Schedule 1
Australia [i]

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
ACT: Information Privacy Act 2014[ii]	Regulates how the ACT public sector agencies handle personal information. **Section 7 Objects** "(a) promote the protection of the privacy of individuals; and (b) recognise that the protection of the privacy of individuals is balanced with the interests of public sector agencies in carrying out their functions or activities; and (c) promote responsible and transparent handling of personal information by public sector agencies and contracted service providers; and (d) provide a way for individuals to complain about an alleged interference with their privacy."	No definition of "privacy" in the Act. Although an "interference with privacy" is a breach of the Territory Privacy Principles (TPPs) (similar to Privacy Act and APPs).	**Section 8 Meaning of personal information** "(1) For this Act, ***personal information***— (a) means information or an opinion about an identified individual, or an individual who is reasonably identifiable— (i) whether the information or opinion is true or not; and (ii) whether the information or opinion is recorded in a material form or not; but (b) does not include personal health information about the individual. (2) In this section: personal health information—see the *Health Records (Privacy and Access) Act 1997*, dictionary."	**Dictionary** "***Consent*** means express or implied consent". The TPPs are very similar (if not exactly the same) to the APPs, so consent is handled similarly.	The ongoing control of personal information is handled in a similar way as the Privacy Act. **Schedule 1 section 10** Integrity of information (ensuring quality at collection but also at use/disclosure). **Schedule 1 sections 12-13** Similar rights of individuals to access, and correction of, personal information that is held about them. There is no mention of the right to erasure or withdrawal of consent. **Section 22** Deemed breach in relation to acts and practices of overseas recipients of personal information. **Section 23 Privacy protection requirements for government contracts** "(1) A public sector agency must not enter into a government contract unless the	**Schedule 1 section 3.5** Collection of personal information to be by lawful and fair means. Implied in: **Section 6** - other acts **Section 18 -** de-identified personal information **Part 4 Exemptions** Existing lawful uses of personal information are exempt. **Schedule 1 section 6** No necessity to obtain consent where it's not reasonable to do so and a permitted general situation exists. Use needs to be for allowed purpose consistent with APPs.	Through the ACT Privacy Commissioner mainly, however, some responsibilities are handled by the OAIC - such as receiving privacy complaints and data breach notices. Ability for individuals to make a complaint to the privacy commissioner (**section 34**). If the privacy commissioner thinks privacy has been interfered with, the complainant can apply for a court order. Court order (**section 47**) can require that the complainant be compensated.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
			Section 18 Meaning of de-identified personal information For schedule 1, personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.		contract contains appropriate contractual provisions requiring the contracted service provider, and any subcontractor for the contract, to comply with— (a) the TPPs; or (b) a TPP code that binds the agency; or (c) a corresponding privacy law."		
ACT: Health Records (Privacy and Access) Act 1997 [iii]	**Section 3** "(a) to provide for privacy rights in relation to personal health information; and (b) to provide for the integrity of records containing personal health information; and (c) to provide for access to personal health information contained in health records; and (d) to provide for a consumer to receive an explanation of the consumer's personal health information; and (e) to encourage agreement, concerning the exercise of a right or performance of an obligation under this	No definition of "privacy" in the Act.	**Dictionary** "***personal health information***, of a consumer, means any personal information, whether or not recorded in a health record— (a) relating to the health, an illness or a disability of the consumer; or (b) collected by a health service provider in relation to the health, an illness or a disability of the consumer", "***personal information***, in relation to a	**Dictionary** "***Consent*** includes implied consent". Particular actions requiring consent: **Section 7**: Consent by consumer to obtaining health status report **Section 13A**: Disclosure in accordance with consent. **Section 20**: Unlawfully requiring consent. Interesting offence under this Act under **section 20**, where they commit an offence if they unlawfully acquire consent (for example through intimidation or threats)	**Section 10** Right of access to an individual's own personal health information held, unless an exception applies. **Schedule 1 Principle 7** Must not delete information from a health record, must ensure information is up to date and accurate. **Schedule 1 Principle 8** Must check for accuracy of information before use. **Schedule 1 Principle 11** Certain rights also arise when a health service provider is intending to relocate or close, including needing to provide notice of this and give individuals the opportunity to receive a	**Schedule 1 Principle 1** "A collector must not collect personal health information by unlawful or unfair means".	**Section 18** Complaints can be made to the human rights commission.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	Act, between the persons concerned."		consumer, means any information, recorded or otherwise, about the consumer where the identity of the consumer is apparent, whether the information is— (a) fact or opinion; or (b) true or false."		copy of their health record. **Schedule 1 Principle 12.1** Where an individual moves from one health service provider to another they are able to request transfer of the information. **Schedule 1 Principle 12.2** Where a health service provider moves practices, and the individual moves with the provider, the individual can request the practice to move their health records.		
NSW: Privacy and Personal Information Protection Act 1998 [iv]	No specifically enumerated objects/purpose in the Act. Explanatory note states the object of the original Bill were: "– to promote the protection of the privacy of individuals, – to specify information protection principles that relate to the collection, use and disclosure of personal information held by public sector agencies,	No definition of "privacy" in the Act.	**Section 4** "(1) In this Act, ***personal information*** means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion."	No definition of "consent" in the Act. Consent is required in certain circumstances. For example: **Section 17** Consent required for use of personal information for a purpose other than that for which it was collected. **Section 19** Disclosure by a public sector agency holding personal information must not disclose the information to any	**Section 14** **R**ight of access to personal information of individual **Section 15** Right to alteration of personal information of individual	**Section 19 Special restrictions on disclosure of personal information** **"**(2) A public sector agency that holds personal information about an individual must not disclose the information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless (a) the public sector agency reasonably believes that the recipient of the	**Section 36** Under this section, the functions of the commissioner largely relate to promoting compliance with the Act and assisting agencies to comply. There are various miscellaneous offences under the Act including: **Section 62** Corrupt disclosure and use of personal information by public sector officials.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	– to require public sector agencies to comply with those principles, – to provide for the making of privacy codes of practice for the purpose of protecting the privacy of individuals, – to provide for the making of complaints about privacy related matters, and for review of conduct that involves the contravention of the information protection principles or privacy codes of practice, – to establish an office of Privacy Commissioner and to confer on the Privacy Commissioner functions relating to privacy and the protection of personal information."		**Section 4** includes specific carve outs including information relating to an individual that has been deceased for 30 years; information that is in a publicly available publication; information arising from a royal commission and so on.	person or body outside New South Wales or to a Commonwealth agency without express consent to the disclosure. **Section 26** Consent may be obtained to avoid compliance with certain principles.		information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the information protection principles," **Section 8 Collection of personal information for lawful purposes** "(1) A public sector agency must not collect personal information unless— (a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and [...] (2) A public sector agency must not collect personal information by any unlawful means." **Section 12 Retention and security of personal information** **"**A public sector agency that holds personal information must ensure— (a) that the information is kept for no longer than is necessary for the purposes for which	**Section 63** Offering to supply personal information that has been disclosed unlawfully. **Section 67** Disclosure by privacy commissioner or staff member. **Section 68** Obstructing, hindering, resisting the privacy commissioner; failing to comply with any lawful requirement of the privacy commissioner; making a wilful false statement or misleading/attempting to mislead the privacy commissioner.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
						the information may lawfully be used, and (b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and (c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and (d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information."	
NSW: Health Records and Information Privacy Act 2002 [v]	**Section 3** "(1) The purpose of this Act is to promote fair and responsible handling of health information by—	No definition of "privacy" in the Act.	**Section 5** "(1) In this Act, ***personal information*** means information or an opinion (including information or an				

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	(a) protecting the privacy of an individual's health information that is held in the public and private sectors, and (b) enabling individuals to gain access to their health information, and (c) providing an accessible framework for the resolution of complaints regarding the handling of health information. (2) The objects of this Act are— (a) to balance the public interest in protecting the privacy of health information with the public interest in the legitimate use of that information, and (b) to enhance the ability of individuals to be informed about their health care, and (c) to promote the provision of quality health services."		opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion." **Section 5** includes specific carve outs including information relating to an individual that has been deceased for 30 years; information that is in a publicly available publication; information arising from a royal commission and so on. **Section 6** "In this Act, health information means— (a) personal information that is information or an opinion about— (i) the physical or mental health or a disability (at any time) of an individual, or (ii) an individual's express wishes about the future provision of				

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
			health services to him or her, or (iii) a health service provided, or to be provided, to an individual, or (b) other personal information collected to provide, or in providing, a health service, or (c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or (d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or (e) healthcare identifiers, but does not include health information, or a class of health information or health information				

