#	Principle Name	SCF Privacy Management Principle (SCF-PMP) Description	AICPA TSC SOC 2 (2017)	APEC	EU GDPR	FIPPs (DHS)	FIPPs (OMB)	GAPP	HIPAA Privacy Rule	ISO 27701 v2019	ISO 29100 v2011	NIST 800-53 rev 4	NIST Privacy Framework [draft]	OECD	OMB A-130	PIPEDA	US - California CCPA	US - Nevada SB820	Secure Controls Framework (SCF)
1.0	Privacy by Design	Establish and maintain a comprehensive privacy program that ensures privacy considerations are addressed by design in the development of policies, standards, processes, systems, applications, projects and third-party contracts.		1	Art 32.1 Art 32.2 Art 32.3 Art 32.4			8.2.1		5.3.2 5.3.3 5.4 5.4.1 5.4.1.1 5.4.2 5.5 5.5.1 5.5.2 5.5.3 5.5.4 5.5.5 5.5.5.1 5.5.5.2 5.5.5.3 6.5 5.6.1 5.6.2 5.6.3 5.6.4 5.7 5.7.1 5.7.2 5.7.3 5.8 5.8.1 5.8.1 6.2 6.2.1 6.2.1.1 7.1 7.4 8.3 8.3.1 8.4	5.1 5.10 5.11	AR-1	GV.PP-P1 CT.PO-P2 CM.PP-P1 CM.AW-P2 PR.DP-P9		4(h) 5(f)(1)(a) App 1 - 3(b) App 1 - 3(b)(1) App 1 - 3(f) App 1 - 4(c)(2) App 1 - 4(e) App 1 - 4(e)(1) App 1 - 4(e)(10)		§ 999.305(a)(4)		GOV-01 PRI-01
1.1	Assigned Responsibilities	Assign accountability through documented roles and responsibilities to qualified individuals, including key internal and external stakeholders, for maintaining compliance with all applicable privacy requirements that involves appropriately monitoring and documenting the privacy program.			Art 35.2 Art 37.1 Art 37.2 Art 37.3 Art 37.4 Art 37.5 Art 37.6 Art 37.7 Art 38.1 Art 38.2 Art 38.3 Art 38.4 Art 38.5 Art 38.6 Art 39.1 Art 39.2	Accountability & Auditing	Accountability	1.1.0 1.1.2 1.2.1 1.2.2 1.2.8 1.2.9 2.1.0 4.2.3 8.2.1	164.530(a)(1)	6.15.1.4 8.5	5.10		CM.PP-P2 CT.PO-P2 CM.PP-P2		4(h) 5(c)(6) 5(f)(1)(b) App 1 - 4(e)	1			PRI-01.1 PRI-01.4
1.2	Data Classification	Classify data according to the sensitivity and type of personal data as defined by appropriate statutory, regulatory and contractual contexts.			Art 4 Art 9					6.5.2.1									DCH-02
1.3	Registering Databases	Register applicable databases containing personal data with the appropriate Data Authority, when required.			Art 30.4							TR-2							PRI-15
1.4	Resource Planning	Identify and plan for resources needed to operate a privacy program and include privacy requirements in solicitations for technology solutions and services.			Art 32.1 Art 32.2					6.3.1.5					5(a)(3)(e)(ii) 5(d)(3)(e) App 1 - 4(b)(1) App 1 - 4(b)(2) App 1 - 4(b)(4) App 1 - 4(e)(6)				PRM-01
1.5	Inventory of Personal Data	Maintain an inventory of both the type of personal data and specific data element, as well as the systems, applications and processes that collect, create, use, disseminate, maintain, and/or disclose that personal data.			Art 4 Art 5.2 Art 9			7.2.2				SE-1	ID.IM-P1 ID.IM-P3 ID.IM-P6		5(a)(1)(a)(ii) 5(f)(1)(e) App 1 - 4(j)(2)(c)				PRI-05.5
1.6	Privacy Training	Provide recurring privacy awareness and training for all employees and contractors.						1.1.1 1.2.10	164.504 164.530	6.4.2.2		AR-5	GV.PP-P1		App 1 - 4(h)(1) App 1 - 4(h)(2) App 1 - 4(h)(3) App 1 - 4(h)(4) App 1 - 4(h)(5)		§ 999.317(a)		SAT-01 SAT-02 SAT-02.1 SAT-03 SAT-03.1 SAT-03.3
2.0	Data Subject Participation	Individuals are directly involved in the decision-making process regarding the fair and lawful processing of the individual's personal data and, to the extent practicable, directly-engaged to receive explicit permission to use their personal data.	P2.1 P3.2	5	Art 6.1 Art 7.1 Art 7.2 Art 7.3 Art 7.4 Art 8.1 Art 8.2 Art 12.6 Art 14.3	Individual Participation	Individual Participation	3.2.1 3.2.2 3.2.3 3.2.4	164.506 164.508	7.2.3 7.2.4 7.3.4 7.3.5 8.5.7	5.2	IP-1 IP-1(1)	CT.PO-P1 CT.PO-P3	7		3	§ 999.315 § 999.315(a) § 999.315(b) § 999.315(c) § 999.315(d) § 999.315(e) § 999.315(f) § 999.315(g) § 999.315(h)		PRI-03
2.1	Clear Choices	Provide clear and conspicuous choices that enable an individual, or a person authorized by the individual, to permit or prohibit the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of the individual's personal data. This is also referred to as the right to "opt out."			Art 7.1 Art 7.2 Art 7.3 Art 7.4 Art 12.2 Art 12.3 Art 12.4 Art 22.1 Art 22.2 Art 22.3 Art 22.4				164.508(a-c) 164.510 (a) and (b)	7.3.4		TR-1 TR-1(1)	CT.PO-P3			3	CT.PO-P3		PRI-03.1
