The controller may process the personal data with and without the consent of the data subject. **Data Security Protections:** The controller and, within its competence, the data processor take care of data security and take all technical and organizational measures necessary for the protection and confidentiality of data. The controller who does not have its seat in Bosnia and Herzegovina and who uses automatic or other equipment located on the territory of Bosnia and Herzegovina for the needs of the data processing must appoint a representative for such processing, unless it uses the equipment only for the purpose of data transit through Bosnia and Herzegovina. **Data Confidentiality:** Employees of the controller or processor, other natural persons who process the personal data on the basis of an agreement concluded with the controller or processor and other persons who come into contact with personal data in the premises of the controller or processor are obliged to maintain the confidentiality of personal data and adhere to the established method of security. Personal data processed by the controller or data processor for employees is an official secret. The obligation to maintain the confidentiality of personal data remains in force even after the termination of employment. **Data Transfer Abroad:** It is allowed to transfer the personal data from BiH to another country if that country applies adequate personal data protection measures prescribed by the PDP Law. The PDP Law provides the conditions under which the adequacy of the protection measures shall be assessed. **Providing personal data to a third party:** The data controller may not provide personal data to a third party before notifying the data subject. If the data subject does not approve the provision of a personal data, the data may not be disclosed to a third party unless a disclosure is in the public interest. **Privacy Breach/Data Loss:** The controller shall compensate the material or non-material damage to the data subject if it was caused to the data subject due to the violation of the privacy rights. The controller may be released from the liability for damage if he proves that he is not responsible for the event that led to the damage. **GDPR**: Note that the EU GDPR also applies to personal data protection issues, although BiH is not a member of the EU. GDPR applies in the following cases: i) if the data controller based in EU has its business branches in BiH or in any way provides services to the citizens in BiH; ii) if the data controller is not based in EU countries but offers	**Femil Čurt** Femil Čurt femil.curt@curtlaw.ba Tel: (387) 33 263 025 Šenoina 2, 71000 Sarajevo Bosnia & Herzegovina www.lexcellence.law

Country	Main laws	Local Summary	Local Expert
		goods and services to EU citizens or monitor their behavior within EU. Therefore, companies from BiH that operate in the EU are required to apply the GDPR. Regardless of the fact that BiH legislation is not currently harmonized with the GDPR, its application in the above situations is mandatory for domestic controllers if they operate within EU.	
BRAZIL (*Updated May 2021*)	Law No. 13,709 of August 14, 2018, also known as General Data Protection Law ("**LGPD**").	In Brazil, the main law that regulates the handling of data about individuals is Law No. 13,709/2018, which was inspired in the GDPR. The law covers the following major topics: • Privacy and data protection principles and concepts; • Personal Data Processing requirements by Private and Public Organizations; • Data Subject Rights; • International Data Transfer; • Mandatory reporting of data incidents; and • Data Protection Authority and sanctions. Velloza Advogados has been assisting national and international clients in complying with privacy and data protection regulations, as well as other demands inherent to the digital world.	**Velloza Advogados Associados** Laércio Sousa, CIPP-E and CIPM certified by IAPP Partner, Velloza Advogados laercio.sousa@velloza.com.br Tel: +55 11 3145 0966 Av. Paulista, 901, 17º floor 01311-100 São Paulo – SP Brazil www.velloza.com.br
BULGARIA *(Updated Jun 2021)*	Personal Data Protection Act 2002, amended in November 2019 General Data Protection Regulation Electronic Commerce Act 2006, amended November 2020	The main law that regulates the processing of personal data is the Personal Data Protection Act. The Act was amended in a way that provides for compliance with the Data Protection Regulation and details the framework of the regulation. Therefore, to a large extent, the requirements are also subject to and correspond to the Data Protection Regulation. Our team has a practice in connection with the preparation of a comprehensive strategy for personal data protection, revision of already prepared personal data protection, as well as assistance in inspections by control authorities or in cases of personal data breaches.	**Emel Bekirova, attorney-at-law** **Stankov · Todorov · Hinkov & Spasov, Attorneys-at-Law** 1000 Sofia, 5 Tsar Shishman Str., floor 1 Tel./fax: +359 2 950 6242 E-mail: e.bekirova@sths-law.com www.sths-law.com
CANADA **(Alberta)** *(Updated July 2021)*	***The Personal Information Protection and Electronic Documents Act*** (PIPEDA)	PIPEDA applies to federal works, undertakings and businesses, and to private sector organizations that collect, use or disclose personal information in the course of commercial activities. Under PIPEDA, "personal information" includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as: • age, name, ID numbers, income, ethnic origin, or blood type;	**Scott Venturo Rudakoff LLP** 1500, 222 3rd Ave. SW Calgary, Alberta, Canada Phone: +1 403 261 9043 **Contacts:** Domenic Venturo, Q.C., Partner d.venturo@svrlawyers.com + 1 403 231 8230

Country	Main laws	Local Summary	Local Expert
		• opinions, evaluations, comments, social status, or disciplinary actions; and • employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs). PIPEDA's application to personal employee information is limited to organizations that are federal works, undertakings and businesses, such as: • airports, aircraft and airlines; • banks and authorized foreign banks; • inter-provincial or international transportation companies; • telecommunications companies; • offshore drilling operations; • offshore drilling operations; and • radio and television broadcasters. The provinces of Alberta, British Columbia and Quebec have their own private-sector privacy laws (*Personal Information Protection Act* (PIPA)) that have been deemed substantially similar to PIPEDA. The provinces of Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador have also adopted substantially similar legislation regarding the collection, use and disclosure of personal health information. Organizations subject to a substantially similar provincial privacy law are generally exempt from PIPEDA with respect to the collection, use or disclosure of personal information that occurs within that province. Organizations in the Northwest Territories, Yukon and Nunavut are considered federally regulated, and are therefore also covered by PIPEDA. All businesses that operate in Canada and handle personal information that crosses provincial or national borders in the course of commercial activities are subject to PIPEDA, regardless of the province or territory in which they are based (including provinces with substantially similar legislation). Compliance with PIPEDA is subject to the standard of reasonableness whereby organizations may only collect, use and disclose personal information for purposes that a "reasonable person would consider appropriate in the circumstances." This requirement applies even if the individual has consented to the collection, use or disclosure of their personal information. Organizations that operate interprovincially or internationally will likely be required to deal with both provincial and federal privacy legislation. To that end, while some provinces have legislation that has been deemed substantially similar to PIPEDA with respect to personal health information, some provinces have health specific legislation that has not been deemed "substantially similar" to PIPEDA. As such, both the health specific legislation and PIPEDA may both apply within certain provinces.	Laura Bracco-Callaghan, Partner lbc@svrlawyers.com + 1 403 231 8245

Country	Main laws	Local Summary	Local Expert
	Privacy Act	The *Privacy Act* sets out individual privacy rights with respect to interactions with the federal government, including when accessing services such as: • old age security benefits • employment insurance • border security • federal policing and public safety • tax collection and refunds It applies to how the government collects, uses and discloses personal information. The *Privacy Act* protects personal information held by government institutions. The Act also gives individuals the right to access their personal information held by the federal government. The *Privacy Act* provides that government institutions can only collect personal information if it directly relates to the operation of one of its programs or activities. A government institution must collect this personal information directly from the individual, whenever possible. A government institution must normally inform an individual about why the information is being collected, subject to some exceptions. Unless an individual consents to other uses, the government may only use an individual's personal information for the purpose for which it was collected or a use consistent with that purpose, or for other specifically identified purposes listed in the *Privacy Act*.	
CANADA **(British Columbia)** *(Updated Jun 2021)*	Personal Information Protection Act, SBC 2003, c. 63 ("**PIPA**"), a British Columbia Provincial statute Personal Information Protection and Electronic Documents Act, SC 2000, c. 5 ("**PIPEDA**"), a federal statute of Canada	**Collection**: PIPA mandates how all private sector organizations must handle the personal information of its employees and the public (your customers) and creates rules about collecting, using and disclosing that personal information. PIPA allows personal information to be collected, used or disclosed for reasonable purposes (section 4(2)). What is deemed reasonable will depend on factors such as the nature or amount of personal information you collect, how you plan to use that information, and where or to whom you plan to disclose that information (Office of the Information & Privacy Commissioner for British Columbia "OIPC" Order P05-01). **Registration**: There is no general requirement of registration within PIPA or PIPEDA **Officer**: PIPEDA and PIPA both expressly require organizations to appoint an individual who is accountable for ensuring compliance with the organization's data protection obligations. Generally, these individuals' roles are to ensure that there is compliance and full transparency regarding the use and dissemination of data	**Lindsay Kenney LLP** Chad Gerson, Partner cgerson@lklaw.ca Tel: 778.289.9509 400, 8621 201st Street, Langley, BC V2Y 0G9, Canada www.lklaw.ca

Country	Main laws	Local Summary	Local Expert
		International Data Transfer: Canadian Privacy Legislation generally permits the non-consensual transfer of personal information to third-party processors outside of Canada, provided the transferring organization uses contractual and other means to provide a comparable level of protection while the data is processed or stored abroad. PIPA in British Columbia specifies that a third party may collect data abroad only if: i) the collection is necessary for providing the contractual service; ii) the third party is an individual acting in a personal or domestic capacity; or iii) the third party is providing the information to the organization (PIPA section 12). Generally, the organization transferring the data to the third-party abroad must keep a record in their privacy policies and practice manuals, of the foreign jurisdictions in which the collection, use, disclosure or storage is taking place, and the purposes for which the foreign service provider has been authorised to collect, us or disclose personal information on its behalf. **Privacy Breach/Data Loss**: Under PIPEDA there is a legal requirement to report a breach of security safeguards involving personal information if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual. The commissioner and individual affected must be notified.	
CANADA **(Ontario)** *(Updated Jun 2021)*	***Personal Information Protection and Electronic Documents Act*** (PIPEDA) Several provinces have additional privacy legislation, for example, Ontario's ***Personal Health Information Protection Act*** which establishes a set of rules regarding collection of personal health information.	In Canada, PIPEDA sets the rules for private-sector organizations that collect, use or disclose personal information. Organizations must follow the 10 principles to protect personal information. Requirements include: - obtaining an individual's consent when collecting, using or disclosing that individual's personal information. - granting people access to the personal information held by an organization, and to challenge its accuracy. - using personal information only for the purposes for which it was collected. Federally regulated industries are subject to specific rules under PIPEDA. Macdonald Sager Manis LLP is a full-service law firm. Our lawyers are experienced in advising clients on privacy policies, data processing agreements, data breaches and other related issues offer a unique combination of skills and expertise.	Michael Carey, Counsel Macdonald Sager Manis LLP mcarey@msmlaw.ca 150 York St, Toronto, ON M5H 3S5 www.msmlaw.ca
Canada **(Quebec)** *(July 2021)*	**The Personal Information Protection and Electronic Documents Act** (PIPEDA)	If a Canadian province has adopted legislation which substantially mirrors the terms of PIPEDA, businesses covered by that provincial legislation may be exempt from the federal legislation. Therefore, in Quebec, PIPEDA only applies to federally incorporated private sector organizations and to personal information obtained in the course of interprovincial or international transactions. Other businesses are subject to the Quebec Civil Code and the provincial Privacy Act.	**PFD Lawyers** 1240 Beaumont, suite 210, Montreal, Quebec, Canada **Contact :**

Country	Main laws	Local Summary	Local Expert
	The Quebec Civil Code (QCC)	The QCC governs persons, relations between persons and property. It provides as a fundamental principle that every person has a right to the respect of his/her reputation and privacy and that the privacy of a person may not be infringed unless authorized by Law. Infringements include: • Intentionally intercepting or using private communications; • Appropriating or using a person's image or voice while in a private premise; • Using a person's name, image, likeness or voice for a purpose other than the legitimate information of the public; Every person who constitutes a file on another person must have a serious and legitimate reason for doing so and cannot, without the consent of the person concerned or authorization by Law, communicate such information to third persons or use it for purposes inconsistent with the purposes for which the file was constituted. The QCC also provides that a person may rectify any inaccurate or incomplete information concerning that person and obtain deletion of any obsolete information or information not justified by legitimate purposes for which it was obtained.	Robert Faguy, Partner r.faguy@pfdlawyers.com + 1 514 735 0099
	Act Respecting the Protection of Personal Information in the Private Sector, LQ 1993, c. 17, a.5 ("**Privacy Act**"), a provincial statute of Quebec Personal Information Protection and Electronic Documents Act, SC 2000, c. 5 ("**PIPEDA**"), a federal statute of	**Application of the Privacy Act:** The purpose of the Privacy Act is to protect the right to privacy of individuals as set out in the QCC. The Act governs situations in which personal information is collected, held, used and disclosed to third parties in the course of operating a business. The two guiding and overriding principles of the Act are consent and necessity. Personal information can only be collected by an organization if it is truly necessary and only if the individual consents to its collection (sections 5 and 6). **Registration**: There is no general requirement of registration within the Privacy Act or PIPEDA **Right to information and right of access**	

Country	Main laws	Local Summary	Local Expert
	Canada **Bill 64, An Act to Modernize Legislative Provisions Respecting** **the Protection of Personal Information**	An organization which collects personal information must allow the individual whose information is requested to know 1) the purpose of collecting such information , 2) the use which will be made of the information and the categories of persons who will have access to it within the enterprise and 3) the place where the file will be kept and rights of access and rectification. **Data Protection Officer:** The Commission d'accès à l'information ("**CAI**") oversees the application of the Privacy *Act.* The CAI may decide to investigate on its own initiative or following a complaint by any interested person. In the event of non-compliance with the requirements of the Act, the CAI may issue any order to compel the non-complying party to comply with the Act. *N.B.:* on June 12, 2020, Bill 64 was introduced in the Quebec National Assembly and has not yet been adopted. Bill 64 addresses concerns surrounding data privacy, from large-scale security breaches to individual rights to personal data collected and stored by businesses. It proposes new requirements which apply to all businesses in every industry if they have a digital presence in Quebec. Businesses failing to comply with these proposed requirements could face substantial fines	
CHILE *(Updated Jun 2021)*	- Article 19 No. 4 and No. 5 of the Political Constitution of the Republic of Chile -Law No. 19,628 about the Protection of Private Life and Personal Data. -Law No. 20,575 which set forth the Principle of Purpose in the processing or treatment of Personal Data.	**Collection:** The collection and processing of personal data is authorized by law only in the following cases: a) if the owner of the personal data has given the express consent for the treatment; or, b) if the processing and treatment of the personal data is authorized by law. **Registration:** Currently there is no registration requirement for data users. **Officer:** Currently there is no legal requirement for data users to appoint a data protection officer. **Data Transfer:** The international data transfer is permitted but is subject to the data subject's consent. **Privacy Breach/Data Loss:** Currently, there is no mandatory legal requirement for data users to notify authorities or data subjects about data breaches in Chile. **Sanctions:** -From 10 up to 50 UTM fines (USD 725 - USD 3,600). In this case, affected personal data owner may claim and prosecuting before a civil court, through the interposition of the judicial appeal named "Habeas Data". Such court shall get knowledge of the claim and resolve in a brief procedure.	**Prieto Abogados** Partners: Juan Tagle Quiroz jtagle@prieto.cl Patricio Prieto Larrain. pdprieto@prieto.cl Associates: María Cristina Ríos Llaneza mrios@prieto.cl Tel: +56 222805077 Av. El Golf 40, floor 13, Las Condes, Santiago. http://www.prieto.cl

Country	Main laws	Local Summary	Local Expert
		- Compensation for material and moral damages caused by an improper personal data treatment. The amount of the compensation shall be determined by the civil court in consideration of the circumstances of the case and the facts' seriousness. The court may also adopt every measure it deems necessary for the protection of the rights established by law.	
CHINA *(Updated June 2021)*	1. Cyber-Security Law (effective as of July 1st, 2017) 2. National Standard- information security technology/personal information security specifications (effective as of October 1st, 2020) E-commerce law (effective as of January 1st, 2019)	In China, collection and use/processing of personal information is primarily governed by the following legal texts: *Cyber-Security Law (effective as of July 1st, 2017)* *National Standard- information security technology/personal information security specifications (effective as of October 1st, 2020)* *E-commerce law (effective as of January 1st, 2019)* The "Cyber-Security Law" defines "personal information" and sets a number of principles for collection and use/processing of personal information. The same law also prohibits a number of practices in using/processing personal information. The above national standard provides essentially (a) the definition of important terms; (b) technical details with respect to the collection, stockage, use, processing, transfer of personal information and the consent required to be solicited from the data subject as well as the exceptions to such consent requirements; (c) the requirement for data security audit, handling of a data leakage accident. The E-commerce Law offers the protection of data of consumers for online shopping. Last but not the least, the bill of the « Personal Information Protection Law » was released earlier this year for comments and will be another legislative milestone in China for data protection.	Jun YANG **Jade & Fountain** Jun.yang@jadefountain.com Tel: +86 21 6235 1488 Add: 43/F, Office Tower I, Grand Gateway 66, 1 Hong Qiao Rd, Shanghai, China www.jadefountain.com
COLOMBIA *(Updated June 2021)*	Habeas Data right law 1581 of 2012 Financial Habeas Data Right Law 1266 of 2008. Criminal Code amendment for the "protection of information and data" Law 1273 of 2009 Article 15 of the National Constitution Decree 1377 of 2013.	**Collection:** Persons or entities that handle personal information must comply with principles provided by law 1581, including freedom, security and confidentiality among others. Personal information shall be handled in accordance with a legitimate purpose, the Constitution and the Law. **Types of data** Personal Data is the information that is linked or that may be linked to a person or persons. In Colombia it may be classified in public data, private data, semiprivate data, sensitive data and data related to children and adolescents. Public data is the information related to civil status and the data contained in public documents, public records and judicial rulings that are not under legal reserve. These information does not require an authorization and is not under reserve. Private data is the information that due its intimate or reserved nature is only relevant for the owner of the information. Authorization of the owner is required to have access to this data.	**Parra Rodríguez** Roberta Gentile, Matias Stazzone Daniela Pérez Mahecha and Juliana Angulo Buitrago Associates, Parra Rodríguez Abogados roberta.gentile@pralaws.com daniela.perez@pralaws.com matias.stazzione@pralaws.com juliana.angulo@pralaws.com Tel: +57 3764200 Carrera 9 # 74-08 office 504, Bogotá D.C. Colombia. http://www.pralaws.com/