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
			contained in a class of documents, that is prescribed as exempt health information for the purposes of this Act generally or for the purposes of specified provisions of this Act."				
NT: Information Act 2002 [vi]	**Section 3 of Act** "(1) The objects of this Act are: (a) to provide the Territory community with access to government information by: (i) making available to the public information about the operations of public sector organisations and, in particular, ensuring that rules and practices affecting members of the public in their dealings with public sector organisations are readily available to persons affected by those rules and practices; and (ii) creating a general right of access to information held by public sector organisations limited only in those circumstances where	**Section 4** **"*privacy*** means privacy with respect to personal information." **Section 67** Similar to other legislation, an interference with a person's privacy is where an "organisation contravenes an IPP, a code of practice or an authorisation."	**Section 4A Personal information** "(1) Government information that discloses a person's identity or from which a person's identity is reasonably ascertainable is ***personal information*.** (2) However, the government information is not ***personal information*** to the extent that: (a) the person's identity is disclosed only in the context of having acted in an official capacity for a public sector organisation; and (b) the government information discloses no other personal information about the person."	**Section 4 Definitions** "***consent*** means consent whether express or implied." Consent can be supplied by the relevant individual in order to surpass certain obligations within the Act. For example: **Section 148** Requiring the administrators of the Act to maintain the confidence of the information they hold. **Schedule 2 IPP 2** Using or disclosing for a purpose other than the purpose for which it was collected. **Schedule 2 IPP 7** Limits the assignment, adoption, use and	**Section 15** Right to access government information **Section 16** Right to access or correct personal information	**Schedule 2, IPP 1** "A public sector organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way."	**Section 82** Commissioner may serve compliance notice whether at their initiative or because of a complaint requiring the public sector organisation to take specified actions. **Section 87** The commissioner has the "powers that are necessary and convenient for the performance of his or her functions under this Act and any other Act." For "dealing with a complaint; or deciding whether to serve a compliance notice or conducting an audit" of records held by a public sector organisation.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	the disclosure of particular information would be contrary to the public interest because its disclosure would have a prejudicial effect on essential public interests or on the private and business interests of persons in respect of whom information is held by public sector organisations; and (b) to protect the privacy of personal information held by public sector organisations by: (i) providing individuals with a right of access to, and a right to request correction of, their personal information held by public sector organisations; and (ii) establishing a regime for the responsible collection and handling of personal information by public sector organisations; and (iii) providing remedies for interference with the privacy of an		**Section 4 Definitions** "***government information*** means a record held by or on behalf of a public sector organisation and includes personal information."	disclosure of unique identifiers			

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	individual's personal information; and (c) to establish an independent officeholder, the Information Commissioner, to oversee the freedom of information and privacy provisions of this Act; and (d) to promote efficient and accountable government through appropriate records and archives management by public sector organisations. (2) This Act is intended to strike a balance between competing interests by giving members of the Territory community a right of access to government information with limited exceptions and exemptions for the purpose of preventing a prejudicial effect on the public interest as described in subsection (1)(a)(ii).						
Qld: Information Privacy Act 2009 [vii]	**Section 3** "(1)The primary object of this Act is to provide for—	No definition of "privacy" in the Act.	**Section 12** "***Personal information*** is information or an opinion, including	**Schedule 5 Definitions** **"*Consent*,** for the NPPs, means express	As with everything in the Act, individual rights are balanced against what is in the "public interest".	**Section 3** **O**bject of the Act "is to ensure the **fair** collection and handling in the public sector	No "interference with privacy" offence specifically enumerated in the Act.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	(a) the fair collection and handling in the public sector environment of personal information; and (b) a right of access to, and amendment of, personal information in the government's possession or under the government's control unless, on balance, it is contrary to the public interest to give the access or allow the information to be amended."		information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." However, under **section 28**, "an agency is not required to comply with a prescribed IPP in relation to an individual's personal information if the information is related to or connected with personal information of the individual that has previously been published, or given for the purpose of publication, by the individual", essentially precluding such information from really being "personal information".	consent or implied consent." **Section 30** ***NPPs*** are the National Privacy Principles in **Schedule 4** which apply to health agencies. They are called as such because of their "correspondence to the National Privacy Principles set out in the **Privacy Act 1988 (Cwlth), Schedule 3**. The NPPs, rather than the IPPs, are applied to health agencies under this chapter because of particular arrangements applying nationally to health agencies, corresponding entities". Otherwise there is no definition of "consent" for the QLD IPPs and no mention of "consent" within this Act (other than in **Schedule 4** where it restates the NPPs; and in needing inter-governmental consent when transferring from one agency to another (**section 57**)). There is mention of where an individual	**Section 40** Right to access particular documents which contain an individual's personal information **Section 41** Right to amend personal information in particular documents However both these rights are curtailed with an agency being able to go through an extensive application process and being able to refuse if in the public interest (**section 58**), if it would substantially and unreasonably divert the resources of the agency from their use by the agency in the performance of its functions (**section 60**).	environment of personal information". **Section 33** Being able to transfer outside of Australia if an entity reasonably believes that the recipient will uphold the principle of "fair handling of personal information"**.** **Schedule 3 IPP 1** "(1) An agency must not collect personal information for inclusion in a document or generally available publication unless— (a) the information is collected for a **lawful** purpose directly related to a function or activity of the agency; and (b) the collection of the information is necessary to fulfill the purpose or is directly related to fulfilling the purpose. (2) An agency must not collect personal information in a way that is **unfair or unlawful**."	

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
				"agrees" to something (For example, **Section 33 Transfer of personal information outside Australia**)			
SA	There is no privacy legislation in South Australia. Instead, SA has the Information Privacy Principles which are set out in the Premier and Cabinet Circular 12 - Information Privacy Principles Instruction (**IPPS**)	No definition of "privacy" in the IPPS.	**Clause 3(1) Interpretation** ***Personal information*** is defined as "information or an opinion, whether true or not, relating to a natural person or the affairs of a natural person whose identity is apparent, or can reasonably be ascertained, from the information or opinion."	**Clause 4(8)** Personal information should not be used by an agency for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose (the secondary purpose) unless under certain circumstances including when the record-subject has expressly or impliedly consented to the use.	**Clause 4(5)** Access to records of Personal Information **Clause 4(6)** Correction of Personal Information	**Clause 4(1)** Personal information should not be collected by unlawful or unfair means, nor should it be collected unnecessarily.	**Clause 8** The Privacy Committee of South Australia may at any time on its own initiative appoint a person (whether or not that person is a public employee) or the Commissioner for Public Employment to investigate or assist in the investigation of the nature and extent of compliance of an agency with the Principles and to furnish a report to the Committee accordingly.
Tas: Personal Information Protection Act (2004) [viii]	There is no "Objects" section in the Act.	No definition of "privacy" in the Act.	**Section 3** "***Personal information*** means any information or opinion in any recorded format about an individual – (a) whose identity is apparent or is reasonably ascertainable from the information or opinion; and	No definition of "consent" in the Act. However, there are certain sections that refer to "consent" as a prerequisite. **Section 12 Use of basic information** "A personal information custodian may use or disclose personal information about an individual for a purpose other than the primary purpose of collection	**Section 17A Person may request amendment of information** "If information of a person is held or used by a personal information custodian, the person can request the amendment of any part of that information if it is incorrect, incomplete, out of date or misleading." **Section 17B Form of request for amendment of information** A request under section	**Schedule 1 Principle 2** Collection must be "necessary", made only by "lawful and fair means" and must not be "unreasonably intrusive". **Schedule 1 Principle 2 Use and disclosure** Use and disclosure of an individual's personal information beyond the primary purpose of collection must be with the individual's consent or determined to be	**Section 18 Making of complaints** "(1) A person may make a complaint to the Ombudsman in relation to a matter referred to in subsection (2) if the person – (a) has raised the matter with the relevant personal information custodian; and (b) is not satisfied with the response from the personal information custodian.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
			(b) who is alive or has not been dead for more than 25 years."	without the individual's consent if – (a) it is a public authority; and (b) the information is basic personal information; and (c) the use or disclosure is reasonably necessary for the efficient storage and use of that information; and (d) the information is only used by, or disclosed to, another public sector body."	17A is to – (a) be in writing and addressed to the personal information custodian; and (b) specify an address to which a notice under section 17F is to be sent; and (c) give particulars of the information the person believes is incomplete, incorrect, out of date or misleading; and (d) specify the amendments that the person wants made to that information. **Section 3** defines "correct" in relation to personal information as meaning to "alter by way of amendment, deletion or addition"). There is no mention of withdrawal of consent.	"necessary" for a permitted purpose (standard public interest exceptions are available including individual/public safety, law enforcement, court proceedings, compilation of de-identified statistics etc). Applicability of exemptions primarily assessed against concepts of "reasonableness", giving Victorian public sector organisations wide discretion in determining what constitutes permitted onward use and disclosure in relation to individuals' personal information it holds.	(2) A complaint may be made by a person in relation to the alleged contravention by a personal information custodian of a personal information protection principle that applies to the person."
Vic: Privacy and Data Protection Act (2014) [ix]	**Section 5** "The objects of this Act are— (a) to balance the public interest in the free flow of information with the public interest in protecting the privacy of personal information in the public sector; and (b) to balance the public interest in	No definition of "privacy" in the Act.	**Section 3** "***personal information*** means information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the	**Section 3 Definitions** "***consent*** means express consent or implied consent**".**	**Section 3 Definitions** **"*correct***, in relation to personal information, means to alter that information by way of amendment, deletion or addition." **Schedule 1 IPP 6** Access and correction	**Schedule 1 IPP 1 Collection** "1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. 1.2 An organisation must collect personal information only by lawful and fair means"	**Section 57 Complaints** "(1) An individual in respect of whom personal information is, or has at any time been, held by an organisation may complain to the Information Commissioner, in writing, about an act or practice that may be an interference with the privacy of the individual."