2.2	Initial Consent	Prior to the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of the individual's personal data, the knowledge and consent of the individual are required.	P2.1 P3.2					3.2.1 3.2.2 3.2.3 3.2.4	164.506(c)(1-4) 164.510 (a)(2) 164.510 (b)	7.2.3 7.2.4 7.3.4 7.3.5 8.5.7	5.2	IP-1 IP-1(1)	CT.PO-P1 CT.PO-P3	7		3	§ 999.315 § 999.315(a) § 999.315(b) § 999.315(c) § 999.315(d) § 999.315(e) § 999.315(f) § 999.315(g) § 999.315(h)		PRI-03
2.3	Updated Consent	Based on changes to privacy practices that affect the parameters of an individual's initial consent, updated consent of the individual is required to continue the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of the individual's personal data. This is also referred to as the right to "opt out" at any time after the initial consent was provided.			Art 7.1 Art 7.2 Art 7.3 Art 7.4 Art 8.1 Art 8.2 Art 12.2 Art 12.3 Art 12.4 Art 13.3 Art 14.3 Art 21.4					7.3.4			CT.PO-P1 CT.PO-P3			3	§999.305(d)(1) §999.305(d)(2) §999.305(d)(2)(a) §999.305(d)(2)(b) § 999.316 § 999.316(a) § 999.316(b)		PRI-03.2

#	Principle Name	SCF Privacy Management Principle (SCF-PMP) Description	AICPA TSC SOC 2 (2017)	APEC	EU GDPR	FIPPs (DHS)	FIPPs (OMB)	GAPP	HIPAA Privacy Rule	ISO 27701 v2019	ISO 29100 v2011	NIST 800-53 rev 4	NIST Privacy Framework [draft]	OECD	OMB A-130	PIPEDA	US - California CCPA	US - Nevada SB820	Secure Controls Framework (SCF)
2.4	Equal Service & Price	Implement business processes to protect the right of data subjects to equal service and price, even if they exercise their privacy rights.							164.524(c)	6.15 6.15.1 6.15.1.1			GV.MT-P3				§ 999.307 § 999.300(a) § 999.300(b) § 999.314 § 999.314(a) § 999.314(b) § 999.314(c) § 999.314(d) § 999.336 § 999.336(a) § 999.336(b) § 999.336(c) § 999.336(c)(1) § 999.336(c)(2) § 999.336(d) § 999.336(e) § 999.336(f) § 999.337 § 999.337(a) § 999.337(b) § 999.337(b)(1) § 999.337(b)(2) § 999.337(b)(3) § 999.337(b)(4) § 999.337(b)(5) § 999.337(b)(6) § 999.337(b)(7) § 999.337(b)(8) § 999.341		CPL-01
2.5	Prohibit The Sale of Personal Data	Provide a clear and conspicuous link on the organization's Internet-based homepage, titled "Do Not Sell My Personal Data" that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal data.								7.3.4		TR-1 TR-1(1)	CT.PO-P3			3	CT.PO-P3		PRI-03.1
3.0	Limited Collection & Use	Ensure that the design of data collection and use are consistent with the intended use of the information, and the need for new information is balanced against any privacy risks.	P3.1	3	Art 5.1			4.1.2 9.2.2	164.506(a-c)	7.2.2 7.3.1 7.3.2 7.4.1 8.2.1	5.4		CT.PO-P1 CT.DM-P1	1		4	§ 999.305(a)(4) § 999.305(a)(5) §999.305(d)(2) §999.305(d)(2)(a) §999.305(d)(2)(b) § 999.330 § 999.330(a) § 999.330(a)(1) § 999.330(a)(2) § 999.330(a)(2)(a) § 999.330(a)(2)(b) § 999.330(a)(2)(c) § 999.330(a)(2)(d) § 999.330(a)(2)(e) § 999.330(a)(2)(f) § 999.330(b) § 999.331 § 999.331(a) § 999.331(b) § 999.332 § 999.332(a)		PRI-04
3.1	Authority to Collect	Identify the lawful basis given to collect, create, use, disseminate, maintain, and/or disclose an individual's personal data. Document this authority in the organization's publicly-facing privacy notice.			Art 5.1		Authority	1.2.5 1.2.11 4.2.2	164.520(a)	7.2.2 7.3.1 7.3.2 7.5 7.5.1 7.5.2 8.1 8.2 8.2.1 8.5.1 8.5.7	5.4	AP-1	CT.DP-P4						PRI-04.1
3.2	Data Minimization	Take steps to minimize the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of the individual's personal data to what is directly relevant and necessary to accomplish a legally authorized purpose.			Art 5.1 Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9 Art 35.11	Data Minimization	Data Minimization		164.502 164.514	7.4.4	5.5	DM-1 DM-3 DM-3(1)	CT.DP-P4 CT.DP-P6		5(f)(1)(f)	4			DCH-18.2
3.3	Internal Use	Restrict the internal use of personal data to only authorized purpose(s) that are consistent with the stated privacy notice.			Art 5.1 Art 9.1 Art 9.2 Art 10 Art 11.1 Art 18.1 Art 18.2 Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9 Art 35.11	Use Limitation	Purpose Specification & Use Limitation	4.1.2 5.2.1 7.2.2 9.2.1 9.2.2	164.502 164.504 164.510 164.512 164.514 164.532	7.4.2 7.4.4 8.2.3		DM-3 DM-3(1) UL-1	CT.DM-P8 CT.DP-P4 CT.DP-P6 CT.PO-P2			5		Sec 2.3	DCH-18.1 PRI-05.1 PRI-05.4

