HERZOG

HERZOG FOX & NEEMAN

The Complete EU v. US Data Protection Laws Playbook

For a Uniform Data Protection Approach

June 2022

Introduction

The European General Data Protection Regulation ("**GDPR**") came into force 4 years ago, and introduced a new uniform and comprehensive data protection regime affecting companies all over the world. Absent a similar comprehensive US Federal legislation, the data protection in the United States was generally left in the various states legislators' hands.

Until recently, the only comprehensive consumer data protection law in the United States was the California Consumer Privacy Act ("**CCPA**"). However, a growing number of US state legislators hav e been adopting similar data protection regulatory regimes, **many of which are coming into effect next year:**

- The **CPRA** | A significant amendment to the California CCPA is coming into effect on 1 January 2023;
- The **VCDPA** | The Virginia Consumer Data Protection Act will too come into effect on 1 January 2023;
- The **CPA** | The Colorado Privacy Act, which was enacted in July 2021, will come into effect on 1 July 2023;
- The **UCPA** | the forth state to adopt a new privacy law was Utah, and its Utah Consumer Privacy Act will come into effect on 31 December 2023.

In addition to the above, Connecticut has also enacted a new privacy framework that will enter into force in 2024, and more states are expected to join the trend. The rise of various states' data protection acts requires companies processing personal data on a global basis to change their regional regulatory approach (as many did with respect to their EU originated data) and **adopt a more uniform approach to addressing their data protection regulatory obligations** in the EU and the United States.

This playbook provides a general **comparison between the relevant concepts and requirements** in the enacted US data protection laws, in addition to the GDPR, consequently assisting in **generating a uniform data protection policy.**

Table of Content

1. Scope

The US data protection laws, similarly to the GDPR, apply to data controllers that are established within the respective territory or - even if not established there - are offering goods or services to the respective residents, and their processors, who collect or process personal data. The laws differ, however, in the definitions of "controller", "processor", and "data subjects" (or their equivalent terms); the scope of types of data subjects; the minimum thresholds for the material and jurisdictional applicability based on the number of respective consumers, the share of revenues derived from such consumer's processing of data of the annual gross revenue, and the business total annual revenue.

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Territorial Scope	1. Established in the EU; or 2. Offers goods or services to data subjects in the EU; or 3. Monitor behavior of data subjects in the EU	Doing Business in CA, and: (a) annual gross revenue exceeding $25M; or (b) buys, receives, sells, or shares, for commercial purposes, more than 100,000 consumers, households, or devices; or (c) derives 50% of its annual revenues from Selling or Sharing consumers' PI	1. Conduct business in VA; or 2. Produce products or services to residents of VA; **and:** a) at least 100,000 consumers during a calendar year; or b) at least 25,000 consumers + derive over 50% of gross revenue from selling personal information ("**PI**")	1. Conduct business in CO; or 2. Produce commercial products or services that are intentionally targeted to residents of CO; **and:** a) at least 100,000 consumers during a calendar year; or b) at least 25,000 consumers + derive revenue or receive discount from the sale of PI	1. Conduct business in UT; or 2. Produce commercial products or services that are intentionally targeted to residents of UT; **and:** 1) over $25M annual revenue; **and:** a) at least 100,000 consumers during a calendar year; or b) at least 25,000 consumers + derive over 50% of gross revenue from selling PI

