UNIVERSAL DATA PROTECTION & PRIVACY IMPACT ASSESSMENT

V1.0
Mar 2024

Background

Generally, a privacy impact assessment, called a Data Protection Impact Assessment under the GDPR, Privacy Risk Assessment under the CCPA and Data Protection Assessment under the Colorado PA and so forth, is a tool to identify and reduce the privacy risks of any project, engagement, or activity (new or change to activity) within the organization.

Irrespective of jurisdiction, such an assessment should be a genuine, thoughtful analysis that:

1. Describes the processing activity or set of related activities;
2. Contemplates the benefits and tradeoffs of the processing;
3. Identifies and describes all risks posed by a processing activity, especially if it presents a heightened risk of privacy harm to the individuals concerns;
4. Documents the measures considered and taken to address or offset those risks through appropriate safeguards (i.e. through technical, organizational and contractual measures); and
5. Demonstrates accountability through stakeholder buy-in of the process and its outcomes.

*The **Lucid Privacy Universal Data Protection Impact Assessment** (UDPIA) is a flexible, consolidated worksheet for companies to identify and reduce the privacy risks of their data uses wherever they operate.*

The UDPIA incorporates essential guidance from European, Canadian and US state authorities, focusing on common requirements and goals that can be addressed using a single form.

References:

- *EDPB Guidelines on DPIAs and High Risk Processing*
- *UK ICO DPIA Guidance*
- *Irish DPC DPIA Guidance*
- *Colorado Privacy Act Regulations*
- *CPPA Proposed CCPA Risk Assessment Regulations*
- *Canadian PIA Guidance*
- *Quebec PIA Guidance*

We will continue to update this document as policy making continues and additional states come on board.

Name of organization and/or functional	

area:	
Document owner's name and contact details:	
Website:	
Privacy Policy:	
About:	
Date Prepared:	

Data Protection Impact Assessment

Section 1: DESCRIPTION		
1.	**What is the nature of the project, engagement or processing activity?** *Explain broadly what the project, engagement, or processing activity aims to achieve and what kinds of technologies and data processing it involves. You may find it helpful to refer or link to other documents, such as a product requirements document. If there are 3rd party vendors or partners engaged, please share any presentations or statements of work related to the engagement.*	
2.	**Is the project similar to other projects or activities which you already carry out?**	☐ Yes ☐ No ☐ Not sure *If yes, please provide details about the similarities:*
3.	**If viewed outside of your organization, would the activity and/or the technologies enabling this activity be considered novel or innovative? (e.g. AI)**	☐ Yes ☐ No ☐ Not sure *Please explain:*
4.	**At what stage is the product in the development process**	☐ Still being scoped - pre-executive review ☐ Received executive approval to implement

		☐ Implementation in process ☐ Ready to release - awaiting final approval ☐ Released - in market
5.	**What is the go-live date?**	
6.	**Have you conducted a DPIA on such an activity previously?** *Are there prior concerns or assessments regarding this type of processing?*	☐ Yes ☐ No ☐ Not sure *If yes, please provide details and/or references:*
Section 2: PROCESSING DETAILS		
Section 2.1: DESCRIBE THE NATURE OF THE PROCESSING		
7.	**How will you collect and use the personal data?**	
8.	**What is the source of the data?**	**Data sources:** ☐ Volunteered on Owned / Operated Properties ☐ Site or App Usage ☐ Authorized Agents & Legal Representatives ☐ Business Operational Processes ☐ Business Partners & Service Providers ☐ Lead Gen / Affiliate Marketers ☐ Data Brokers Resellers ☐ Website Directories ☐ Public Record / Publicly Available Information ☐ Surveys, Polls & Panels ☐ System Generated ☐ Inferred or Predicted ☐ Other *If other, please provide details:*
9.	**How and where is the data stored?** *For example, in the Cloud in a regional instance vs your equipment hosted in a colocation data center.*	**Data format:** ☐ Physical ☐ Electronic **Storage environment:** ☐ On-Premise (fully owned facilities and equipment)

		☐ Co-Located Data Center (leased facilities, owned equipment) ☐ Cloud (leased facilities and equipment) *Please explain:*
10.	**Will you disclose data to anyone outside the organization?** *You might find it useful to refer to a flow diagram, brief or other way of describing data flows that result in a disclosure.*	☐ Yes ☐ No ☐ Not sure *Please explain:*