		Semiprivate data is the information that has a private nature but is information that can be disclosed to third parties. This is the case of credit information. Authorization of the owner is also required for this data. Sensitive data is the information that may lead to discrimination such as data related to health, sexual orientation, biometric data, racial or ethnic origin, political orientation, religious or philosophical convictions, membership in trade unions and social organizations, among others. Sensitive data cannot be collected and handled without the express authorization of the owner. **Registration:** Corporations and non-profit organizations with minimum total assets of COP $ 3.630.800.000 (roughly USD $1.000.), require to register their data bases that contain personal information in the National Registry of Data Bases of the Superintendence of Industry and Commerce (SIC). The responsible must provide a data policy in order to get the registration. The deadline for the Company and non-profit organizations to register the data bases for the first time is 2 months from the date of creation. Registry shall be made with the Superintendency of Industry and Commerce (SIC). Additionally, the Company and non-profit organizations shall register the data bases every year. **Officer:** An entity can be directly responsible for its habeas data obligations or can appoint an officer for these effects. **Data Transfer:** The international Data Transfer is permitted. The countries on which the data is transferred must have at least the same protection of Colombia. If the countries to which the data is transferred does not have the same protection of Colombia, permission must be asked to the Superintendence of Industry and Commerce (SIC). **Privacy Breach/Data Loss:** You must inform any breach or data loss to the Habeas Data Office (SIC) in the following 15 working days from breach or loss. Habeas Data is a fundamental right as per Colombian law. Any infringement to this right can be protected through a constitutional remedy called “Tutela”. **Electronic Direct Marketing:** Personal data may not be disclosed in massive media, unless data owners provides authorization. **Sanctions:** Persons or entities that do not comply with personal data protection regulations may be sanctioned by the Superintendence of Industry and Commerce (SIC), as follows: • Penalties up to roughly USD $479.618 • Suspension or definitive of activities related to data handling.	
CROATIA *(Updated June 2021)*	General Data Protection Regulation 2016/679 (EU) “**GDPR**” Law on	Since Croatia is a member of the European Union, the GDPR is directly applicable on the territory of Croatia while the LIGDPR regulates specific issues only such as organization of Croatian Data Protection Agency, processing genetic, biometric, and health data which implement GDPR Article 9(4), video surveillance, processing data for statistical purposes. There is no	**Law Firm Glinska & Mišković Ltd.** **Key contacts:** Aleksej Mišković Partner

	Implementation of General Data Protection Regulation (Official Gazette no. 42/2018) "**LIGDPR"** Electronic Communications Act (Official Gazette no. 73/2008, 90/2011, 133/2012, 80/2013, 71/2014, 72/2017) "**ECA**"	registration requirement for entities that collect, store or use personal data. ECA regulates the issue of direct marketing and the use of cookies by prescribing that before commencing such data processing, consent from the data subject must be obtained. **Law Firm Glinska & Mišković Ltd.** has extensive experience in advising both domestic and international clients on a wide range of data compliance issues such as drafting privacy policies and data processing agreements, mitigating privacy breaches, conducting privacy due diligence, data protection litigation (including out-of-court settlements) and undertaking privacy risk assessments.	aleksej.miskovic@gamc.hr Tihana Krajnović Associate tihana.krajnovic@gamc.hr Tel: +38516199930 Ulica grada Vukovara 269f, 10000 Zagreb, Croatia https://www.gamc.hr/
REPUBLIC OF CYPRUS *(Updated June 2021)*	Law 125(I)/2018, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.	**Collection:** The collection and processing of personal data must be processed lawfully, fairly and in a transparent manner. Principles such as Lawful basis for processing, Purpose Limitation, Data minimisation, accuracy, retention must be strictly adhered as per the provisions of Law 125(I)/2018. **Registration:** Entities which process personal data must be registered with the Data Protection Commissioner when such process concerns sensitive personal data, data in large and processing of personal data outside of the EU. **Officer:** Currently the appointment of a data protection officer is mandatory when sensitive personal data is collected or processed but also in occasions where big data is been collected or processed. **Data Transfers from EU:** The data transfer within EU is permitted considering that the principles of Law 125(I)/2018 are duly applied. **Privacy Breach/Data Loss:** There is legal requirement to inform the Data Protection Commissioner & Data subjects within a specific timeframe from the time such breach was detected. **Electronic Direct Marketing:** Currently regulated by the Department of Electronic Communications but also through the imminent ePrivacy Regulation (EU).	**Christodoulos G. Vassiliades & Co. LLC** Mrs. Annamaria Vassiliades annamaria.vassiliades@vasslaw.com Phone: +00357 22556677 Ledra House 15, Ayiou Pavlou Street, Ayios Andreas, CY-1105, Nicosia, Cyprus. www.vasslaw.com
CZECH REPUBLIC *(Updated June 2021)*	General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) Act no. 110/2019 Coll., act of 12 March 2019 on personal data processing	**Collection:** Collection of personal data as well as other means of data use is contingent upon the lawfulness of processing, which is further described in art. 6 of the GDPR. However, some other correctives apply such as principles of accuracy, integrity and confidentiality, and especially the purpose limitation principle. Further, the controller must duly abide the information duty. **Registration:** The registration duty has ended with the moment GDPR has become effective and was replaced with the principle of accountability. As such, a controller shall be able to prove her abidance with GDPR at any given time. **Officer:** In accordance with GDPR a controller or data processor might (except for a fairly specific situations, where it must) designate a Data Protection Officer, who shall monitor the regulation, conduct internal audits,	**Josef Aujezdský** josef.aujezdsky@mkanosko.cz Mašek, Kočí, Aujezdský, Opletalova 1535/4 110 00 Praha 1, Czech Republic email: info@mkanosko.cz tel.+420 233 375 542

		educate and train employees and otherwise direct the internal data protection agenda. **Data Transfer:** GDPR applies the principle of free movement of personal data in the European Union and European Economic Area. Pursuant to this principle, data transfers from a member state to another member state shall not be prohibited for the sole reason of individuals personal data processing protection. Transferring data outside of the European Union or European Economic Area might be complicated and shall be addressed on case by case basis. **Privacy Breach/Data Loss:** in case of a privacy reach or data breach GDPR requires that a supervisor authority is informed without undue delay.	
DENMARK *(June 2021)*	EU General Data Protection Regulation (2019/679) ("GDPR") Danish Data Protection Law (502/2018) ("DPL") Danish E-commerce Act (227/2002) Danish Marketing Act (426/2017) Other privacy acts and regulations	Denmark is, as an EU Member State, subject to EU GDPR. Specific national regulation adds a supplementary extended secrecy obligation for certain data, data processors and controllers, and certain forms of data processing. The national age requirement for valid consent is 13 years of age. The Danish Data Protection Agency (www.datatilsynet.dk) is the independent supervisory authority, that supervises compliance, provide guidance, and handle complaints, breach reports and make inspections. The agency has a very informative website. Besides GDPR and DPL there are several sector-specific regulations the constitutes different privacy levels.	**Codex Advokater** Jacob Plum Tholle jpt@codexlaw.dk Tel: +45 75 72 41 00 Damhaven 5 C DK-7100 Vejle Denmark www.codexlaw.dk
DOMINICAN REPUBLIC *(Updated Jun2021)*	National Constitution (Article 44.2) Constitutional Court and constitutional procedures Law No. 137-11 dated as June 13th, 2011. (Habeas Data dispositions) Data Protection Law No.172-13 dated as December 13th, 2013 High-Technology Crimes Law No. 53-07 dated as April 23rd, 2007	**Collection:** Individuals or entities that collect, store or use personal information must guarantee habeas data rights to data owners according to the Dominican constitution and applicable laws. Every individual has the right to know of the existence and access of all personal data registered in public and private registries, as well as request any corrections or updates if needed. The responsible entity must modify/ correct/ update information within 10 days of the request made, if necessary. Habeas Data is a fundamental right as per the Dominican constitution and it is a constitutional action that can be used by any individual or company (Sentencia No. TC/0404/16 del Tribunal Constitucional) upon any infringement of the applicable laws related to data protection. **Officer:** An entity is directly responsible for the treatment of the personal data under its custody, or it can appoint an officer for these purposes. **Registration:** Credit Information Offices (Sociedades de Información Crediticia – SIC in Spanish) contain all personal data regularly requested by banks and financial entities. Banks and financial entities must request individuals their consent to access their personal	**Cáceres Torres** Juan Manuel Cáceres Torres Partner, Cáceres Torres juan.caceres@cacerestorres.com Tel: 809-542-2012 Avenida Gustavo Mejía Ricart esq. Avenida Abraham Lincoln, Torre Piantini, Piso 9, Suite 901, Piantini, Santo Domingo – República Dominicana. www.cacerestorres.com

		information before the Credit Information Offices. Any modification or update must be informed. **Data Transfers:** According to Article 80 of Law 172-13, the transfer of personal data of any kind with other countries, which require the consent of the owner of the data, will only be carried out on several scenarios: 1) When the individual grants authorization or is legally enforced, 2) medical or public health purposes, 3) bank and stock transfers, 4) international treaties and/or agreements, 5) international cooperation to fight crime, terrorism, human/drug trafficking…etc., 6) execution of contracts or pre-contractual measures. 7) upon request for judicial purposes, defence rights and public interest. 8) international legal assistance and 9) request by international organism for public registry purposes. **Privacy Breach/Data Loss:** Authorized entities must report any disclosure, breach or data loss to the Credit Information Offices (Sociedades de Información Crediticia – SIC in Spanish) within the following 15 working days of the disclosure, breach or loss.	
FRANCE (*Updated Aug 2021*)	The Data Protection Act No. 78-17 dated 6 January 1978 ("Loi informatique et libertés") amended by the Law n°2018-793 of June 20, 2018 transposing the GDPR, the ordinance 2018-1125 of December 12, 2018 and the Implementing Decree n° 2019-536 of May 29, 2019 General Data Protection Regulation (GDPR) Regulation (EU) 2016/679	**Collection:** Companies or organisation are responsible for compliance with GDPR core principles when collecting and processing personal data. They must (i) obtain the data subject's informed and unambiguous consent (unless some legitimate reasons listed in law can ground the collection and processing), grant a right of access, modification, restriction of processing, data portability, objection and deletion; (ii) collect and process data for specific, explicit and legitimate purposes only; (iii) ensure that the data are collected and processed fairly and lawfully; (iv) ensure that the data collected are adequate, relevant and not excessive; (v) ensure the safety and the confidentiality of the collected data, (vi) ensure that the time the data are stored is proportionate to the processing purpose and in any case limited. **Registration:** The general requirement of registration has disappeared with the GDPR The controller must be able to demonstrate, at any time, his compliance with the GDPR requirements (principle of accountability). The authorisation of the CNIL required on the basis of a data protection impact assessment has been maintained only for health data processing under certain conditions, **Officer:** A data protection officer (DPO) must be designated by a controller or a processor in accordance with the terms of the GDPR. **Data Transfers from EU:** A data controller can only transfer personal data from EU to a non-EU member state if: (i) the transfer is made to an "Adequate jurisdiction", (ii) the transfer is based on appropriate safeguards or (iii) the controller relies on one of the exceptions of Article 49 GDPR. **Privacy Breach/Data Loss:** Controllers must notify a breach to the data controlling body without undue delay and where feasible, no later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). When the breach is likely to result in high risk to the data subject, the controller is also required to inform the affected data subject without undue delay. **Electronic Direct Marketing:** Regulated by the French Postal and Electronic Communications Code. Electronic	**Stehlin & Associés** Frédéric Lecomte Partner, Stehlin & Associés f.lecomte@stehlin-legal.com Phone: +33 1 44 17 07 70 48, avenue Victor Hugo 75116 Paris - France www.stehlin-legal.com

		marketing activities are authorised provided that the data subject has given consent at the time of collection (opt-in), that it has been informed of his right to object to the use of its personal data and the right to withdraw its consent at any time.	
GERMANY *(updated Jun 2021)*	Federal Data Protection Act 2017 (Federal Data Protection Act, FDPA) Telemedia Act 2007 General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)	**Collection:** All modalities of data use (collection, storage, modification and transfer of personal data) are restricted in the same way: personal data may only be processed if the data subject has unambiguously given his or her prior consent or if data processing is permissible under and performed in compliance with the statutory exemptions applying to the specific modality of data processing (Art. 5/ 6 GDPR). In addition, the principles of "purpose limitation," "data minimization," "accuracy," "storage limitation," and "integrity and confidentiality" must be observed when processing personal data (Art. 5 GDPR). **Registration**: There is no general registration requirement towards a supervisory authority for entities that collect, store or use personal information. Only internal obligations to document data processing operations apply. In the case of special forms of data processing by third parties, there is also an internal obligation to conclude contracts with the respective data processors. However, there is a public registration requirement for certain automated and for various specific types of processes prior to the processing. **Officer**: Every company with more than 19 employees who work with personal data must appoint a data protection officer (Section 38 BDSG). The appointment of a data protection officer is required in the cases Art. 37 GDPR as well as in the special cases of § 38 BDSG (Art. 35 GDPR) regardless of the number of employees. The officer has specific obligations, as defined by the law, primarily to help ensuring compliance with the FDPA/ GDPR and other data protection law. **Data Transfers to third countries**: German entities can transfer data to non-EU countries based on the EU standard contracts, transfers to safe third countries (such as Switzerland) or Binding Corporate Rules (BCR). **Privacy Breach/Data Loss**: There is the legal requirement to notify the supervisory authority in the event of unauthorised use/disclosure of data, Art. 33 GDPR and of the data subject in a high-risk situation pursuant to Art. 34 GDPR. **Electronic Direct Marketing**: Regulated by, *inter alia*, the Federal German Telemedia Act 2007 and the Federal German Act Against Unfair Competition (AAUC).	**Hamburg** **SKW Schwarz** Jens Borchardt LL.M. Partner Certified IT Law Lawyer / Certified Data Protection Officer (TÜV) j.borchardt@skwschwarz.de Tel: +49-40-334010 Ludwig-Erhard-Straße 1, 20459 Hamburg, Germany www.skwschwarz.de **Frankfurt am Main** **Danckelmann und Kerst** Moritz Bohner bohner@danckelmann-kerst.de Tel: +49-69-9207270 Mainzer Landstraße 18, 60325 Frankfurt am Main, Germany www.danckelmann-kerst.de **München / Munich** SLB Kloepper Ferdinand zur Lippe Partner zurlippe@slb-law.de Tel: +49-89-5124270 Leopoldstr. 175, 80804 München, Germany www.slb-law.de
GREECE	EU Regulation 2016/679: General Data Protection Regulation (“GDPR”) Law 4624/2019 regarding the Data Protection Authority, the implementation of the GDPR and the transposition into Greek law of EU	**Processing (Including Collection):** The rules for processing personal data derive mainly from the GDPR in combination with the implementing measures provided by law 4624/2019. **Registration:** There is no registration requirement for persons or entities collecting and processing personal data. **Officer:** Specific sectors’ laws provide for the appointment of a person responsible for data security. Under the GDPR, a Data Protection Officer is appointed where a) the processing is carried by a public authority (with the exception of courts acting in their judicial	**Christodoulos G. Vassiliades Law Firm** Tel: +30 2103388625 Akadimias 34, P.C. 10672, Athens, Greece www.vassiliades.gr **Iro Synodinou** Advocate (Registered

	Directive 2016/680 Law 3471/2006: Protection of personal data and private life in electronic communications Certain provisions of law 2472/1997 which have expressly not been abolished by law 4624/2019 Specific sectors' data protection laws	capacity), b) the main activities of the organization are processing operations which require regular and systematic monitoring of data subjects on a large scale and c) the main activities of the organization consist of large scale processing of special categories of data and data relating to criminal convictions and offences. Such appointment must be notified to the competent supervisory authority. **Cross- Border Transfer of Personal Data:** Under the GDPR, transfers to non- EU countries may be carried out on the basis of either 1) an adequacy decision of the European Commission, 2) appropriate safeguards, 3) binding corporate rules approved by the competent supervisory authority or 4) one of the derogations provided by the GDPR. **Privacy Breach/ Data Loss:** In the event of a breach of personal data, the controller must notify the Authority without delay and, where possible, within seventy-two (72) hours of being aware of the breach, unless it considers that the breach is unlikely to establish endangering the protected interests of a natural person. Where the breach is likely to result in a high risk to the rights and freedoms of natural persons, the breach must be communicated to the data subject as well. Potential fines, depending on the breach, may be 1) up to 10 million Euros or 2% of the global annual turnover or 2) up to 20 million euros or 4% of the global annual turnover. Under Law 4624/2019 there are a series of criminal offences concerning personal data that apply to unauthorized processing and unauthorized disclosure of personal data. These offences are punishable by up to 20 years' imprisonment and fine of up to €300,000. **Electronic Direct Marketing:** Regulated by Law 3471/2006: Protection of personal data & private life in electronic communications, transposing Directive 2002/58/EC. ***Christodoulos G. Vassiliades Law Firm has experience in the provision of services related to data protection and privacy matters, including advising on data collection and compliance issues, drafting all requisite data protection documentation, notices and policies.***	European Lawyer) iro.s@vasslaw.gr **Gianna Tanasidou** Advocate gianna.t@vasslaw.gr
GUATEMALA *(Updated Jun2021)*	Constitution of the Republic of Guatemala, Law on Access to Public Information	There is no specific regulatory body within the Guatemalan legal system which regulates personal data protection. The Law on Access to Public Information, establishes important issues related to the subject (personal data, confidential information, treatment and access to personal data) but it does so, essentially, from the perspective of the handling of personal data by public registries. The Constitutional Court has established that as long as this regulatory absence persists, any commercialization of personal data that takes place in the country must meet the following requirements to be valid and legitimate according to the parameters protection of fundamental rights o According to a fully defined purpose. o In a legitimate way.	**Lexincorp Central America Law Firm** **Gonzalo Menéndez González** gonzalomenendez@lexincorp.com Tel: (502) 5708 1122 9a Avenida 14-78, Zona 10, Ciudad de Guatemala www.lexincorp.com

		o On a voluntary basis by the person whose data is going to be commercialized. o With the consent of the person concerned. o With a purpose compatible with that for which they were obtained. o Implementation of adequate controls that allow the determination of the veracity and updating of the same. o Right to rectification in case of an erroneous or improper update. o Right to exclude the information or data that the owner considers sensitive or whose disclosure may result in damage to their privacy, honor or privacy.	
HONG KONG *(Updated Jun2021)*	Personal Data (Privacy) Ordinance (Cap. 486) (PDPO)	The PDPO governs the various aspects of the use of personal data in Hong Kong. It requires that personal data must be collected in a lawful and fair way, and data subjects must be notified of the purpose and the classes of persons to whom the data may be transferred. However, it does not require registration of data users, the appointment of data protector officers, and data breach notification, etc. Reform proposals on the PDPO are discussed in recent years. In 2020, 6 key directions for reform have been proposed: 1. Establishing a mandatory mechanism for data breach notification; 2. Strengthening obligations on personal data retention; 3. Increasing the enforcement powers of the Privacy Commissioner; 4. Introducing direct regulation of data processors; 5. Amending and expanding the PDPO's definition of 'personal data'; and 6. Strengthening regulation of the improper disclosure of personal data of other data subjects. Though no amendment bill has been tabled yet, data processors in Hong Kong will need to plan ahead and review their existing practices.	**Weir & Associates** Shane F. Weir Partner, Weir & Associates sfw@weirandassociates.com Tel: +852 2526 1767 6/F, Wings Building 110 Queen's Road Central, Hong Kong www.weirandassociates.com
INDIA *(Updated June 2021)*	Information Technology Act, 2000 (the "**IT Act**"). Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 ("**IT Rules 2009**").	**Important Definitions:** **(i)** "**Information**" is defined under the IT Act to include any data, text, images, sound, voice, codes, computer programmes, software and databases or microfilm or computer-generated micro fiche; **(ii)** **"Personal Information"** as per the IT Rules 2011, means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. (iii) "**Sensitive Personal Data or Information**" as per the IT Rules, 2011 means such personal information in relation to a person which consists of information relating to:— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and	**RAJINDER NARAIN & CO.** Ravi Nath, Partner Ravi.nath@rnclegal.com Tel: +91.11.4122.5000 Maulseri House 7, Kapashera Estate New Delhi-110037 India www.rnclegal.com **MURALI & CO., ADVOCATES** C.Muralidhara Managing Partner

