



Information Privacy Decoded

The Five Elements of Proactive Privacy Stewardship

16 December 2021

Scott Foote, Phenomenati Consulting

© 2021 Phenomenati. All Rights Reserved.



Introductions

- I am...
 - a Privacy professional and advocate
 - a Data Protection Officer (DPO), CIPM (IAPP), CDPSE (ISACA)
 - a Security professional
 - a Chief Information Security Officer (CISO), CISSP, CCSA, CCSP, CISM, etc.
 - an Auditor
 - CISA (ISACA), ISO 27001 Auditor, etc.
- I am not...
 - A lawyer
 - Always consult a *qualified* Privacy Attorney or Legal Practice in putting together your Privacy Program.



Five Elements of Proactive Privacy Stewardship

- Reviewing the Foundations of a Privacy Program
 - e.g., Who, What, Why, How, Where
- Conducting Privacy "Risk Assessments"
 - e.g., PIA, DPIA
- Establishing Security & Privacy Controls
 - e.g., Preventative, Detective, Corrective, Administrative, Physical, Technical
- Building "Trust Through Transparency"
 - e.g., Certification against Security & Privacy Standards ISO/IEC 27001, 27017, 27018, 27701
 - e.g., Certification against Industry Regulations PCI DSS, HITRUST
- Engaging with the Subjects (people) of the Privacy Information
 - e.g., Notice/Policy, Consent/Opt-In/Opt-Out,
 - e.g., Data Subject Requests, Notification of Breaches



Foundations of a Privacy Program

- Scope: Aspects of your Organization that are "In Scope" for Privacy
 - Marketing target market demographics
 - Sales contact information about prospects and clients
 - Employees full-time and part-time staff, benefits info includes \$ and Health privacy data
 - Vendors contact information about vendors and service providers
 - End-Users of the Company's services
- What: Data Elements Considered in scope by Privacy Laws and Regulations
 - Non-Special Category Data
 - Special Category Data
 - Data Minimization: Are you collecting only the minimum PI/PII data necessary to achieve your organization's lawful purpose?
 - Consult a competent Privacy Attorney or Law Practice
- Why: Have you documented your lawful purpose for collecting/processing PI/PII?
 - Is Consent necessary? Given freely? Easily removed?
 - Is the PI/PII necessary "for the performance of a contract" to which the data subject is party?
 - Is the PI/PII necessary "for compliance with a legal obligation"?
 - Is the PI/PII necessary "to protect the vital interests of the data subject"?
 - Is the PI/PII necessary "to perform a task carried out in the public interest", or via official authority?
- Is the PI/PII necessary "for the purposes of legitimate interests"?

 © 2021 Phenomenati. All Rights Reserved.

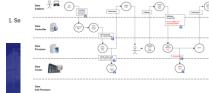
- How: Is PI/PII Processed by (or on behalf of) your organization?
 - How is PI/PII collected? Directly, Indirectly, etc.
 - How is PI/PII processed?
 - How is PI/PII stored?
 - How LONG is PI/PII stored? (minimize Data Retention)
 - Have you documented all of the Data Flows of PI/PII through your organization?
- Who: Processes the PI/PII you collect?
 - Internal parties with access to PI/PII
 - External parties with access to PI/PII
- Where: Are the Locations of
 - Data Collection
 - Data Storage
 - Data Processing
 - Data Accesses