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	promoting open access to public sector information with the public interest in protecting its security; and (c) to promote awareness of responsible personal information handling practices in the public sector; and (d) to promote the responsible and transparent handling of personal information in the public sector; and (e) to promote responsible data security practices in the public sector."		information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies."				
Vic: Health Records Act (2001) [x]	**Section 1 Purpose** "The purpose of this Act is to promote fair and responsible handling of health information by— (a) protecting the privacy of an individual's health information that is held in the public and private sectors; and	No definition of "privacy" in the Act. **Section 18 What is an interference with privacy?** "For the purposes of this Act, an act or practice of an organisation is an interference with the privacy of an individual if, and only if—	**Section 3 Definitions** "***personal information*** means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is	**Section 3 Definitions** "***consent*** means express consent or implied consent." Consent is required in certain circumstances. For example: **Schedule 1 Principle 1 1—Collection** ***"When health information may be collected***	**Section 3 Definitions** "***correct***, in relation to health information, means to alter that information by way of amendment, deletion or addition;" **Schedule 1 Principle 5 - Openness** "5.2 On request by an individual, an organisation must take reasonable steps— (a) to let the individual know— (i) whether the	**Schedule 1 Principle 1 - Collection** "***How health information is to be collected*** 1.2 An organisation must collect health information only by lawful and fair means and not in an unreasonably intrusive way."	**Section 45 Complaints** "(1) An individual may complain to the Health Complaints Commissioner about an act or practice that may be an interference with the privacy of the individual." Offences arising under the Act: **Section 80** Unlawfully requiring consent

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	(b) providing individuals with a right of access to their health information; and (c) providing an accessible framework for the resolution of complaints regarding the handling of health information."	(a) the act or practice breaches Part 5 or a Health Privacy Principle in relation to health information that relates to the individual; or (b) the act or practice breaches HPP 7 in relation to an identifier; or (c) the act or practice is or results in a failure to provide access to health information that relates to the individual in accordance with Part 5 or HPP 6."	apparent, or can reasonably be ascertained, from the information or opinion, but does not include information about an individual who has been dead for more than 30 years;"	1.1 An organisation must not collect health information about an individual unless the information is necessary for one or more of its functions or activities and at least one of the following applies— (a) the individual has consented; (b) the collection is required, authorised or permitted, whether expressly or impliedly, by or under law (other than a prescribed law); [...]". **Schedule 2 Principle 2 - Use and Disclosure** "2.1 An organisation may use or disclose health information about an individual for the primary purpose for which the information was collected in accordance with HPP 1.1. 2.2 An organisation must not use or disclose health information about an individual for a purpose (the secondary purpose) other than the primary purpose for which the information was collected unless at	organisation holds health information relating to the individual; and (ii) the steps that the individual should take if the individual wishes to obtain access to the information; and [...]". **Section 28 How right of access may be exercised** "(1) A right of access may be exercised in any one or more of the following ways— (a) by inspecting the health information or, if the health information is stored in electronic form, a print-out of the health information, and having the opportunity to take notes of its contents; (b) by receiving a copy of the health information; (c) by viewing the health information and, if it is held by a health service provider, having its content explained." **Schedule 1 Principle 6** Access and Correction		**Section 81** Unlawful destruction etc. or removal of health information **Section 82** Unlawfully requesting or obtaining access to health information

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
				least one of the following paragraphs applies10— (a) both of the following apply— (i) the secondary purpose is directly related to the primary purpose; and (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or (b) the individual has consented to the use or disclosure; or [...]".			
WA: Freedom of Information Act 1992 [xi]	No specific privacy legislation in WA, though the Freedom of Information Act 1992 does cover some elements of privacy. **Section 3 Objects of the Act** The Act provides for public access to documents, and to enable the public to ensure that personal information in documents is accurate, complete, up to date and not misleading, and for related purposes.	No definition of "privacy" in the Act.	**Section 9 (clause 1) Glossary** "***personal information*** means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead — (a) whose identity is apparent or can reasonably be ascertained from the information or opinion; or (b) who can be identified by reference to an identification number or other identifying particular such as a		**Section 45 (Right to apply for information to be amended)** (1) An individual (the person) has a right to apply to an agency for amendment of personal information about the person contained in a document of the agency if the information is inaccurate, incomplete, out of date or misleading. (2) A dead person's closest relative has a right to apply to an agency for amendment of personal information about the dead person and this section has effect as if the information were		

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
			fingerprint, retina print or body sample".		information about the closest relative. (3)If the circumstances of the person require it, the agency has to take reasonable steps to help the person make an application for amendment in a manner that complies with this Act. (4)In particular, if an application for amendment does not comply with the requirements of section 46 the agency has to take reasonable steps under subsection (3) to help the person to change the application so that it complies with those requirements. (5)This section does not apply if another enactment provides a means or procedure by which the person can have the information amended.		
Online Safety Act [xii]	**Section 3** The objects of this Act are: (a) To improve online safety for Australians; and	No definition of "privacy" in the Act. "Privacy" appears to be treated as an '**attribute**' of certain types of material, rather than as a right (see below).	No definition of "personal information" in the Act.	**Section 21 Consent** "For the purposes of the application of this Act to an intimate image or private sexual material, consent means ***consent*** that is: (a) express; and	**Section 194 and Part 15** The eSafety Commissioner has the right to obtain the identity information and contact details of an end-user of a social media service, relevant electronic service or designated		**Part 3 of the Act** In relation to the material outlined in column 3, if their right to be protected from online harm is violated, they have a right to make a complaint.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	(b) To promote online safety for Australians.	**Section 5(a)(ii) Definitions** ***'Private sexual material'*** is defined as material…where the depiction is in circumstances that reasonable persons would regard as giving rise to an expectation of privacy. **Section 15(b)(ii)** '***Intimate image***' is defined as material… **…**in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy.		(b) voluntary; and (c) informed; but does not include: (d) consent given by a child; or (e) consent given by an adult who is in a mental or physical condition (whether temporary or permanent) that: (i) makes the adult incapable of giving consent; or (ii) substantially impairs the capacity of the adult to give consent."	internet service if they believe on reasonable grounds that the information, or the contact details are, relevant to the operation of this Act. **Explanatory Memorandum[xiii], p 54** "The Act enables the Commissioner to disclose information in certain circumstances, including to the Minister, Australian Public Service (APS) employees for the purpose of advising the Minister, Royal Commissions, certain authorities, teachers or school principals, and parents or guardians. This Bill enables the Commissioner to disclose information to teachers or school principals, for example, to assist in the resolution of complaints made under the Act, which may be particularly important in cases of cyber-bullying among school children."		**Explanatory Memorandum, p 59** Human Rights Implications of the Act The principle human rights that the legislation engages: the prohibition on interference with privacy and attacks on reputation primarily contained in Article 17 of the ICCPR, and also referred to in Article 16 of the CROC, and Article 22 of the CRPD; The EM does not address the risk to a person's right to privacy because of the unchecked powers of the Commissioner, rather, the EM argues that the legislation is fundamentally directed towards protecting the privacy of vulnerable people.
f. Criminal Code Amendment(Sharing of Abhorrent Violent Material) Act 2019 [xiv]	**Explanatory Memorandum [xv], Para 3** General Outline	No definition of "privacy" in the Act..	No definition of "personal information" in the Act..	**Section 474.370**		**Explanatory Memorandum,** Section @474.31—Abhorrent violent material	**Explanatory Memorandum, para 5** Human rights implications

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	"This Bill will make amendments to the *Criminal Code Act 1995* to introduce new offences to ensure that internet, hosting or content services are proactively referring abhorrent violent material to law enforcement, and that hosting and content services are expeditiously removing abhorrent violent material that is capable of being accessed within Australia." **Explanatory Memorandum, para 2** <u>Overview of the Bill</u> "The objective of the Bill is to address significant gaps in Australia's current criminal laws by ensuring that persons who are internet service providers, or who provide content or hosting services, take timely action to remove or cease hosting abhorrent violent material when it can be accessed using their services."	On its face, privacy does not seem to be a consideration at all. **Section 474.33 Notification obligations of internet service providers, content service providers and hosting service providers** Under the Act, it is an offence for an internet service provider, content service or hosting service to fail to refer abhorrent violent material to the AFP where the underlying conduct occurred or is occurring in Australia. The provisions are similar to the existing notification obligations for child pornography under the Criminal Code. If an internet service provider, content service or hosting service: • is aware that their service can be used to access particular material;		"***consent*** means free and voluntary agreement." **Explanatory Memorandum, Para 6 -** <u>Consent</u> "Consent is used in Subdivision H in relation to rape and kidnapping. These two aspects of an agreement are commonly used in State and Territory Acts to define "consent" in relation to sexual offences."		**Para 16** "The definition of "abhorrent violent material" is not intended to capture footage of violent sporting events (for example, boxing), medical procedures, or consensual sexual acts that involve elements of violence." **Para 17** " "Additionally, the material must be produced by a person who is, or by two or more persons each of whom is: - a person who engaged in the abhorrent violent conduct - a person who conspired to engage in the abhorrent violent conduct - a person who aided, abetted, counselled or procured, or was in any way knowingly concerned in, the abhorrent violent conduct, or - a person who attempted to engage in	"This Bill engages the following rights: - the right to procedural guarantees in article 14 of the International Covenant on Civil and Political Rights [1976] ATS 5 (**ICCPR**) - the right to freedom from interference in privacy and correspondence in article 17 of the ICCPR - the right to freedom of expression in article 19(2) of the ICCPR, - the right to freedom from propaganda, discrimination and hatred in article 20 of the ICCPR, and - the right of the child to be protected from all forms of physical and mental violence including sexual abuse in articles 19 and 34 of the Convention on the Rights of the Child [1991] ATS 4 (CRC)."