	Information Technology (Reasonable security practices and procedure and sensitive personal data or information) Rules, 2011 ("**IT Rules, 2011**").	mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided for rendering services; and (viii) any of the information received by a person under the above clauses for or processing, stored or processed under lawful contract or otherwise. (iv) "**Body Corporate**" as per the IT Act means any Company and includes a firm, sole proprietorship or other association of individuals engaged in any commercial or professional activities. **Collection:** Any Body Corporate that collects, receives, possesses, stores, deals or handles any Information (including Sensitive Personal Data or Information) must comply with the provisions of the IT Rules, 2011. Particularly, such Body Corporate must: i) Obtain consent in writing from the provider of the Information regarding the purpose of usage before collection of such Information; ii) Formulate a 'Privacy Policy' and publish the same on its website, for the handling of or dealing in any 'Personal Information' including any 'Sensitive Personal Data or Information' and ensure that the same is available for view by the providers of such Information. iii) Utilise the Information only for the purpose for which it is collected and not retain such Information for any period longer than as required for such purpose or as otherwise provided in any applicable law. iv) Permit the provider of Information to review the Information provided and ensure that any information found to be inaccurate or deficient is corrected and/or amended as feasible. v) Disclose Sensitive Personal Data or Information only upon obtaining consent of the provider of the information.	102, Haudin House, 5, Haudin road, Bangalore-560042 Tel: 080 41515161 Fax:080 41510421 Mob: +919844019835 murali@muraliandco.com **Malvi Ranchoddas & Co.** 302-304, 3rd Floor, Regent Chambers, Jamnalal Bajaj Marg, Nariman Point, Mumbai -400 021. Tel: +912266331801 prakashmehta@malvirco.com
	Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("**IT Rules, 2021**")	As per the IT Rules, 2009, the Government, can direct an agency of the Government to intercept, monitor, decrypt or cause to be intercepted or monitored, or decrypted any information generated, transmitted, received or stored in any computer resource. The IT Rules, 2011 require that any Body Corporate collecting any Information, must keep such Information secure and exercise reasonable security practices and procedures in relation to the same. In this regard, as per Rule 8 of the IT Rules, 2011 such Body Corporate shall be considered to have complied with reasonable security practices and procedures, if it has implemented security	

		practices and standards that have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In this context, the International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is one such standard referred to hereinabove. **Registration**: Any Body Corporate collecting Information, as a general rule, are not required to register itself before collecting such Information but it must comply with the various requirements, procedures and standards as stated hereinabove. **Officer:** Any Body Corporate which collects Personal Information (including Sensitive Personal Data or Information) must have a Grievance Officer for the purposes of addressing any discrepancies and grievances of any provider of Information with respect to processing of such Information, in a time bound manner. The name and contact details of such Grievance Officer must appear on the website of such Body Corporate. **Data Transfer:** Transfers of Information are allowed only if necessary, for performance of a lawful activity between the Body Corporate and the information providers, or where consent has been obtained from the information providers. **Privacy Breach/Data Loss:** If there is a security breach, a Body Corporate is obligated to demonstrate that they had implemented security procedure and safeguards under the IT Rules, 2011. They may also be called upon to do so by the agency under the law (Indian Computer Emergency Response (CERT-In) or National Critical Information Infrastructure Protection Centre (NCIIPC)), that it has implemented security control measures as per its documented information security programme and information security policies. Further, as per the IT Rules 2021, any "significant social media intermediary", who have over 5 million registered users in India must establish a three-tier system for observing due diligence, comprising of a Chief Compliance Officer, a Nodal Contact Person and a Resident Grievance Officer, all residing in India.	
IRELAND *(Updated Jun2021)*	From 25 May 2018 the key legislative frameworks are: General Data	**Collection:** Data Protection Officer appointed by Processor **Registration:** Certain types of Data Controllers must register with Data Protection Commissioner e.g. Banks,	**Crowley Millar** John Carroll

	Protection Regulation (GDPR) Data Protection Act 2018. The "Law Enforcement Directive" (Directive (EU) 2016/680) which has been transposed into Irish law by way of the Data Protection Act 2018.	Credit Institutions Governments and Direct Marketers. **Officer:** Good Practice for Data Protection Officer to be appointed by Processor post GDPR 2017 certain organisation are mandated to have a DPO **Data Transfers from EU:** Governed by Safe Harbour rules but Privacy Shield arrangement effective in EU from 12 July 2016. Processors accountable for onward transfer. Data subjects must have choice and access and processors must make policy clear to subjects. Complaints must be dealt with within 45 days. Companies' processors may commit to advice of a EU Data Protection Authority. This regime places more obligations on US companies and recognises rights of the individual to data protection and end to an indiscriminate monitoring of data. Early days remains to be seen. **Privacy Breach/Data Loss:** Mandatory notification to Data Protection Authority within 72 hours until no risk or as soon as practicable critical time frame. **Fines** of up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher. If breach is likely to result in high risk to affected data subjects, the controller must inform data subjects without undue delay. Data subject now entitled to General and Special Damage for breach. **Electronic Direct:** Marketing Directive 95/46/EC/Eprivacy Directives/Data Protection Acts 1988/2003/SI336/2100 Requirements for Consents and Opt Out. Must inform at time of data capture of Direct Mail Purpose and give easy and free Mechanism of Opt Out. Must inform who is sending. SMS also covered. Nothing yet vis Skype/WhatsApp/Twitter etc. but assumed covered Data controllers whose business consist wholly or mainly in direct marketing must register with Data Protection Commissioner/DPA	Partner, Crowley Millar Head of Business Development jc@crowleymillar.com Neil Millar Solicitor, Crowley Millar Corporate Department neil@crowleymillar.com Crowley Millar Solicitors 2/3 Exchange Place George's Dock IFSC Dublin 1 Ireland Tel: +353-1-676 1100 Fax: +353-1-676 1630 www.crowleymillar.com
ITALY *(Updated June 2021)*	General Data Protection Regulation 2016/679 (EU) "**GDPR**" In limited and specific matters: Italy's privacy law ("**Privacy Code"**, legislative Decree no. 196/2003), Legislative Decree no. 101/2018 effective September 19, 2018, which has amended and mostly suppressed he Privacy Code to comply with GDPR	**Collection:** Collection and processing of data is subject directly to the rules of GDPR with reference to information to be given to data subject, rights of data subject, consent and other basis for lawfulness of processing, data security etc. The correspondent Italian provisions of the Privacy Code were all replaced by GDPR provisions directly, without amendments or specifications. Some Italian law provisions remain in force to regulate specific aspects only (such as for instance, organisation of the Italian DPA, processing of data by public bodies or for compliance with anti- money laundering provisions, e-commerce, etc.…). Italy had a relevant number of Measures of the Italian DPA in various matters, that remained in force if not conflicting with GDPR (worth of note those related to processing of data of workers and controls on workers' activity) **Registration:** There is no registration requirement for entities that collect, store or use personal data. **Officer:** This matter is subject to the same provisions of GDPR. Italy does not have specific provisions. Appointment of a data protection officer is mandatory only in the cases provided by GDPR. **Data Transfers from EU:** The provisions of GDPR and the	**Mondini Bonora Ginevra Studio Legale** Aldo Lorenzo Feliciani Partner, **Mondini Bonora Ginevra Studio Legale** Professional Association aldo.feliciani@mbg.legal Tel: +39 02.76013210 Corso di Porta Vittoria 5 20122 Milano

		general EU directions about adequacy decisions and appropriate safeguards apply. Italy does not have specific provisions, further limitations or derogations. **Privacy Breach/Data Loss:** The provisions of GDPR apply. Italy does not have specific provisions. **Sanctions:** The provisions of GDPR apply. Italy does not have specific provisions. **Electronic Direct Marketing:** Sections 121-132 of the Privacy Code requires prior explicit consent of recipients of marketing communications (both natural and legal persons), aside from limited exceptions. Cookies are regulated by specific Measures of the Italian DPA. These Measures have been recently reviewed to comply with GDPR and recent interpretations of the EDPB.	
JAPAN *(Updated June 2021)*	Act on the Protection of Personal Information Unfair Competition Prevention Act Act on Regulation of Transmission of Specified Electronic Mail	In Japan, collection and use/processing of personal information is primarily governed by the Act on the Protection of Personal Information ("Act"). The Act imposes significant obligations on a company, including: i) to notify the owner of personal information of the purpose of the utilization of personal information obtained, or make that purpose public; ii) to obtain consent from the owner of personal information before transferring that person's personal information to a third party (and, if the third party is outside Japan, consent to transfer the personal information outside Japan); and iii) to respond to personal information disclosure requests from the owner of personal information. In 2019, the European Commission formally declared that Japan's privacy laws provide adequate data protection, enabling transfers of data from EU. The latest amendment, which will take effect two years from June 2020, adds an obligation for companies to notify both the authorities and the owner of personal information about any leakage, loss, or damage to personal information obtained under the Act.	Osamu Ishida Kojima Law Offices ishida@kojimalaw.jp Tel: +81-3-3222-1401 Gobancho Kataoka Bldg. 4F, Gobancho 2-7, Chiyoda-ku, Tokyo http://www.kojimalaw.jp/
KENYA *(Updated May 2021)*	The Data Protection Act. **(Came into effect November, 2019)** The Data Protection (General) Regulations, 2021 The Data Protection (Compliance and Enforcement) Regulations, 2021 The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 Kenya Information & Communications Act, 1998 AML & Proceeds of Crime Act, 2009	**Registration:** The Data Protection (Registration of Data Controllers and Processors) Regulations 2021 requires every data controller and data processor to register with the Office of the Data Protection Commissioner unless they are exempt. Registration shall be renewed annually and a Certificate of Registration issued which must be displayed prominently in the premises or on their website. **Officer:** It is not mandatory for an organization to hire a Data Protection Officer, they can either designate someone to perform this role, or they could outsource it. A DPO can perform this role for multiple organizations. **Data Transfers from Kenya:** If a data controller wishes to transfer personal data outside Kenya, it must decide whether or not the country ensures an adequate level of protection of that personal data. This decision is normally based on either: (a) A reciprocal data protection agreement with Kenya (b) has ratified the Malabo Protocol (African Union Convention on Cyber Security and Personal Data Protection (c) An adequate data protection law as shall be determined by the Data Commissioner **Privacy Breach/Data Loss:** Notification to the ODPC must be made without undue delay and in any event within 48 hours of becoming aware of the essential facts of the breach. Individuals must also be told about data breaches	**Igeria & Ngugi Advocates** 4th Floor, Avenue 5 Building, Rose Avenue, Kilimani, Nairobi, KENYA Benson Ngugi benson.ngugi@attorneysafrica.com Tel: +254 2675 1221

	Kenya Citizens & Immigration Act, 2011	if the breach is likely to result in a high risk to the rights and freedoms of individuals so that they can take protective measures. Organizations may be exempted from notifying the data subject if they had taken protective measures such as encryption of data.	
REPUBLIC OF SOUTH KOREA *(Updated June 2021)*	Personal Information Protection Act (took effect on September 30, 2016)	In Republic of Korea, data protection/privacy is primarily governed by the Personal Information Protection Act (PIPA). According to Article 15 Section 1 under the PIPA, personal information may be collected in six (6) cases, covering the cases where the consent of a subject of information has been obtained, in order to be in compliance with the applicable statutes, or it is necessary for a public institution to perform its duties in accordance with the relevant rules and regulations. When obtaining a consent to collect personal information, the subject of information must be notified of certain information such as the purpose of the collection and use. Article 16 of the same Act prescribes that only the minimum personal information necessary for achieving the purpose of the collection must be collected. Please note, however, that amendment to Article 15 of the Act expanded the scope of the use of personal information. This new Section 3, became effective August 5, 2020, allows a personal information controller to use or provide personal information without obtaining the consent of the subject of information so long as such use or provision is within the scope reasonably related to the original purpose of collection taking into account certain prescribed conditions (e.g., whether there are any disadvantages to the subject of information, whether necessary security measures, such of encryption, have been taken). Sojong has been providing both domestic and overseas clients with a full range of data protection/privacy services including risk assessment, compliance advice and civil/criminal actions.	**Sojong Partners** Benjamin O. Kim Partner, Sojong Partners bokim@sojong.com Tel: +82-2-311-1114 8F, Daegong Building 126Teheran-ro, Gangnam-gu Seoul 06234, Korea www.sojong.com/eng
LUXEMBOURG *(Updated Jun2021)*	General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") Data protection law related to the protection of physical persons with regards to the use and utilization of their personal data, dated 1 August 2018 (the "**2018 Law**") Data protection law related to the organization of the national commission (the "CNPD") responsible for the protection of personal data, dated 1 August 2018	**Collection, processing and utilisation**: collection and processing of personal data is only allowed if at least one of the conditions mentioned in article 6 of the GDPR are being met (i.e., if the data subject has given consent to the processing of its personal data or if the processing is necessary for compliance with a legal obligation). Article 6 (*lawfulness of processing*) and article 7 (*conditions for consent)* of the GDPR also apply. **Registration**: article 23 of the 2018 Law laids down certain conditions under which there is an obligation to maintain a record of processing activities. **Data Protection Officer ("DPO")**: the designation of a DPO is required when any one of the conditions provided for in article 37 of the GDPR are met. The specific tasks of the DPO are mentioned in article 39 of the GDPR (as well as in article 33 of the 2018 Law which lists the same tasks as the GDPR). **Data transfer to third countries**: Chapter 5 of the 2018 Law underlines the conditions which have to be given in order to authorise a transfer of personal data from Luxembourg to a third country. **Unauthorized use of personal data**: In accordance with Chapter 7 of the 2018 Law, any person who becomes aware (i) of an unauthorized use of personal data or, more generally, (ii) of any violation of the 2018 Law, can inform the Luxembourg national data protection authority, who	VANDENBULKE 35, Avenue Monterey, L-2163 Luxembourg, Grand Duchy of Luxembourg Tel: +352 26 383 350 Denis Van Den Bulke DV@vdblaw.com Valérie Kopéra VAK@vdblaw.com Thomas Le Tallec TLT@vdblaw.com

		shall take the necessary actions and sanctions in line with the provisions of the 2018 Law and the GDPR.	
REPUBLIC OF NORTH MACEDONIA **(Updated Jun2021)**	Law on protection of personal data (Official gazette n.42/2020)	**Collection**: All different manners in which date can be used (collection, storage, modification and transfer of personal data etc.) are normed with obligatory law provisions. Namely, data may be used only if (i) the subject (natural person which owns and it is concerned withthe personal data usage, hereinafter: subject) has given consent for the processing of his/her personal data for one or more specific purposes, or (ii) processing is required to fulfill agreement where the subject is a contracting party, or (iii) the processing is necessary for fulfilling of legal obligation by the controller, or (iv) the processing is necessary for the protection of the essential interests of the subject or to another natural person, or (v) the processing is necessary for protection of public interest or when performing public authorization by the controller, determined by law, or (vi) processing is required when protecting the legitimate interests of the controller or the third party, unless such interests conflict with the interests or the fundamental rights and freedoms of the subject seeking protection of personal data, especially when the subject is a child. Furthermore, date usage is limited by the principles of "purpose limitation," "data minimization," "accuracy," "storage limitation," and "integrity and confidentiality" which are explicitly incorporated in our law. **Registration**: Every controller has obligation only to introduce the regulatory body with the appointment of personal data officer. The controller shall provide information about the personal data officer (name, surname, contact number etc). There is no general registration requirement towards a supervisory authority for entities that collect, store or use personal information. However, when there is a high risk to the rights and freedoms of individuals, when using technologies for some type of processing, while taking into consideration the nature, scope, context and purposes of personal data processing, the controller has obligation to inform and register to the Agency. In this instance the controller shall provide all necessary information/documents about the processing of the personal data normed in the law provisions. **Officer**: Every company, that process personal data, must appoint a personal data officer. For the appointment the regulatory body shall be informed. The officer has specific obligations, as defined by the law, primarily to help ensuring compliance with the GDPR and other data protection law. Lastly, the law stipulates that his/her job responsibilities regarding data protection have primary status over other job responsibilities. **Data Transfers to third countries**: Macedonian entities can transfer data to (i)EU/EEC without any limitations; (ii)non-EU countries, only after permission issued by the regulatory body, or (iii) under Binding Corporate Rules (BCR), which are approved by the regulatory body.	**Law firm Konstantinovic-Milosevski Skopje** 31 Prolet street - Skopje Darko Konstantinovic darko@konstantinovic-milosevski.mk Official web site and email: www.konstantinovic-milosevski.mk office@konstantinovic-milosevski.mk