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Material Scope	**"Data Subject":** 1. Natural persons (not legal entities) 2. identified or identifiable 3. Not necessarily EU residents **"Controller":** Determines the means and purposes of processing activities **"Processor":** Processes Personal Data on behalf of a Controller	**"Consumer":** 1. Natural person (not legal entities) 2. California resident **"Business":** 1. For-profit 2. Collects consumers' PI 3. Determines purposes & means 4. Does business in CA (as defined under the Territorial Scope) **"Service Provider":** Processes PI on behalf of a Business **"Contractor":** PI is made available from Business for a Business Purpose	"Consumer": 1. Natural person (not legal entities) 2. VA resident 3. Only in an individual or household context, and not when acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context **"Controller":** Determines the means and purposes of processing activities, excluding authorities of VA **"Processor":** Processes PI on behalf of a Controller	**"Consumer":** 1. Natural person (not legal entities) 2. CO resident 3. Only in an individual or household context, and not when acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context **"Controller":** Determines the means and purposes of processing activities **"Processor":** Processes PI on behalf of a Controller	"Consumer": 1. Natural person (not legal entities) 2. UT resident 3. Only in an individual or household context, and not when acting in a commercial or employment context, as a job applicant, or as a beneficiary of someone acting in an employment context **"Controller":** Determines the means and purposes of processing activities, excluding: 1. Governmental entities 2. Tribes 3. Higher education institutions 4. Nonprofit corporations **"Processors":** Processes PI on behalf of a Controller
Date In-Effect	25 May 2018	CCPA - 1 January 2020 CPRA - 1 January 2023	1 January 2023	1 July 2023	31 December 2023

2. Key Definitions

Key definitions in data protection regulations affect the regulations' applicability and obligations. The GDPR has, generally, a more extensive definition of personal data than the various US laws, extending its applicability. However, the various US laws include variable definitions for "selling", imposing additional obligations for certain sharing for monetary consideration, which are not specifically addressed by the GDPR. The US laws also exclude from their applicability various types of data that are regulated by specific Federal or sectorial privacy laws, and in some cases treats business purpose and business data differently than under the GDPR.

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Personal Data / Information	Information relating to an identified or identifiable natural person, excluding: 1. Non-automated nor a part of a filing system information 2. Processed by a natural person purely for personal or household purposes	Information that identifies, relates to, describes, is reasonably capable of being associated to or linked with a Consumer of household, excluding: 1. Information regulated under other Federal legislations (e.g., HIPAA, GLBA) 2. Publicly available PI, including information made available by Consumer	Information that is linked or reasonably linkable to an identified or identifiable natural person, excluding: 1. Information regulated under other Federal legislations (e.g., HIPAA, GLBA) 2. Publicly available PI	Information that is linked or reasonably linkable to an identified or identifiable natural person, excluding: 1. Information regulated under other Federal legislations (e.g., HIPAA, GLBA) 2. Publicly available PI	Information that is linked or reasonably linkable to an identified or identifiable natural person, excluding: 1. Information regulated under other Federal legislations (e.g., HIPAA, GLBA) 2. Publicly available PI

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Selling	Not specifically defined	Communicate PI for monetary or other valuable consideration except for: 1. If directed by Consumer 2. Opt-out signaling 3. Necessary for "Business Purpose" 4. Merger, acquisition, bankruptcy, or similar transaction	Exchange of PI for monetary consideration except for: 1. Disclosure to Processor 2. Third party with whom the Consumer has a direct relationship for the same purpose 3. Affiliate of the Controller 4. Consumer intentionally made available to the general public or didn't restrict to a specific audience 5. Merger, acquisition, or bankruptcy.	Exchange of PI for monetary or other valuable consideration except for: 1. Disclosure to Processor; 2. Third party for providing a service or product that the Consumer requested. 3. Affiliate of the Controller; 4. Consumer intentionally made available to the general public or didn't restrict to a specific audience; 5. Merger, acquisition, or bankruptcy.	Exchange of PI for monetary consideration except for: 1. Disclosure to Processor 2. Affiliate of the Controller 3. Consistent with a consumer's reasonable expectations 4. If the Consumer directs the Controller 5. Consumer intentionally made available to the general public or didn't restrict to a specific audience 6. Merger, acquisition, or bankruptcy
Business Purpose	N/A	1. Auditing interactions with Consumers 2. Security 3. Debugging/repair 4. Certain short-term uses 5. Performing services 6. Internal research for tech development 7. Quality and safety maintenance and verification	N/A	N/A	N/A

3. Principles

Article 5 of the GDPR outlines key principles for its data protection regime. The key principles are the heart of data protection best practices under the GDPR, and as such, they are fundamental for full compliance. While the US data protection laws do not include distinguished principles provisions, many have embedded similar principles through other provisions relating to the Controller's obligations.

