Data Privacy

Jurisdiction + Legislation	Scope	Right to Access	Right to Portability	Right to Correction	Right to Stop Processing	Right to Stop Automated Decision Making	Right to Stop Third Party Transfer	Right to Erasure	Right to Equal Services and Price	Private Right of Action Damage	Regulator Enforcement Penalties	Data Breach Notification	Data Localization Requirement
EU **(GDPR)**	EU personal data processed.	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	〰 Data can be stored outside of the EU, but only if the collector still abides by EU regulations in foreign data centers.
Brazil ***(LDPR)**	Applies to data processed in Brazil and collected in Brazil.	✔	✔	✔	✔	〰 Data subjects have the right to review the data but not to stop it.	〰	✔	〰 At most, implicitly required.	✔	✔	✔	〰 Similar to the GDPR, data can be stored outside of the country, but only if it is put under the same regulations as exist within Brazil.
China ***Cybersecurity Law Peoples Republic of China** **China's Personal Information Security Specification**	Any system that operates within the networks of China and compiles data of users within China.	✔	〰 Only certain kinds of personal information need to be made portable.	✔	✔	〰 Can appeal an automated decision.	〰 Must be notified of any third-party transfer before information is collected, no way to stop such transfer after the initial consent.	〰 Erasure can only take place after account deletion, or when a data breach occurs.	✘	✘	✔	✔	✘ Comprises not only citizens' personal data but any and all data outside of China.
India ***The Personal Data Protection Bill**	Any data processed or collected on government entities, businesses, or citizens in India.	✔	✔	✔	✘ Right to restrict data from being used and collected after it has fulfilled the purpose for which it was collected, or when consent has been withdrawn. All previous data collected may be stored in perpetuity.	✘ No clear language that discusses this.	✘	〰 The right to restrict or prevent continuing disclosure of personal data under certain conditions. Erasure is not specifically mentioned. Data must be deleted if it is no longer necessary for it to be retained by the data fiduciary.	✘ No clear language discussing this in the text.	✔	✔	〰 All breaches must be reported to the government, who will then make a call as to whether or not the breach should be shared with the public, and determine what actions need to be done in response.	✘
Russia	All companies, persons, and agencies collecting data within Russia that are not engaging in personal/family needs, organization of archives, forming the Unified State Register of Individual Entrepreneurs, or the processing of personal data classified as data constituting state secrets following the statutory procedures.	✔	✘	✔	✔	〰 Right to raise an objection, and a need for response from the company.	〰 Within Russia no, but companies must have the same amount of security as the initial data collector.	✘ Similar to in China this is only for companies, the state absolutely has power to keep all data in perpetuity.	✘	✔	〰 No monetary penalty specified, Roskomnadzor has the right to close a website.	✘ Once notified of a breach by either the Roskomnadzor or a customer, they must report it. However, there is no requirement to reach out to either beforehand.	✘

Data Privacy

Jurisdiction + Legislation	Scope	Right to Access	Right to Portability	Right to Correction	Right to Stop Processing	Right to Stop Automated Decision Making	Right to Stop Third Party Transfer	Right to Erasure	Right to Equal Services and Price	Private Right of Action Damage	Regulator Enforcement Penalties	Data Breach Notification	Data Localization Requirement
California **(CCPA and other proposed laws)**	California residents' personal data collected.	✔	✔	✘	✔	✘	✔	〰 Right to erase personal data collected, under certain conditions.	✔	✔	✔	✔	✘
New York Laws ***Right to Know Act of 2019 and the *SHIELD Act**	Both the SHIELD Act and Right to Know Act apply to companies who gather a New York resident's personal information, whether the company is based in the state or not.	✔	✘ Not mentioned in the laws.	✘	✘ Not mentioned in the laws.	✘ Not mentioned in the laws.	〰 Does not state that individuals can stop the transfer, but the company must notify individuals when transferring data to third parties.	✘	✘ Not explicitly stated or discussed in the laws.	✘ Right to Know Act 2019 allows an individual to bring a civil action to recover penal-ties. Specific amounts are not mentioned.	✘ Right to Know Act 2019 allows an attorney general, a district attorney, a city attorney, or a city prosecutor to bring a civil action to recover penalties. Specific amounts are not mentioned.	✘ Part of Section 899-AA of the General Business Law, to be expanded in the proposed SHIELD Act.	✘
Washington ***2SSB 5376 and RCW 19.255.010**		✔	✔	✘ Must delete the consumer's personal data if certain grounds apply.	〰 Can restrict processing under certain grounds. Unclear language on stopping it completely.	〰 When facial recognition is involved, human review is necessary. No specific language on stopping this after consent is given.	〰 When a consumer objects to targeted advertising, the controller must no longer process the personal data subject to objection and communicate the consumer's objection to any known third parties to whom the controller sold the data.	✔	✔ No explicit language discussing this in the text.	✔	✔	✔	✘