11.	**What kinds of Personal Data may be involved?**	**Personal data:**
		☐ Name (first/last)
		☐ Email address
		☐ Phone number
		☐ Postal address
		☐ Non-precise location information (e.g. derived from IP address)
		☐ Zip/Zip4
		☐ IP address
		☐ User ID/Device ID/Cookie ID/Mobile AdID
		☐ Statistical ID/Probabilistic ID
		☐ Sales transactions/conversions
		☐ Demographics/segments/models
		  ☐ Age
		  ☐ Gender
		  ☐ Income
		  ☐ Education
		☐ Inferred/expressed consumer interests
		☐ Other
		Sensitive personal data (explicit or implicated):
		☐ Mental / physical health (expressed or inferred)
		☐ Biometric data (uniquely identifiable)
		☐ Genetic data (uniquely identifiable)
		☐ Payment transactional data
		☐ SSN / Government IDs
		☐ Precise location information (lat/long)
		☐ Browsing history/App use data
		☐ Ethnic origin
		☐ Religious / political beliefs
		☐ Citizenship / Immigration status
		☐ Union membership
		☐ Communication contents
		☐ Financial account + authentication details
		☐ Other
		
		If other, please provide details:

12.	**Will you be inferring characteristics about individuals?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
13.	**Will any of this data be de-identified hashed, tokenized, aggregated, truncated or otherwise obfuscated?**	☐ Yes ☐ No ☐ Not sure *Please explain:* Sold data is plain-text and not otherwise sanitized or obfuscated. However, access to the data is strictly controlled and the data is hosted in secure cloud storage environments (e.g. Snowflake).
14.	**Will this involve a data clean room environment?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
Section 2.2: DESCRIBE THE SCOPE OF THE PROCESSING		
15.	**How many individuals are affected?** **What geographical area does the processing cover?**	☐ < 1,000 ☐ 1,000 - 99,000 ☐ 100,000 - 999,000 ☐ > 1,000,000 **Geographical areas / jurisdictions:**
16.	**Roughly, how many data points will you collect per unique individual?** *Please explain or provide an illustrative example of a common dataset.*	☐ < 25 ☐ 25 - 100 ☐ 100 – 500 ☐ >500 *Please explain:*
17.	**Is this a one-off or ongoing activity?**	☐ One-off ☐ Ongoing ☐ Seasonal ☐ Other

		If other, please provide details:
18.	**What entities will be involved with the processing activity?** **Processors or co-controllers?** **Where are they located?**	
Section 2.3: DESCRIBE THE CONTEXT OF THE PROCESSING		
19.	**What kind of people are the subject of this processing?** *If you are capturing general purpose 'consumer' data and cannot differentiate the groups further, please use 'Customers / Consumers'.*	**General groups:** ☐ Customers / Consumers ☐ Website Visitors ☐ Business Customers ☐ Prospects ☐ Employees ☐ Job Applicants ☐ Vendors **Sensitive groups:** ☐ Patients ☐ Children (<13 y.o) ☐ Teens (14 - 16 y.o.) ☐ Elderly ☐ Convicts ☐ Immigrants / Migrants ☐ Public servants ☐ Other *If other groups, please provide details:*
20.	**What is the nature of your relationship with the individuals?** **How much control will they have?** **Would they expect you to use their data in this way?**	**Relationship proximity:** **Control:** **Expectations:**
Section 2.4: DESCRIBE THE PURPOSES OF THE PROCESSING		
21.	**In business terms, what do you want to achieve?**	

	Please provide business and/or use cases and any supporting information such as briefs. *In particular, consider primary vs secondary data uses.*	
22.	**Will you be compiling and linking information about identifiable individuals such as through a unique ID? (i.e. profiling)** *Please note that 'profiling' is defined differently under the various US state laws.* *Generally, 'profiling' is taken to be a kind of automated process that evaluates certain personal aspects relating to an identified/identifiable natural person so as to analyze or predict their characteristics, interests, habits and behaviors.*	☐ Yes ☐ No ☐ Not sure *Please explain:*
23.	**Will information about the individuals be evaluated, analyzed or scored?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
24.	**Will information about the individuals be evaluated, analyzed or scored using purely automated means?** *In other words, using algorithmic and/or AI-powered systems.*	☐ Yes ☐ No ☐ Not sure *Please explain:*
25.	**Will any decisions made based on the above have a legal or similarly significant effect?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
26.	**Will there be human review or intervention with those decisions?**	