#	Principle Name	SCF Privacy Management Principle (SCF-PMP) Description	AICPA TSC SOC 2 (2017)	APEC	EU GDPR	FIPPs (DHS)	FIPPs (OMB)	GAPP	HIPAA Privacy Rule	ISO 27701 v2019	ISO 29100 v2011	NIST 800-53 rev 4	NIST Privacy Framework [draft]	OECD	OMB A-130	PIPEDA	US - California CCPA	US - Nevada SB820	Secure Controls Framework (SCF)
4.0	Transparency	Provide a transparent notice to the public about privacy practices through a clear and conspicuous notice on all organizational websites, mobile applications, and other digital services regarding the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of the personal data.	P1.1	2	Art 11.2 Art 12.1 Art 13.1 Art 13.2 Art 13.3 Art 14.1 Art 14.2 Art 14.3 Art 26.1 Art 26.2	Transparency	Transparency	2.1.1 2.2.1 2.2.2 2.2.3 3.1.0 3.1.1 3.1.2 4.1.0 4.1.1 4.2.4 5.1.0 5.1.1 6.1.0 7.1.0 7.1.1 8.1.0 8.1.1 9.1.0 9.1.1 10.1.0 10.1.1	164.520	7.3 7.3.1 7.3.2 8.2.2 8.2.3 8.5.1 8.5.2 8.5.6	5.2 5.8	DI-2(1) TR-1 TR-1(1) TR-3	CM.PP-P1 CM.AW-P1	6	5(f)(1)(j)	8	§ 999.305 § 999.305(a) § 999.305(a)(1) § 999.305(a)(2) § 999.305(a)(2)(a) § 999.305(a)(2)(b) § 999.305(a)(2)(c) § 999.305(a)(2)(d) § 999.305(a)(2)(e) § 999.305(b) § 999.305(b)(1) § 999.305(b)(2) § 999.305(b)(3) § 999.305(b)(4) §999.305(c) §999.305(d) § 999.306 § 999.306(a) § 999.306(a)(1) § 999.306(a)(2) § 999.306(a)(2)(a) § 999.306(a)(2)(b) § 999.306(a)(2)(c) § 999.306(a)(2)(d) § 999.306(b) § 999.306(b)(1) § 999.306(b)(2) § 999.306(b)(3) § 999.306(c) § 999.306(c)(1) § 999.306(c)(2) § 999.306(c)(1) § 999.306(c)(2) § 999.306(c)(3) § 999.306(c)(4) § 999.306(c)(5) § 999.306(d) § 999.306(d)(1) § 999.306(d)(2) § 999.305(e) § 999.306(e)(1) § 999.306(e)(2) § 999.307 § 999.307(a) § 999.307(a)(1) § 999.307(a)(2) § 999.307(a)(2)(a) § 999.307(a)(2)(b)		PRI-02
4.1	Notice & Purpose Specification	Provide notice of the specific purpose(s) for which personal data is collected, created, used, disseminated, maintained, retained and/or disclosed.			Art 13.1 Art 14.1 Art 14.2	Purpose Specification	Purpose Specification & Use Limitation	4.2.1	164.520	7.2 7.2.1 8.2.2 8.5.1	5.3	AP-2 DI-2(1) TR-1 TR-1(1)	CM.PP-P1	3	5(f)(1)(d)	2	§ 999.308 § 999.308(a) § 999.308(a)(1) § 999.308(a)(2) § 999.308(a)(2)(a) § 999.308(a)(2)(b) § 999.308(a)(2)(c) § 999.308(a)(2)(d) § 999.308(a)(2)(e) § 999.308(a)(3) § 999.308(b) § 999.308(b)(1) § 999.308(b)(1)(a) § 999.308(b)(1)(b) § 999.308(b)(1)(c) § 999.308(b)(1)(d) § 999.308(b)(1)(d)(1) § 999.308(b)(1)(d)(2) § 999.308(b)(1)(e) § 999.308(b)(1)(e)(1) § 999.308(b)(1)(e)(2) § 999.308(b)(1)(e)(3) § 999.308(b)(2) § 999.308(b)(2)(a) § 999.308(b)(2)(a) § 999.308(b)(2)(b) § 999.308(b)(2)(c) § 999.308(b)(2)(c) § 999.308(b)(3) § 999.308(b)(3)(a) § 999.308(b)(3)(b) § 999.308(b)(4) § 999.308(b)(4)(a) § 999.308(b)(5) § 999.308(b)(5)(a) § 999.308(b)(6)		PRI-02.1
5.0	Data Lifecycle Management	Limit the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of personal data to that which is legally authorized, relevant, and deemed "reasonably necessary" for the proper performance of business functions.	P2.1 P4.1 P4.2 P4.3	4	Art 5.1 Art 18.1 Art 18.2 Art 21.1 Art 21.2 Art 21.3 Art 32.1 Art 32.2			4.1.2 5.2.2 5.2.3	164.502 164.504	6.5.2 6.5.3.3 7.4.2 7.4.8 8.2.3 8.4.2	5.6		CT.DM-P5	4	4(g) 5(a)(1)(c)(i) 5(b)(4) App 1 - 4(b)(2)	5	§ 999.305(a)(3)		DCH-01 PRI-05
5.1	Processing Records	Maintain a record of processing activities that documents the organization's necessary records to support its obligations for the processing of sensitive data.								7.2.8 8.2.6 8.5.3			CM.AW-P4 CM.AW-P6						PRI-09
5.2	Data Flow Mapping	Maintain a record of processing activities that documents the flow of personal data that includes: - Geographic locations and third-parties involved in the storage, transmission and/or processing of personal data; - Contact details of the controller(s) involved in the storage, transmission and/or processing of personal data; - The purposes of the storage, transmission and processing; - A description of the categories of data subjects and personal data; - Where possible, the time limits for erasure of the different categories of data; and - Where possible, a description of the cybersecurity and privacy measures of the data controller.			Art 30.1 Art 30.2 Art 30.3 Art 30.4 Art 30.5							UL-2	ID.IM-P1						AST-04
5.3	Data Custodians	Identify the owners or operators of systems/products/services that process data, or with which data subjects are interacting.								6.5.1.2			ID.IM-P2						AST-03 AST-03.1