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	The Act was introduced in the wake of the March 2019 Christchurch terrorist attack to create new offences under the Criminal Code Act 1995 (Cth) (Criminal Code) that would require social media platforms and other websites and providers to expeditiously remove abhorrent violent material and refer such material to the Australian Federal Police (AFP). In order to do so, the Act adds two new offences to the Criminal Code dealing with any failure to refer and failure to remove abhorrent violent material. The Act is intended to complement the existing take-down and referral procedures for online content under Schedules 5 and 7 of the Broadcasting Services Act 1992 (Cth). The Act is, on its face, a direct response to the Christchurch attacks. However, it is also part of a broader global trend to regulate	• they have reasonable grounds to believe that material is abhorrent violent material; and • the material records or streams abhorrent violent conduct that has occurred or is occurring in Australia, the provider or service is required to refer details of the material to the AFP within a reasonable time unless they reasonably believe that the AFP would already be aware of such details. Furthermore, this obligation applies regardless of where the internet service provider or content service is located. **Section 474.30 Definitions** The Act covers internet service providers, content service providers and hosting service providers. The Act is not limited to social media. At a high level, this would include:				the abhorrent violent conduct." **Para 18** "This requirement is intended to ensure that only material recorded or streamed by the perpetrator(s) and their accomplice(s) will be captured by the definition of abhorrent violent material. Material recorded or streamed by other persons, such as victims of the conduct, bystanders who are not complicit in the conduct, or media organisations, will not be considered to be caught by this definition even though such material may record or stream abhorrent violent conduct. Material recorded or streamed by persons who are not the perpetrator(s) or their accomplice(s) will therefore not be captured by the new offences under sections @474.33-@474.34."	

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	the activities of online platforms, as seen in the ACCC's digital platforms inquiry and the United Kingdom's recently released online harms white paper which proposes various measures to stop the spread of harmful content online. The Act was passed quickly with minimal consultation. (See Ashurst media update: A*ustralian government pushes through expansive new legislation targeting abhorrent violent material online (19 April 2019*)	• any internet site that allows users to interact with one another; and • any electronic service that allows users to communicate with one another (for example, email and instant messaging). Examples of services covered by these laws include Gmail, Google Drive, DropBox and Microsoft OneDrive. For many of these services, the service provider typically has no or very little visibility over what content is being stored or communicated (and this reflects the expectations of users). Where relevant 'abhorrent violent material' is being live-streamed or otherwise displayed on a person's social media page, then it is obvious what the law is seeking to prevent (even if the drafting of the legislation is					

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
		unclear in some areas). However, where the material is in a user's private email or storage account and not being publicized (the Act simply requires that the service is used to "access" the material), it is far less clear what behaviour the law is seeking to change – particularly as the Act is focused on the providers of those services, and not their users.					
g. Data breaches: Mandatory Data Breach Notification (MDBN) - Part IIIC of the Privacy Act [xvi]	Makes it mandatory for people to be notified of data breaches if the entity in breach is regulated under the Privacy Act. (i.e. organisations with an annual turnover of more than $3 million, and some other organisations, handle personal information).	No definition of "privacy" in the MDBN. And technically, hard to define. **Serious Invasions of Privacy in the Digital Era** (ALRC Report 123) [xvii] - A test for what is private, Para 6.6 In *ABC v Lenah Game Meats*, Gleeson CJ said:	**Section 6 (Privacy Act) Interpretations** **"*personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not."				There is an avenue of redress which is usually by way of a class action under section 38 Privacy Act. However, it is not very effective. "This avenue of redress has existed even before enacting the NDB (Notification of Data Breach) scheme and continues to apply after its enactment. However, little success existed in making such complaints as it required that the victims prove that 'harm' had been caused, rather than the fact that the victims had experienced embarrassment, anger, or unhappiness." Hence, it is difficult to prove harm in

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
		"There is no bright line which can be drawn between what is private and what is not. Use of the term 'public' is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private." However, the MDBN refers to the APPs (Australian Privacy Principles).					such cases. [see Alazab, Seung & Ng (2021) at para 3.2.] [xviii]. There have been calls for improvements in the law in this area where it was argued that a privacy tort or statutory cause of action for serious privacy breaches would be a way forward because it does not require for 'harm' to be proven. [See Alazab, Seung & Ng (2021) at paras 3.2, 4.1, 4.2]
g. Data Breaches: Security of Critical Infrastructure Act 2018 [xix]	**Section 3** "The object of this Act is to provide a framework for managing risks relating to critical infrastructure, including by: (a) improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks; and (b) facilitating cooperation and collaboration between all levels of government, and regulators, owners and	No definition of "privacy" in the Act.	The SOCI Act is primarily concerned with protecting critical infrastructure assets, which may include *personal information*. **Sections 5, 6, and 7** Certain terms in the SOCI Act include, as part of their definition, "***personal information***" as understood in Privacy Act 1988 (therefore, an overlap). Those terms are: **"*Business critical data*";** **"*interest and***	No definition of "consent" in the Act. **Section 45** 'Consent' is used as a defence or exception to offence for unauthorised use or disclosure. This section gives rise to an offence (in relation to an entity) for unauthorised use or disclosure of protection information. **Section 46(4)(c)**	- Information on the Register can only be accessed and disclosed in authorised circumstances. - Unauthorised use or disclosure of information on the Register is a criminal offence (unless exceptions under section 46 apply). - Any personal information provided to the Register is also subject to the Privacy Act.		The Act may require a reporting entity for, or an operator of, a critical infrastructure asset to provide certain information or documents. The making of a record, or the use or disclosure, of protected information is authorised in particular circumstances but is otherwise an offence. As such, in relation to this information generated by operation of the SOCI Act, **Part 4 Division 3 Subdiv A** of the Act sets out a list of provisions for the authorised use and disclosure of protection information. **Subdiv B** sets out the

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	operators of critical infrastructure, in order to identify and manage those risks; and (e) providing a regime for the Commonwealth to respond to serious cyber security incidents. **Home Affairs webpage** [xx] "The Act seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure. The SOCI Act applies to 22 asset classes across 11 sectors including: communications, data storage or processing, defence, energy, financial services and markets, food and grocery, health care and medical, higher education and research, space technology, transport, water and sewerage." The Act introduces new obligations on		***control information*"; and "*operational information*".** Additionally, certain information obtained or generated under, or relating to the operation of, this Act is protected information. There are restrictions on when a person may make a record of, use or disclose protected information. However, it is to be noted that there are several **authorisation of disclosure provisions** that are for the purposes of other laws, including the APPSs. **See sections 41, 42,43, 43A, 43B, 43C, 43D, 44** and **60**.	Section 45 does not apply if the making of the record, or the disclosure or use, of the protected information is in accordance with the express or implied consent of the entity to whom the information relates.			penalty for unauthorised use and disclosure.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	entities responsible for "critical infrastructure assets" to report cyber security incidents affecting those assets to the Australian Signals Directorate (**ASD**), with the aim of facilitating the development of an aggregated threat picture and comprehensive understanding of cyber security risks to critical infrastructure, and to enable proactive and reactive cyber response options. This obligation does not apply to entities who only own / operate "critical infrastructure sector assets". [xxi]						
g. Data Breaches: Ransomware Payments Bill 2021 (No.2) [xxii]	On 21 June 2021, the Ransomware Payments Bill 2021 (the **Bill**) was introduced in the Federal Parliament. **Explanatory Memorandum, p 4** The Bill was introduced to establish a mandatory reporting requirement for Commonwealth entities, State or	No definition of "privacy" in the Act. **Section 3** However, in terms of overlap with the Privacy Act, it is to be noted that the terms '***de-identified***' and '***personal information***' have the same meaning as in the Privacy Act.	The Bill is not concerned with protecting information - however, operation of the Bill will lead to the collection of information, information that will be 'personal information' under the Privacy Act 1988 and the Bill does provide a mechanism to protect this	No definition of "consent" in the Act. **Section 9** "Consent" is used as a defence for the offence arising under **section 9(5)** i.e. there is no penalty if the entity that gave the original notification to the ACSC consents to the disclosure of information (that would otherwise be protected	**Section 8** Information will be collected by operation of the Bill**.** Information that needs to be reported as soon as practicable are in relation to the ransomware payment; name and details of the entity making the payment; details of the attacker and ransomware attacker.		In relation to the collection of information (that would be personal information under the Privacy Act 1988), before disclosure - this information will be de-identified (**Section 9**). There are no other provisions outlining how this information will be protected.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	Territory agencies, corporations, and partnerships who make ransomware payments in response to a ransomware attack to the Australian Cyber Security Centre (**ACSC**). There is an exemption for small businesses with an aggregate turnover of less than $10 million, charities, sole traders and unincorporated entities. The Explanatory Memorandum sets out the objectives (high-level) which are: • Reporting and sharing information about ransomware payments could, arguably, facilitate cooperation against cyber threats, help regulators trace back the money. • The collection of information will inform policy making and help track the effectiveness of policy responses. It could also serve as a deterrent for entities considering payments.		information (see **section 9**).	under the Bill (**Section 9(6)(b)**).	The need to protect personal information is not the purpose of the Bill, rather this need arises from the operation of this Bill. **Section 9** This section gives the ACSC a broad ability to disclose any information gathered by virtue of section 8 to law enforcement agencies and to any person (including the public). **Explanatory Memorandum, p 6** While the Bill engages the right to privacy and reputation – this right is mitigated by the requirement that ACSC de-identify this information and through the inclusion of penalties for misuse of the collected information – however, it is to be noted that while personal information of individuals will be de-identified, there is no such protection in relation to a company.		