		☐ Yes ☐ No ☐ Not sure *Please explain:*
27.	**Will you be 'selling' the data to third parties?** *In other words, disclosing personal data for 'monetary or other valuable consideration'., as notably defined in the CCPA.*	☐ Yes ☐ No ☐ Not sure *Please explain:*
28.	**Will you be 'sharing' the data with providers of cross-context behavioral advertising / targeted advertising?** *In other words, will adtech providers be receiving personal data through your website, app or other means, as notably defined in the CCPA?*	☐ Yes ☐ No ☐ Not sure *Please explain:*
29.	**Will you or another line of business / corporate affiliate be providing cross-context behavioral advertising / targeted advertising services?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
Section 2.5: DESCRIBE THE BENEFITS OF THE PROCESSING		
30.	**What are the benefits of the processing – for individuals / consumers?** **Are there benefits to the general public?**	
31.	**What are the benefits of the processing – for you? For your customers and partners?**	
Section 2.6: DESCRIBE THE DETRIMENTS OF THE PROCESSING		
32.	**What tradeoffs do you anticipate from the processing – for the individual? For your organization?**	

	For example, a change in a consumer's ability to access a certain service; the business being perceived in a certain light by the public.	
Section 3: PRIVACY ANALYSIS		
33.	**What steps have you taken to ensure that the data are processed in a transparent manner?** *For example, how you provide individuals with necessary and timely disclosures such as through a registration process or similar where a privacy policy link is provided.*	☐ Privacy Policy / Notice ☐ Terms of Service ☐ In-line disclosures at points of collection ☐ Just-in-Time disclosures (e.g. app prompt) ☐ Other *Please provide details:*
34.	**What steps have you taken to ensure that the data are collected and used only for specified, explicit and legitimate purposes?** *Specifically, how do you ensure data is not used for purposes that consumers may not have been explicitly told about and/or they would not reasonably expect?*	
35.	**What steps have you taken to ensure that data are not further processed in a manner that is incompatible with those purposes?**	
36.	**If there are secondary purposes, what steps have you taken to explicitly inform individuals about those purposes?**	
37.	**What steps have you taken to ensure that the data are limited to what is necessary for the purpose(s) of this activity?**	
38.	**What steps have you taken to ensure that the data are relevant to the purposes of this activity?**	
39.	**What steps have you taken to ensure that the data are accurate?**	
40.	**What steps have you taken to ensure you are not selling the data of opted out individuals or without their prior opt-in, as required?**	

41.	**What steps are you taking to reduce the risk of unfair or deceptive treatment of, or unlawful disparate impact on, consumers – particularly vulnerable groups?** *For example, ensuring there is human review or intervention with any automated decisions made.*	
42.	**Describe the data retention time limits.** **How is the data handled / sanitized when the retention limit is reached?** *Please refer to a retention policy and schedule, linking to the reference if possible.*	
Section 4: CONSUMER / DATA SUBJECT RIGHTS		
43.	**Can data subjects access the personal data associated with this processing activity?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
44.	**Can data subjects modify the personal data associated with this processing activity?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
45.	**Can data subjects delete the personal data associated with this processing activity?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
46.	**Can data subjects object to some uses of their personal data? In particular, sensitive (special category) data?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*

47.	**Can data subjects receive their data in a portable format to, for example, transfer it to a competitive service?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
48.	**Can data subjects opt-out of profiling?** **Automated decision-making with serious effect?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
49.	**Can data subjects appeal decisions/actions leading to serious adverse effects?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
Section 5: PROTECTIVE MEASURES		
50.	**Describe the organizational measures to protect the data and prevent its misuse/abuse.**	
51.	**Describe the technical measures to protect the data and prevent its misuse/abuse.**	
52.	**Describe the legal/contractual measures to protect the data and prevent its misuse/abuse.**	
53.	**Is the processing activity covered by any security or another compliance certification?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
54.	**Is the processing activity subject to any applicable industry codes of conduct?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
55.	**Do you maintain third-party audits or certifications that validate your controls?**	☐ Yes ☐ No ☐ Not Sure