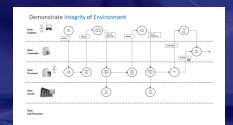


Foundations of a Privacy Program – Inventories & Diagrams

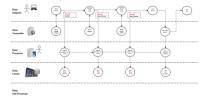
			lan Shi
What this Online Priva	acy Policy Covers	Examples of Personal Data We Collect	Categories of Third Parties With Whom We Share this Personal Data:
Account or Contact D	Data	1. First and last name 2. Email	1. Bank partners, other financial institutions and financial services companies
		3. Postal address	2. Service Providers
		4. Phone number	3. Postal address
		5. Unique identifiers such as passwords	4. Parties You Authorize, Access or Authenticate
Contemporate id	antification and a loss	1. First and last name	1. Bank partners, other financial institutions
Customer records ide	entified by state law	2. Social Security number	and financial services companies
		3. Address	2. Service Providers
		4. Phone number	3. Postal address
		 Tokenized bank account information, debit card information, other financial information 	4. Parties You Authorize, Access or Authenticate
Customer records ide	antification and a loss	1. bank account number	1. Service Providers (specifically Plaid, as
Customer records lat	entitled by state law	2. debit card information	described below)
		3. Payment card type	2. Bank Partners
		4. Billing address, phone number, and email	3. Parties You Authorize, Access or Authenticate
		5. Account balance, transactional histories and other financial information	P IN LEVEL IN TRADUCTOR
Commercial Data		 Transaction history associated with your bank accounts and cards 	1. Service Providers (specifically Plaid, as described below)
		2. Purchase history	2. Parties You Authorize, Access or
		 Records of personal property, products or services obtained, or considered 	Authenticate
		4. Consumer profiles	
		5. Purchasing or consuming tendencies	
Device/IP Data		1. IP address	1. Know-your-customer (KYC) service
Devicent Data		2. Device ID	providers
		3. Domain server	2. Parties You Authorize, Access or Authenticate
		Type of device/operating system/browser used to access the Services	
Web Analytics		1. IP address	1. Service Providers
the Paragoos		2. Device ID	2. Business Partners
		2 Domain conver	3. Participation Automation
	End-User Account Regist	tration	Au End-User Authentication
	Dete Soljesta		
			1. Se
Consumer Demo	Dens Controller		
			Marchanter Marchanter
	Prosessor 🛐 🛄 🔅		Data Preessar
THE KA			Territorian (
and the second	Cantar Cantar	(=)	Center III