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
h. Open data regimes & data related initiatives: **Data Availability and Transparency Bill 2020** [xxiii]	**Section 3** The **objects** of this Act are to: (a) serve the public interest by promoting better availability of public sector data; and (b) enable consistent safeguards for sharing public sector data; and (c) enhance integrity and transparency in sharing public sector data; and (d) build confidence in the use of public sector data; and (e) establish institutional arrangements for sharing public sector data**.** **Explanatory Memorandum, p 5** "The Bill authorises and regulates controlled access to ('sharing' of) Commonwealth data, with safeguards in place to manage risk and streamline processes. This pathway for sharing is	No definition of "privacy" in the Act. "Privacy" is not treated as a 'right'. This term is used numerous times in the Bill, but in a vague manner. It almost appears to be used as a 'comfort-word' or 'consolation' for the Bill's apparent overriding of APP 6. 'Data custodians' have to ensure protection of personal information by taking certain privacy measures - however, there is no minimum privacy protection. The privacy measures to be taken are discretionary. **Explanatory Memorandum, para 23 -** Overlaps with Privacy Act "Existing legal obligations and policies for handling government data continue to apply, including the APPs in the Privacy Act." **Para 63**	**Section 9** "***personal information*** has the same meaning as in the Privacy Act 1988".	No definition of "consent" in the Act. **Explanatory Memorandum, para 118 -** Data sharing principles under section 16 "Subclause (1) establishes the project principle, which addresses the intended purpose or use of sharing the data. The project principle requires consideration of a number of factors to ensure data is only shared for appropriate projects or programs of work, described in subclause (2). The factors include but are not limited to public interest, ethics, and use of consent." **Para 121** "Where the data being shared includes personal information, subclause (2)(c) requires consent for sharing to be sought from the individuals concerned unless it is unreasonable or impracticable for the data scheme entities to		**Section 16(8) - Data principles** The data principle includes (but is not limited to) the following elements: (a) only the data reasonably necessary to achieve the applicable data sharing purpose is shared; (b) the sharing of personal information is minimised as far as possible without compromising the data sharing purpose.	**Explanatory Memorandum, paras 226-227** **"Section 28** ensures personal information shared under this scheme is handled in accordance with privacy obligations to the standard set in the *Commonwealth Privacy Act*. This privacy coverage ensures personal information shared under this Bill is handled properly, and works with **part 3.3** to ensure accountability through oversight and redress. All data scheme entities must be subject to the Privacy Act or comparable privacy protections. Commonwealth bodies and non-government entities that are APP entities under the Privacy Act must comply with their obligations under the Privacy Act for their acts and practices relating to personal information under the Bill. Non-government entities and State and Territory government authorities that are not covered by the Privacy Act must either become covered by the Privacy Act or be covered by their own jurisdiction's privacy laws

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	optional. Existing mechanisms and arrangements for sharing continue to be available." "The Bill takes a principles-based approach to data sharing, providing parties with flexibility to tailor sharing arrangements, and ensuring the scheme can respond to evolving technologies and community expectations. Modernising the approach to sharing public sector data will empower government to deliver effective services and better-informed policy, and support research and development." "In developing the Bill, PM&C has taken a privacy by design approach to identify, minimise and mitigate privacy impacts wherever possible. Two independent Privacy Impact Assessments were undertaken to identify strengths and weaknesses in the early policy positions and planned legislative	"If a serious data breach involves personal information, it must also be reported to the Australian Information Commissioner. The Bill preserves the Australian Information Commissioner's oversight of data breaches involving personal information by engaging the notifiable data breach scheme, under Part IIIC of the Privacy Act. Responsibility for notification rests with the data custodian or an accredited entity covered by the Privacy Act involved in sharing. A copy of the statement provided to the Information Commissioner must be given to the National Data Commissioner, to ensure their continuing oversight over the data sharing scheme."		do so. The standard of consent required is that set by the Privacy Act. The 'unreasonable or impracticable' language is drawn from section 16A of that Act, and should be interpreted using relevant guidance on consent made by the Australian Information Commissioner." **Para 122** "The question of whether seeking consent is reasonable or impracticable may depend on the amount, nature and sensitivity of the data involved, and whether individuals gave informed consent for uses including the proposed sharing at the point the data was originally collected. Where it is unreasonable or impracticable to seek consent, parties must still consider implementing other controls to protect privacy, under this and other data sharing principles."			(where these exist and are comparable to the Privacy Act)."

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	framework, and the draft Bill itself. Privacy safeguards were also strengthened in response to guidance and advice from the National Data Advisory Council and privacy experts, including the OAIC."						

Schedule 2
International

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
General Data Protection Regulation (GDPR)[xxiv]	**Article 1 Subject-matter and objectives** 1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. 2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. 3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.	No definition of "privacy" in the GDPR. For organizations subject to the GDPR, there are two broad categories of compliance: data protection and data privacy. **Data protection** means keeping data safe from unauthorized access. **Data privacy** means empowering your users to make their own decisions about who can process their data and for what purpose.	**Article 4 Definitions** "The GDPR defines '***personal data***' as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person as one that can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." **GDPR personal data – what information does this cover? (gdpreu.org)**[xxv] The GDPR states that data is classified as **"personal data"** an individual can be identified directly or indirectly, using online identifiers such as their name, an identification number, IP addresses, or their location data.	**Article 4 Definitions** "***'consent'*** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". **Article 6 GDPR Lawfulness of processing** "1. Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; [...]" **Article 7 GDPR Conditions for consent**	**Chapter 3 Articles 12 - 23** **Article 14** Information to be provided where personal data have not been obtained from the data subject **Article 15** Right of access by the data subject **Article 16** Right to rectification **Article 17** Right to erasure ('right to be forgotten') **Article 18** Right to restriction of processing **Article 19** Notification obligation regarding rectification or erasure of personal data or restriction of processing **Article 20** Right to data portability **Article 21** Right to object **Article 22** Automated individual decision-making, including profiling	The first of the seven data processing principles outlined in the GDPR is the principle of lawfulness, fairness, and transparency of data processing. **Article 5** provides that personal data shall be: "processed lawfully, fairly and in a transparent manner in relation to the data subject". Under this principle, processing personal data of EU citizens must be *lawful* and meet the GDPR requirements. GDPR text on the lawfulness of processing **Article 6(1)** defines the lawfulness of processing as: "Processing shall be lawful only if and to the extent that at least one of the following applies: (a) data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) necessary for the performance of a contract to which the	**Article 77** Data subjects have a right to complain. **Articles 82 - 84** The rights of data subjects are protected through fines, penalties, and the right to compensation. **GDPR Fines & Data Breach Penalties** [xxvi] "It can be challenging to understand exactly what a violation of GDPR is, and that's because the language of the legislation is deliberately vague. The intent behind this was to have some flexibility in the system and to differentiate between deliberate attempts to ignore the regulations and errors being made when attempting to follow its requirements and become GDPR compliant. Some of the most significant GDPR fines issued to date provide an insight into the often-historical mismanagement of how personal data is processed. This includes the concept of consent, respect for its privacy and the disregard for data

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
				"1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia,		data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (c) necessary for compliance with a legal obligation to which the controller is subject; (d) necessary in order to protect the vital interests of the data subject or of another natural person (e) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."	security. And with organizations the size of Google receiving fines for violation of GDPR it's no wonder that it can be challenging for smaller businesses to find their way around the regulations." "When a data protection authority becomes alerted to GDPR non-compliance within an organization, it can issue information notices, enforcement notices, penalty notices."