		Privacy breach/Data Loss: In instances when there is privacy breach/data loss, the controller is obliged, immediately and no later than 72 hours, to inform the regulatory body. Furthermore, in instances of privacy breach/data loss and when there is a high risk to the rights and freedoms of individuals, the controller, has obligation to inform the subject about the violation of security of the personal data immediately and wihtout any delay. **Electronic Direct Marketing**: The processing of personal data for the purposes of direct marketing, which includes profiling to the extent that it is related to direct marketing, is allowed only if the personal data is processed after a previous explicit consent from subject.	
MALAYSIA *(Updated May 2021)*	Personal Data Protection Act 2010 (PDPA)	**Collection:** Persons or entities that collect, store or use personal information must comply with seven Personal Data Protection Principles. Non-compliance with any of the Principles constitutes an offence under the law. Certain Principles are qualified by exceptions and exemptions. **Registration:** There are classes of data users who must be registered under the legislation. The said classes are: Communications, Banking & Financial institutions, Insurance, Health, Tourism & Hospitalities, Transportation, Education, Direct Selling, Services, Real Estate and Utilities. Registrations have to be renewed every 2 years. **Officer:** There is currently no obligation for a data user to appoint a data protection officer. **Data Transfers from EU:** The European Commission has not so far recognised that Malaysia's privacy laws provide adequate data protection, enabling transfers of data from the EU. **Privacy Breach/Data Loss:** There are no obligations for notification in the event of a breach. **Electronic Direct Marketing:** There are no specific laws on electronic direct marketing as yet.	**Ram Caroline Sha & Syah** Anita Kaur Gerewal Partner, Ram Caroline Sha & Syah anita.gerewal@ramcss.com Tel: +60 3 2692 5266 Level 31, Menara TH Perdana 1001, Jalan Sultan Ismail 50250 Kuala Lumpur Malaysia www.ramcss.com
MAURITIUS *(Updated Jun2021)*	The Data Protection Act 2017	**Introduction:** Data protection legislations are essentially designed to protect the individual's right to privacy especially in the advent of modern technologies. As personal Information is nowadays collected, stored, and used through elaborate automated and electronically generated means and moves via the internet, Article 12 of the UN Universal Declaration of Human Rights and Article 8 of the European Convention on Human Rights fall short of affording the degree of protection needed in today's digitalized world. The same can be said of Sections 3 and 9 of the Constitution of Mauritius (modeled on the European Convention on Human Rights) and Article 22 of the Code Civil Mauricien (which dates to Napoleonic times). Hence, the coming into force of the Mauritius Data Protection Act 2017 (''MDPA''). The MDPA is inspired from the EU GDPR. **Application:** The MDPA applies to a controller or processor who (i) is established in Mauritius and processes personal data in the context of that establishment, and (ii) is not established in Mauritius but uses equipment in Mauritius for processing personal data, other than for the purpose of transit through Mauritius. Any person who is resident in Mauritius, or who carries out processing	**The Chambers of Gavin Glover** Gavin Glover Senior Counsel The Chambers of Gavin Glover, SC gglover@gloverchambers.com Tel: +230 208 2299 River Court, St Denis Street, Port Louis Post Code: 11411 www.gloverchambers.com

		operations through an office, branch or agency in Mauritius shall be treated as being established in Mauritius for the MDPA purposes. Mauritian-based controllers and processors dealing with personal data of a citizen of any of the EU Member States must be compliant and accountable under the EU GDPR. Europe still being the largest trading bloc for Mauritius, the EU GDPR is of high relevance in Mauritius. **Supervisory Authority:** The MDPA provides for the establishment of a Data Protection Office and the appointment of a Data Protection Commissioner (''the Commissioner''). The latter has wide powers including delegation of authority to the Police and powers of entry and search of premises. Obstructing the work of the Commissioner or refusing access to premises to the Commissioner are offences under the MDPA. **Custodial Sentence:** Mauritius has adopted a different dissuasive approach. Breaches of the MDPA attract relatively low fines but contraveners are liable to custodial sentences ranging between 2- and 5-years imprisonment. **Registration:** No person shall act as a data controller or processor unless registered as such with the Commissioner. Registration is mandatory, valid for 3 years and is renewable. **Certification:** To encourage compliance of processing operations by controllers and processors with the MDPA, the supervisory authority lays down technical standards for data protection certification mechanisms and data protection seals and marks. A certification is voluntary, valid for 3 years and renewable. A certification shall not alter the responsibility of the controller or processor for compliance with the MDPA. **Officer:** Every data controller established in Mauritius must designate a Data Protection Officer responsible for data protection compliance issues. Controllers or processors not established in Mauritius but using equipment in Mauritius for processing personal data, other than for the purpose of transit through Mauritius, must nominate a Data Protection Representative established in Mauritius. **Data Transfers:** A controller or processor established in Mauritius may transfer personal data to another country where (i) there are appropriate or adequate safeguards for the protection of the personal data in that other jurisdiction, (ii) the other jurisdiction has at least the same level of protection as in Mauritius, (iii) the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer owing to the absence of appropriate or adequate safeguards, (iv) the transfer is necessary for one of the purposes set out in section 36 of the MDPA. It is apposite to note that Mauritius is the 6th State worldwide and the 1st in Africa to have ratified the Protocol amending the Convention for the Protection of individuals about automatic processing of personal data.	

		Privacy Breach/Data Loss: Controllers must notify a breach to the Commissioner without undue delay and where feasible, no later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). When the breach is likely to result in high risk to the data subject, the controller is also required to inform the affected data subject without undue delay. **Electronic Direct Marketing:** Electronic marketing activities are authorized provided that the data subject has given his consent to the use of his personal data with the possibility to opt-out and withdraw his consent at any time. **DPMP:** It is mandatory for every controller to adopt policies and implement appropriate technical and organizational measures to ensure and be able to demonstrate compliance with the MDPA and other relevant data protection laws. This is achieved by drafting and implementing a robust Data Protection Management Program (''DPMP''). **Our services:** We have the expertise and experience for advising on all data protection issues, drafting tailor-made DPMPs, conducting Data Protection Impact Assessments, Data Protection Reviews and Data Protection Training. We also offer services as out-sourced Data Protection Officer and Representative.	
MEXICO (Private Sector) *(Updated September 2019)*	Federal Law on the Protection of Personal Data Held by Private Parties (the "Private Parties Law") (in Spanish: "*Ley Federal de Protección de Datos Personales en Posesión de los Particulares*") Regulations to the Private Parties Law (the "Regulations") (in Spanish: "*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*") Privacy Notice Guidelines (in Spanish: "*Lineamientos del Aviso de Privacidad")*	Persons or entities that collect, use, disclose or store personal data, must comply with several obligations established in the applicable Mexican laws, including: - Mandatory disclosures at the time the information is collected. - The processing of all personal data is subject to the data subjects' consent, with certain exceptions established in law. - The transfer of personal data is subject to the data subjects' consent, with certain exceptions established in law; additionally, data transfers must comply with specific formalization requirements. - Certain types of data breaches must be informed to data subjects. - Controllers must appoint a personal data officer or department. The European Commission has not deemed that Mexico's privacy laws provide an adequate protection to personal data. Gonzalez Calvillo has developed a sophisticated privacy practice, which has developed expertise in: (i) general privacy compliance; (i) data transfers; (iii) privacy-related agreements; (iv) privacy notices, policies, and programs: (v) product and strategy analysis and advising; (vi) privacy due diligences; (vii) data protection litigation; (viii) marketing compliance analysis and strategies; and (ix) legal assistance in data breaches and incident response.	**González Calvillo, S.C.** **Rodrigo Rojas** Partner rrojas@gcsc.com.mx **Lucía Fernández** Associate lfernandez@gcsc.com.mx Tel: +52 (55) 5202-7622 Montes Urales 632 Lomas de Chapultepec 11000, Ciudad de México www.gcsc.com.mx

NETHERLANDS *(Updated June 2021)*	General Data Protection Regulation (EU) "**GDPR**" The Dutch implementation of the GDPR and sector-specific (legal) obligations e-Privacy directive and the Dutch implementation in the **Act on Telecommunications**	With a multidisciplinary approach, THNa can assist its clients in complex data protection and privacy-related issues. Our privacy team provides different services, such as tailor-made privacy programmes to in-depth sector-related advice and litigation. Our lawyers focus on specific market areas. Therefore we have extensive knowledge in the construction industry, healthcare, government and, with a Rotterdam based office, the maritime industry. Next to the general implementation of the applicable European and Dutch privacy laws and regulations, we offer the following services. 1. Structural assistance for your data protection officer and/or privacy programme 2. First aid for data breaches 3. Maturity assessments & privacy programmes 4. Data subject requests 5. Training and awareness	**Ten Holter Noordam** Emiel de Joode Partner, Ten Holter Noordam joode@thna.nl Tel: +31 88 234 45 20 Veerhaven 17, 3016 CJ, Rotterdam, Netherlands www.tenholternoordam.nl/en
NEW ZEALAND *(Updated May 2021)*	Privacy Act 2020 Several industry-specific Privacy Codes Unsolicited Electronic Messages Act 2007	In New Zealand, collection and use/processing of personal information is primarily governed by the Privacy Act 2020. The Act imposes 13 specific privacy principles, including: • Mandatory disclosures at the time personal information is collected; • Specific restrictions on the transfer of personal information offshore; and • Mandatory reporting of data breaches where harm is likely. Each entity must appoint one or more persons to be a privacy officer, who have specific obligations. In 2012 the European Commission formally declared that New Zealand's privacy laws provide adequate data protection, enabling transfers of data from the EU. Clendons have experience and expertise in advising clients on a wide range of privacy and data protection issues, including data processing agreements, data and privacy policies, data collection and compliance issues, data loss and privacy breach scenarios (including cross-border) and cross-border data transfers. James Carnie (Partner, Clendons) is a Registered Privacy Professional with the Office of the Privacy Commissioner in New Zealand.	James Carnie Partner, Clendons Barristers and Solicitors james.carnie@clendons.co.nz Tel: +64 9 306 8002 PO Box 1305, Auckland, New Zealand www.clendons.co.nz
NIGERIA *(Inserted June 2021)*	The Constitution of the Federal Republic of Nigeria, 1999 (As amended) Nigeria Data Protection Regulation 2019 (NDPR) The Nigerian Communications (NCC) Act of 2003 The Cybercrime Act National Identity	**Collection:** Anyone who collects, receives or stores data must comply with the NDPR. The data must be collected for a specific and lawful purpose. The data subject must be informed of the purpose for collection and his/her consent must be obtained. Any medium through which personal data is being collected or processed shall display a simple and conspicuous privacy policy. **Registration:** There is no registration requirement for entities that collect, store or use personal information. **Officer:** Data Controllers are to designate a data protection officer for purpose of ensuring adherence to the NDPR**.** **Data Transfers:** Transfer of data from Nigeria is allowed,. This is however subject to certain restrictions. The Nigeria	Osayaba Giwa-Osagie SAN Senior Partner, Giwa-Osagie & Co giwa-osagie@giwa-osagie.com Tel: +234 (1) 270 7433 www.giwa-osagie.com

	Management Commission (NIMC) Act 2007. Credit Reporting Act, 2017	Data Protection Implementation Framework contains a white list of countries with adequate level of data protection to which data can be transferred.. **Privacy Breach/Data Loss:** Data controllers and administrators are to report breach to the National Information Technology Development Agency, within 72 hours of having knowledge of the breach. The report is expected to include the number of data likely to be affected, the cause of the breach and remedial actions being taken. **Electronic Direct Marketing:** Regulated by the Code of Advertising Practice, Sales Promotion and Other Rights/Restrictions on Practice (APCON Code) and the NDPR. All marketing communications sent by electronic media should include a clear and transparent mechanism that allows consumers to express the wish not to receive future solicitations.	
NORWAY *(Updated June 2021)*	Data Protection Act of 2018. Data Protection Regulation of 2018 The above law and regulation also include the incorporation of Regulation 2016/679/EU – GDPR Special laws with specific regulation of privacy - Patient Journal Act - Criminal Record's Act	The main Norwegian legal framework for privacy consists of: - The Data Protection Act of 2018 1) National Rules chapter 1-9 2) Regulation 2016/679/EU (GDPR) incorporated into Norwegian law - Data Protection regulation of 2018 - Special privacy laws The Data Protection Act imposes several obligations for most entities in Norway (as for entities in other EU/EEA-countries). As an example of such obligations – it stipulates requirements to grounds for processing of personal information, obligations for some entities to have a Data Protection Officer and obligations to deal with petitions from citizens to have their personal data deleted or to limit the processing of such data. Further to the above, it secures equivalent rights for citizens regarding protection of their personal data, including right to access to data/information processed about them, or the right to have personal data about them deleted. Langseth Advokatfirma DA have expertise within this area of law and its lawyers have assisted both businesses to manage compliance requirements and advising private citizens about their rights, including invoking them.	**Langseth Advokatfirma DA** Cato Myhre Partner/advokat, Langseth Advokatfirma DA myhre@ladv.no Tel: +47 920 96 030 Trude Stormoen Partner/advokat, Langseth Advokatfirma DA stormoen@ladv.no Tel: +47 900 55 266 Box 1371, NO-1371 Vika Oslo, Norway www.ladv.no
PALESTINE *(Updated Jul 2021)*	Palestinian Constitution of 2003 Electronic Transactions Law of 2013 (Gaza) Cabinet Decision no.3 of 2019 (West Bank)	There is no data protection regime in Palestine. There is no data officer position, data protection authority, regulation of cross-border transfer of personal data, or an obligation to notify of data breach. Nevertheless, Cabinet Decision no.3 of 2019 in the West Bank prohibits service providers from using personal data of consumers for commercial purposes without obtaining their consent. A similar provision is in-force in Gaza, pursuant to the Electronic Transactions law of 2013. There are also different provisions on data protection of consumers in specific industries and sectors, such as banking services, medical data, electronic payments, and internet service providers.	**Kamal and Associates – Attorney's and Councillors-at-Law** www.Kamallaw.com +970 224 24460 P.O. Box 1591 Fifth floor – Ammar Tower – Ersal Al-Bireh – Ramallah - Palestine Rasem Kamal, Partner

			Rkamal@kamallaw.com +972 599 720 721 Fouad Massad, Associate fmassad@kamallaw.com +972 568 886 692
PERU *(Updated Jun2021)*	Law N° 29733: Protection of Personal Data Act Supreme Decree N° 003-2013-JUS: Regulation for the Protection of Personal Data Act	**Collection:** The law protects the personal data stored or to be stored on databases owned by the government and by private entities. **Registration:** The entities that collect, store or use personal information shall register in the General Directorate for Personal Data Protection of the Ministry of Justice and Human Right the databases that they will manage and the personal data that such databases will contain. Personal data can be stored only with previous consent of its owner, except for some exceptions. **Officer:** The entities do not need to appoint a person to be a privacy officer. **Privacy Breach/Data Loss:** In case of privacy breach, an infringement proceeding shall be initiated by the government with the possible result that the offender must pay a fine. **Cross border transfers**: Data subject's prior consent is required for this purpose.	**Berninzon & Benavides Abogados** Nadia Berdichevsky Associate, Berninzon & Benavides Abogados Professional with the General Directorate for Personal Data Protection nadiaberdichevsky@berlegal.com Tel: +51 1 222 5252 San Isidro, Lima, Peru www.berlegal.com
POLAND *(Updated Jun2021)*	EU General Data Protection Regulation Constitution of the Republic of Poland of 2 April, 1997 (Articles 47 and 51) Act of May 10, 2018 on the protection of personal data Act of July 16, 2004 Telecommunications Law Act of July 18, 2002 on the provision of electronic services	Poland is a member of the European Union and is subject to EU data protection regulations, such as: the General Data Protection Regulation (GDPR), Directive 2002/58/EC (Directive on privacy and electronic communications) and Directive (EU) 2018/1972 establishing the European Electronic Communications Code. All main principles of EU law on data privacy and protection of personal data apply in Poland, however Poland took advantage of the possibility of introducing its own regulations where allowed by European Union law. There are a number of specific requirements that should be taken into account when making business in Poland, especially in the area of: - the rules of the procedure before the supervisory authority (one-instance proceedings and judicial control of the decisions, the possibility of reporting the data protection officer only via the electronic form, the obligation to publish full data of the DPO on data controller's website, including the name and surname of the DPO), - labor law, including issues related to the limited scope of data that can be collected about an employee, employee monitoring, processing of specific categories of employee data, - providing services by electronic means, in particular in the field of: concluding contracts, the obligation to include specific provisions in terms and conditions of services provided by electronic means, the use of cookies and other technologies to track user behavior, - processing medical data and access to information contained in medical records, - conducting direct marketing with the use of	Michał Czuryło Senior Counsel, Konieczny, Wierzbicki Kancelaria Radców Prawnych Sp.p. michal.czurylo@kwkr.pl Tel: +48 504 035 553 ul. Kącik 4, 30-549 Kraków, Poland koniecznywierzbicki.pl

		telecommunications end devices. KWKR has extensive experience and expertise in advising entrepreneurs on the protection of privacy and personal data, including in sectors such as IT / TMT, e-commerce, insurance, gambling, and the medical sector. Our team represents clients before the supervisory authority and administrative courts as well as provide a wide variety of services: implementation of data protection procedures and policies, audits, support in the event of a data protection breach, assessment of compliance of personal data transfers, drafting and negotiating data processing agreements. In terms of compliance with GDPR we also support entities from outside the European Union that want to start operating in Poland or aim to provide services to data subjects in Poland, which may be related to, inter alia, the obligation to appoint a representative in the European Union or a personal data protection officer, which we also provide.	
PORTUGAL (*updated Jul 2021*)	Law n.º 58/2019, of 8 August ("Lei da Proteção de Dados Pessoais") ensures the implementation into Portuguese law of the EU Regulation 2016/679: General Data Protection Regulation ("GDPR") General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)	**Collection:** In order to be able to process data Controller must comply with all the principles of the GDPR. Thus, for data processing it is necessary: - The informed and unambiguous consent of the data subject, being granted the right of access, modification, restriction of processing, data portability, objection and deletion; - Ensure that the processing is restricted to specific, explicit and legitimate purposes; - Assure that the data is processed lawfully; - The collection of data should be limited to what is necessary, avoiding the collection of excessive data; - To guarantee the security and confidentiality of the data collected. The following type of info cannot be processed: • racial or ethnic origin; • sexual orientation; • political opinions; • religious or philosophical convictions; • union membership; • genetic, biometric and health-related data, except in specific cases; • personal data relating to criminal convictions and offences, unless authorized by European or national law. The above shall not apply on the situations of article 9 (2) of the GDPR. Specific rules applicable to children: If a company collects personal data from children based on consent, for example to create a social network account or download web content, it should start by obtaining parental consent, for example by sending a notification to a parent.	**BRAM Legal -Sociedade de Advogados** Miguel Braga da Costa Partner mbc@bramlegal.pt Miguel Ramos Ascensão Partner mra@bramlegal.pt Phone: +351 210 734 790 Adress: Av. 5 de Outubro, n.º 85 – 5º floor, 1050-050 Lisboa www.bramlegal.pt

		Failure to comply with the General Data Protection Regulation ('GDPR') can result in significant fines, which, for certain infractions, can reach 20 million euros or an amount equivalent to 4% of the company's worldwide turnover. The data protection authority may impose additional corrective measures, such as forcing the company to stop processing personal data. **Registration:** There is no general obligation to register with a supervisory authority for entities that collect, store or use personal data. However, the Controller must be able to demonstrate at any time that it acts in compliance with the GDPR. **Officer**: In accordance with the terms of the GDPR the Controller must designate a Data Protection Officer (DPO) (art. 37 GDPR). **Data Transfers to third countries**: The transfer of personal data to a third country or an international organisation may take place where the Commission has decided that third country in question ensures an adequate level of protection. In the absence of a decision, a Controller may transfer personal data to a third country or an international organisation only if there are appropriate safeguards. In the absence of a decision, the Controller may transfer personal data to a third country or an international organisation only if adequate safeguards are in place. If there is no decision and no safeguards the transfer will only be possible under the conditions of Article 49 of the GDPR. **Privacy Breach/Data Loss**: In case of unauthorised use/disclosure of data, the Controler have a legal obligation to notify the supervisory authority. (Art. 33 and 34 GDPR) **Electronic Direct Marketing**: There is no uniform framework applicable to electronic marketing, in Portugal. In addition to the GDPR there is the Advertising Code, applicable to all marketing activities and also the Law on the Protection of Personal Data and Privacy in Telecommunications (Law 41/2004 of 18 August), which determines that all unsolicited direct marketing communications are dependent on the prior express consent of the subscriber, providing, however, some exceptions.	
ROMANIA *(Updated June 2021)*	Law no. 365/2002 on e-commerce Law no.506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector Law no. 102/2005 on	**Collection:** Persons or private and/or governmental entities that *process** personal data must comply with the data protection provisions. **Processing personal data means any operation or set of operations that is performed upon personal data, by automatic or non-automatic means, such as collecting, recording, organizing, storing, adapting or modifying, retrieval, consultation, use, disclosure to third parties by transmission, dissemination or by any other means, combination, alignment, blocking, deletion or destruction.	**Iordache Partners** Adrian Iordache, Managing Director Iordache Partners T: +40.374.616.161 | +40.374.676.76 London Street no 18, Ground Floor, ap 6, 011763, Sector 1, Bucharest, Romania.