5.4	Retention of Personal Data	Ensure that all records containing personal data are maintained in accordance with the organization's records retention schedule and comply with applicable statutory, regulatory and contractual obligations.			Art 5.1					6.5.3 6.15.1.3 7.4.7		DM-2			5(f)(1)(h)	5			DCH-18
5.5	Secure Destruction of Personal Data	Utilize secure methods to dispose of or destroy both physical and digital media that contains personal data.			Art 5.1					7.4.8		DM-2	CT.DM-P5			5			DCH-09.3
5.6	Geolocation Restrictions	Restrict the location of processing, storage and service locations to comply with the privacy notice, as well as applicable statutory, regulatory and contractual obligations.			Art 6.1 Art 26.1 Art 26.2 Art 27.3 Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10 Art 29 Art 44 Art 45.1 Art 45.2 Art 46.1 Art 46.2 Art 46.3 Art 47.1 Art 47.2 Art 48 Art 49.1 Art 49.2														DCH-24 DCH-25 SEA-15 TPM-04.4

#	Principle Name	SCF Privacy Management Principle (SCF-PMP) Description	AICPA TSC SOC 2 (2017)	APEC	EU GDPR	FIPPs (DHS)	FIPPs (OMB)	GAPP	HIPAA Privacy Rule	ISO 27701 v2019	ISO 29100 v2011	NIST 800-53 rev 4	NIST Privacy Framework [draft]	OECD	OMB A-130	PIPEDA	US - California CCPA	US - Nevada SB820	Secure Controls Framework (SCF)
5.7	Data Portability	Provide the functionality to export personal data in a structured, commonly-used and machine-readable format that can be transferred to another controller without hindrance.			Art 20.1 Art 20.2 Art 20.3 Art 20.4								ID.DE-P4 CT.DM-P2 CT.DM-P6						PRI-06.6
5.8	Record of Disclosures	Develop and maintain an accounting of personal data disclosures that upon request can be made available to the individual whose personal data was disclosed.	P6.2 P6.3		Art 30.1 Art 30.2 Art 30.3 Art 30.4 Art 30.5			7.2.1 7.2.4	164.502 164.504 164.506 164.508 164.528	7.2.8 7.5.3 7.5.4		AR-8	CM.AW-P4						PRI-14.1
5.9	Integrity Protections	Maintain the accuracy and relevance of personal data across the information lifecycle as personal data is collected, created, used, disseminated, maintained, retained and/or disclosed.			Art 5.1	Data Quality & Integrity	Quality & Integrity	9.2.1		7.4.3	5.7	DI-2	PR.DS-P6			6			PRI-05.2
5.10	De-Identification	Process personal data in such a manner that it is not attributable to a data subject through technical or organizational measures (e.g., anonymization, pseudonymization or data minimization).			Art 4.5 Art 5.1 Art 6.4 Art 32.1				164.514(a) 164.514(b)						5(f)(1)(f)				PRI-05.3
5.11	Quality Management	Maintain quality assurances throughout the information lifecycle with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.	P7.1	6	Art 5.1	Data Quality & Integrity	Quality & Integrity			7.4.3			CT.PO-P4 CT.DM-P8	2		6			PRI-10
5.12	Secure Data Processing	Implement secure data processing practices so that the confidentiality, integrity and pertinent attributes of sensitive data is maintained throughout the data lifecycle.								6.3.1.5 6.11 6.11.1 6.11.2 6.11.2.1 6.11.2.2 6.11.2.5 7.4 8.4			ID.DE-P4 ID.IM-P5 PR.PP-P3 PR.PP-P4 PR.PP-P5 CT.PO-P1 CT.DM-P7 CT.DM-P8 CT.PO-P4 CM.AW-P3						PRM-04 PRM-05 PRM-06 PRM-07 PRM-08 SEA-01 TDA-06
5.13	Data Lineage	Maintain records of the inputs, entities, systems, applications and processes that influence data of interest, providing a historical record of the data and its origins.											ID.IM-P7 ID.IM-P8 ID.BE-P3 IN.AW-P6 PR.DP-P4						IAO-03
5.14	Updated Use Permissions	Implement data management processes to adjust data that is able to be collected, created, used, disseminated, maintained, retained and/or disclosed, based on updated data subject authorization(s).								7.3.4			CT.PO-P1 CT.PO-P3				§999.305(d)(1) §999.305(d)(2) §999.305(d)(2)(a) §999.305(d)(2)(b) § 999.316 § 999.316(a) § 999.316(b)		PRI-03.2
5.15	Flaw Remediation with Personal Data	Identify and correct flaws related to personal data as it is collected, created, used, disseminated, maintained, retained and/or disclosed.			Art 5.1					6.9.6 6.9.6.1						6			VPM-04.2
5.16	Analytical Biases	Understand and evaluate data analytic inputs and outputs for potential bias.											ID.RA-P2						PRI-10.2