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
				the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." The GDPR r**ecognises consent** as a legal basis to process personal information. However, consent under the GDPR cannot be implied.			
California Consumer Privacy Act[xxvii]	**1.81.5. California Consumer Privacy Act of 2018 section 1798.100 & 1798.175** The purpose of the privacy policy is to provide consumers with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information. This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information.	No definition of "privacy" in the GDPR.	**Section 1798.140** (o) (1) "***Personal information***" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security	**Section 1798.105(9)** The Act does not provide an express provision for consent, however, the Act allows business to otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.	**State of California Department of Justice, Office of the Attorney General - Privacy, California Consumer Privacy Act** [xxviii] **Section 1798.150** "The Act gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law. This landmark law secures new privacy rights for California consumers, including: - The right to know about the personal information a business collects about them and how it is used and shared; - The right to delete personal information collected from them (with some exceptions);		Consumers may litigate the violation of their rights and recover damages in an amount not less than ($100 and not greater than $750 per consumer per incident or actual damages. Consumers may additionally seek injunctive or declaratory relief as well as any other relief the court deems proper, akin to an equity savings clause. Consumers may join together in a class and litigate their rights as well.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
			number, driver's license number, passport number, or other similar identifiers. (B) Any categories of personal information described in subdivision (e) of Section 1798.80. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information. (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g). (K) Inferences drawn from any of the information identified in this subdivision		- The right to opt-out of the sale of their personal information; and - The right to non-discrimination for exercising their CCPA rights."		

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
			to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. (2) "Personal information" does not include publicly available information. (3) "Personal information" does not include consumer information that is de-identified or aggregate consumer information."				
Canada: Privacy Act R.S.C., 1985 c. P-21[xxix]	**Section 2** "The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."	No definition of "privacy" in the Act.	**Section 3 Definitions** "***personal information*** means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing, (a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual, (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they are about another individual or	No definition of "consent" in the Act. **Section 7 Use of personal information** "Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except (a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the institution under subsection 8(2)." **Section 8 Disclosure of personal information "(1)** Personal information under the control of a government institution	**Sections 10 and 11** The head of a government institution shall cause to be included in personal information banks all personal information under the control of the government institution that (a) has been used, is being used or is available for use for an administrative purpose; or (b) is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. At least yearly, an index identifying these information banks as well as the governmental organization which has control of the bank shall be published. The Governor in Council may designate certain personal information banks as exempt.	**Sections 9 and 11(2)** Disclosure of personal information is allowed for the purpose for which it was collected as well as for government purposes, prosecution purposes, and other enunciated purposes. Personal information can be used for other purposes but these purposes must be disclosed in the next index of personal information, which shall be published no less than annually. **Section 8** Personal information may be used for any purpose where, in the opinion of the head of the institution, (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or	**Sections 29-35 & sections 41-52** The Privacy Commissioner may receive and investigate complaints as well as initiate complaints regarding violations of the Act as well as the use of personal information. The Privacy Commissioner may initiate and investigate complaints *sua sponte*. Upon completion of this review, the complainant may have access to the information or will be told that access will not be allowed and a judicial determination of the application of the *Privacy Act* will be necessary.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
			about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations, (f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, [...]". The definition provides some specific carve out for the purposes of the Access to Information Act.	shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section." **Section 8(2)** sets out the circumstances under which personal information may be disclosed without consent.	**Section 12(1) Right of Access** "Subject to this Act, every individual who is a Canadian citizen or a permanent resident within the meaning of subsection 2(1) of the Immigration and Refugee Protection Act has a right to and shall, on request, be given access to (a) any personal information about the individual contained in a personal information bank; and (b) any other personal information about the individual under the control of a government institution with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution." **Section 12(2) Other rights relating to personal information** "Every individual who is given access under paragraph (1)(a) to personal information that has been used, is being used or is available for use for an administrative purpose is entitled to (a) request correction of the personal information where the individual believes there is an error or omission therein; (b) require that a notation be attached to the information reflecting any correction requested but not made; and	(ii) disclosure would clearly benefit the individual to whom the information relates.	

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
					(c) require that any person or body to whom that information has been disclosed for use for an administrative purpose within two years prior to the time a correction is requested or a notation is required under this subsection in respect of that information (i) be notified of the correction or notation, and (ii) where the disclosure is to a government institution, the institution makes the correction or notation on any copy of the information under its control."		
Canada: Personal Information Protection and Electronic Documents Act [xxx]	**Section 3** The purpose is to provide rules to govern the collection, use and disclosure of personal information in a manner that recognizes the individual's right of privacy under the circumstances.	No definition of "privacy" in the Act. However, under **section 11**, an individual may file a written complaint with the Privacy Commissioner of Canada or the Commissioner may initiate a complaint.	**Section 2(1) Definitions** "***personal information*** means information about an identifiable individual." "***personal health information***, with respect to an individual, whether living or deceased, means (a) information concerning the physical or mental health of the individual; (b) information concerning any health service provided to the individual; (c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual; (d) information that is collected in the course of providing health services to the individual; or (e) information that is collected incidentally to the	**Section 6.1** The consent of an individual is only valid if it is reasonable to expect that an individual, to whom the organization's activities are directed, would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.	**Sections 8(8) & 37** An organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have. A requirement under a provision of a federal law to retain a document for a specified period is satisfied, with respect to an electronic document, by the retention of the electronic document in the format sent or received, is readable or understandable by a person entitled to it, and transmission and receipt information of the record is retained. **SCHEDULE 1 (Section 5) Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information**	**Sections 7.2, 7.3, 7.4, 7.5, 7.4(1) & 7.4(2).** The Act allows for collection, use, and disclosure without consent in a limited set of circumstances.	**Section 11** The individual may file a complaint in writing with the Privacy Commissioner within 6 months of violation or longer time as the Commissioner may allow, or the Commissioner may initiate a complaint.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
			provision of health services to the individual."		Principle 9 - Individual Access "Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."		
New Zealand: Privacy Act 2020[xxxi]	**Section 3** The purpose of the Act is to promote and protect individual privacy by - (a) providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognizing that other rights and interests may at times also need to be taken into account; and (b) giving effect to internationally recognized privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and the International Covenant on Civil and Political Rights.	There is no definition of "privacy" in this Act. **Privacy Bill, Government Bill 34-1, Explanatory note** **"**The Act regulates the collection, use, and disclosure of personal information." **Section 22** Agencies are subject to 13 information privacy principles. **Privacy Bill, Government Bill 34-1, Explanatory note** If a person thinks their privacy has been breached resulting in harm, they can complain to the Privacy Commissioner who will attempt to resolve the dispute. If not resolved, the person may take the complaint to the Human Rights Review Tribunal and may seek compensation.	**Section 7** The Act protects '***personal information***', which is defined as information about an identifiable individual, which includes information relating to a death that is maintained by the Registrar-General under the Births, Deaths, Marriages, and Relationships Registration Act 1995 or any former Act (as defined in section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995). **Section 113** The Act does not contain a separate category of sensitive information to which special restrictions apply. However, agencies are required to consider whether the data is 'sensitive' when assessing the likelihood of serious harm being caused by a privacy breach. The *Health Information Privacy Code 2020 (NZ)* covers health information.	The Act does not rely on consent. Agencies do not require individual authorization provided it lawfully collects personal information, does only what it intends to do with the information at the time of collection, and is clear about how it is doing so.	**IPP 6 Access to personal information** (1) An individual is entitled to receive from an agency upon request— (a) confirmation of whether the agency holds any personal information about them; and (b) access to their personal information. (2) If an individual concerned is given access to personal information, the individual must be advised that, under IPP 7, the individual may request the correction of that information. (3) This IPP is subject to the provisions of Part 4. **IPP 7 Correction of personal information** (1) An individual whose personal information is held by an agency is entitled to request the agency to correct the information. (2) An agency that holds personal information must, on request or on its own initiative, take such steps (if any) that are reasonable in the circumstances to ensure	**IPP 4** **Manner of collection of personal information** **"**An agency may collect personal information only— (a) by a lawful means; and (b) by a means that, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons),— (i) is fair; and (ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned." The Act requires there is a 'lawful purpose' for collecting, using, holding, or disclosing personal information. The lawful purpose must be connected with a function or activity of the agency collecting the personal	The Act operates on a 'principle' (opposed to more prescriptive) basis. The 13 information privacy principles (IPPs) set out the requirements for the collection, use and disclosure of personal information. **Section 22** The Act attempts to minimize the data collected – clause 22(2) of the Act states that if the lawful purpose for which personal information is being collected does not require the collection of identifying information, then the agency may not require the individual to provide its identifying information.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	Privacy Bill, Government Bill 34-1, Explanatory note[xxxii] The Privacy Act 2020 repealed and replaced the Privacy Act 1993. The key purpose of reforming the Act was to promote people's confidence that their personal information is secure and will be treated properly.		**Sections 164 to 166 and schedule 3.** The Act regulates 'identity information' as a type of information held by one 'holder agency' (a specified list of governmental departments) and accessed by another 'accessing agency' (a similar specific list of government departments) in a manner agreed between the two agencies. There are no specific provisions regulating identity information for non-governmental agencies, other than to the extent it falls into another category of personal information. 'Identity information' includes an individual's biographical details, biometric information, photograph or visual image, New Zealand travel document or certificate of identity, and details of any distinguishing features eg. tattoos and birthmarks. **IPP 4** IPP 4 states an agency may only collect personal information which, in the circumstances of the case (particularly in circumstances where personal information is being collected from children or young persons), (i) is fair; and (ii) does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.		that, having regard to the purposes for which the information may lawfully be used, the information is accurate, up to date, complete, and not misleading. (3) When requesting the correction of personal information, or at any later time, an individual is entitled to— (a) provide the agency with a statement of the correction sought to the information (a statement of correction); and (b) request the agency to attach the statement of correction to the information if the agency does not make the correction sought. Personal information must not be retained indefinitely. **IPP 9** requires agencies not to retain personal information for longer than is necessary for the purposes for which it may lawfully be used. **IPP 11 Limits on disclosure of personal information** (1) An agency that holds personal information must not disclose the information to any other agency or to any person unless the agency believes on reasonable grounds that the disclosure is under certain conditions.	information, and the collection of information must be necessary for that purpose.	