	the establishment, organisation and functioning of the National Supervisory Authority for Personal Data Processing Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Law no. 190/2018 on measures implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) Law no. 129/2018 for the amendment and completion of Law No. 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for the Processing of Personal Data, as well as on the repeal of Law No 102/2005 on the establishment, organisation and functioning of the National Supervisory Authority for the Processing of Personal Data, 677/2001 for the protection of persons with regard to the processing of personal data and the free movement of such data; Law no. 363/2018 on	**Registration:** There is no obligation for the data controller to register with the National Supervisory Authority for Personal Data Processing and no registration number for the data controller shall be provided. This was a legal requirement provided by Law no. 677/2001 on the Data Protection of Persons with regard to the processing of personal data and the free movement of such data repealed by Law no. 129/2018. **Officer:** In accordance with the General Data Protection Regulation, the designation of a data protection officer is mandatory in the following cases: 1. where the processing is carried out by a public authority or body, except for courts acting in their judicial capacity. 2. where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale. 3. where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences. In addition, the provisions of Law no. 190/2018 list the obligation to appoint a data protection office in case of processing of a national identification number and of personal data and special categories of personal data in the context of performing a task serving a public interest. **Data Transfers from EU:** Data transfer to/from EU is allowed. **Privacy Breach/Data Loss:** In accordance with the provisions of the General Data Protection Regulations and Article 29 Working Party – guidelines on notification of personal data breaches pursuant to Regulation 2016/679, all organizations are required to report certain types of personal data breaches to the National Supervisory Authority for Personal Data Processing and, where possible, this should be done immediately. **Electronic Direct Marketing:** Regulated by Law no 506/2004 transposing the Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, published in the Official Journal of the European Communities no. L 201 of July 31st, 2002.	E: adrian@iordache.partners W: www.iordache.partners

	the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of preventing, discovering, investigating, prosecuting and combating criminal offences or the execution of penalties, educational and safety measures, and on the free movement of such data		
RUSSIAN FEDERATION *(Updated Jun2021)*	Law dated 27 July 2006 No. 152-FZ "On personal data"	**Collection:** Individuals or entities that process personal data ("data operators"), must comply with data protection requirements. In many cases, collection and processing of personal data require prior informed consent of the relevant individual(s), subject to a number of statutory exceptions (for example, where personal data is collected to perform a contract with the relevant individual). Apart from that, collection of personal data should be strictly limited to the legitimate aim sought. Data operators are also obliged to keep the personal data secure and confidential. There are also other obligations, such as to ensure that individuals can access their personal data upon request. A peculiar feature of Russian law is that personal data of Russian citizens has to be stored physically in Russia, even if the data operator is located abroad. Non-compliance may lead to public penalties and, in the worst case, to access restrictions to relevant websites (for example, LinkedIn was blocked in Russia on this basis). It is, however, generally possible to keep a copy of the relevant database abroad, provided that this database is secondary in nature and subject to cross-border transfer requirements (see below). **Registration**: Generally, no registration is required to collect and process personal data. However, in some cases it may be necessary to submit an advance notice to the Russian data protection authority Roskomnadzor before processing personal data (for example, this is relevant in some cases of automated data processing). In some cases, data operators may be obliged to formally adopt a corporate Personal Data Processing Policy in accordance with Russian law (particularly in employment contexts). **Officer:** Legal entities have to appoint an employee responsible for personal data protection. It is also possible for the company CEO to assume this responsibility. **Data Transfer to third countries:** Cross-border transfer of personal data is normally allowed to countries that are parties to the 1981 Council of Europe Convention No. 108 or to other countries that are formally recognized to adequately protect personal data by the Russian authorities (e.g. Australia, Canada, Singapore). Data transfer to other countries is permitted in statutorily defined cases, for example where the relevant individual separately	**Sirota & Partners law firm** Artem Sirota Partner artem.sirota@sirotapartners.com Office address: Ducat Place II Ul. Gasheka 7, bld.1, 123056 Moscow Tel.: +7 (495) 234 18 75 Fax: +7 (495) 234 18 76 www.sirotapartners.com info@sirotapartners.com

		consented to such transfer in writing. **Privacy Breach/Data Loss:** There is no mandatory requirement to report data breaches or losses to the Russian authorities or to the affected individuals. However, a privacy breach/data loss may be revealed during an inspection of the supervisory authorities, which may lead to public liability. The recent trend is to increase penalties for personal data breaches. **Electronic Direct Marketing**: Electronic direct marketing requires prior consent of the relevant individual and should be discontinued upon demand. Some other restrictions apply. For example, Russian law formally prohibits automated distribution of marketing messages.	
RWANDA ***(Updated July 2021)***	Art 23 of the Constitution of the Republic of Rwanda as amended to date Draft Law on Data Protection and Privacy Information and Communication Technologies Law No. 24/2016 Law No. 18/2010 of 12/05/2010 relating to Electronic Messages, Electronic Signatures and Electronic Transactions Regulation No. 02/2018 published on 05/02/2018 on Cybersecurity Law nº 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes	Currently, the main source for data protection is the constitution Rwanda. This article guarantees the right to private life, family, home or correspondence of a person. It prohibits the arbitrary interference with privacy and enshrines respect for a person's honour and good reputation. It provides that the confidentiality of correspondence and communication shall not be subject to waiver except in circumstances and in accordance with procedures determined by law. To give effect to the constitutional right to privacy under Article 23 of the Constitution, Rwanda has drafted, and cabinet has approved the Draft Law on Data protection. The purpose of this draft law is to enable citizens to exercise their right to data privacy and have enforceable recourse should the right be infringed upon. However, as of writing, this draft Law has not been signed into law and is not yet published. There are however other laws and regulations in Rwanda that contain ancillary provisions concerning the protection of personal data. This law was promulgated in 2016 in order to regulate electronic communications, information society, the broadcasting sector, and the postal sector. Promulgated in 2010 to regulate the electronic collection of personal information, This regulation aims to establish minimum standards for banks to protect against cybersecurity threats and promote the protection of customer information as well as the information technology systems of banks. While the purpose of this law is to prevent and punish cyber-crimes, it has provisions for protection of critical information and infrastructure. It also makes it an offence to unlawfully intercept/obtain data.	**Shield Associates** **Partners:** Isaac Ndahiro & Maggie Baingana **Address:** KG 7th Avenue, 3rd Kigali Heights Bldg. East Wing P.O.Box 155 Kigali Rwanda **Email:** info@shield-associates.com **Website:** http://www.shield-associates.com

SAUDI ARABIA *(Updated June 2021)*	There is no specific Saudi privacy and personal data law; however, various laws and circulars may apply depending on context.	In absence of specific Data Protection law, various sectors of Saudi Arabia Law and Shariah's Principles regulate data protection. Therefore, Saudi Courts will apply concepts of Shari'ah or Islamic law. Data Protection under Saudi Law is regulated under Anti-Cyber Crime Law, Executive Regulations for Electronic Publishing Activity, Law of Printing and Publication Telecommunications Act, Telecommunications by Law, Cloud Regulation and Anti-Terrorism Law among other regulations. Under Shariah's Principles and law, it establishes a framework for individuals to be compensated based on loss or harm as a result of the disclosure of his or her personal information by another party. Liability for disclosure will pass to any third party who improperly discloses personal information obtained unlawfully. Liability and penalties are determined on a case by case basis.	Chris Johnson and Jeanina Awni The Law Firm of Mohammed Alsharif in Association with Johnson and Pump chris@alshariflaw.com Jeanina@alshariflaw.com Tel: +(966-11)462-5925 P. O. Box 9170, Riyadh 11423 Kingdom of Saudi Arabia
SERBIA (*Updated Jun 2021)*	Data Protection Act	**Collection:** Personal data must be collected in a lawful, fair and transparent way for a specified, explicit, justified and lawful purpose. **Registration:** There is no general registration requirement. **Officer:** There is a legal requirement for appointing a data protection officer when the person whose personal data are being collected has a permanent or temporary residence in the Republic of Serbia and the collector does not have a registered seat, i.e. permanent or temporary residence in the Republic of Serbia. **Data Transfers from Serbia:** • Transfer based on an adequate level of protection; • Transfer in case there is no adequate level of protection (with and without permission of the authority); • Transfer in special circumstances. **Privacy Breach/Data Loss:** The controller is obliged to notify the Commissioner for every infringement of data that could cause risk for violating human rights. **Electronic Direct Marketing:** Advertising Act, E-Commerce Act, and Data Protection Act.	**Belgrade** **SOG / Samardžić, Oreški & Grbović law firm** www.sog.rs **Miloš Velimirović** Partner milos.velimirovic@sog.rs **Katarina Živković** Senior Associate Certified Data Protection Manager katarina.zivkovic@sog.rs
SINGAPORE *(Updated June 2021)*	Personal Data Protection Act Cybersecurity Act 2018 and the Computer Misuse Act Spam Control Act	The collection, use and disclosure of personal data is primarily governed by the Personal Data Protection Act ("PDPA") which regulates:- • Organisations' care of personal data including accuracy, protection, retention and cross-border transfers; • Designation of data protection officers by organisations to ensure compliance; • Individuals' right to access and correct personal data and data portability; and • Mandatory reporting of data breaches where it results in significant harm or is of a significant scale.	Lee Soo Chye Partner, Wee Swee Teow LLP lee.soochye@wst.com.sg Jacqueline Teo Senior Associate, Wee Swee Teow LLP Jacqueline.teo@wst.com.sg Tel: +65 6532 2966 491B River Valley Road #10-

		Any organization that collects, uses or discloses personal data in Singapore must comply with the PDPA regardless of where it is formed or located, and non-compliance may attract financial penalties and remedial directions from the PDPC. At Wee Swee Teow LLP, we advise clients on a range of data protection issues, including formulation of data privacy policies, preparation of data processing agreements, compliance issues and assisting in the management of data breaches.	03/04 Valley Point Singapore 248373 www.wst.com.sg
SLOVENIA (*Updated June 2021)*	Personal Data Protection Act (*ZVOP-1*) General Data Protection Regulation (EU) 2016/679 (*GDPR*) Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences (*ZVOPOKD*) Personal Data Protection Act (*ZVOP-2*) – *currently in the legislative process*	The data collection, use and processing are governed by the currently valid Personal Data Protection Act (ZVOP-1), which is out of date and in places even contrary to the GDPR provisions. The new Personal Data Protection Act (ZVOP-2) – the first draft was presented in October 2017 and has undergone several revisions – that will implement essential aspects of the GDPR has not been adopted yet and is – as of June 2021 – still in the legislative process. With respect to the implementation of the Directive 2016/680, a specific legal act has been enacted. The law regulates the collection, use and processing of personal data by administrative bodies, which may use coercive powers in connection with criminal offences. Law firm Sibinčič Križanec has extensive up-to-date knowledge of local and international personal data protection laws and experience with privacy and regulatory compliance to generate privacy policies and strategies that protect clients from any threats. We provide wide range of services, including assessment of breaches and their impacts, investigations, crisis communication management, drafting appropriate documentation and preparation of clients for potential litigation.	**Law firm Sibinčič Križanec l.f. Ltd.** Dinar Rahmatullin, Senior Associate Teja Podržaj, Senior Associate E: dinar.rahmatullin@s-k.law teja.podrzaj@s-k.law T: +386 59 097 400 Dalmatinova ulica 2, 1000 Ljubljana, Slovenia https://www.s-k.law/
SOUTH AFRICA *(Updated Jun2021)*	The Protection of Personal Information Act ("**POPIA**")	**Summary** - The protection of individuals and their right to privacy is enshrined in section 14 of the Constitution of the Republic of South Africa. - POPIA was signed into law on 19 November 2013 and on 1 July 2020, President Ramaphosa, by way of proclamation, implemented the remaining provisions of the Act to commence from 30 June 2021. - **Compliance with POPIA** is compulsorily, with section 114(1) providing that all forms of processing of personal information in South Africa must, within 1 (one) year after the commencement of the section, conform to the and comply by 30 June 2022. - The legal requirements in respect of the processing of personal information by safeguarding personal information when processed by a responsible party or operator, subject to justifiable limitations which include balancing the right to privacy against other rights specially the right to access information and protecting interests which include the free flow of information within South Africa and across international borders. - Responsible parties (those with the information) are obliged to carefully consider their methods of capturing, managing, storing, and securing any personal information. - POPIA places an obligation on responsible parties (those who have the information) or operators to	**Ramsay Webber Incorporated** **Shawn van Heerden** **Managing Director** **svh@ramweb.co.za** **Gerhard Human** **Associate Director** **gh@ramweb.co.za** **Steven Saunders** **Candidate Attorney** **ss@ramweb.co.za** 2nd Floor, the Reserve. 54 Melville Road, Illovo, Johannesburg

		disclose breaches of information, to provide data subjects with remedies where the Act makes provision for them, and it confers authority upon the Information Regulator to impose severe penalties for such conduct. - **The conditions for the lawful processing of personal information** under POPI can be found in sections 8 to 25 of the act and include for the purposes of accountability (section 8), processing limitations (sections 9 to 12), purpose specifications (section 13 and 14), further processing limitations (section 15), information quality (section 16), openness (section 17 and 18), security safeguards (section 19 to 22); and data subject participation (section 23 to 25). - **Contraventions of POPIA include** hindering, obstructing or unlawfully influencing the regulator, a responsible party failing to comply with an enforcement notice, offences by witnesses, and/or unlawful acts by responsible parties or third parties in connection with account numbers. - **Punitive consequences for non-compliance are** set out in sections 100 to 107, which endorses punitive action by way of criminal sanctions, penalties and administrative penalties against persons or parties who contravene any provision/s of the Act of a maximum penalty of R10 million fine or imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment.	Tel: +27 11 778 0600 www.ramweb.co.za
SPAIN (*Updated May 2021)*	Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation") – GDPR Organic Law 3/2018, on Personal Data Protection Law 34/2002, on Information Society Services	Our services include support, maintenance, auditing and specialized legal advice, aimed at ensuring continued compliance with data protection regulations and linked issues, as well as servicing and managing any claim, inquiry or proceedings relating to the said matters. Among others, we cover: ▪ Audits, consultancy and action plans ▪ NDAs, Joint Controllers, Data Processor, data disclosure and related clauses and agreements ▪ Data Subjects´ requests and complaints ▪ Data Protection Officer (DPO) role & Privacy Boards ▪ Marketing and advertising activities (e.g. newsletters and cookies) ▪ Privacy policies, rules and procedures ▪ Privacy Impact Assessments (PIA) & Data Breaches ▪ International Data Transfers ▪ Supervisory Authorities´ requests and complaints ▪ Training & awareness	**Santiago Mediano Abogados, S.L.P.** Javier Berrocal, Partner jberrocal@santiagomediano.com Tel: +34 91 310 63 63 Address: c/ Campoamor 18 – 1º; 28004 Madrid, Spain www.santiagomediano.com
SWEDEN *(Updated June 2021)*	Law with Supplementary Provisions to the EU Data Protection Regulation (2018:218) Ordinance with Supplementary Provisions to the EU Data Protection Regulation (2018:219)	As an EU Member State, collection and use/processing of personal information is primarily governed by the EU General Data Protection Regulation 2016/679. Specific national regulation adds a statutory secrecy obligation for data protection officers, sets a national age requirement for valid consent at 13 years of age and regulates levels of administrative fines that can be levelled at public authorities. The Swedish Authority for Privacy Protection www.imy.se provides basic information in English on its website, including the possibility to submit a notification of a personal data breach or the appointment of a data	**Wesslau Söderqvist Advokatbyrå** Henrik Nilsson Partner, Wesslau Söderqvist henrik.nilsson@wsa.se

	Electronic Communications Act (2003:389) Several (approx.100) Public Authority-specific Privacy Acts and Regulations Marketing Act (2008:486)	protection officer. Wesslau Söderqvist has a strong privacy and data protection team which regularly advises domestic and international clients on a wide range of privacy and data protection issues, with a particular expertise in IT and Information Security matters. We provide an overview of the Swedish regulatory regime at https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2021/sweden and https://www.lexology.com/gtdt/workareas/data-protection-and-privacy	Tel: +46 8 407 88 00 Box 7836, SE-103 89 Stockholm, Sweden www.wsa.se
SWITZERLAND *(Updated JUN 2021)*	Federal Constitution of the Swiss Confederation of 18 April 1999 (Status as of 23 September 2018) – article 13 Federal Act on Data Protection (FADP) of 19 June 1992 (Status as of 1 March 2019) Ordinance to the Federal Act on Data Protection of 14 June 1993 (Status as at 16 October 2012)	The protection of personal data is mainly governed by the Federal Act on Data Protection (FADP) and the associated Ordinance to the Federal Act on Data Protection (DPO). This is the case regardless of whether the processing of the data is carried out in the private sector or by federal bodies. Switzerland is not a member of the EU or the European Economic Area, but Swiss companies and organisations must nevertheless also comply with European data protection regulations. Since the EU General Data Protection Regulation (EU GDPR) came into force on 25 May 2018, many companies in Switzerland fall directly under EU law. In addition to these general legal bases, there are other area-specific laws, such as for the processing of patient data in the healthcare sector, the processing of employee data in the employment relationship or for bank customer data.	**Peyer Partner Rechtsanwaelte** Tobias Bonnevie-Svendsen, Partner t.bonnevie@peyerpartner.ch Tel: +41 43 888 68 36 Peyer Partner, P.O. Box, 8021 Zurich
TAIWAN (Updated June 2020)	Personal Data Protection Act (PDPA):	Government or Non-Government agency need to obey the Taiwan Personal Data Protection Act (PDPA) for Collecting, processing, using or cross-border transferring of any personal data. Some bullet point: - Require to provide a privacy notice to the data subject - Specific restrictions on “sensitive personal data”. - Government agencies need to assign appropriate Personnel (s) to protect the data. - A cross-border Data Transfer requires proper approval, considering law and national security. However, transferring subscribers' personal data to China is prohibited. - For the first time marketing purpose, a non-government agency need to provide the data subject of the ways that he/she can object to such use. - On data breach liability may be civil and criminal, as well as administrative penalties and orders.	Louis & Charles Attorneys at Law Raymond Yu info@louisilf.com Arpita Dutta info@louisipo.com Tel: (886) 2 2395 6566 9F. No.15-1, Sec. 1, Hangzhou S. Road, Taipei, 100024, Taiwan
TANZANIA (*Updated June 2021*)	**The Constitution of the United Republic of Tanzania, 1977**	**The right to privacy** This right is enshrined under Article 16 of the Constitution. Every person in the United Republic of Tanzania is entitled to respect and protection of his/her person**, the privacy of his/her own person**, his/her family, and of his/her	**Kkb Attorneys At Law** Partner, Frank Kifunda