		Please explain:
Special 1: CONSULTATION		
56.	**Do you have a process for consulting with relevant stakeholders about a known or suspected high risk activity?** *Depending on the situation, you may need to or wish to consult with a relevant supervisory authority. For example, with the UK ICO.* *At minimum, you should be seeking the advice of your privacy officer and/or Data Protection Officer (if you have one in the UK and EU).* *Other relevant stakeholders and subject matter experts include business process and system owners, and any other relevant stakeholders throughout the process.* *In some cases you may be expected to consult with members of the public to understand their expectations, views or attitudes regarding the activity.*	☐ Yes ☐ No ☐ Not Sure *Please explain:*
57.	**Did you consult with or plan to consult with company advisors?** **If so, please describe their views here and/or in the relevant "Risk Identification" and "Risk Mitigation" sections.**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
58.	**Did you consult with or plan to consult with external experts?** **If so, please describe their views here and/or in the relevant "Risk Identification" and "Risk Mitigation" sections.**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
59.	**Did you consult with or plan to consult with the intended data subjects?**	☐ Yes ☐ No ☐ Not Sure

	If so, please describe their views here and/or in the relevant "Risk Identification" and "Risk Mitigation" sections.	*Please explain:*
Special 2: LAWFULNESS OF PROCESSING		
Modern privacy and data protection laws require that you identify your legal role and establish valid lawful grounds (legal bases) for processing personal data. To be lawful, processing must meet the criteria (usually itemized) set out under the law. These are the so-called legal bases or lawful grounds for processing. This depends on the jurisdiction, the nature of the processing, and the context of the processing. You should think about why you want to process the data, and consider which lawful basis best fits the circumstances. *Please consult with competent legal counsel as needed, particularly if operating in jurisdictions where the distinctions are less clear. For example, in Japan and China.*		
60.	**Do you determine the purpose and means of the processing?** *Meaning, do you make decisions about what data is collected, from whom, how it is used and who it is shared with?* *If you do, you are what is known as a "Data Controller" (also called a "Business" in California among other US states).*	☐ Yes ☐ No ☐ Not Sure *Please explain:*
61.	**Does another entity determine the purpose and means of processing together with you?** *Meaning, do you make joint decisions with another business about what data is collected, from whom, how it is used and who it is shared with?* *If you do, then you and the other entity are what is known as "Joint Controllers" of the data in question.* *(US/California does not have an equivalent concept.)*	☐ Yes ☐ No ☐ Not Sure *Please explain:*
62.	**Will you process the personal data in question on behalf of another organization?** *Meaning, do you follow the instructions of an organization that*	☐ Yes ☐ No ☐ Not Sure

	determines the purpose and means of the processing? *If you do, then you are what is known as a "Data Processor" (also called a "Service Provider" in California among other US states).*	*Please explain:*

63.	**What is the legal basis for this processing activity?**
	
	Note that your legal bases are not the specific purposes for which you are collecting and using the data. Rather, these are the legal mechanisms by which the processing can be justified as legitimate under laws such as the GDPR, LGPD, CCPA, Colorado PA, VCDPA etc. Different laws use different standards and definitions. For example, the GDPR provides six co-equal legal basis (lawful grounds for processing), the most popular of which are Contractual Basis, Legitimate Interest and Consent.
	
	Conceptually, if you are a Data Controller, you determine the purpose and means of processing and are responsible for determining the most appropriate legal basis for this activity. Conceptually, if you are a Data Processor, you do not determine the purpose, means or legal basis of the processing. Instead, you rely on the written (i..e. contractual) instructions of the Controller.
		European Union & UK
		
		☐ Contract with Data Subject
		☐ Legal Obligation
		☐ Vital Interests of Data Subject
		☐ Public Interest
		☐ Legitimate Interests of the Business
		☐ Consent
		☐ Applicable derogations
		
		California & US
		
		☐ Business Purposes
		  ☐ Auditing Interactions with Consumers
		  ☐ Security
		  ☐ Debugging/Repair
		  ☐ Certain Short-term Uses
		  ☐ Performing Services
		  ☐ Internal Research for Tech Development
		  ☐ Quality and Safety Maintenance and Verification
		☐ Commercial Purpose
		
		☐ I'm a Processor/Service Provider -- determining the legal basis is the Controller's responsibility
		
		☐ Not Sure
		☐ Other
		
		Please explain:

64.	**If you are relying on consent, how is it obtained?**	☐ I obtain consent in the following ways:
		  ☐ Checkbox with form
		  ☐ Written or electronic signature