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
Hong Kong: Personal Data (Privacy) Ordinance[xxxiii]	An ordinance to protect the privacy of individuals in relation to personal data, and to provide matters incidental thereto or connected therewith. **Office of the Privacy Commissioner for Personal Data, Hong Kong**[xxxiv] It was introduced to "ensure an adequate level of data protection to retain its status as an international trading centre and give effect to human rights treaty obligations."	There is no definition for "privacy" in the Act.	**Section 2** "***personal data*** means any data— (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable;" "***Data user***, in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data." However, the Office of the Privacy Commissioner for Personal Data has issued guidance in relation to the more stringent collection, use, retention and deletion requirements of certain types of personal data, including identity card numbers, personal identifiers, consumer credit data and biometric data. "Health data" is not specifically defined in the Act and is regarded as "personal data". The Privacy Commission for Personal Data has issued guidance for the handling of patients' health records.	**Data Protection Principle (DPP) 3** If the data user intends to use personal data collected for a new purpose other than that for which it is collected, a data subject's consent must be obtained. **Section 26** A data user must obtain a data subject's consent or indication of no objection before using their personal data for direct marketing purposes. Where the data subject is a minor (i.e. under the age of 18), any prescribed consent required for using personal data for a new purpose can be given on his or her behalf by an individual who has parental responsibility for the minor (see **DPP 3** and **Section 2(1)** of the Act). Such individuals may also make a data access request or a data correction request on behalf of a minor.	**DPP 2—accuracy and duration of retention of personal data** "(1) All practicable steps shall be taken to ensure that— (a) personal data is accurate having regard to the purpose (including any directly related purpose) for which the personal data is or is to be used; (b) where there are reasonable grounds for believing that personal data is inaccurate having regard to the purpose (including any directly related purpose) for which the data is or is to be used— (i) the data is not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or (ii) the data is erased Data users are obliged to ensure personal data is not retained for longer than necessary for the purposes for which the data is to be used." "(2) All practicable steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data is or is to be used." **DPP 6** - Access to personal data	**DPP 1—purpose and manner of collection of personal data** "Personal data must not be collected unless— (a) the data is collected for a lawful purpose directly related to a function or activity of the data user who is to use the data; (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and (c) the data is adequate but not excessive in relation to that purpose. Personal data shall be collected by means which are— (a) lawful; and (b) fair in the circumstances of the case. Where the person from whom personal data is or is to be collected is the data subject, all practicable steps shall be taken to ensure that (a) he is explicitly or implicitly informed, on or before collecting the data, of— (i) whether it is obligatory or voluntary for him to supply the data; and (ii) where it is obligatory for him to supply the data, the consequences for him	Data subjects have a right to bring proceedings in court to seek compensation for damage, including damages for injury to feelings. **Section 38** The Privacy Commissioner has powers under the Act to initiate an investigation when it receives a complaint or on its own initiative if there are reasonable grounds to believe that an act or practice has contravened the requirements under the Act. **Section 36** The Privacy Commissioner also has power to inspect a personal data system for the purposes of ascertaining information to assist the Privacy Commissioner in making recommendations for compliance with the Act. In carrying out an investigation or an inspection, the Privacy Commissioner may enter into premises with either a warrant or prior notice. **Section 48** Apart from issuing an enforcement notice, the Privacy Commissioner may also publish reports in respect of its

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
						if he fails to supply the data; and (b) he is explicitly informed— (i) on or before collecting the data, of— (A) the purpose (in general or specific terms) for which the data is to be used; and (B) the classes of persons to whom the data may be transferred; and (ii) on or before first use of the data for the purpose for which it was collected, of— (A) his rights to request access to and to request the correction of the data; and (B) the name or job title, and address, of the individual who is to handle any such request made to the data user, unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data was collected and that purpose is specified in Part 8 of this Ordinance as a purpose in relation to which personal data is exempt from the provisions of data protection principle 6.	investigation or inspection. **Section 47** Data subjects have the right to be informed on or before the collection of his/her personal data, of whether it is obligatory or voluntary for him/her to supply the data, and the consequences for failing to provide personal data where such provision is obligatory (**DPP 1**).
Personal Data Protection Act (Singapore) [xxxv]	**Section 3** "The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations	No definition of "privacy" in the Act.	**Section 2(1)** '***Personal data***' means data, whether true or not, about an individual who can be identified — (a) from that data; or	No definition of "consent" in the Act. However, "consent" is one of the ten data protection obligations -	Organisations are required to comply with the various data protection obligations[xxxvii] if they undertake activities relating	**Section 14 Provision of consent** **"(2)** An organisation must not —	**Advisory Guidelines on the Key concepts in the PDPA** [xxxix] **Para 10.2**

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances."		(b) from that data and other information to which the organisation has or is likely to have access; **Scope of the PDPA** [xxxvi] "The PDPA covers personal data stored in electronic and non-electronic formats. It generally does not apply to: (a) Any individual acting on a personal or domestic basis. (b) Any individual acting in his/her capacity as an employee with an organisation. (c) Any public agency in relation to the collection, use or disclosure of personal data. (d) Business contact information such as an individual's name, position or title, business telephone number, business address, business email, business fax number and similar information."	i.e. consent is required. The PDPA allows organisations to only collect, use or disclose personal data for purposes which an individual has given his/her consent to. **Section 13** "An organisation must not, on or after 2 July 2014, collect, use or disclose personal data about an individual unless — (a) the individual gives, or is deemed to have given, his or her consent under this Act to the collection, use or disclosure, as the case may be; or (b) the collection, use or disclosure (as the case may be) without the individual's consent is required or authorised under this Act or any other written law." **Section 16 Withdrawal of consent** Allow the individual to withdraw consent, with reasonable notice, and inform him/her of the likely consequences of withdrawal. Once consent is withdrawn, make sure that you cease to collect, use or disclose the individual's personal data. **Section 17**	to the collection, use or disclosure of personal data. The sections of the PDPA which set out these obligations are noted below for reference. (1) The **Consent** Obligation (ss 13 - 17) (2) The **Purpose Limitation** Obligation (s18) (3) The **Notification Obligation** (s 20) (4) The **Access and Correction** Obligations (ss 21, 22 and 22A) (5) The **Accuracy Obligation** (s 23) (6) The **Protection** Obligation (s 24) (7) The **Retention Limitation** Obligation (s 25) (8) The **Transfer Limitation** Obligation (s 26) (9) The **Data Breach Notification** Obligation (ss 26A to 26E) (10) The **Accountability** Obligation (ss 11 and 12) See also: Data portability (**Part VIB - Personal Data Protection (Amendment) Bill**) [xxxviii]	(a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or (b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices." **Collection, Use And Disclosure Of Personal Information Without Consent -** ***First Schedule Part 3 Legitimate Interests*** "1.—(1) Subject to sub-paragraphs (2), (3) and (4) — (a) the collection, use or disclosure (as the case may be) of personal data about an individual is in the legitimate interests of the organisation or another person; and (b) the legitimate interests of the organisation or other person outweigh any	"Organisations are required to comply with the Data Protection Provisions in Parts 3 to 6A of the PDPA (**para 10.1**). Broadly speaking, the Data Protection Provisions contain ten main obligations which organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data." **Para 22.1** "Offences under **Part 9B** of the PDPA hold individuals accountable for egregious mishandling of personal data in the possession of or under the control of an organisation (including a public agency). The offences are for: a) Knowing or reckless unauthorised disclosure of personal data; b) Knowing or reckless unauthorised use of personal data for a gain for the individual or another person, or to cause a harm or a loss to another person; and c) Knowing or reckless unauthorised re-identification of anonymized information."