6.0	Data Subject Rights	Provide individuals with appropriate access to their personal data.	P5.1 P6.7	8	Art 12.1 Art 12.2 Art 13.2 Art 14.2 Art 15.1 Art 15.2 Art 15.3 Art 15.4 Art 16 Art 26.3		Access & Amendment	6.2.1 6.2.2 6.2.3 6.2.4 6.2.5 6.2.6	164.502 164.522 164.524	7.3.6 8.2.5			CT.DM-P1			9	§ 999.312 § 999.312(a) § 999.312(b) § 999.312(c) § 999.312(c)(1) § 999.312(c)(2) § 999.312(d) § 999.312(e) § 999.312(f) § 999.312(f)(1) § 999.312(f)(2) § 999.324 § 999.324(a) § 999.324(b) § 999.325 § 999.325(a) § 999.325(b) § 999.325(c) § 999.325(d) § 999.325(e) § 999.325(e)(1) § 999.325(e)(2) § 999.325(f) § 999.326 § 999.326(a) § 999.326(a)(1) § 999.326(a)(2)	Sec 2.1	PRI-06
6.1	Inquiry Management	Maintain a capability to receive and respond to privacy-related requests, complaints, concerns or questions from individuals.	P8.1		Art 18.1 Art 18.2 Art 18.3 Art 19 Art 21.1 Art 21.6 Art 22 Art 26.3			6.2.5 6.2.6 7.1.2 10.2.1 10.2.2	164.522	7.3.9			GV.MT-P4 GV.MT-P7 CM.AW-P2			10	§ 999.312 § 999.312(a) § 999.312(b) § 999.312(c) § 999.312(c)(1) § 999.312(c)(2) § 999.312(d) § 999.312(e) § 999.312(f) § 999.312(f)(1) § 999.312(f)(2) § 999.313 § 999.313(a) § 999.313(b) § 999.313(c) § 999.313(c)(1) § 999.313(c)(2) § 999.313(c)(3) § 999.313(c)(4) § 999.313(c)(5) § 999.313(c)(6) § 999.313(c)(7) § 999.313(c)(8) § 999.313(c)(9) § 999.313(c)(10) § 999.313(c)(10)(a) § 999.313(c)(10)(b) § 999.313(c)(10)(c) § 999.313(c)(10)(d) § 999.313(c)(11) § 999.313(d) § 999.313(d)(1) § 999.313(d)(2) § 999.313(d)(2)(a) § 999.313(d)(2)(b) § 999.313(d)(2)(c) § 999.313(d)(3) § 999.313(d)(4) § 999.313(d)(5) § 999.313(d)(6) § 999.313(d)(6)(a) § 999.313(d)(6)(b) § 999.313(d)(6)(c) § 999.313(d)(7) § 999.324 § 999.324(a) § 999.324(b)	Sec 2.1 Sec 2.2 Sec 2.4	PRI-06.4

#	Principle Name	SCF Privacy Management Principle (SCF-PMP) Description	AICPA TSC SOC 2 (2017)	APEC	EU GDPR	FIPPs (DHS)	FIPPs (OMB)	GAPP	HIPAA Privacy Rule	ISO 27701 v2019	ISO 29100 v2011	NIST 800-53 rev 4	NIST Privacy Framework [draft]	OECD	OMB A-130	PIPEDA	US - California CCPA	US - Nevada SB820	Secure Controls Framework (SCF)
6.2	Updating Personal Data	Provide individuals with appropriate opportunity to correct or amend their personal data.			Art 5.1				164.526	7.3.6 7.4.3 8.2.5			CT.DM-P1 CT.DM-P3				§ 999.312 § 999.312(a) § 999.312(b) § 999.312(c) § 999.312(c)(1) § 999.312(c)(2) § 999.312(d) § 999.312(e) § 999.312(f) § 999.312(f)(1) § 999.312(f)(2) § 999.324 § 999.324(a) § 999.324(b) § 999.325 § 999.325(a) § 999.325(b) § 999.325(c) § 999.325(d) § 999.325(e) § 999.325(e)(1) § 999.325(e)(2) § 999.325(f) § 999.326 § 999.326(a) § 999.326(a)(1) § 999.326(a)(2) § 999.326(b)	Sec 2.3	PRI-12
6.3	Redress	Provide individuals with appropriate opportunity to challenge the organization's compliance with its privacy principles.			Art 12.3 Art 14.2 Art 16 Art 18.1 Art 26.3		Access & Amendment	6.2.5 6.2.6 10.2.1 10.2.2	164.522	7.3.6			CT.DM-P3			10			PRI-06.1
6.4	Notice of Correction or Amendment	Notify affected individuals when their personal data is corrected or amended.	P5.2	8	Art 12.3 Art 18.3 Art 19 Art 26.3				164.526	8.5.8			CT.PO-P4 CM.AW-P1 CM.PP-P1				§ 999.305(a)(3) §999.305(d)(1) §999.305(d)(2) §999.305(d)(2)(a) §999.305(d)(2)(b)		PRI-06.2
6.5	Appeal	Provide individuals with appropriate opportunity to appeal an adverse decision to have incorrect personal data amended.			Art 21.1 Art 21.2 Art 21.3 Art 26.3				164.526				CM.AW-P8						PRI-06.3
6.6	Right to Erasure	Provide individuals with appropriate opportunity to request the deletion of personal data where it is used, disseminated, maintained, retained and/or disclosed, including where the personal data is stored or processed by third-parties.			Art 17.1 Art 17.2 Art 17.3					7.3.6			CT.DM-P4				§ 999.313(b)(1) § 999.313(d)(2) § 999.313(d)(2)(a) § 999.313(d)(2)(b) § 999.313(d)(2)(c) § 999.313(d)(3) § 999.313(d)(4) § 999.313(d)(5) § 999.313(d)(6) § 999.313(d)(6)(a) § 999.313(d)(6)(b) § 999.313(d)(6)(c) § 999.313(d)(7) § 999.318 § 999.318(a) § 999.318(b) § 999.323 § 999.323(a) § 999.323(b) § 999.323(b)(1) § 999.323(b)(2) § 999.323(b)(3) § 999.323(b)(3)(a) § 999.323(b)(3)(b) § 999.323(b)(3)(c) § 999.323(b)(3)(d) § 999.323(b)(3)(e) § 999.323(b)(3)(f) § 999.323(c) § 999.323(d) § 999.323(e) § 999.324 § 999.324(a) § 999.324(b) § 999.325 § 999.325(a) § 999.325(b) § 999.325(c) § 999.325(d) § 999.325(e) § 999.325(e)(1) § 999.325(e)(2) § 999.325(f) § 999.326 § 999.326(a) § 999.326(a)(1)		PRI-06.5