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Legal Grounds for Processing	A general principle, implemented through legal grounds limitations for processing Personal Data: 1. Consent 2. Performance of a contract 3. Legal obligation 4. Vital interest of the Data Subject; 5. Public interest; 6. Legitimate interest.	No requirement for a defined legal grounds	No requirement for a defined legal grounds	ENo requirement for a defined legal grounds	No requirement for a defined legal grounds
Fairness	Personal Data shall be processed fairly	Embedded through the right to no discrimination	Embedded through the right to no discrimination	Imposes a "duty to avoid unlawful discrimination"	Embedded through the right to no discrimination
Transparency	Personal Data shall be processed transparently, + specific requirements regarding information to be provided by privacy notice	Embedded through the privacy notice disclosure obligations	Embedded through the privacy notice disclosure obligations	Imposes "duty of transparency" on Controllers	Embedded through the privacy notice disclosure obligations
Purpose Limitation	Personal Data shall be collected for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes	The CPRA prohibits the collection of PI for additional purposes that are incompatible with the disclosed ones	Prohibits processing of PI for additional purposes not reasonably necessary to, or compatible with, the disclosed purposes	Imposes "duty of purpose specification" and "duty to avoid secondary use", prohibiting the processing of PI for purposes that are not reasonably necessary to, or compatible with, the disclosed specified purposes	Only partially embedded through the right to opt-out of processing for certain purposes, and by generally referring in a clause header to Controller's responsibility to "consent for secondary use" without further specifications

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Data Minimization	Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the disclosed purposes	Prohibits Businesses from collecting PI only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used, and shared	Limits the collection of PI to what is adequate, relevant, and reasonably necessary in relation to the disclosed purposes	Imposes "duty of data minimization" limiting the PI collection to adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes	Only partially embedded by generally referring in a clause header to Controller's responsibility to "data minimization" without further specifications
Accuracy	Personal Data shall be accurate and kept up to date + specific requirements through Data Subjects rights	Embedded by the CPRA through the Consumers' right to correct inaccurate PI	Embedded through the Consumers' right to correct inaccuracies in their PI	Embedded through the Consumers' right to correct inaccuracies in their PI	N/A
Storage Limitation	Personal Data shall be kept in a form that permits identification for no longer than necessary for the purposes, excluding: 1. Public interest 2. Scientific or historical research 3. Statistical purposes	Only partially embedded in the CPRA through the following two alternatives: 1. If the retention period is disclosed – no specific length limitation applies 2. If criteria for retention period determination are disclosed – retention will be limited to what is reasonably necessary for the disclosed purpose	N/A	N/A	N/A
Integrity & Confidentiality	Personal Data shall be processed in a manner that ensures appropriate security	The CPRA imposes a duty on Businesses to implement reasonable security procedures and practices appropriate to the nature of PI, to protect them from unauthorized or illegal access	PI shall be subject to reasonable administrative, technical, and physical measures to protect the confidentiality, integrity, and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to Consumers	Embedded through the "duty of care", obliging Controllers to take reasonable measures to secure PI during both storage and use	Embedded through the Controller's obligation to implement security measures to protect the confidentiality and integrity of PI
Accountability	Regarding the principles, the Controller is: 1. Responsible 2. Able to demonstrate compliance	Business is directly accountable to Consumers	Controllers are responsible for complying with the "duties" towards Consumers	Controllers are responsible for complying with the principles towards Consumers	Controllers are responsible for complying with the principles towards Consumers

4. Data Subjects Rights

Data Subjects' rights mostly resemble in both GDPR and the US data protection law. However, the US data protection laws developed a new right to no discrimination against Consumers for exercising their rights. In addition, the US data protection laws limited the right to opt-out only from several types of processing, unlike the GDPR's wider approach to opting-out of processing.