	The Cybercrime Act No. 14 of 2015 **The Electronic and Postal Communications Act, 2010** **The Electronic and Postal Communications Regulations, 2020** **The Banking and Financial Institutions Act, 2006** **Bank of Tanzania (Credit Reference Bureau) Regulations, 2012**	matrimonial life, and respect and protection of his/her residence and private communications. However, these rights should not be used to infringe on the freedoms of other persons or public interest. **Privacy Breach & Loss:** • **Data espionage**, section 8 of the Cybercrimes Act makes it illegal to obtain computer data protected against unauthorized access without permission. • **Intentional and unlawful hindrance or interference** with- (a) the functioning of a computer system; or (b) the usage or operation of a computer system. It is an offence to intercept personal communications and interfere with data by damaging, deleting, altering, obstructing, and interrupting it. The Cybercrimes Act also prohibits operators and other service providers from monitoring activities or data being transmitted in their systems. The disclosure of data for the purposes of a criminal investigation or the prosecution of an offence is dealt with in Section 32 of the Cybercrimes Act **Protection of Privacy** Section 98 of the Electronic and Postal Communications Act imposes a duty of confidentiality upon the Tanzania Communication Regulatory Authority (TCRA) and companies licensed to offer services pursuant to the TCRA, unless disclosure is allowed by law. **Accountability for data protection** Subscribers and users of online content shall be responsible and accountable for the information they post in an online forum, social media, blog, and any other related media, and are required to ensure that their posts do not contravene the provisions of the Online Content regulations. **Protection of Personal Information** Section 48 of the Banking and Financial Institutions Act prohibits banks from disclosing their customer's affairs and information, unless required by law. **Protection of personal Information** The Regulations prohibit credit reference bureaus from maintaining any information relating to the borrower's race, creed, colour, ancestry, ethnic origin, religious or political affiliation, state of health, or criminal record except financial fraud and other similar types of offences (Regulation 20) **Kkb Attorneys At Law** has been assisting national and international clients in complying with privacy and data protection regulations, as well as other demands inherent to the digital world.	frank@kkbattorneys.co.tz Tel : +255 713 996 828 Practice Manager, Njile Bwana njile@kkbattorneys.co.tz Tel : +255 743 923 763 Associate, Kemilembe Barongo kemilembe@kkbattorneys.co.tz Tel: +255 788 098 539 Second Floor, Oyster Plaza, Haille Selassie, Oyster Bay P.O. Box 13989, Dar es Salaam, Tanzania www.kkbattorneys.co.tz
THAILAND *(Updated May 2021)*	Personal Data Protection Act, B.E. 2562 (C.E. 2019)	The Act covers the following matters among others: 1. Specifies what data activities are covered under	**Ploypratthip International Law Office (PILO)** Mr. Edward T. Ploysongsang

	Data protection provisions will become enforceable on 31 May 2022	the Act; 2. Specifies the qualities of a Data Controller and Data Processor; 3. Specifies what disclosures must be made before data can be collected; 4. Outlines the requirements for a data protection officer; 5. Outlines the rights of data subjects; 6. Requires that countries receiving data from Thailand must have adequate protection standards; 7. Requires Controllers to notify of any data breach; 8. Provides for the destruction of data; and 9. Outlines procedures for filing complaints and provides for penalties. It does not specifically mention electronic direct marketing, though it would nonetheless apply to businesses engaging in direct sales and direct marketing activities. PILO can advise clients on a full range of privacy and data protection issues including data processing agreements and compliance.	Managing Partner edward@ploypathip.com Mr. Manuttsak Khamchay Senior Associate manuttsak@ploypathip.com Mr. Thananthon Khamwaen Associate thananthon@ploypathip.com 11/15-16 Ratchadaphisek Road; Chong Nonsi Sub-District, Yannawa District; Bangkok 10120, Thailand Tel: +662 678 2995 www.ploypathip.com
TURKEY (*Updated June 2021)*	Turkish Constitution Turkish Law on the Protection of Personal Data (no. 6698, dated April 7, 2016) Regulation on Deletion, Removal, and Anonymization of Personal Data (no. 30224, dated October 28, 2017 and entered into force on January 1,2018) Communiqué on Procedures and Principles of Obligation to Inform (no. 30356, dated March 10, 2018) Communiqué on Procedures and Principles of Application to Data Controller (no. 30356, dated March 10,2018) Regulation on Data Controllers' Registry (no. 30286, dated December 30, 2017 and entered into force on January 1, 2018) Regulation on Protection of	**Data processing:** Any operation which is performed upon personal data such as collection, recording, storage, preservation, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization or blocking its use by wholly or partly automatic means or otherwise than by automatic means which form part of a filing system. Real or legal persons that process data must comply with 5 specific general principles. In addition, as a rule, personal data cannot be processed unless there is an explicit consent of the data subject. There are seven conditions under which personal data can be processed without explicit consent. Special categories of personal data can be processed under more specific conditions. **Registration:** Real or legal persons processing personal data must enrol to the publicly available Data Controllers' Registry before they start processing personal data. **Officer:** optional. **Data Transfer from EU:** The European Commission has not recognized Turkey as a country providing adequate protection without any further safeguard being necessary yet. **Data Transfers Abroad:** As a rule, personal data cannot be transferred unless there is an explicit consent of the data subject. There are seven conditions under which personal data can be transferred without explicit consent. However, in order to transfer data abroad with these conditions, the third country must be declared a country with adequate level of protection by the Turkish Board of Protection of Personal Data ("Board"). Yet, the Board has not determined and announced the countries with adequate level of protection. Therefore, regarding data transfers abroad without explicit consent, currently commitment for adequate protection in writing by the data controllers in Turkey and in the relevant foreign country is requested, and it is subject to the authorization of the Board. **Privacy Breach/Data Loss:** In case processed personal data are acquired by others through unlawful means, the	**Herdem Attorneys at Law** Şafak Herdem Founder Partner safak.herdem@herdem.av.tr Tel: +90 212 288 4959 www.herdem.av.tr

	Personal Health Data (no. 30808, dated and entered into force on June 21,2019)	data controller shall notify the Board of such situation without undue delay and in any event within 72 hours of becoming aware of the essential facts of the breach. The Board, if necessary, may declare such situation on its official website or by other means which it deems appropriate.	
	Law on Electronic Communication (no. 5809, dated November 10, 2008) Law on Arrangement of Electronic Commerce (no. 6563, dated October 23, 2014 and entered into force on May 1, 2015) Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector (no. 31324, dated December 4, 2020 and entered into force on June 4,2021) Regulation on Remote Identification Methods to Be Used by Banks and Establishing Contracts in Electronic Environment (no.31441, dated April 1, 2021 and entered into force on May 1, 2021)	**Electronic Direct Marketing:** Commercial Electronic Message is defined under the Law no.6563. An approval in writing or by any means of electronic communication of data subject must be obtained before sending the messages which contain commercial purposes. **Electronic Communications:** The confidentiality of electronic communications and related traffic data is protected. Unless otherwise agreed and permitted by laws, relevant legislation and judicial decisions, it is forbidden to listen, record, store, interrupt and follow the communication without the consent of all parties to the communication. Traffic, location and personal data may be processed within the scope of examinations of subscriber/user complaints and auditing activities, limited to the specified activities.	
	Turkish Criminal Code (no. 5237, dated September 26, 2004)	**Article 135 and 136** define the act of unlawful record, delivery, and publication of personal data. **Article 138** defines the act of failure to destroy data in compliance with the timeline regulated by laws.	
UNITED ARAB EMIRATES *(updated June 2021)*	UAE Constitution (Federal Law No. 1 of 1971) UAE Penal Code (Federal Law No. 3 of 1987)	Article 8: guarantees the secrecy of communication by post, telegraph and other means. Article 379: Forbids an individual from disclosing any 'secrets' or personal information belonging to another person(s), unless with prior consent or lawful sanction. A breach of this Article is punishable by imprisonment of a minimum of one year, or a fine of a minimum of AED 20,000, or both. Article 377: Consent to disclose personal data is not required if information involving a crime is in good faith	James Berry & Associates Legal Consultants https://jamesberrylaw.com/ Tel: +971 4 3317552 Email: enquiries@jamesberrylaw.ae

		shared with the relevant authorities.	
	SFV Regulation	Article 10: All customer data is required to be stored as well as maintained in the UAE. Authority: UAE Central Bank oversees SVF	
	Federal Law on the Practice of Human Medicine Profession: (Federal Law No. 7 of 1975)	Forbids the medical practitioner from disclosing without consent, any 'secrets' that a patient has mentioned to them.	
	Federal Law by Decree 3 of 2003 as amended)	The Law regulating the Telecommunication sector: Article 72: Punishment of an individual who reveals the content of a call or message sent through the network. Authority: Telecommunications Regulatory Authority (TRA) oversees telecoms laws and licensees' communication with subscribers with regard to online marketing	
	Transfer (Telecommunications) TRA Consumer Protection Regulations v.1.5	Article 15.11.5 If a breach is reported and verified, the TRA will direct the service provider 'to undertake any remedy deemed reasonable and appropriate'. Article 20.8: If a third party is involved in data collection in the course of providing a telecommunications service, confidentiality and subscriber protection must be preserved.	
	Cyber Crime Law (Federal Law No. 5 of 2012)	Articles 12 and 22: Prohibit the use of cyber networks to access and divulge private information without authorization such as but not limited to: Medical records, electronic documents and financial information). If found guilty, the offender may face imprisonment for up to 1 year and/or a fine between AED 150,000 and 1,000,000. Online privacy is protected under this law.	
	ICT Health Law (Federal Law No. 2 of 2019)	Article 13: UAE origin Health data and information cannot be stored, processed, generated or transferred outside of the UAE, unless permission to do so is given by the Local or Federal Health Authority.	
	Dubai Data Law: Dubai Law No. 26 of 2015	Private data to be shared only between authorized individuals within the private sector. Provides a framework for companies to disseminate and exchange data and requires data providers to take all measures necessary to maintain privacy.	
	DHCC Health Data Protection Regulation (2013): DHCC Regulation No. 7 of 2013	Regulates licensees in their management of Patient Health information and requires that they comply with Health Data Protection Regulation rules. Regulation applies to the following information: (a) Information about the health of a patient (including medical history).	

	DIFC Data Protection Law: DIFC Law No. 5 of 2020 ADGM Data Protection Regulations 2021 Registration: Breach notification: GDPR:	(b) Information about a patient's disabilities. (c) Information about any healthcare services provided. (d) Information about a patient's body part donations Provides a framework of standards and controls for the processing of personal data by a Controller and protects the rights of data subjects in emerging technologies. Provide a basis for regulating Personal Data within ADGM and provide a means for individuals to register complaints about an alleged infringement of their rights There are no data protection registration requirements in the UAE. There are no mandatory requirements in the UAE to report data security breaches. However, data subjects are entitled to hold entities liable if loss or damage is suffered Companies that align with EU Laws are required to follow GDPR guidelines	
UNITED KINGDOM *(Updated Jun 2021)*	The UK GDPR (the UK's retained version of the EU General Data Protection Regulation 2016/679 (EU GDPR)). Data Protection Act 2018 (DPA).	The UK GDPR and DPA regulate the 'processing' of personal data in the context of the activities of an establishment of a controller or processor in the UK, regardless of whether the processing takes place in the UK or not. The UK GDPR sets out seven key principles that organisations should use as the foundations for their approach to the processing of any personal data. These are: · Lawfulness, fairness and transparency · Purpose limitation · Data minimisation · Accuracy · Storage limitation · Integrity and confidentiality (security) · Accountability ENGLAND: Mackrell. Solicitors has extensive experience in advising across a number of jurisdictions in relation to a wide range of data protection issues including: 1. Registration with the ICO and dealing with ICO investigations. 2. Privacy policies and data processing agreements. 3. Advising on subject access requests. 4. Dealing with data breaches.	**England:** **Mackrell. Solicitors** Maung Aye – Partner Mackrell. Solicitors Savoy Hill House Savoy Hill WC2R 0BU United Kingdom Email: Maung.Aye@mackrell.com Tel: +44 (0) 207 240 0521. www.mackrell.com **SCOTLAND:** **BTO Solicitors LLP** Paul Motion – Partner Level 2,Edinburgh Quay One, 133 Fountainbridge Edinburgh EH3 9QG Email: prm@bto.co.uk

		5. Advising on complex cross border data transfers issues. 6. Advising on regulatory issues connected with direct marketing. SCOTLAND: BTO Solicitors has unique experience in conducting DPA and PECR appeals before the Tribunal. BTO's Solicitor Advocate is an accredited data protection specialist.	Tel: 44 (0)131 222 2939 www.bto.co.uk
USA **(Federal)** *(Updated June 2021)*	**There is currently no comprehensive federal privacy or data security law in the United States. Rather, the landscape is comprised of a patchwork of sector-specific federal laws that apply to specific types of personal information and specific technologies, media or methods used to collect information. The primary federal laws are summarized below.**		
	Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506	Operators of websites and online services (including apps and connected products) directed to children under 13, and operators of general audience websites and online services with actual knowledge that they are collecting "personal information" (as defined in the Act) from children under 13 must: Post an online privacy policy; provide notice to parents and obtain verifiable parental consent before collecting "personal information" online from children; provide parents access to their children's personal information and an opportunity to prevent further use or collection of personal information; and maintain the confidentiality and security of personal information. Some exceptions apply. Safe harbour programs may be approved by the Federal Trade Commission (FTC).	**Keller and Heckman LLP** 1001 G Street, NW Suite 500 West Washington, DC 20001 Sheila A. Millar millar@khlaw.com Tel: (202) 434-4143 Tracy P. Marshall marshall@khlaw.com Tel: (202) 434-4234 www.khlaw.com
	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. §§ 7701–7713	Establishes labelling and opt-out requirements for commercial e-mail messages.	
	Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227	Restricts telemarketing calls, the use of automatic telephone dialing systems and artificial or prerecorded voice messages to send automated calls and text messages ("robocalls"), as well as unsolicited fax advertisements.	
	Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq., amended by Fair and Accurate Credit Transaction Act of 2003 (FACTA) FTC Red Flags Rule, 16 CFR 681.1	FCRA (1) requires consumer reporting agencies (CRAs) to adopt "reasonable procedures" to protect the confidentiality, accuracy, and relevancy of consumer credit information, (2) restricts the furnishing of consumer reports by CRAs except for specified permissible purposes, such as credit checking, offering employment, or issuing insurance, and (3) imposes obligations on users of consumer reports. Under FACTA, any entity that uses a consumer report for a business purpose is subject to the Disposal Rule. The FTC Red Flags Rule implements FACTA. "Financial institutions" and "creditors" with "covered accounts" must have written identity theft prevention programs.	
	Gramm-Leach-Bliley (GLB) Act, 15 U.S.C. § 6801	Governs the privacy and security of non-public personal information (NPI) held by financial institutions. Limits reuse and disclosure of NPI obtained from a financial institution.	

	Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1320d Health Information Technology for Economic and Clinical Health (HITECH) Act 42 U.S.C. § 17938	Governs the privacy and security of sensitive health data. Covered entities (health plans, health care clearinghouses, and certain health care providers) must adopt administrative, technical, and physical security measures to protect health information. The HITECH Act requires breach notifications; HIPAA covered entities must notify affected individuals and business associates must notify covered entities.	
	Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-22 Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030	Title I of ECPA (Wiretap Act) prohibits the interception of wire, oral, or electronic communications. Title II (Stored Communications Act) protects communications in electronic storage, notably, messages stored on computers. The CFAA makes it a criminal offense to access a protected computer "without authorization."	
	Stored Communications Act of 1986, 18 U.S.C. §§ 2701-2712	Governs the storage of electronic communication data by Internet Service Providers and specifies when a warrant must be obtained, or when a subpoena or court order will suffice.	
	Federal Trade Commission Act (FTCA), 15 U.S.C. 41 et seq.	The FTC's jurisdiction extends to any entity engaged in commerce, except banks, savings and loan institutions, federal credit unions, air carriers, meatpackers and poultry dealers, and common carriers (but only when engaged in common carrier activity). The FTC has general authority to halt unfair and deceptive acts and practices in commerce. Failure to adhere to privacy and security promises or false representations (such as misrepresentations regarding participation in a privacy safe harbor like the EU-U.S. Privacy Shield) has been actionable as a deceptive practice.I Inadequate security practices have also been enforced under the FTC's deception and unfairness authority.	
	National Labor Relations Act (NLRA), 29 U.S.C. § 151–169	Prohibits actions by employers that interfere with employee protected activities, e.g., the right to form a union. The National Labor Relations Board has struck down all or portions of employer social media policies for infringing on these rights.	
USA (Alabama) *(updated JUN2021)*	Alabama Data Breach Notification Act Ala. Code §§ 8-38-1 to 8-38-12	**Data Breach Notification:** If a data breach is reasonably likely to cause substantial harm to individuals, then notice must be provided expediently and without unreasonable delay, but within 45 days, subject to the needs of law enforcement. Baker Donelson's Data Protection, Privacy, and Cybersecurity Team is highly skilled in all areas of privacy and security – from information governance to compliance to data incident responses, crisis management, and defense. We provide our clients with concise counsel and resources designed to address the entire information lifecycle and develop practical privacy management programs. More than one-third of our team is credentialed with the world's largest privacy organization, the International Association of Privacy Professionals (IAPP) in U.S., European, and Canadian privacy laws. We provide thoughtful, comprehensive and dependable guidance to our	**Baker, Donelson, Bearman, Caldwell & Berkowitz PC** Alex Koskey, CIPP/US, CIPP/E, PCIP Shareholder akoskey@bakerdonelson.com Tel: (404) 443-6734 3414 Peachtree Road NE Suite 1500 Atlanta, GA 30326 www.bakerdonelson.com

		clients across multiple industries regarding their data privacy obligations along with real-time legal and technical advice for data incidents and breach response.	
USA (Arizona)	Arizona Revised Statutes 18-551, -552 Family Education Rights and Privacy Act 20 USC 1232g	Arizona Revised Statutes 18-551 and -552 identify the obligations of a business, political subdivision or organization that maintains personal information of Arizona residents. An entity experiences a data breach when there is an unauthorized acquisition and access that materially compromises the personal information of multiple individuals. Arizona law defines "personal information" as first name and last name plus an email account or username and password or security question answer. An entity that has experienced a possible data breach is required to conduct a reasonable investigation to determine whether a breach occurred and notify affected persons with 45 days of such a determination. If more than 1000 individuals are affected by the breach, the entity must report the incident to the 3 major credit bureaus and the Arizona Attorney General's office. The notification to affected persons may be delayed at the direction of law enforcement. Gust Rosenfeld assists business and public entities with potential data breaches to comply with obligations of Arizona law and applicable federal law.	Gust Rosenfeld Robert Haws rhaws@gustlaw.com 602.257.7976 Carrie O'Brien cobrien@gustlaw.com Tel: 602.257.7414 Bill Sowders wsowders@gustlaw.com Tel: 602.257.7478 One E. Washington Street, Suite 1600 Phoenix, AZ 85004 www.gustlaw.com
USA (California) *(Updated JUN2021)*	California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §§ 1798.100 – 1798.199.100 California Privacy Rights and Enforcement Act of 2020 ("CPRA"), amends and expands the CCPA and goes into effect Jan. 1, 2023 California Electronic Communications Privacy Act ("CalECPA"), Cal. Penal Code §§ 1546, et seq. The California Online Privacy Protection Act (CalOPPA), Cal. Bus. & Prof. Code §§ 22575-22579 California Data Breach Notification Statute, Cal. Civ. Code §§ 1798.80 - 1798.84 California Shine the Light Law, Cal. Civ. Code § 1798.83	Headquartered in Silicon Valley, Hoge Fenton has been involved in U.S. privacy and data security since California enacted the first U.S. data breach notification law in 2003. Hoge Fenton has been in the trenches handling data breach crises, developing compliance programs and strategies, and keeping companies in defensible positions. We eagerly share our knowledge on the continuously evolving landscape of data privacy with audiences worldwide. **Video**: ***California Consumer Privacy Act: What You Need to Know*** - Data breach crisis management - Processing subpoenas, search warrants, electronic surveillance, other court orders - Compliance programs and impact assessments - Executive and workforce training • Company policies and procedures: privacy policies, info security plans, records management, data minimization, MDM, BYOD, data breach incident response, etc. - Data hosting, transfer and processing agreements under GDPR, HIPAA, CCPA/CPRA, etc. - Legal/litigation hold implementation - Representation before regulatory agencies - Alternative dispute resolution and litigation	**Hoge Fenton Jones & Appel** Stephanie O. Sparks, Chair, Privacy & Data Security Group 55 South Market St. Suite 900 San Jose, CA 95113-2324 Stephanie.Sparks@hogefenton.com Tel: (408) 947-2431 www.hogefenton.com