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
				Collection, use and disclosure without consent - in some circumstances.		adverse effect on the individual."	
Artificial Intelligence Act (EU) [xl]	Key purpose is a risk based framework for participants in the European Union (**EU**) Artificial Intelligence (**AI**) systems market. Regulation is proportionate to risk - from minimal risk or limited risk to prohibition of AI systems with unacceptable risks. For the establishment of common standards for providers and operators of high-risk AI systems to ensure a consistent high level of protection of public interests regarding health, safety and fundamental rights. **Article 3** AI system means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with. **Article 1**	There is no definition of "privacy" in the proposed Act. However, the proposed Act was drafted on the basis of existing fundamental rights to privacy or private life, which is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8), and the European Charter of Fundamental Rights (Article 7). In addition, the European Charter of Fundamental Rights (Article 8) also enshrines the right to the protection of personal data. **UDHR Article 12** [xli] No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.	Personal information/data based on four tiers of risk. **Article 5** Tier 1: Unacceptable risks are prohibited: certain types of social scoring and biometric surveillance to be an "unacceptable" risk to privacy, nondiscrimination, and related human rights **Articles 6 and 7** Tier 2: "High-risk" AI systems: regulation designates an expansive list of AI systems as "high-risk" that would require extra safeguards. For example: - determining access to education and vocational training; - recruitment or selection of natural persons; - decision making on promotion and termination of work-related contracts; - access to and enjoyment of essential private and public services and benefits; - law enforcement; - migration, asylum and border control management; - administration of justice and democratic processes. Two main categories of high-risk AI systems: - AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment;	The term 'consent' is not expressly mentioned. Consent may be more related to the specific uses of the AI systems after entry into the market. Because the AI Act is concerned with regulating the types of AI systems and requiring regulatory compliance, consent is not expressly provided for. Though presumably, any existing EU regulation related to data privacy would capture consent and should apply to high-risk AI systems. The Act is primarily aimed at regulating operators, providers, distributors of AI systems rather than the point at which natural persons may interact with the AI system.	No specific ongoing measures to deal with personal information/data. **Chapter 2 (Articles 8 to 15)** sets out the requirements for high-risk AI systems to comply with including: **Article 9**: a risk management system; **Article 14**: human oversight aimed at preventing or minimising the risks to health, safety or fundamental rights that may emerge; **Article 15**: accuracy, robustness and cybersecurity requirements In addition, there is a requirement for providers to have a quality management system (**Article 17**) and an obligation to take corrective actions (**Article 21**).	This is more in relation to the risks and uses associated with AI system products. **Article 3 Definitions** "'**intended purpose**' means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation; '**reasonably foreseeable misuse**' means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems. **Article 9** requires high risk AI systems to have a risk management system, which includes: identification and analysis of the known and foreseeable risks associated with each high-risk AI system; and estimation	Risk-based approach from limited risk to prohibited unacceptable risks. But again, focus is not on the end user or natural persons who may be affected by the AI systems. Their rights are not expressly protected by the proposed Act.

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	(a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('**AI systems**') in the Union; (a) prohibitions of certain artificial intelligence practices; (b) specific requirements for high-risk AI systems and obligations for operators of such systems; (c) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content; (d) rules on market monitoring and surveillance. **See also context of the proposed AI Act from explanatory memorandum** "Based on EU values and fundamental rights and aims to give people and other users the confidence to embrace AI-based solutions, while encouraging businesses to develop them.		- other stand-alone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III. **Article 52** Tier 3: Limited-risk AI systems: systems include "biometric categorization," emotion recognition, and deep fake systems. Tier 4: Minimal-risk AI systems are all other systems not covered by the regulation's requirements and safeguards.			and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse. **Article 13** This Article also references the provision of information to users including the intended purpose or reasonably foreseeable misuse. **Article 29** Users of high-risk AI systems shall use such systems in accordance with the instructions of use accompanying the systems.	

Regulations	Purpose of legislation	How is privacy defined and treated?	How is personal information defined?	How is consent dealt with?	How is ongoing control of personal information/data dealt with?	Fair and reasonable and legitimate use	How are rights protected?
	Proposed regulatory framework on Artificial Intelligence with the following specific objectives: - ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values; - ensure legal certainty to facilitate investment and innovation in AI; - enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; - facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.”						

End Note References

[i] These Schedules 1 & 2 have been prepared as part of the background research and analysis required to formulate the DLA's submission the Privacy Act Discussion Paper 24 January 2022. Compilation of this table has been a joint effort by numerous DLA contributors. While every effort has been made to ensure correct citation and references, readers should confirm citations, references and quotations before relying, citing or referencing any information in this table. Some citations may be lost in conversion of the file format of this document. Unless stated otherwise, websites have been viewed between November 2021 and January 2022.

[ii] https://www.legislation.act.gov.au/a/2014-24/

[iii] https://www.legislation.act.gov.au/a/1997-125/

[iv] https://legislation.nsw.gov.au/view/html/inforce/current/act-1998-133

[v] https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-071

[vi] https://legislation.nt.gov.au/en/Legislation/INFORMATION-ACT-2002

[vii] https://www.legislation.qld.gov.au/view/html/inforce/current/act-2009-014

[viii] https://www.legislation.tas.gov.au/view/html/inforce/current/act-2004-046

[ix] https://www.legislation.vic.gov.au/in-force/acts/privacy-and-data-protection-act-2014

[x] https://www.legislation.vic.gov.au/in-force/acts/health-records-act-2001/046

[xi] https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_43115.pdf/$FILE/Freedom%20Of%20Information%20Act%201992%20-%20%5B07-d0-00%5D.pdf?OpenElement

[xii] https://www.legislation.gov.au/Details/C2021A00076

[xiii] https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6680_ems_3499aa77-c5e0-451e-9b1f-01339b8ad871/upload_pdf/JC001336%20Clean4.pdf;fileType=application%2Fpdf

[xiv] https://www.legislation.gov.au/Details/C2019A00038

[xv] https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fs1201_ems_08b22f92-a323-4512-bf31-bc55aab31a81%22

[xvi] https://www.legislation.gov.au/Details/C2021C00452

[xvii] https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/6-reasonable-expectation-of-privacy/a-test-for-what-is-private/#_ftn1

[xviii] https://doi.org/10.1016/j.future.2020.10.017

[xix] https://www.legislation.gov.au/Details/C2021C00570

[xx] Home Affairs website (accessed on 14 Dec 2021): https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018

[xxi] G+T Law, Security of Critical Infrastructure Act reforms – what your business needs to know (Nov 2021) Mandatory Reporting of cyber incidents, https://www.gtlaw.com.au/knowledge/security-critical-infrastructure-act-soci-reforms-what-your-business-needs-know

[xxii] https://www.legislation.gov.au/Details/C2021B00108

[xxiii] https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6649_first-reps/toc_pdf/20174b01.pdf;fileType=application%2Fpdf

[xxiv] https://gdpr.eu/tag/gdpr/

[xxv] https://www.gdpreu.org/the-regulation/key-concepts/personal-data/#:~:text=The%20GDPR%20states%20that%20data%20is%20classified%20as,identification%20number%2C%20IP%20addresses%2C%20or%20their%20location%20data.

[xxvi] https://www.gdpreu.org/compliance/fines-and-penalties/#:~:text=%20Has%20Anyone%20Been%20Fined%20for%20GDPR%20Breaches%3F,its%20employees.%20The%20German%20data%20protection...%20More%20

[xxvii] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375

[xxviii] https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act,how%20to%20implement%20the%20law.&text=The%20right%20to%20non%2Ddiscrimination%20for%20exercising%20their%20CCPA%20rights

[xxix] https://laws-lois.justice.gc.ca/eng/acts/p-21/page-1.html#h-397172
[xxx] https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html
[xxxi] https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html
[xxxii] https://www.legislation.govt.nz/bill/government/2018/0034/29.0/d56e2.html
[xxxiii] https://www.elegislation.gov.hk/hk/cap486!en-zh-Hant-HK.pdf?FROMCAPINDEX=Y
[xxxiv]https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html#:~:text=DPP3%20prohibits%20the%20use%20of,previously%20given%20by%20written%20notice
[xxxv] https://sso.agc.gov.sg/Act/PDPA2012
[xxxvi] https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act#:~:text=The%20Personal%20Data%20Protection%20Act,for%20personal%20data%20in%20Singapore.&text=It%20comprises%20various%20requirements%20governing,Not%20Call%20(DNC)%20Registry.
[xxxvii] https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act/Data-Protection-Obligations
[xxxviii] https://sso.agc.gov.sg/Bills-Supp/37-2020/Published/20201005?DocDate=20201005#:~:text=26H.,in%20the%20data%20porting%20request.
[xxxix] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Oct-2021.pdf?la=en
[xl] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206
[xli] https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=eng