7.0	Security by Design	Establish administrative, technical, and physical safeguards to protect sensitive data commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss or dissemination. Selected practices are in accordance with industry-leading practices (e.g., ISO 27002, NIST 800-53, etc.).			Art 5.2 Art 24.1 Art 24.2 Art 24.3 Art 25.1 Art 25.2 Art 25.3 Art 32.1 Art 32.2 Art 40.2	Security	Security	8.2.2	164.502 164.504 164.530							7			SEA-01.1 TDA-01
7.1	Cybersecurity Considerations	Incorporate privacy requirements into enterprise architecture to ensure that risk is addressed so systems, applications and services achieve the necessary levels of trustworthiness, protection, and resilience.		7	Art 5.2 Art 24.1 Art 24.2 Art 24.3 Art 25.1 Art 25.2 Art 25.3 Art 32.1 Art 32.2 Art 40.2	Security	Security	4.2.3 6.2.2 7.2.2 7.2.3	164.504 164.530	6.11.2.5 7.4 8.4			ID.DE-P4 PR.PP-P3 PR.PP-P4 PR.PP-P5 CT.PO-P1 CT.DM-P7 CT.DM-P8 CM.AW-P3	5	App 1 - 4(b)(5)	7			SEA-01
7.2	Cryptographic Protections	Ensure personal data is encrypted both at rest and in transit.			Art 5.1				164.502 164.504 164.530	6.7 6.7.1 6.7.1.1 6.10.2.3			PR.DS-P1 PR.DS-P2						CRY-01 CRY-03 CRY-05
7.3	Physical Protections	Ensure physical security and environmental controls provide appropriate protection for environments where personal data is stored, transmitted and/or processed.			Art 32.1 Art 32.2	Security	Security	8.2.3 8.2.4	164.504 164.530	6.8.1.4 6.15.1.4			PR.AC-P2 PR.DP-P4			7			PES-01
7.4	Embedded Technology	Facilitate the secure implementation of embedded technologies so sensors minimize the collection of personal data and alert individuals to the personal data collected by those sensors.			Art 5.1 Art 5.2 Art 32.1 Art 32.2	Transparency	Transparency		164.504 164.530										EMB-01 END-13.1 END-13.2 END-13.3
7.5	Retire Outdated Systems	Upgrade, replace, or retire any system, application or service for which appropriate protections, commensurate with risk, cannot be effectively implemented.							164.504 164.530						App 1 - 4(b)(3)				TDA-17
7.6	Personnel Security	Implement personnel management practices, covering employees, contractors and other entities, that ensures appropriate vetting and clearance to systems, applications and/or services that contain, store or transmit personal data.			Art 32.1 Art 32.2 Art 32.4				164.504 164.530	6.4.2.2			GV.PP-P1		5(c)(2) App 1 - 4(h)(1)-(2) App 1 - (4)-(7)	7			SAT-01

#	Principle Name	SCF Privacy Management Principle (SCF-PMP) Description	AICPA TSC SOC 2 (2017)	APEC	EU GDPR	FIPPs (DHS)	FIPPs (OMB)	GAPP	HIPAA Privacy Rule	ISO 27701 v2019	ISO 29100 v2011	NIST 800-53 rev 4	NIST Privacy Framework [draft]	OECD	OMB A-130	PIPEDA	US - California CCPA	US - Nevada SB820	Secure Controls Framework (SCF)
7.7	Rules of Behavior	Require employees and contractors to read and agree to abide by the organization's rules of behavior, prior to being granted access to systems, applications and/or services that store, transmit or process personal data.	CC1.1						164.504 164.530	6.4.2.1 6.5.1.3					App 1 - 4(h)(6) App 1 - 4(h)(7)				HRS-05.1
7.8	Employee Sanctions	Utilize employee sanctions to hold personnel accountable for complying with the organization's privacy policies and processes.	CC1.5						164.504 164.530	6.4.2.3					App 1 - 3(b)(9)				HRS-07
7.9	Workforce Management	Respond to changing mission requirements and maintain workforce skills in a rapidly-developing technology environment through recruiting and retaining the talent needed to support the organization's mission.			Art 32.1 Art 32.2 Art 32.4				164.504 164.530				PR.DP-P9		5(c)(1) 5(c)(7)				HRS-01
7.10	Professional Competency	Develop and enforce privacy competency requirements for staff members involved in the acquisition, management, maintenance and use of information resources, to ensure they have the appropriate knowledge and skill.			Art 32.1 Art 32.2 Art 32.4				164.504 164.530	6.4 6.4.1 6.4.1.1					5(c)(1)				HRS-04
8.0	Incident Response	Maintain adequate incident response plans, capabilities and training for employees and third-party stakeholders on how to report and respond to incidents.			Art 33.1 Art 33.2 Art 33.3 Art 33.4 Art 33.5			1.2.7 7.2.4		6.13 6.13.1 6.13.1.1 6.13.1.5			GV.MT-P4 GV.MT-P5 PR.DP-P7		App 1 - 4(b)(3) App 1 - 4(f)(1) App 1 - 4(f)(3) App 1 - 4(f)(4) App 1 - 4(f)(5) App 1 - 4(f)(6) App 1 - 4(f)(7) App 1 - 4(f)(8) App 1 - 4(f)(9) App 1 - 4(f)(10) App 1 - 4(j)(2)(e)				IRO-01 IRO-04 IRO-04.1
