PAN-US DATA PROTECTION IMPACT ASSESSMENT

March 2024
v1.0

Background

The Lucid Privacy Pan-US Data Protection Impact Assessment (Pan-US DPIA) is a holistic, unified worksheet for companies assessing privacy risks in-line with comprehensive US state privacy laws.

A US Data Protection Impact Assessment (called Privacy Risk Assessment under CCPA, Data Protection Assessment under Colorado PA, and Privacy Impact Assessment generically) is a tool used to identify and reduce the privacy risks of any project, engagement, or activity (new or change to activity) within the organization.

As of the date above, there are eight (8) US state privacy laws in effect or coming into effect in 2024-5 that obligate certain Controllers (Businesses under CCPA) to complete a DPIA (by any name). Each state offers slightly varying triggers and substantive requirements for a DPIA but otherwise overlap and generally align with GDPR DPIAs.

Scope

This document takes into account requirements under the CCPA (California), VCDPA (Virginia), CPA (Colorado), CTDPA (Connecticut), and UCPA (Utah). OCPA (Ohio), TXDPSA (Texas), and MTCDPA (Montana)

Where state regulators have released regulations associated with their respective DPIA requirements (i.e. Colorado), we have incorporated those requirements into the template accordingly.

PLEASE NOTE, *this Pan-US DPIA version only covers finalized text and rulemaking as of the date above. For the sake of clarity, this document anticipates but does not explicitly include finalized requirements concerning CCPA Privacy Risk Assessments.*

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:	

Pan-US 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.	**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?**	☐ Currently in market ☐ Within 3 months ☐ Within 6 - 12 months ☐ In >12 months ☐ Not sure
6.	**Have you conducted a data protection / privacy impact assessment 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 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 US 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.	**Are you a registered data broker?** *Have you registered in CA, OR, TX, and VT?*	☐ Yes ☐ No ☐ Not sure *Please explain:*

12.	**What kinds of Personal Data may be involved?**
	
	IMPORTANT NOTE: *Personal data today includes direct identifiers like email address and indirect identifiers like an IP address or a cryptographically hashed email address.*
	
	Modern privacy and data protection laws and outflowing regulatory guidance confirm that inferential data is also 'personal'.
	
	Inferences about individuals -- their behaviors, interests and other characteristics -- can be made after comparing two or more data sets., or combining two or more data sets.
	
	The resulting insights can be used for a range of governmental, commercial and societal purposes ranging from public health administration to personalized advertising.
		Personal data:
		
		☐ Name (first/last)
		☐ Email address
		☐ Phone number
		☐ Postal 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:
		
		☐ 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
		☐ Inferred/expressed sensitive characteristics
		☐ Other
		
		If other, please provide details:

13.	**Will you be inferring characteristics about individuals?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
14.	**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).
15.	**Will this involve a data clean room environment?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
Section 2.2: DESCRIBE THE SCOPE OF THE PROCESSING		
16.	**How many individuals or devices 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:**
17.	**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:*
18.	**Is this a one-off or ongoing activity?**	☐ One-off

		☐ Ongoing ☐ Seasonal ☐ Other *If other, please provide details:*
19.	**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		
20.	**What kind of people are the subject of this processing?**	☐ Consumers ☐ Business Customers ☐ Employees ☐ Job Applicants ☐ Prospects ☐ Vendors ☐ Website Visitors ☐ Patients ☐ Children (<13 y.o) ☐ Teens (14 - 16 y.o.) ☐ Elderly ☐ Convicts ☐ Immigrants / migrants ☐ Public servants ☐ Other groups *If other groups, please provide details:*
21.	**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		
22.	**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.*	
23.	**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:*
24.	**Will information about the individuals be evaluated, analyzed or scored?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
25.	**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:*

26.	**Will any decisions made based on the above have a legal or similarly significant effect?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
27.	**Will there be human review or intervention with those decisions?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
28.	**Will you be 'selling' the data to third parties?** *In other words, disclosing personal data for 'monetary or other valuable consideration'.*	☐ Yes ☐ No ☐ Not sure *Please explain:*
29.	**Will you be 'sharing' the data with providers of cross-context behavioral advertising (CCBA) / targeted advertising services?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
30.	**Will you or another corporate affiliate or division be providing CCBA / targeted advertising services?**	☐ Yes ☐ No ☐ Not sure *Please explain:*
Section 2.5: DESCRIBE THE BENEFITS OF THE PROCESSING		
31.	**What are the benefits of the processing for individuals (consumers)?** **For the general public?**	