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Erasure / Delete	V	V	V	V	V
Rectification / Correction	V	V - granted in the CPRA	V	V	V
Access / Disclosure	V	V - limited to PI collected in the past 12 months	V	V	V
Portability	V	V - granted in the CPRA	V	V	V
Object / Opt-Out	1. Object Processing that is based on public interest of the controller's legitimate interest 2. Object Processing for direct marketing purposes 3. Object Processing for scientific or historical research or statistical purposes 4. Restrict Processing 5. Object automated decision-making, including profiling	1. Selling or Sharing of PI used for cross-context behavioral advertising (including "Do Not Sell or Share My Personal Information" box) 2. Automated decision-making technology 3. Limit the use of Sensitive PI (including "Limit the Use of my Sensitive Personal Information" box) Additional requirements: 1. Not to require Consumers to create an account 2. Not to require additional information	of Processing for the purposes of: 1. Targeted advertising 2. Sale of PI 3. Profiling	of Processing for the purposes of: 1. Targeted advertising 2. Sale of PI 3. Profiling	of Processing for the purposes of: 1. Targeted advertising 2. Sale of PI
No Discrimination	X	V	V	V	V

5. Categories of Sensitive Data

Data protection regulations imposes additional requirements for two types of data considered sensitive. The first is the "Special Categories" of data under the GDPR or "Sensitive Personal Information" under US data protection laws. The laws differ in both the types of personal data included in the heightened protection and the special measures required to protect such sensitive data. The second type is children's personal data, regarding which there are sometimes different age threshold, and various heightened measures to protect children's data.

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Types of Personal Data	1. Racial or ethnic origin 2. Political opinion 3. Religious or philosophical beliefs 4. Genetic or biometric data 5. Health data 6. Sex life or sexual orientation 7. Trade union membership	1. Race, ethnicity, religious or philosophical beliefs 2. Genetic or biometric data 3. Health information 4. Sex life or sexual orientation 5. Union membership 6. Content of nonpublic communication (mail, email, and text messages) 7. Government identifier 8. Precise geolocation 9. Financial account and login information	1. Racial or ethnic origin 2. Religious beliefs 3. Genetic or biometric data 4. Mental or physical health 5. Sexual orientation 6. Citizenship or immigration status 7. Known child 8. Precise geolocation	1. Racial or ethnic origin 2. Religious beliefs 3. Genetic or biometric data 4. Mental or physical health 5. Sex life or sexual orientation 6. Citizenship or citizenship status 7. Known child	1. Racial or ethnic origin 2. Religious beliefs 3. Genetic or biometric data 4. Mental or physical health 5. Sexual orientation 6. Citizenship or immigration status 7. Precise geolocation