8.1	Coordinated Response	Respond to incidents in a coordinated and structed manner to ensure the appropriate steps are taken to identify and respond to potential incidents.								6.13.1.4									IRO-07
8.2	Breach Notification	Report data breaches involving personal data to relevant regulators, law enforcement and affected parties in accordance with applicable statutory, regulatory and contractual obligations for breach notification.	P6.6		Art 33.1 Art 33.2 Art 33.3 Art 33.4 Art 33.5 Art 34.1 Art 34.2 Art 34.3 Art 34.4			1.2.7	164.400 164.402 164.404 164.406 164.408 164.410 164.412 164.414	6.13.1.2 6.13.1.3					App 1 - 4(b)(3)				IRO-10 IRO-11.2
9.0	Risk Management	Implement a risk management framework to ensure that risks are identified, evaluated and addressed to achieve necessary levels of trustworthiness, protection, and resilience.			Art 32.1 Art 32.2					6.8.1.4			ID.DE-P1		4(i)				RSK-01
9.1	Evaluate Risks	Utilize appropriate risk analysis methods to evaluate the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of personal data where it is stored, transmitted and/or processed.			Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9 Art 35.11			1.2.4		5.4.1.2 6.8.1.2			ID.DE-P1 ID.DE-P5		5(d)(3) 5(d)(4)(b)				RSK-04
9.2	Assess Supply Chain Risk	Assess supply chain risks associated with systems, system components and services for privacy implications.			Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.8 Art 35.9 Art 35.11 Art 36.3								ID.DE-P2 ID.DE-P3 ID.DE-P5						RSK-08 RSK-09 RSK-09.1
9.3	Risk Awareness	Maintain a current and accurate register of risk.			Art 35.1								ID.DE-P1						RSK-04.1
9.4	Risk Response	Responses to identified risks are appropriately identified, categorized and prioritized.											ID.DE-P1 ID.RA-P5 RS.MI-P3 ID.RA-P5						RSK-06.1
9.5	Data Protection Impact Assessment (DPIA)	Utilize Data Protection Impact Assessments (DPIAs) to effectively identify and reduce privacy risks to an acceptable level.			Art 35.1 Art 35.2 Art 35.3 Art 35.6 Art 35.7 Art 35.8 Art 35.9 Art 35.11 Art 36.1 Art 36.2 Art 36.3			1.2.4 4.2.3		7.2.5			ID.IM-P7 ID.RA-P1 ID.RA-P2 ID.RA-P3 ID.RA-P4 ID.RA-P5 ID.DE-P2 ID.DE-P3 GV.MT-P4 GV.MT-P5		5(f)(1)(i)				RSK-10
10.0	Third-Party Management	Provide privacy oversight of third-parties with access to personal data, so that only trusted third-parties are contracted with.			Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10 Art 32.1 Art 32.2				164.514	6.12 6.12.1 6.12.1.1									TPM-01
10.1	Supply Chain Protections	Govern the disclosure of personal data to ensure it is only provided to trusted third-parties that can store, process and/or transmit it in a secure manner.			Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10					6.12.1.3					App 1 - 4(j)(2)(b) App 1 - 4(j)(3)				TPM-03

#	Principle Name	SCF Privacy Management Principle (SCF-PMP) Description	AICPA TSC SOC 2 (2017)	APEC	EU GDPR	FIPPs (DHS)	FIPPs (OMB)	GAPP	HIPAA Privacy Rule	ISO 27701 v2019	ISO 29100 v2011	NIST 800-53 rev 4	NIST Privacy Framework [draft]	OECD	OMB A-130	PIPEDA	US - California CCPA	US - Nevada SB820	Secure Controls Framework (SCF)
10.2	Secure Disclosure To Third-Parties	Govern third-party use of personal data to ensure privacy requirements are enforced when a third-party stores, processes or transmits personal data on behalf of the organization.	P6.1		Art 6.1 Art 6.4 Art 15.2 Art 20.2 Art 26.1 Art 26.2 Art 26.3 Art 44 Art 45.1 Art 45.2 Art 46.1 Art 46.2 Art 46.3 Art 47.1 Art 47.2 Art 48 Art 49.1 Art 49.2 Art 49.6			7.2.1 7.2.2 7.2.3	164.502 164.504	7.4.9 7.5 8.4.3 8.5.1 8.5.7			CT.PO-P2		5(e)(1)(b) 5(e)(1)(c) 5(e)(1)(d) 5(e)(7)(h) App 1 - 3(c)				PRI-07
10.3	Contractual Obligations for Third-Parties	Require terms and conditions in contracts and other agreements to cover the collection, creation, use, dissemination, maintenance, retention, and/or disclosure of personal data.	P6.4 P6.5		Art 6.1 Art 6.4 Art 26.1 Art 26.2 Art 26.3 Art 28.1 Art 28.2 Art 28.3 Art 28.4 Art 28.5 Art 28.6 Art 28.9 Art 28.10 Art 29			4.2.3 7.2.4	164.502 164.504 164.514	6.10.2.4 6.12.1.2 7.2.6 8.2.5 8.5.8			ID.DE-P3		5(a)(1)(b)(ii) 5(d)(1)(j) App 1 - 3(d) App 1 - 4(j)(1)				PRI-07.1 TPM-05