32.	**What are the benefits of the processing for your business?** **For your business customers and partners?**	
Section 2.6: DESCRIBE THE DETRIMENTS OF THE PROCESSING		
33.	**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: ANALYSIS		
34.	**What privacy laws apply? (e.g., CCPA/CPRA, VCDPA, CPA, CTDPA etc.)** *Please refer to an applicability assessment if one has been completed.*	
35.	**Do you have a public privacy policy or statement discussing this processing activity?** *This is to ensure individuals have appropriate notice of this activity taking place.*	☐ Yes ☐ No ☐ Not sure *Please provide details:*
36.	**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?	
37.	**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.*	
38.	**What steps have you taken to ensure that data are not further processed in a manner that is incompatible with those purposes?**	
39.	**If there are secondary purposes, what steps have you taken to explicitly inform individuals about those purposes?**	
40.	**What steps have you taken to ensure that the data is necessary and relevant for the purpose(s) of this activity?**	
41.	**What steps have you taken to ensure that the data are accurate?**	
42.	**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?**	
43.	**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.*	

44.	**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		
45.	**Can data subjects access the personal data associated with this processing activity?**	☐ Yes ☐ No ☐ N/A ☐ Not Sure *Please explain:*
46.	**Can data subjects modify the personal data associated with this processing activity?**	☐ Yes ☐ No ☐ N/A ☐ Not Sure *Please explain:*
47.	**Can data subjects delete the personal data associated with this processing activity?**	☐ Yes ☐ No ☐ N/A ☐ Not Sure *Please explain:*
48.	**Can data subjects opt-out of the 'sale' of their personal data?**	☐ Yes ☐ No ☐ N/A ☐ Not Sure *Please explain:*

49.	**Can data subjects opt-out of data 'sharing' for Cross-Context Behavioral Advertising / targeted advertising uses?** *Notably, not just through a cross-industry tool like DAA AdChoices but via a company-specific opt-out mechanism.*	☐ Yes ☐ No ☐ N/A ☐ Not Sure *Please explain:*
50.	**Do you honor universal opt-out preference signals?** Notably, Global Privacy Control (GPC) signals.	☐ Yes ☐ No ☐ N/A ☐ Not Sure *Please explain:*
51.	**Can data subjects opt-out of profiling?** **Automated decision-making with serious effect?**	☐ Yes ☐ No ☐ N/A ☐ Not Sure *Please explain:*
52.	**Can data subjects appeal decisions/actions leading to serious adverse effects?**	☐ Yes ☐ No ☐ N/A ☐ Not Sure *Please explain:*
53.	**Can data subjects opt-in to the use and disclosure of their sensitive information, where required?**	☐ Yes ☐ No ☐ N/A ☐ Not Sure *Please explain:*
Section 5: PROTECTIVE MEASURES		

54.	**Describe the organizational measures to protect the data and prevent its misuse/abuse.**	
55.	**Describe the technical measures to protect the data and prevent its misuse/abuse.**	
56.	**Describe the legal/contractual measures to protect the data and prevent its misuse/abuse.**	
57.	**Is the processing activity covered by any security or another compliance certification?**	
58.	**Is the processing activity subject to any applicable industry codes of conduct?**	
Special: DIGITAL MARKETING SELF-REGULATION		
59.	**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.*
60.	**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 ☐ Other
61.	**If you engage in mobile, how do you obtain consent in iOS and Android?** *Please provide screenshots of your ATT and Google consent.*	*Please explain:*

	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.	

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 GSPO before going ahead*
Summary of privacy/compliance advice:		

Summary of legal advice:
When should we re-review this project, engagement or activity?

Appendix A

When Data Protection Assessments are triggered						
CCPA	**VCDPA**	**CPA**	**CTDPA**	**OCPA**	**TXDPSA**	**MTCDPA**
TBD, subject to further rulemaking	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	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	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	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	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	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

	of targeted advertising; (2) The sale of personal data; (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	presents a reasonably foreseeable risk of: (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.	presents a reasonably foreseeable risk of: (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.	purpose of targeted advertising; (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	for purposes of targeted advertising; (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	advertising; (b) The sale of personal data; (c) The 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

	reasonable person; or (iv) Other substantial injury to consumers; (4) The processing of sensitive data; and (5) Any processing activities involving personal data that present a heightened risk of harm to consumers.			would be offensive to a reasonable person; or (iv) Other substantial injury to consumers.	reasonable person; or (D) Other substantial injury to consumers; (4) The processing of sensitive data; and (5) Any processing activities involving personal data that present a heightened risk of harm to consumers.	offensive to a reasonable person; or (iv) Other substantial injury to consumers; and (d) The processing of sensitive data