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Special Data Protection Requirements	Processing is prohibited, except for: 1. Explicit consent 2. Necessary for exercising rights of employment, social security, and social protection law 3. Necessary to protect vital interests of the Data Subject or another person when the Data Subject is physically or legally incapable of giving consent 4. By a non-profit body, on its members or former members, with appropriate safeguards and no further disclosure 5. Manifestly made public by the Data Subject 6. Proportionate substantial public interest 7. Preventive or occupational medicine 8. Public health 9. Proportionate scientific, historical, or statistical research	1. Disclosure of categories of Sensitive PI collected, shared, and sold 2. Purpose limitation to the disclosed purpose 3. Opt-out right of use and disclosure, despite what is necessary to perform the services or provide the goods reasonably expected by an average Consumer EXCEPTIONS: 1. Sensitive PI that is collected or processed without the purpose of inferring characteristics about a Consumer	1. Processing requires consumers' consent. Children's processing of sensitive data shall be according to Children's Online Privacy Protection Act 2. Risk assessment on the processing of sensitive data	1. Processing requires consumers' consent. Children's processing of sensitive data shall be according to Children's Online Privacy Protection Act 2. Risk assessment on the processing of sensitive data	1. Clear notice 2. Opportunity to opt-out of processing 3. Children's processing of sensitive data shall be according to Children's Online Privacy Protection Act
Children's Data	Required guardian consent up to the age of 13-16, depending on the EU Member.	1. Required guardian's consent up to the age of 16 2. Exceptions for Businesses that didn't have actual knowledge of the child's age 3. Selling or Sharing of minors' data is subject to explicit opt-in consent 4. If an opt-in request is declined, Businesses cannot ask again for 12 months	1. Required guardian consent up to the age of 13 (according to COPPA) 2. Defined as a "Sensitive PI"	1. Processing requires guardian consent up to the age of 13 (as well as according to COPAA)	1. Required guardian consent up to the age of 13 (according to COPPA) 2. Defined as a "Sensitive PI"

6. Controller and Processor Obligations

Under the GDPR and US data protection laws, every person or entity that collects or processes personal data, wither as a controller or processor, is subject to specific obligations with respect to the processing. The following tables list the key obligations each law imposes, with a specific comparable focus on the more central and rigorous ones.

6.1 Privacy Notice

The US data protection law, similarly to the GDPR, requires a disclosure through a privacy notice, that includes the following information:

GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
1. Contact details of the Controller, and its representative 2. Contact details of the DPO 3. Purposes of processing 4. Legal basis 5. Legitimate interests 6. Categories of recipients 7. Cross-border transfers' existence and basis 8. Retention period or the determination criteria 9. Data Subjects rights 10. The right to withdraw consent 11. The right to lodge a complaint with a supervisory authority 12. Automated decision-making Personal data not obtained from the data subject requires the additional following disclosures: 1. Categories of Personal Data 2. Sources of Personal Data	1. Categories of PI 2. Categories of sources 3. Business or commercial purposes 4. Categories of recipients 5. Consumers' rights 6. Categories of PI sold or shared 7. Categories of PI disclosed for Business Purpose 8. Purposes of Selling or Sharing PI, including the PI value 9. Categories of Sensitive PI 10. Retention period 11. Automated decision-making 12. Authorized agent instructions 13. Actual knowledge of selling children's PI 14. If collects over PI of over 10M Consumers annually - metrics of Consumer's requests 15. Update every 12 months	1. Categories of PI 2. Purpose of processing 3. Consumers' rights procedure and right to appeal 4. Categories of shared PI 5. Categories of recipients 6. Selling PI for targeted advertising 7. Contact of Attorney General for lodging a complaint 8. Commitment not to re-identify de-identified data	1. Categories of PI 2. Purpose of processing 3. Consumers' rights procedure and right to appeal 4. Categories of shared PI 5. Categories of recipients 6. Selling PI for targeted advertising 7. Contact of Attorney General for lodging a complaint	1. Categories of PI 2. Purpose of processing 3. Consumers' rights procedure and right to appeal 4. Categories of shared PI 5. Categories of recipients 6. Selling PI for targeted advertising

6.2 Data Processing Addendum

Both the GDPR and the various US data protection laws impose requirements concerning mandatory data processing agreements contracts governing data transfer between controllers and processors, subjecting the data receiving party to the following key obligations:

GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
"Processor": Processes personal data on behalf of the Controller	"Contractor": Business makes PI available for a Business Purpose "Service Provider": Processes PI on behalf of a Business	"Processor": Processes personal data on behalf of the Controller	"Processor": Processes personal data on behalf of the Controller	"Processor": Processes personal data on behalf of the Controller
1. Process Personal Data only according to documented instructions (including the duration, nature and purpose of processing, the type of personal data and categories of data subjects) 2. Personnel's confidentiality (contractual or statutory) 3. Appropriate security measures 4. Sub-processors engagement conditions 5. Data Subject requests assistance 6. Assistance in complying with security breach notifications and data impact assessments 7. Delete or return Personal Data at the end of the services 8. Make available information necessary to demonstrate compliance	1. Purposes of processing 2. Same level of privacy protection as required under the CPRA 3. Grant Businesses the right to take reasonable and appropriate steps to ensure compliance 4. Notify if it can no longer meet its obligations 5. Grant Businesses the right to take reasonable and appropriate steps to stop and remediate unauthorized use of PI. 6. Prohibits from Selling or Sharing of PI 7. Prohibits from retaining, using, or disclosing PI other than for the Business Purpose 8. Prohibits from retaining, using, or disclosing PI outside the direct business relationship with the Business 9. Prohibits combining PI with other Businesses' PI 10. Certification that the Contractor understands the restrictions and complies with them 11. Permit monitoring to ensure compliance, including ongoing manual review, automated scans, and regular assessments and audits every 12 months 12. Sub-Contractors/Service Providers: Notify Business and a written contract binding to the same requirements 13. Take reasonable measures to ensure that de-identified information cannot be associated with a Consumer or household, and publicly commit not to re-identify	1. Instructions for processing 2. Nature and purpose of processing 3. Type of data subjects 4. Duration of processing 5. Personnel's confidentiality 6. Delete or return Personal Data at the end of the services 7. Make available information necessary to demonstrate compliance 8. Allow and contribute to reasonable audits and inspections 9. Take reasonable measures to ensure that de-identified information cannot be associated with a Consumer or household, and publicly commit not to re-identify	1. Instructions for processing 2. Nature and purpose of processing 3. Type of data subjects 4. Duration of processing; 5. Personnel's confidentiality 6. Subcontractors' engagement is subject to Controller's right to object, and subcontractor's requirement to meet the same obligations 7. Appropriate security measures 8. Delete or return Personal Data at the end of the services 9. Make available information necessary to demonstrate compliance 10. Allow and contribute to reasonable audits and inspections	1. Instructions for processing 2. Nature and purpose of processing 3. Type of data subjects 4. Duration of processing 5. Personnel confidentiality 6. Subcontractors to meet the same obligations pursuant to a written contract 7. Take reasonable measures to ensure that de-identified information cannot be associated with a Consumer or household, and publicly commit not to re-identify

6.3 Other Obligations

In addition to the obligation of disclosure through a privacy notice and to put in place agreements with processors, the GDPR and the US data protection laws impose various obligations on controllers and processors. The following chart lists the notable ones:

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Cross-Border Data Transfers	Only based on either adequacy decision or the following appropriate safeguards: 1. A legally binding and enforceable instrument between public bodies 2. Corporate binding rules 3. Standard contractual clauses ("SCCs") 4. An approved code of conduct 5. An approved certification mechanism	N/A	N/A	N/A	N/A
Records Obligations	Processing activities, including: 1. Contact of Controller, its representative, and DPO 2. Purpose of processing 3. Categories of Personal Data and Data Subjects 4. Categories of recipients 5. Transfers to third countries 6. Envisages time limits for erasure 7. Technical and organizational security measures. Processors are required to record the foregoing 1, 2, 4, 7	For all Businesses - Consumer requests shall be recorded for 24 months For Businesses with over 10M Consumers annually, annual metrics of: 1. number of Consumer requests 2. the median or mean number of days to respond to Consumer requests to know, delete and opt out	N/A	N/A	N/A

