From: Soutar, Colin <csoutar@deloitte.com>
Sent: Thursday, October 24, 2019 10:52 AM
To: privacyframework <privacyframework@nist.gov>
Cc: csoutar@deloitte.com; Sargsyan, Tatevik <tsargsyan@deloitte.com>
Subject: Deloitte & Touche LLP Comments on the NIST Privacy Framework Preliminary Draft

Dear NIST Team:

Enclosed are Deloitte's comments on the NIST Privacy Framework Preliminary Draft. As one of the largest professional services organizations in the United States, Deloitte provides a vast array of privacy and data protection services to clients in many industries, including Technology, Media and Telecom, and Life Sciences and Healthcare. We serve these clients by helping them solve complex issues at the intersection of technology, risk, and regulation. As a result, we hold a broad, yet specialized, perspective on privacy risk management, which is reflected in the submitted comments.

Please let me know if you have any follow-up questions.

Respectfully submitted,

Colin Soutar
Managing Director
Deloitte Government and Public Services
Risk & Financial Advisory, Cyber Risk
Deloitte & Touche LLP
1919 North Lynn Street, Arlington, VA 22209
www.deloitte.com

Comment #	Organization Name	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial /Technical)
1	Deloitte & Touche LLP	N/A	N/A	N/A	We recognize that NIST is a non-regulatory organization and therefore will not relate adoption of the Privacy Framework to conformance with laws and regulations. Furthermore, the Privacy Framework is presented as voluntary (e.g., line 87). However, NIST publications are regularly used by commercial organizations to demonstrate the adoption of leading practices. In light of this, and the international aspirations of the Framework (e.g., https://www.nist.gov/privacy-framework/frequently-asked-questions), we respectfully suggest that a more explicit link between the Framework and international laws and regulations such as the General Data Protection Regulation (GDPR), the Brazilian General Data Protection Regulation (LGPD) and the California Consumer Privacy Act (CCPA) and respective concepts (e.g., Privacy by Design, etc.) be included. This link could be included either directly in the Framework, or as "sanctioned" mappings on the NIST web site. Otherwise, commercial adoption may be limited, as organizations will need to focus time and effort on their required regulatory efforts.		General
2	Deloitte & Touche LLP	4	129-132	1	We recommend incorporating more data privacy elements (e.g., governance of how data is collected, used, and shared) in the definition of privacy.		General

3	Deloitte & Touche LLP	4	129-130	1	"…safeguards important values such as human autonomy and dignity…"	We suggest changing to: "…safeguards important values and rights, such as human autonomy and dignity…"	Editorial
4	Deloitte & Touche LLP	4	127-128	1	"…continue to derive benefits from data while simultaneously protecting individuals' privacy…"	We suggest rewording to: "…continue to derive benefits based on data and its processing, while simultaneously protecting individuals' privacy…"	Editorial
5	Deloitte & Touche LLP	4	126	1	The Framework states that failure to manage privacy risk can have adverse consequences for people at both the individual and societal level. Recommend providing some examples related to adverse impacts on society (e.g., democratic process, inhabitation of access to certain programs, etc.).		General
6	Deloitte & Touche LLP	5	189-195	1.1	We respectfully recommend that NIST consider deferring the inclusion of Implementation Tiers as defined until a later revision of the Privacy Framework. The use of Implementation Tiers for privacy risk does not have the history that it does for cybersecurity risk, so has the potential to be misunderstood or misused. We think that it is more beneficial for organizations to self-define levels of implementation in the Current State and Target State profiles, so that they are actionable to the organization and so that a perception of "compliance with the Privacy Framework" is diminished.		General

7	Deloitte & Touche LLP	8	278	1.2.2	"Lastly, privacy risk assessments help organizations distinguish between privacy risk and compliance risk,"	We suggest changing to: "…help organizations understand and manage their privacy risks, independent of any compliance requirements."	General
8	Deloitte & Touche LLP	9	303-304	2	"…tool for aligning policy, business, and technological approaches to managing that risk"	We suggest rewording to: "…tool to identify policy, business, and technological approaches that can manage that risk"	Editorial
9	Deloitte & Touche LLP	11	394-396	2.2	We suggest including a statement that the more tailored Profiles are, the less they can be used for comparability purposes.		General
10	Deloitte & Touche LLP	14	479	3.3	We suggest that "continuously" be changed to "continually".		Editorial
11	Deloitte & Touche LLP	18	611	Appendix	We recommend showing an example of a profile and tier in the appendix to enable use and adoption.		General
12	Deloitte & Touche LLP	22	684	Appendix (Core)	GOVERN • We recommend adding implementation of policies in addition to establishing and communicating policies. • We recommend adding oversight mechanisms for implementation of policies, processes, and procedures for privacy risk management.		Technical

13	Deloitte & Touche LLP	24	684	Appendix (Core)	CONTROL • Control should address data retention as well (i.e., limits on data retention consistent with the scope and purpose disclosed in the notice). • We recommend including / mentioning affirmative consent (i.e., inaction cannot be considered one). • CT.DP-P6: Limiting data processing to fulfillment of "business objectives" can potentially mean prioritizing data aggregation and correlation contradicting the intended outcomes of "Disassociated Processing." Recommend editing to clarify that data processing should be done for delivering services and not for making secondary inferences about individuals. • CT.DP-P1: Data actions taking place on local devices may only make sense in limited scenarios. We recommend adding qualifiers to make it less prescriptive. • We recommend adding accountability mechanisms for enforcing data management policies.		Technical
14		25-26	684	Appendix (Core)	COMMUNICATE • We recommend making it more explicit that the types and/or names of third parties that are part of the data processing ecosystem should also be communicated.		Technical
15	Deloitte & Touche LLP	20	683	Appendix A	PROTECT • We recommend incorporating "Monitoring and Testing" into this category.		Technical
16	Deloitte & Touche LLP	36	820	Appendix D	We suggest providing examples / catalog of potential problematic data actions. Also, it is worth highlighting that these actions are not inherently problematic, but they could lead to increased risk in certain circumstances.		General

17	Deloitte & Touche LLP	7-8	258-267	1.2.2	We suggest realigning bullets in the order of 3, 2, 1, 4 (e.g., avoid, transfer, mitigate, then accept.)		Editorial