10.4	Third-Party Compliance	Validate that privacy controls for systems, applications and services used or operated by third-parties are effectively-implemented and align with industry-recognized secure practices, as well as comply with applicable statutory, regulatory and contractual obligations.			Art 32.1 Art 32.2			1.2.6 10.2.3 10.2.4 10.2.5		6.15.2.2 6.15.2.3					App 1 - 4(j)(2)(b)				PRI-08
11.0	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.								6.12 6.12.1 6.12.1.1									TPM-01
11.1	Privacy Protections Context	Identify and document the organization's role as a controller and/or processor of sensitive data, including instances involving more than one party.								7.2.7 7.4.9 8.4.3 8.5.7			ID.IM-P5 ID.BE-P1 ID.BE-P2				§ 999.315(f) § 999.316 § 999.316(a) § 999.316(b)		GOV-08 PRI-07.2
11.2	Policies, Standards & Procedures	Ensure appropriate policies, standards and procedures exist to operationalize the privacy program.			Art 32.1 Art 32.2 Art 32.3 Art 32.4			8.2.1	164.530(h)(1)	6.2 6.2.1 6.2.1.1			GV.PP-P1 GV.MT-P3 GV.MT-P4 GV.MT-P5 GV.MT-P6 GV.MT-P7 CT.PO-P1 CT.PO-P2 CT.PO-P3 CM.PP-P1 PR.DP-P4		App 1 - 4(j)(2)(a)				GOV-02
11.3	Periodic Review	At planned intervals or after significant changes, review policies, standards and procedures to ensure the continuing suitability, adequacy and effectiveness to meet the organization's applicable statutory, regulatory and contractual needs.			Art 5.2 Art 32.1 Art 32.2 Art 32.3 Art 32.4			8.2.1 10.2.4	164.530(h)(2)	6.2.1.2			GV.MT-P2						GOV-03 CPL-03
11.4	Oversight	Provide oversight of privacy controls throughout the lifecycle of systems, applications and services to ensure that in a timely manner, senior leaders with the organization are made aware of privacy-related risks that are not appropriately remediated.			Art 5.2	Accountability & Auditing	Accountability & Auditing	8.2.7	164.530(c)(1)				GV.MT-P4 PR.DP-P5		App 1 - 3(a) App 1 - 3(b)(4) App 1 - 3(f) App 1 - 3(g) App 1 - 4(b)(2)				CPL-02
11.5	Management Visibility	Provide performance metrics and trend analysis to enable management visibility and coordinate privacy efforts across the organization.		9	Art 31			10.2.3 10.2.5					CM.AW-P4 CM.AW-P6 CM.AW-P7	8	5(a)(1)(c)(ii) App 1 - 3(b)(10) App 1 - 4(1)		§ 999.317 § 999.317(a) § 999.317(b) § 999.317(c) § 999.317(d) § 999.317(e) § 999.317(f) § 999.317(g) § 999.317(g)(1) § 999.317(g)(1)(a) § 999.317(g)(1)(b) § 999.317(g)(1)(c) § 999.317(g)(1)(d) § 999.317(g)(2) § 999.317(g)(3)		PRI-14

#	Principle Name	SCF Privacy Management Principle (SCF-PMP) Description	AICPA TSC SOC 2 (2017)	APEC	EU GDPR	FIPPs (DHS)	FIPPs (OMB)	GAPP	HIPAA Privacy Rule	ISO 27701 v2019	ISO 29100 v2011	NIST 800-53 rev 4	NIST Privacy Framework [draft]	OECD	OMB A-130	PIPEDA	US - California CCPA	US - Nevada SB820	Secure Controls Framework (SCF)
11.6	Compliance	Oversee the execution of privacy controls to create appropriate evidence of due care and due diligence, demonstrating compliance with all applicable statutory, regulatory and contractual obligations, including age-based restrictions.			Art 1.2 Art 2.1 Art 2.2 Art 3.1 Art 3.2 Art 3.3 Art 6.1 Art 17.3 Art 20.3 Art 23.1 Art 23.2 Art 24.1 Art 24.2 Art 24.3 Art 25.1 Art 25.2 Art 25.3 Art 27.1 Art 27.2 Art 27.3 Art 27.4 Art 27.5 Art 32.1 Art 32.2 Art 32.3 Art 32.4 Art 40.1 Art 40.2 Art 42.2 Art 43				164.530(c)(1) 164.500 164.501 164.502(a-j)	6.15 6.15.1 6.15.1.1			GV.MT-P3		4(g) 5(e)(1)(d) 5(f)(1)(a) 5(f)(1)(c) 5(f)(1)(g) App 1 - 3(a) App 1 - 3(b)(4) App 1 - 3(f) App 1 - 3(g) App 1 - 4(j)(3)		§ 999.300 § 999.300(a) § 999.300(b) § 999.314 § 999.314(a) § 999.314(b) § 999.314(c) § 999.314(d) § 999.336 § 999.336(a) § 999.336(b) § 999.336(c) § 999.336(c)(1) § 999.336(c)(2) § 999.336(d) § 999.336(e) § 999.336(f) § 999.337 § 999.337(a) § 999.337(b) § 999.337(b)(1) § 999.337(b)(2) § 999.337(b)(3) § 999.337(b)(4) § 999.337(b)(5) § 999.337(b)(6) § 999.337(b)(7) § 999.337(b)(8) § 999.341 § 999.341(a)		CPL-01
11.7	Critical Business Functions	Ensure systems/products/services that support organizational priorities are assessed so that critical assets are identified and key functional requirements communicated.											ID.BE-P3						BCD-02 TDA-06.1 TPM-02