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Risk Assessments	Data protection impact assessment ("DPIA") with prior consultation before processing, if it may result in a high risk to rights and freedoms of natural persons, in particular: 1. Automated, systematic, and extensive evaluation of personal aspects 2. Processing large scale of special categories of data 3. Systematic monitoring of publicly accessible areas on a large scale	Businesses whose processing of PI presents a significant risk to Consumers' privacy or security shall: 1. perform cybersecurity annual audit 2. submit to the CPPA a risk assessment, on a regular basis	Every Controller shall conduct a data protection assessment for: 1. Targeted advertising processing 2. Sale of PI 3. Processing of PI for profiling 4. Processing of sensitive data 5. Heightened risk of harm processing if PI	Every Controller shall conduct a data protection assessment for: 1. Targeted advertising processing 2. Sale of PI 3. Processing of PI for profiling 4. Processing of sensitive data5. Heightened risk of harm processing if PI.	N/A
Data Breach Notification	1. To the supervisory authority within 72 hours 2. To data subjects when the breach is likely to result in a high risk to their right and freedoms, without undue delay	Under CA Civil Code §1798.29: 1. To Consumers 2. If over 500 CA residents from a single breach - to CA Attorney General	Under Code of VA §18.2-186.6: 1. To Consumers. 2. If over 500 CA residents from a single breach - to CA Attorney General	Under CO Civil Code §1798.29: 1. To Consumers. 2. If over 1,000 VA residents from a single breach - to CO Attorney General	Under UT Code §13-44-202: 1. To Consumers. 2. If over 1,000 UT residents from a single breach - to UT Attorney General
Data Protection Officer ("DPO)	Controllers and Processors shall designate a DPO if: 1. Processing by a public authority or body 2. Their core activities consist of processing that requires regular and systematic monitoring of data subjects on a large scale 3. Their core activities consist of the processing of large-scale special categories	Not a mandatory requirement	Not a mandatory requirement	Not a mandatory requirement	Not a mandatory requirement
Local Representative	Controllers and Processors shall designate a representative in the Union (or UK for UK GDPR). Exceptions: 1. Occasional, no large scale of special categories, and unlikely to result in a risk of the rights and freedoms of natural persons 2. A public authority of body	N/A	N/A	N/A	N/A

7. Enforcement

Under both the GDPR and the US data protection laws, incompliance may result in monetary penalties. Jurisdictions defer in terms of the penalties' amount, procedure, and supervisory authority. Generally, the GDPR imposes a stricter penalties mechanism, both in amount, the inexistence of cure period, and by granting a private right of action.

	GDPR	CCPA (as amended by CPRA)	VCDPA	CPA	UCPA
Monetary Penalties	The GDPR imposes two penalty mechanisms, depending in the nature of the infringement: 1. Up to €10M, or 2% of annual turnover 2. Up to €20M, or 4% of annual turnover	1. $2,500 for each violation 2. $7,500 for each intentional violation 3. $7,500 for each violation involving PI of consumers under the age of 16	$7,500 for each violation	Defines CPA infringement as a deceptive trade practice under the Colorado Consumer Protection Act, imposing up to $20,000 for each violation	$7,500 for each violation (allocated to a consumer privacy restricted account)
Cure Period	N/A	N/A (the CCPA cure period was eliminated in the CPRA)	30 days	30 days	30 days
Supervisory Authority	Established in each Member State	California Privacy Protection Agency ("CPPA")	Virginia Attorney General	Colorado Attorney General	Utah Attorney General
Private Right of Action	1. lodging complaints with the supervisory authorities 2. direct claims for compensation 3. instructing representative bodies to bring class-action claims on their behalf	Only in PI security breaches, in an amount between $100 to $750 per Consumer per incident or actual damage, whichever is greater	N/A	N/A	N/A

8. Conclusion

The GDPR has led to a revolution in EU residents' data protection and privacy and required an **extensive ongoing compliance process from various businesses.** The various US data protection laws coming into effect **extending the compliance requirements** to businesses who process personal information of the receptive states' residents. While the core elements of the various regulatory regimes are common, there are concrete differences that require an adaptation of a uniform approach throughout all processing activities of the business, while implementing the relevant obligations that apply to each type of data.
We encourage businesses to review their data processing practices, map the applicable obligations that apply in each case of data source, and amend their data protection policies and procedures in order to adopt an up-to-date and harmonized approach. Such approach would assist with achieving both improved legal compliance and straight forward business processes.