	And substantial experience representing online service providers under U.S. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2523, and U.S. Stored Communications Act, 18 U.S.C. §§ 2701-2713.		
USA (Colorado) *(Updated Jun2021)*	Notification of Security Breach, C.R.S. §6-1-716 (Effective September 1, 2018) Protection of personal identifying information, C.R.S. § 6-1-713.5	Among other things, Colorado's data breach notification law requires (1) notice to affected Colorado residents; (2) notice to the Colorado attorney general if the data breach affects more than 500 Colorado residents; (3) notice must be provided within 30 days of determining a security breach occurred via either written, telephonic, or electronic means; (4) imposes content requirements for the notice to residents; and (5) establishes data security requirements applicable to business and their third-party service providers. The statute applies to any individual or commercial entity (collectively "entity") that conducts business in Colorado and that owns, licenses, or maintains computerized data that includes personal information. Personal Information is defined as a Colorado resident's first name or first initial and last name in combination with one or more of the following data elements: (1) Social Security Number (2) Student, Military, or Passport Identification Number (3) Driver's License Number or Identification Card Number (4) Medical Information (5) Health Insurance Identification Number (6) Biometric Data Personal Information also includes a resident's username or email address, in combination with a password that would permit access to an online account or and account number or credit card number in combination with any required security code, access code, or password that would permit access to that account. Notice to affected Colorado residents of a data breach must include the following: (1) the date, estimate date, or estimated date range of the breach; (2) a description of the Personal Information acquired; (3) contact information for the entity; (4) the contact information for consumer reporting agencies and the FTC;	Danny Foster Foster, Graham, Milstein & Calisher, LLP Tel: 303-333-9810

		(5) a statement that the Colorado resident can obtain information from the FTC and credit reporting agencies about fraud alerts and security freezes (6) if the breach involves a username or email address in combination with a password or security questions/answers, the entity must direct affected individuals to promptly change their password and security questions/answers, or to take other steps to protect the online account with the entity and all other online accounts for which the resident used the same or similar information. Entities must implement and maintain "Reasonable security procedures and practices" to protect personal information that are appropriate to "the nature and size of the business and its operations." An entity that fails to comply with these statutes may be subject to civil actions by the Colorado Attorney General.	
USA (Connecticut) *(updated June 2021)*	Social Security Number and Personal Information Protection Laws (*CGS 42-470; 42-471*) Data Breach Notification Law (*CGS 36a-701b*) Data Security Laws (*CGS 4e-70; 38a-38*) Student Data Privacy	The handling of Social Security Numbers by any individual or entity is strictly limited; businesses are required to create and publicly display a privacy protection policy. Specified personal information must be safeguarded and disposed of securely by both individuals and entities, subject to civil and criminal penalties. Subject to limited exception, the loss of unencrypted, "personal information" by a business triggers notice to affected individuals and to the Attorney General without unreasonable delay, not later than 60 days from discovery. Personal information includes first name/first initial and last name plus any: • Social Security or taxpayer ID number • IRS-issued identity theft protection ID number • Driver's license / state ID number • Passport/military/other government ID number • Credit card or financial account access numbers • Medical information / health insurance plan numbers • Biometric ID information Personal information also includes online account login credentials such as user name/e-mail address plus password or security question answer. For breaches involving Social Security or taxpayer ID numbers, entities must offer at least 24 months of identity theft prevention and mitigation services. Compliance with security rules of applicable federal regulations will be deemed compliance with state breach notification law, except that notification to Attorney General is still required. Breach investigation materials turned over in response to the Attorney General's investigative demand are exempt from public disclosure under the state Freedom of Information Act. State contractors, insurance businesses, and school boards must implement and maintain written information security programs and conduct annual cybersecurity assessments. Insurance businesses must annually certify	**Carmody Torrance Sandak & Hennessey LLP** Sherwin Yoder, Esq., CIPP/US, CIPP/E, CIPP/M Carmody Torrance Sandak & Hennessey LLP syoder@carmodylaw.com Tel: (203) 777-5501 195 Church Street, New Haven, Connecticut 06509 www.carmodylaw.com

	Act (*CGS 10-234aa*) Computer Crimes Act (*CGS 53a-251; 52-570b*)	under oath that such program is being updated and maintained. School board contracts with service providers must be published and contain specified student privacy provisions. Unauthorized access to, or use of, computerized data, or knowing receipt of such data, by any individual or entity, is subject to criminal and civil liability, including treble damages and attorney's fees.	
USA (District of Columbia) *(Updated June 2021)*	Security Breach Notification and Security Requirements, D.C. Code §§ 28-3851 et seq.	**Data Breach Notification:** Notification of a security breach must be made to affected D.C. residents in the most expedient time possible and without unreasonable delay. If 50 or more D.C. residents are affected, notice must also be provided to the Office of the Attorney General no later than when notice is provided to residents. The law specifies content that must be included in notices. If more than 1,000 residents must be notified, then all national consumer reporting agencies must also be notified. A security breach is defined as the unauthorized acquisition of electronic data, or any equipment or device storing such data, that compromises the security, confidentiality, or integrity of personal information. Personal information is defined to include: • An individual's first name, first initial and last name, or any other identifier, which, in combination with any of the following, can be used to identify a person: Social security number, passport number, driver's license number, or other unique identification number; account number, credit card number or debit card number, or any other number or code that allows access to or use of an individual's financial or credit account; medical information; genetic information; health insurance information; and biometric data. • A username or email address plus a password, security question and answer, or any combination of data elements that permits access to an individual's e-mail account. **Data Security:** Any person or entity that owns, licenses, maintains, or otherwise possesses personal information of D.C. residents must implement and maintain reasonable security safeguards, and entities that contract with service providers must require service providers to implement reasonable security procedures and practices.	**Keller and Heckman LLP** 1001 G Street, NW Suite 500 West Washington, DC 20001 Sheila A. Millar millar@khlaw.com Tel: (202) 434-4143 Tracy P. Marshall marshall@khlaw.com Tel: (202) 434-4234 www.khlaw.com
USA (Florida) *(updated JUN2021)*	§ 501.171, Fla. Stat.	Florida's data breach notification law applies to most commercial and governmental entities that acquire, maintain, store, or use personal information. The statute imposes obligations on any person or entity that maintains computerized data that includes personal information on behalf of another business entity. The statute requires notification to affected persons regarding unauthorized access to computerized data containing personal information. The notice must include	**Zimmerman Kiser & Sutcliffe, P.A.** Bill Robbinson brobbinson@zkslawfirm.com Erin Gray

		statutory requirements and must be provided without unreasonable delay, but no later than 30 days after determining the breach. If the breach affects 500 or more individuals, notice must also be provided to the Florida Department of Legal Affairs no later than 30 days after determining a breach has occurred. Upon certain conditions, Covered Entities may opt out of providing notice after consultation with law enforcement and a reasonable determination that the breach will not likely lead to identity theft or financial harm.	egray@zkslawfirm.com Tel: (+1) 407 425 7010 Zimmerman Kiser & Sutcliffe assists clients addressing data security issues as part of M&A transactions, services and license agreements, and data processing agreements. ZKS also assists with investigations, notification requirements and other compliance and mitigation issues with § 501.171, Fla. Stat.
USA (Georgia) *(updated JUN2021)*	Georgia Data Breach Notification Law Ga. Code Ann. §§ 10-1-911, 10-1-912	**Data Breach Notification:** Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay. Baker Donelson's Data Protection, Privacy, and Cybersecurity Team is highly skilled in all areas of privacy and security – from information governance to compliance to data incident responses, crisis management, and defense. We provide our clients with concise counsel and resources designed to address the entire information lifecycle and develop practical privacy management programs. More than one-third of our team is credentialed with the world's largest privacy organization, the International Association of Privacy Professionals (IAPP) in U.S., European, and Canadian privacy laws. We provide thoughtful, comprehensive and dependable guidance to our clients across multiple industries regarding their data privacy obligations along with real-time legal and technical advice for data incidents and breach response.	**Baker, Donelson, Bearman, Caldwell & Berkowitz PC** Alex Koskey, CIPP/US, CIPP/E, PCIP Shareholder akoskey@bakerdonelson.com Tel: (404) 443-6734 3414 Peachtree Road NE Suite 1500 Atlanta, GA 30326 www.bakerdonelson.com
USA **(Illinois)**		Illinois led the way in consumer privacy as the second US state to pass a consumer information protection act in 2005 with the Personal Information Protection Act ("PIPA"). PIPA required data collectors to use reasonable means of protection and inform consumers of any known breaches. Post-GDPR, Illinois followed with three attempts of consumer-driven privacy legislation, the foremost being the 2020 Data Transparency Privacy Act. While the Act took a backseat during the pandemic and is now tabled indefinitely, the Illinois House introduced two new Consumer Privacy bills in February, 2021. The first bill, HB2404 gives consumers the right the right to know a business's data collection habits and entitles consumers to the contact information of third parties to whom businesses have sold their information. HB3910, aka the Consumer Privacy Act, is a modified version of the California CPA. Both bills currently await review by the Rules Committee. Kelleher + Holland LLC stands ready to assist with Illinois compliance in the event these bills become law.	**Kelleher & Holland LLC** Douglas Hanson dhanson@kelleherholland.com Tel: (+1) 847 852 1169 102 S. Wynstone Park Drive North Barrington, Illinois 60010

USA **(Indiana)** *(updated JUN2021)*	Disclosure of Security Breach, Indiana Code §§ 24-4.9-1-1 to 24-4.9-5-1. Right of Inspection and challenge by Data Subject or Agent Indiana Code §4-1-6-3, 5 User Data Held in Electronic Storage Indiana Code §35-33-5-11	When a data breach occurs, we respond quickly to help clients secure data, notify law enforcement and government agencies, communicate with affected individuals and businesses, conduct forensic investigations and prevent future breaches. Our attorneys collaborate with qualified IT consultants and provide access to the award-winning Strategic Communications Group of our affiliate, Bose Public Affairs Group. The Data Privacy Group's first priority is containing data breach damage and expense. After a breach is managed, we can represent your organization in litigation or government investigations that follow. Ideally, we work proactively to advise on prevention and insurance. We assist clients with • Corporate information management programs • Crisis communications • Reputation management • Investigations, in cooperation with forensic firms • Incident response plans • Insurance policy reviews / recommendations • Litigation • Mitigation • Notification to affected entities • Notification to proper agencies • Privacy policies • HIPAA compliance • Security filing disclosures	**Bose McKinney & Evans LLP** Brian Jones b.jones@boselaw.com Tel: 317-684-5462 Craig Pinkus cpinkus@boselaw.com Tel: 317-684-5358 111 Monument Circle, Suite 2700 Indianapolis, IN 46204 USA www.boselaw.com
USA **(Kansas)** *(Updated Jun 2021)*	Personal Information Protection Law – K.S.A. § 50-6,139b Security Breach Notification – K.S.A. §§ 50-7a01 through 50-7a04	Kansas requires any person who in the ordinary course of business collects, maintains, or possesses, or causes to be collected, maintained, or possessed, any other person's personal information to (1) implement and maintain reasonable procedures and practices appropriate to the information's nature, (2) exercise reasonable care to protect the personal information from unauthorized access, use, modification, or disclosure, and (3) unless federal law or regulation otherwise requires, take reasonable steps to destroy or arrange for the destruction of any records that contain personal information that are within the person's custody or control when the person no longer intends to maintain or possess such records. Record destruction shall be by shredding, erasing, or otherwise modifying the personal identifying information in the records to make the	**Sandberg Phoenix & von Gontard PC** Timm Schowalter, CIPP/US tschowalter@sandbergphoenix.com Tel: (+1) 314 231 3332 600 Washington Ave. – 15th Floor St. Louis, Missouri 63101 www.sandbergphoenix.com

		information unreadable or undecipherable through any means. Additionally, Kansas law requires any person who conducts business in the State and who owns or licenses computerized data that includes personal information to conduct good faith investigations into the likelihood that personal information has been or will be misused when the person becomes aware of any breach of the system's security. The person must notify the affected Kansas resident without unreasonable delay and as soon as possible if the investigation reveals personal information has been or is likely to be misused. Additionally, Kansas law requires the person to notify all nationwide consumer reporting agencies of the security breach when the breach requires more than 1,000 consumers at a time to be notified. Keep in mind law enforcement may determine the best course of action is to delay notice to a consumer if notice could impede a criminal investigation. Sandberg Phoenix's Cybersecurity & Privacy Risk Management litigation team is a collective of highly experienced litigators that represents organizations, insurers, and reinsurers throughout the United States in complex litigation, including class actions, involving civil claims and government enforcement actions under specific privacy laws, FTC Act, HIPAA/HITECH, FCRA, GLBA, FIRREA, Dodd-Frank, FACTA, FERPA, CAN-SPAM, VPPA, and GDPR (EU), and Illinois Biometric Information Privacy Act, state data breach notification and disposal laws, misappropriation of trade secrets, nondisclosure and noncompete agreements, computer tampering, copyright trademark and patent infringement, common law privacy tort claims, and breach of contract claims related to cyber agreements and addenda.	
USA (Louisiana) *(updated JUN2021)*	Database Security Breach Notification Law LSA-R.S. §§ 51:3071 to 51:3077	**Data Breach Notification:** Notification must be provided in the most expedient time possible and without unreasonable delay but not later than sixty days from the discovery of the breach. Notification may be delayed if law enforcement determines that notification would impede a criminal investigation. Baker Donelson's Data Protection, Privacy, and Cybersecurity Team is highly skilled in all areas of privacy and security – from information governance to compliance to data incident responses, crisis management, and defense. We provide our clients with concise counsel and resources designed to address the entire information lifecycle and develop practical privacy management programs. More than one-third of our team is credentialed with the world's largest privacy organization, the International Association of Privacy Professionals (IAPP) in U.S., European, and Canadian privacy laws. We provide thoughtful, comprehensive and dependable guidance to our clients across multiple industries regarding their data privacy obligations along with real-time legal and technical advice for data incidents and breach response.	**Baker, Donelson, Bearman, Caldwell & Berkowitz PC** Alex Koskey, CIPP/US, CIPP/E, PCIP Shareholder akoskey@bakerdonelson.com Tel: (404) 443-6734 3414 Peachtree Road NE Suite 1500 Atlanta, GA 30326 www.bakerdonelson.com

USA (Maryland) *(Updated June 2021)*	Security Breach Notification and Security Procedures, MD Code Com. Law §§ 14-3501 et seq.	**Data Breach Notification:** Notification of a security breach must be given to affected Maryland residents as soon as reasonably practicable, but not later than 45 days after discovery, and the Office of the Attorney General must be notified before residents. The law specifies content that must be included in notices to residents, and provides an alternative process for notifying residents if a breach only involves personal information that permits access to an individual's email account and no other personal information. If more than 1,000 residents must be notified, then all national consumer reporting agencies must also be notified. A security breach is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. Personal information is defined to include: • An individual's first name or first initial and last name plus any of the following, when the name or the data elements are not encrypted, redacted, or protected: Social Security number, passport number, or other identification number issued by the federal government; driver's license number or state identification number; account number, a credit card number, or a debit card number plus any required code or password; health information; health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier; or biometric data. • A user name or email address plus a password or security question and answer that permits access to an individual's e-mail account. **Data Security:** Any business that owns or licenses personal information of a Maryland resident must implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information and the nature and size of the business. In addition, a business that contracts with a service provider that will acquire personal information must require the service provider to implement and maintain reasonable security procedures and practices.	**Keller and Heckman LLP** 1001 G Street, NW Suite 500 West Washington, DC 20001 Sheila A. Millar millar@khlaw.com Tel: (202) 434-4143 Tracy P. Marshall marshall@khlaw.com Tel: (202) 434-4234 www.khlaw.com
USA (Massachusetts) *(updated*	HIPAA: Pub.L. 104–191 GLB Act: Pub.L. 106-	*The United States does not recognize a fundamental right to data privacy. Federally, the US has a patchwork of privacy laws mostly covering specific industries (e.g., health care, financial services, education) or classes of*	**Gesmer Updegrove LLP** Joseph Laferrera Joe.Laferrera@gesmer.com