	In other words, describe the methods by which valid consent is captured. *If you are a Controller, consider whether you are receiving consent directly from an individual or indirectly through another party.* *If you are a Processor, consider whether you are relying on a Controller to attain valid consent.* ***For reference see:*** *UK ICO's - Guide to Obtaining Consent* *IAPP - The UX Guide to Getting Consent* *CNIL - Guidelines on Cookie Consent (FR)*	☐ Consent Management Platform (e.g. cookie banner) ☐ I'm a Processor -- this is the Controller's responsibility ☐ Not Sure *Please explain:*
Special 3: INTERNATIONAL DATA TRANSFERS		
65.	**Will data be transferred or access outside of the country where data was collected? If so, where?** *Note that international access is also a form of transfer.*	☐ Yes ☐ No ☐ Not Sure *Please explain:*
66.	**If not transferred offshore would the data be accessible from offshore locations? If so, where.**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
67.	**Does the transfer or access involve cloud storage providers?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
	Which legal basis is the transfer/access relying on? *Exporters and importers must ensure data transfers are lawful, necessary, proportional and secure.*	☐ Country-level adequacy decision ☐ Binding Corporate Rules ☐ Data transfer agreement with EEA Standard Contractual Clauses ☐ Consent of the data subject ☐ Other

		Please explain:
68.	**Do you have appropriate data transfer agreements in place with the cloud provider?**	☐ Yes ☐ No ☐ Not Sure *Please explain:*
Special 4: DIGITAL MARKETING SELF-REGULATION		
69.	**Is the project, engagement or activity subject to marketing / advertising industry codes of conduct or commitments?**	☐ ANA/DMA Direct Marketing Code of Ethics ☐ BBB Business Partner Code of Conduct ☐ IAB Code of Conduct ☐ IAB US Multi-State Privacy Agreement ☐ DAA/EDAA Self-Regulatory Principles ☐ NAI Code of Conduct ☐ Other *If none or other, please explain.*
70.	**Is the project, engagement or activity subject to any cross-industry consumer privacy choice framework or cooperative?**	☐ IAB Transparency & Consent Framework ☐ IAB Global Privacy Platform ☐ DAA/EDAA YourAdChoices ☐ NAI Opt Out ☐ ANA DMAChoice ☐ FCC Do Not Call
71.	**If you engage in mobile, how do you obtain consent in iOS and Android?** *Please provide screenshots of your ATT and Google consent.* *Please also provide any relevant details about your compliance with Apple's (e.g. ATT, Manifests) and Google's app store policies as part of your U.S. privacy strategy.*	☐ Yes ☐ No ☐ Not Sure *Please explain:*

Identified Risks

This section is to be prepared by persons responsible for privacy, data protection and legal risk management in consultation with the Data Protection Officer (as needed).

Describe source of risk and nature of potential impact on individuals. *Include associated compliance and corporate risks as necessary.*	**Likelihood of harm** *(Remote, Possible or Probable)*	**Severity of harm** *(Minimal, Significant, or Severe)*	**Overall risk** *(Low, Medium or High)*

Measures to Reduce Risks

Identify measures that can reduce or eliminate High and Medium risks				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** *(Eliminated, reduced, accepted)*	**Residual risk** *(Low, medium, high)*	**Measure approved** *(Yes/no)*

Sign-Off and Outcomes

This section documents advice on compliance and remediation measures, and whether processing can proceed without undertaking a full Privacy Impact Assessment. The Data Protection Officer should be consulted as necessary.

Item	Name/date	Notes
Risks reviewed by:		
Measures approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the senior business sponsor for this activity before proceeding. In higher risk scenarios this may be the CEO, CFO, CIO or similar.*
Summary of privacy/compliance advice:		
Summary of legal advice:		

When should we re-review this project, engagement or activity?

Appendix A

When GDPR Data Protection Impact Assessments are triggered
Article 35(1): "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks." **Article 35(3):** 1. **Systematic and extensive profiling with significant effects:** any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person." 2. **Large scale use of sensitive data:** processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10. 3. **Public monitoring:** a systematic monitoring of a publicly accessible area on a large scale. Additional criteria by the **Article 29 Working Party**, now the European Data Protection Board: 1. Evaluation or scoring. 2. Automated decision-making with legal or similar significant effect. 3. Systematic monitoring. 4. Sensitive data or data of a highly personal nature. 5. Data processed on a large scale. 6. Matching or combining datasets. 7. Data concerning vulnerable data subjects. 8. Innovative use or applying new technological or organisational solutions. 9. Preventing data subjects from exercising a right or using a service or contract. Guidance from the UK Information Commissioner's Office: 1. **Innovative technology**: processing involving the use of innovative technologies, or the novel application of existing technologies (including AI). A DPIA is required where this processing is combined with any of the criteria from the European guidelines. 2. **Denial of service:** Decisions about an individual's access to a product, service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data. 3. **Large-scale profiling:** any profiling of individuals on a large scale.