Our HERZOG privacy and data protection team has gained a unique worldwide specialization in data protection and privacy legal, regulatory, and other practical aspects. Our team is studying the upcoming US data protection laws since their initial drafting and is well-prepared for assisting our clients with the process ahead.

HERZOG Technology & Regulation Department

Herzog's **Technology & eCommerce Regulation Department** is a recognized market leader in its field. The team is led by domain experts who possess a unique set of vital, **interdisciplinary** and **global** regulatory advisory skills, and are uniquely positioned to advise a range of clients, including leading multinational technology companies as well as start-ups and disruptive technologies vendors, on applicable regulatory and compliance considerations in numerous technological areas.

We understand that the **regulatory exposure** and scope of required **attention** of almost any company operating in the **digital and technological sphere** are much wider than one specific jurisdiction or legal discipline. As our clients are often on the forefront of this ever-evolving landscape, we further understand the impact of industry trends and compliance demands on our clients' businesses. Therefore, our team possesses in-depth knowledge of the increasing volume of regulations, enforcement actions, legislative and industry trends in a **myriad of jurisdictions, digital platforms** and leading **self-regulatory** guidelines. This enables our team to offer **practical, holistic** and **comprehensive** solutions for complex situations often presented by innovative technologies and disruptive business solutions, providing "hands-on" support to our clients on the strategic, corporate and operational aspects of their business, with the aim of mitigating our clients' legal and business risks.

Regulation of **personal data** has been dramatically expanding on a global basis. Companies processing data of hundreds of millions of data subjects as well as small start-ups - all are required to spend significant resources on understanding and implementing the constantly evolving legal challenges. Our **Privacy & Data Protection** team guides our clients on all matters relating to their data usage and assist them in navigating the numerous data protection regimes, in all the jurisdictions in which they operate.

This document does not constitute an exhaustive legal opinion or regulatory overview of any and all applicable regulatory requirements regarding the topics addressed by it, but rather, only outlines the key issues arising from the regulatory requirements. Since we are not licensed to practice law outside of Israel, this document is intended to provide only a general background regarding this matter. This document should not be regarded as setting out binding legal advice, but rather a general overview which is based on our understanding of the practical interpretation of the applicable laws, regulations and industry guidelines.

Ariel Yosefi | Partner
Head of Technology & eCommerce Regulation
yosefia@herzoglaw.co.il

Dan Shalev | Partner
Technology & eCommerce Regulation
shalevd@herzoglaw.co.il

Ido Manor | Partner
Technology & eCommerce Regulation
manori@herzoglaw.co.il

Ruly Ber | Partner
Technology & eCommerce Regulation
berr@herzoglaw.co.il

Dima Zalyalyeyev | Associate
Technology & eCommerce Regulation
zalyalyeyevd@herzoglaw.co.il

Eden Lang | Associate
Technology & eCommerce Regulation
lange@herzoglaw.co.il

Moran Bergman | Associate
Technology & eCommerce Regulation
bergmanm@herzoglaw.co.il

Kevin David Gampel | Associate
Technology & eCommerce Regulation
gampelk@herzoglaw.co.il

On Dvori | Associate
Technology & eCommerce Regulation
dvorio@herzoglaw.co.il

Tom Borenstein | Associate
Technology & eCommerce Regulation
borensteint@herzoglaw.co.il

Or Noy | Associate
Technology & eCommerce Regulation
noyo@herzoglaw.co.il

Mai Arlowski | Intern
Technology & eCommerce Regulation
arlowskim@herzoglaw.co.il

Lior Sokol | Intern
Technology & eCommerce Regulation
sokoll@herzoglaw.co.il