JUN2021)	102 COPPA: 15 USC 91 Massachusetts Data Breach Notification Law: MGH c. 93H Massachusetts Data Privacy Regulation: 201 CMR §17	*individuals (e.g., children under 13, drivers, recipients of commercial email). In addition, individual states may enact their own privacy laws if they are not inconsistent with federal mandates. For example, most states have laws requiring notification of data subjects in the event of breaches involving their "personally identifiable information" ("PII"). PII is defined much more narrowly than the GDPR's concept of "personal data," and is often limited to full name paired with financial account numbers or governmental identifiers. Some states go much further. Massachusetts has a broad mandate regarding the use and storage of PII, and California has enacted a regulatory scheme similar to the GDPR.*	Tel: (+1) 617 350 6800 40 Broad Sreet Boston MA 02109 www.gesmer.com
USA (Mississippi) *(updated JUN2021)*	Mississippi Data Breach Notification Law Miss. Code Ann. § 75-24-29	**Data Breach Notification:** If required, disclosure must be made without unreasonable delay subject to the needs of law enforcement and to the completion of an investigation by the person to determine the nature and scope of the incident. Baker Donelson's Data Protection, Privacy, and Cybersecurity Team is highly skilled in all areas of privacy and security – from information governance to compliance to data incident responses, crisis management, and defense. We provide our clients with concise counsel and resources designed to address the entire information lifecycle and develop practical privacy management programs. More than one-third of our team is credentialed with the world's largest privacy organization, the International Association of Privacy Professionals (IAPP) in U.S., European, and Canadian privacy laws. We provide thoughtful, comprehensive and dependable guidance to our clients across multiple industries regarding their data privacy obligations along with real-time legal and technical advice for data incidents and breach response.	**Baker, Donelson, Bearman, Caldwell & Berkowitz PC** Alex Koskey, CIPP/US, CIPP/E, PCIP Shareholder akoskey@bakerdonelson.com Tel: (404) 443-6734 3414 Peachtree Road NE Suite 1500 Atlanta, GA 30326 www.bakerdonelson.com
USA **(Missouri)** *(Updated Jun 2021)*	Security Breach Notification – R.S.Mo. § 407.1500	Missouri requires any person or business that owns or licenses Missouri residents' personal information to notify a consumer that there has been a security breach following discovery or notification of the breach. The disclosure notification must be (1) made without unreasonable delay, (2) consistent with law enforcement's needs, and (3) consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the data system's reasonable integrity, security, and confidentiality. Similarly, any person or business that maintains or possesses records or data containing Missouri residents' personal information that the person or business does not own or license must notify the owner or licensee of the information of any security breach	**Sandberg Phoenix & von Gontard PC** Timm Schowalter, CIPP/US tschowalter@sandbergphoenix.com Tel: (+1) 314 231 3332 600 Washington Ave. – 15th Floor St. Louis, Missouri 63101 www.sandbergphoenix.com

		immediately following the breach's discovery consistent with law enforcement's legitimate needs. In either case, the notice may be delayed if a law enforcement agency informs the person that notification may impede a criminal investigation or jeopardize national or homeland security. Sandberg Phoenix's Cybersecurity & Privacy Risk Management litigation team is a collective of highly experienced litigators that represents organizations, insurers, and reinsurers throughout the United States in complex litigation, including class actions, involving civil claims and government enforcement actions under specific privacy laws, FTC Act, HIPAA/HITECH, FCRA, GLBA, FIRREA, Dodd-Frank, FACTA, FERPA, CAN-SPAM, VPPA, and GDPR (EU), and Illinois Biometric Information Privacy Act, state data breach notification and disposal laws, misappropriation of trade secrets, nondisclosure and noncompete agreements, computer tampering, copyright trademark and patent infringement, common law privacy tort claims, and breach of contract claims related to cyber agreements and addenda.	
USA (Nevada) *(Updated Jun2021)*	Security and Privacy of Personal Information Act Nev. Rev. Stat. §§ 603A.010-.360	Nevada's privacy laws are contained in Nevada Revised Statutes ("NRS") Chapter 603A (Security and Privacy of Personal Information). Although Nevada does not have a significant amount of law concerning privacy, it continues to grow and evolve, with amendments adopted as recently as 2019. Generally, Nevada requires any "operator" or "data collector" to implement and maintain security measures to protect data from unauthorized access, acquisition, destruction, use or modification. NRS 603.210(1). An "operator" means a person who owns or operates an Internet website for commercial purposes, collecting and maintaining covered information from consumers who reside in Nevada or visit the online service. NRS 603A.330. Exceptions to the definition, include, but are not limited to, financial institutions or affiliates subject to the Gramm-Leach-Blilely Act. or entities subject to HIPAA. Nor do they apply if the operator is located in Nevada, deriving its revenue primarily from a source other than the sale or lease of goods, services, or credit on internet websites, and whose online service has fewer than 20,000 unique visitors per year (NRS 603A.340(3)(c)).	**Kaempfer Crowell, Ltd.** Steven E. Tackes stackes@kcnvlaw.com 1980 Festival Plaza Dr., Suite 650, Las Vegas, NV 89135-2958 Tel: (1) 702 792 7000 www.kcnvlaw.com
USA (New York) *(Updated Jun2021)*	New York State Information Security Breach and Notification Act, NY CLS Gen Bus § 899-aa (as amended by the Stop Hacks and Improve Electronic Data Security Handling ("SHIELD") Act, effective October 23, 2019 in part, and March 21, 2020 in part, NY CLS Gen Bus § 899-bb) NY DFS	**Data Breach Notification:** Any person or business that owns or licenses private information, as defined in the statute (including biometric data) concerning a New York resident is required to disclose a breach of security of such information in the most expedient time possible and without unreasonable delay to the affected persons (and others, under certain circumstances). **Data Security Protections:** Applicable persons and businesses will be required to implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of private information, including implementing administrative, technical and physical safeguards (some detail about what this program must include is dictated by statute). Those persons required to, and who actually, comply with security requirements of under HIPAA, GLBA, or the NY Department of Financial	**Morrison Cohen LLP** Jessica L. Lipson, Partner jlipson@morrisoncohen.com Tel: (212) 735-8683 Morrison Cohen LLP 909 Third Avenue New York, NY 10027 https://www.morrisoncohen.com/

	Cybersecurity Regulation, 23 NYCRR 500	Services ("DFS") Cybersecurity Regulation, 23 NYCRR 500, are considered compliant with the statute. There is no private cause of action under this law but any person who fails to comply will be deemed to have violated section 349 of the NY General Business Law (generally regulating deceptive acts or practices in business in New York State). **The DFS Cybersecurity Regulation:** requires Covered Entities (as defined therein – generally including banks, money services businesses and insurance companies, among others) to maintain a written cybersecurity program designed to protect the confidentiality, integrity and availability of its information systems and the non-public information stored therein. There are specific requirements in the regulation pertaining to the contents of the program (e.g., the program must be based on risk assessments, and address areas such as information security, data governance and classification, asset inventory and device management, access controls and identity management; business continuity and disaster recovery planning and resources, systems and networks operations, monitoring and security, physical security and environmental controls, customer data privacy; vendor management, and incident response), training and how the program must be managed and by whom. Covered Entities must notify DFS within 72 hours if a determination is made that a cybersecurity event (e.g., a breach) has occurred.	
USA (North Carolina) *(Updated June 2021)*	Identity Theft Protection Act N.C. Gen. Stat. §§ 75-60 to -66	**Data breach notification:** Any person or business that owns or licenses personal information of North Carolina residents, whether computerized, on paper, or otherwise, shall provide notice of a security breach (defined as the unauthorized access to and acquisition of unencrypted and unredacted personal information) without unreasonable delay subject to the legitimate needs of law enforcement. The notice shall include: descriptions of the incident in general terms, the type of personal information involved, and the acts taken to protect the information from further unauthorized access; a telephone number for the business; advice to remain vigilant by reviewing account statements and monitoring free credit reports; and contact information for the Federal Trade Commission and the North Carolina Attorney General's Office. Notice must also be provided to the Consumer Protection Division of the North Carolina Attorney General's Office. **Social Security Number Protection:** Prohibits businesses from communicating, printing, imbedding, or requiring a consumer to disclose or transmit a social security number except under certain circumstances as defined by statute. **Destruction of Personal Information Records:** Any business that conducts business in North Carolina or maintains personal information of North Carolina residents must take reasonable measures to protect against unauthorized access or use of such information in connection with or after its disposal. A business that retains the services of a records-disposal business must first conduct due diligence. A violation of this section is a violation of N.C. Gen. Stat. § 75-1.1 (Unfair Trade Practices), except that damages will not be trebled for actions of non-managerial employees unless the business was negligent in training or supervising them. **Publication of Personal Information:** It is a violation of this statute to publish in any form the personal information of another with knowledge that the person has objected to	**Nexsen Pruet** Kirsten Small, Member Certified Information Privacy Professional (CIPP) / US 104 South Main St. Suite 900 Greenville, SC 29601 ksmall@nexsenpruet.com Tel: 864-370-2211 www.nexsenpruet.com

		the disclosure of the information. Violators are subject to civil liability under N.C. Gen. Stat. 1-539.2C (Damages for Identity Theft).	
USA **(Ohio)** *(Updated July 2021)*	Ohio Rev. Code § 1349.19 (private entities); § 1347.12 (public agencies)	**This summary focuses on the law for private entities:** • Personal information is defined as an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements: (i) Social security number; (ii) Driver's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account. • This definition of personal information only applies to "when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable." • A "breach" is defined as "unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state." • Any entity that owns or licenses computerized data that includes personal information must disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident whose personal information was part of the breach within the most expedient time possible, but not later than forty-five days following its discovery or notification of the breach in the security of the system. • The timing of the notification is "subject to the legitimate needs of law enforcement activities . . . and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system." • Notification can be given by (1) Written notice, (2) Electronic notice, or (3) Telephone notice. Substitute notice is also available if certain thresholds as to cost or number of residents to receive notice is met. • For breaches that involve more than 1,000 residents, notification to credit reporting agencies is also required. • The Ohio Attorney General is authorized to investigate any breach and to bring a civil action for any alleged failure to comply with this statute.	**Roetzel & Andress** 222 South Main Street Akron, OH 44308 Chad L. Mowery cmowery@ralaw.com (330) 849-6782 www.ralaw.com
USA **(South Carolina)** *(Updated June 2021)*	S.C. Code Ann. § 39-1-90 (Security Breach Notification) S.C. Code Ann. §§ 38-99-10 to -100	**Security Breach Notification:** Any person or business that owns or licenses personal identifying information of South Carolina residents that suffers a breach of the security of the system (i.e., unauthorized access to and acquisition of computerized information not rendered unusable through encryption or redaction) shall provide	**Nexsen Pruet** Kirsten Small, Member Certified Information Privacy Professional (CIPP) / US 104 South Main St.

	(Insurance Data Security Act)	notice when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. If notice is provided to more than 1,000 South Carolina residents, the business must also notify, without unreasonable delay, the Consumer Protection of the Department of Consumer Affairs. **Insurance Data Security Act:** Requires licensed insurers in South Carolina to adopt data security measures commensurate with the size, complexity, and nature of the licensee's business, and sets certain minimum requirements for such programs. Specifies requirements for investigating potential cybersecurity events and establishes notification requirements if an event has occurred. Provides the Director of Insurance with the power and authority to investigate licensees to identify violations of the Chapter. Violations are subject to administrative penalties.	Suite 900 Greenville, SC 29601 ksmall@nexsenpruet.com Tel: 864-370-2211 www.nexsenpruet.com
USA (Tennessee) *(updated JUN2021)*	Tennessee Data Breach Notification Law T.C.A. §§ 47-18-2107 to 47-18-2105	**Data Breach Notification:** Notification must be provided immediately, but not later than 45 days from the discovery or the notification of the breach. Baker Donelson's Data Protection, Privacy, and Cybersecurity Team is highly skilled in all areas of privacy and security – from information governance to compliance to data incident responses, crisis management, and defense. We provide our clients with concise counsel and resources designed to address the entire information lifecycle and develop practical privacy management programs. More than one-third of our team is credentialed with the world's largest privacy organization, the International Association of Privacy Professionals (IAPP) in U.S., European, and Canadian privacy laws. We provide thoughtful, comprehensive and dependable guidance to our clients across multiple industries regarding their data privacy obligations along with real-time legal and technical advice for data incidents and breach response.	**Baker, Donelson, Bearman, Caldwell & Berkowitz PC** Alex Koskey, CIPP/US, CIPP/E, PCIP Shareholder akoskey@bakerdonelson.com Tel: (404) 443-6734 3414 Peachtree Road NE Suite 1500 Atlanta, GA 30326 www.bakerdonelson.com
USA **(Texas)** Notification Required Following Breach of Security of Computerized Data, Tex. Bus & Com. Code §521.002, et seq. (updated eff. Sept. 1, 2012)	Persons or entities in or doing business in Texas that own or license computerized data that includes sensitive personal information (SPI) must comply with the law's notification requirements after learning of a breach. Notification Required Following Breach of Security of Computerized Data Tex. Bus & Com. Code §521.002, et seq.	**Privacy Breach Notification**: Disclosure must be made "without unreasonable delay **and** in each case not later than the 60th day after the date on which the person determines that the breach occurred." Notice to the Texas AG is required if the breach involves 250 or more Texas residents. Penalty for failure to notify is up to $100.00 per individual per day of delay, not to exceed $250,000 per breach. Scheef & Stone's Privacy & Data Security Practice includes attorneys with years of experience in data protection and privacy issues. Our team regularly advises clients throughout the entire information lifecycle to assist in domestic and international compliance, including conducting privacy audits, creating privacy policies and website terms of use, negotiating and mitigating data privacy risk in commercial contracts and corporate transactions, as well as representing clients in litigation.	**Scheef & Stone LLP** Tom Kulik Partner, Scheef & Stone, L.L.P. Shawn.Tuma@solidcounsel.com Phone: 214-706-4223 Dallas: 500 N Akard, Suite 2700 Dallas, TX 75201 Frisco: 2600 Network Blvd., Suite 400, Frisco, Texas 75034 www.solidcounsel.com

USA (Virginia) *(Updated June 2021)*	Virginia Consumer Data Protection Act (S.B. 1392)	On March 2, 2021, the Commonwealth of Virginia became the second U.S. state to enact a comprehensive privacy law for its residents, the Consumer Data Protection Act (CDPA). The CDPA will take effect on January 1, 2023. The CDPA applies to businesses that operate in Virginia or offer products or services that are targeted to Virginia residents, and (1) in any calendar year, control or process personal data of at least 100,000 residents, or (2) control or process personal data of at least 25,000 residents and derive more than 50% of gross revenue from the sale of personal data. The CDPA does not apply to employee data. The CDPA provides several rights to consumers and imposes obligations on data controllers and processors that handle personal data. Personal data is any information that is linked or reasonably linkable to an identified or identifiable natural person. Consumers have the right to access, correct, delete, or obtain a copy of their personal data and the right to opt out of (1) the processing of personal data for the purposes of targeted advertising, (2) the sale of personal data, or (3) profiling. The CDPA allows for a parent or legal guardian to invoke these rights on behalf of a child (i.e., an individual under age 13). Data controllers must provide a privacy notice that describes the categories of personal data processed, the purposes for processing data, how consumers can exercise their rights, the categories of personal data shared with third parties, the categories of third parties with whom personal data is shared, and how consumers can opt out of the sale of personal data to third parties or the processing of personal data for targeted advertising (if applicable). Controllers are also required to establish, implement, and maintain reasonable security practices to protect personal data. In addition, controllers are required to conduct and document a data protection assessment in certain circumstances. Processors are required to assist controllers in meeting their obligations, controllers must have contracts in place with processors that impose specific requirements. The Virginia Attorney General has exclusive authority to enforce violations of the CDPA; there is no private right of action. Civil penalties of up to $7,500 may be imposed for each violation.	**Keller and Heckman LLP** 1001 G Street, NW Suite 500 West Washington, DC 20001 Sheila A. Millar millar@khlaw.com Tel: (202) 434-4143 Tracy P. Marshall marshall@khlaw.com Tel: (202) 434-4234 www.khlaw.com
USA (Washington) *(Updated Jun 2021)*	Wash. Rev. Code § 19.255.005 et seq., § 42.56.590 Note: Washington unsuccessfully attempted in 2019, 2020, and 2021 to pass the Washington Privacy Act (“WPA”). It is expected a similar bill will be	**Definition of Personal Information:** • Personal Information (“PI”) does not include publicly available information that is lawfully made available to the general public from governmental records. **Requirements:** • Notice generally required within 30 days after breach. • A breach affecting more than 500 Washington residents requires notice to the Attorney General. • There are requirements for form and content of notices.	**Cairncross & Hempelmann** 524 Second Ave, Suite 500 Seattle, WA 98104 Susan Wright Geiger SGeiger@Cairncross.com Tel: (206) 254-4424 www.cairncross.com

	introduced in 2022.	**Application:** • Applies to any state or local agency or any person/entity that conducts business in WA and that owns or licenses data that includes PI. • Also applies to any person or entity that maintains data that includes PI that the person/entity does not own but holds or processes the data for others. • Does not apply to entities subject to HIPAA/HITECH and certain financial entities. • WA residents have a private right of action. The WA AGO may bring action on behalf of WA residents.	
URUGUAY *(Updated Jun 2021)*	**Personal Data Protection Act (**Law N° 18.331) Amended by Law N° 19.670	**Collection:** All public entities, private companies and individuals who intend to collect personal data for database are identified as "responsible persons" and must comply with seven main principles. In order to collect personal data for a database, individuals must previously be informed on the purpose of the database and expressly consent the collection. **Registration:** All databases consisting of personal data must be registered. When submitting a registration, the responsible person for the database must disclose the purpose of the database, and collection and privacy protection procedures applied. **Officer:** Those responsible for a database must appoint an individual in charge for the management of the personal data collected. For public databases and big volume private databases, a data protection delegate must also be appointed. **International Data Transfer:** The transfer of data is restricted to countries and international agencies that hold international and regional data privacy standards. **Privacy Breaches:** Responsible persons must immediately disclose any privacy breaches to authorities and individuals whose personal is included in the compromised database.	**Bado, Kuster, Zerbino & Rachetti** Marcelo Femenías (mfemenias@bkzr.com.uy) Pedro González (pgonzalez@bkzr.com.uy) Tel: (598) 29160310 Address: Treinta y Tres 1271, CP 11000, Montevideo https://www.bkzr.com.uy
VENEZUELA *(Updated July 2021)*	National Constitution 1999 (Constitución de la República Bolivariana de Venezuela) Cyber Crime Act 2001 (Ley Especial contra los Delitos Informáticos) Ruling No. 1.318 dated August 4, 2011 from the Constitutional Chamber (Sentencia No. 1318 dictada por la Sala Constitucional del Tribunal Supremo de Justicia el 4 de agosto de 2011) Access and Electronic Exchange of Data Info Between Government Entities	**Collection:** Persons or entities that collect, store or use personal information must guarantee *habeas data* rights to data owners. The jurisprudence has set 9 principles that must be included in a future Data Privacy Act, that remain as a Best Practice standard for the industry in Venezuela. **Registration:** There is no registration requirement for entities that collect, store or use personal information. **Officer:** The figure of a "privacy officer" does not exist in the Venezuelan legislation. **Data Transfers from EU:** The Commission has not recognized Venezuela as providing adequate protection. **Privacy Breach/Data Loss:** There is no legal requirement to perform any action or notification in the event of unauthorised use/disclosure of data. **Electronic Direct Marketing:** There are no direct regulations regarding EDM in Venezuela. Opt-out procedures are considered a best practice.	**AraqueReyna** Pedro I. Sosa Samuel Morales Partner and associates, ARAQUEREYNA psosa@araquereyna.com, smorales@araquereyna.com, Phone: +58 212 953 9244 +58 414 314 7777 Centro Lido, Torre "C", Piso 8, Av. Francisco de Miranda, El Rosal. Caracas 1060, Venezuela. www.araquereyna.com

	Act, 2012 (Ley sobre Acceso e Intercambio Electrónico de Datos, Información y Documentos entre los órganos y Entes del Estado) Info-government Act, 2013 (Ley Infogobierno)		