4. **Biometrics: any processing of biometric data.** A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
5. **Genetic data:** any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
6. **Data matching:** combining, comparing or matching personal data obtained from multiple sources.
7. **Invisible processing**: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
8. **Tracking:** processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment. A DPIA is required where this processing is combined with any of the criteria from the European guidelines.
9. **Targeting of children or other vulnerable individuals:** the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
10. **Risk of physical harm**: where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

Appendix B

When US Data Protection Assessments are triggered						
CCPA	**VCDPA**	**CPA**	**CTDPA**	**OCPA**	**TXDPSA**	**MTCDPA**
TBD, subject to formal rulemaking and finalization. Draft rules concern: (1) Selling or sharing/using PI for targeted ads (sharing) (2) Processing SPI and PI of minors (<16 y.o.) (3) ADMT for significant decision-making or	A controller shall conduct and document a DPA of each of the following processing activities involving personal data: (1) The processing of personal data for purposes of targeted advertising; (2) The sale of personal data;	Where there is a heightened risk of harm to a consumer. A heightened risk of harm includes: (a) Processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of:	Where there is a heightened risk of harm to a consumer. A heightened risk of harm includes: (a) Processing personal data for purposes of targeted advertising or for profiling if the profiling presents a reasonably foreseeable risk of:	Where there is a heightened risk of harm to a consumer. Processing activities that present a heightened risk of harm to a consumer include: (A) Processing personal data for the purpose of targeted advertising;	A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data: (1) The processing of personal data for purposes of targeted advertising;	Where there is a heightened risk of harm to a consumer. A heightened risk of harm to a consumer includes: (a) The processing of personal data for the purposes of targeted advertising; (b) The sale of personal data; (c) The

"extensive profiling", including for behavioral advertising (4) Training ADMT or AGI for: (i) Significant decisioning concerning a consumer, (ii) Establishing individual identity, (iv) Physical or biological identification or profiling, (v) Generation of a deepfake, or operation of generative models.	(3) The processing of personal data for purposes of profiling, where such profiling presents a reasonably foreseeable risk of (i) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical, or reputational injury to consumers; (iii) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (iv) Other substantial injury to consumers; (4) The processing of sensitive data; and	(i) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) Financial or physical injury to consumers; (iii) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or (iv) Other substantial injury to consumers; (b) Selling personal data; and (c) Processing sensitive data.	(i) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) Financial or physical injury to consumers; (iii) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or (iv) Other substantial injury to consumers; (b) Selling personal data; and (c) Processing sensitive data.	(B) Processing sensitive data; (C) Selling personal data; and (D) Using the personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of: (i) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) Financial, physical or reputational injury to consumers; (iii) Physical or other types of intrusion upon a consumer's solitude, seclusion or private affairs or concerns, if the intrusion would be offensive to a reasonable person; or (iv) Other substantial injury to consumers.	(2) The sale of personal data; (3) The processing of personal data for purposes of profiling, if the profiling presents a reasonably foreseeable risk of: (A) Unfair or deceptive treatment of or unlawful disparate impact on consumers; (B) Financial, physical, or reputational injury to consumers; (C) A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or (D) Other substantial injury to consumers; (4) The processing of	processing of personal data for the purposes of profiling in which the profiling presents a reasonably foreseeable risk of: (i) Unfair or deceptive treatment of or unlawful disparate impact on consumers; (ii) Financial, physical, or reputational injury to consumers; (iii) A physical or other form of intrusion on the solitude or seclusion or the private affairs or concerns of consumers in which the intrusion would be offensive to a reasonable person; or (iv) Other substantial injury to consumers; and (d) The processing of

	(5) Any processing activities involving personal data that present a heightened risk of harm to consumers.				sensitive data; and (5) Any processing activities involving personal data that present a heightened risk of harm to consumers.	sensitive data