and unit. Paint																	
Article	10.04.04		Page a									Natara af the Peacewing					
	100 0000		Page 1	kishinar (in Canang Jila)		-1-14-1		and a closed		and a standard		n in here of the second se	iste Presse Discolored adte stor period	Del Marca esta cherra di e pris candif			maghtikistan districtionsky
To by take	formåld han omen linde i prom førde	al un a			11. 41414	a har sec and process	Separation 1	na na ing na ing na ing ang ang ang ang ang ang ang ang ang a		der ferbauterstadentes fahr for	alt-handlen a	un bereinen? Anteilie in en sternigen (d. sternigen in gestigt in der sternigen in der sternigen im der sternigen im der stern	v. Dý últoma septara ageringt dy na.	the second significant process of proceedings	mo. Perallakatet	Lowert means to be levels	in te de la constantione and
	(h landaje).			t a	94410 2004) 2011 2011 2011	B Supply hereign and partner for glasks and being of a strategy of allowed being in the line of the for- al conference of the strategy of the sector behavior and the still of the sec- tor behavior and the still of the sec- tor behavior and the still of the sec- tor behavior and the still of the se- tor behavior and the still of the sec- tor behavior and the still of the sec- tor behavior and the still of the sec- tor behavior and the sector and the sec- tor behavior and the sector and the sec- tor behavior and the sector and the sec- tor and the sector and the sector and the sec- tor and the sector and the sector and the sector and the sec- tor and the sector a		han da Gan Ganaka mata Canpany Jalan. Inan ad 21 aliang an Panan Kanin alian si di Panga da Pati Kanit angkanin an Ipaga	u (+)	dae .			ly de instant de art de art de Anneigist Ayder de an	samā ļabirins ie gāpiet jartud ies ļasamen salatis ie Mongardzaniņ Lotin Lathschalger nova armatienņ	nitis telas Paras	rte is fille en richegen di fi	na 20 seu ne Nord, kalan kooken 10 nord keel delgeven 1 0 ne
(in the state	in kin dynafor (naf ar line ki podrigg om och dynar)	fan fergende fan skillen style noes fade natioerige útstefigen úts	hous fof a far indiaelpadarina indiae	ge. Balderlandt om Halerlyne hen etter and legte Handler fogde av proverset.	Sector Sector Sector Sector Sector Sector Sector	at blev som groud plane, om som angeskaphenskipsstand prositioner det levelsengels opsåter att det sing of de fot fot da mytempered opsåter att det sing om de fot of planets to jotsteppels for of opsystem dependent og som de entype fot andre softerpered dependent det som de entype fot andre softerpered dependent det softerpingt on alle fot andre fot de		a, Magneed a Barlands Laging gro	k naražio djenica de ministroj te applicajo gle Ne line	ia liyok Delwani Encapile in endologie Ja Neol Egistekoj	-	et manafissonia versioningiga konse pipalajevana, tan ante possilara na mengang mengang serai konstanta mata s a do taka takan kan ante (second) takapa limbel peros.	÷	10 h	5,5.	4 1	far i an d-fo-face an de colair afair di colo color. P
in a start of the second s	del de l'ar har dy armen men parte men de Breilland Breinen en altres metro fais Les demolte (Carller de - Lan armon i lo insging ef de la baien non. Lo gen Aprile	n an an the integration of the last of the base of the	Deve to ingly the last of the ex-	Aprilado Alticario Alticario Alticario Antigene	energy) The balance is a stream that advances a stre- istic produces to the face to streng three. To obtain the subscend of The balance is a deviation or new downly business part of energy on the stream of the sub- part of energy on the stream of the theorem of the subscender.		fachardian patrian dha fa dalaga ta' fa dalaga a cinta tala patrian fa fa factorego aj		inde sond San Landow Law and with H i nal and Difference in San San San San San San San San San Sa	rikų, kr stanoj deirogijuolės kr	ðar aðlask skinnar meðir skundar Irðani menskyðir sjól í fræðarar fir markadi se af fel pro	ich machaire dao chokaring Tealannin alle aig i sha (talg ar neiligdo Cargar) hone Milice ar mano (tradicales, a the fact from top of the mail)		tiop. Date skylister a salare a Date skylister skilder a	An increase of the later state	fal i an d de lacen
	della Bascingdyr Medialler Kristel	piantijeg (anarosovite in piantiky alterationie)	circular Communic the file line for All public streets	te Same en de la desta de la		k konstant. Si Taka se malaga Maria sa kalaga ka si Ibat.		a alcoline to dy to constant	 A bi largesita posisionessantito la 	nine Breisstellenlievslijkenenlegise	anticer/patienersy for	en en tingen fan in en en en in de en eit heter an par et de	in Diparterini consiste Action Pressonation Centelle Inco	14	Can a more depty	a traphy frank for increases the Data	Tati is an of the lapson.
_							_										
and the local	ene lint die dyr in Me	(unlosed analyses also being the doublet as a	t ter mytelsen standen tertradit et entre ter	n hairman ha jua (114 an parato indonés)	han dinya didini	res adapa bill d blackmelle black	Solija kao akt	ar hypothese annual ar		Cartest ogistely (self k agus) des sandstare da	nis de standig setta est	r kola Saciaja seta "Alfon?) zistejuna:		n arte de popular té câplica câneres possai de	galar ang kacila at Kanakasay) Salah pakamar ang sanakasay	Vagacity and Page other diffe as the Company over the Mathematical Mathematical Advancements and a second	an fa ingegra a biologi ta 19 king gan a biologi
calco be	gala bea may medilatan dari gar selian interinter Autor	ako di mada ang da kadi aka guring di mang mang kadi kada ing ka mga kuda kang di di kada ing kadi kadi kadi kada kadi	n Tan ny komulayaka belovaki, storka antoro II. oskog jarte Dr. Ko		Bellapayta das Norm Bellapáyta das Norm	nem, and kyne hefel i de fan schonelse felle son kom Marslan De velle Marsla Marsla gebre He	Constantination (a grane (constantination) (a faile procession) (a faile constantination) (a faile constantination) (a faile constantination)	By edited induces at reserving forwards, induces at second at the algorization of a second at the second at the algorization of a second at the second at	An faith are	ng lalang hang tang kang ding lalang hang ding kang ding kang ding ding ding kang ding kang ding kang ding kang Kang ding kang ding kang Kang ding kang ding ka	falqo: qarlab Laur Cador	ala ny mana	- gjiler textledi 20	n ay terda yang sa shi si gina sa sa sa ya sa fa San Davida	This is an argument of the	n i fe fragge ynwe bût fan interf e. Dy eng frag wij en wit en yn de en leftillete eiler wie noai	anda kayayan sekini pakyi
teginis teg marganing Alpracticis Labolicação	gint for any non-life cap- ge of the cale of the distribution into the case of the distribution of the target of the distribution of the target of the distribution of the cale of the case of the distribution of the cale of the distribution of the distribution of the distribution of the cale of the distribution of the distribution of the distribution of the cale of the distribution of the distribution of the distribution of the cale of the distribution of the distribution of the distribution of the cale of the distribution of the distribution of the distribution of the distribution of the distribution of the distribution of the distribution of the distribution of the distribution of the	at statutes and each professional and a statute profession of the statute of a statute profession of the statutes of the statute of the statutes of the statutes of the statutes of the statutes of the statutes of the statutes of the statutes of the statutes of the statut	E to tran y definition of any definition of any definition of a polarization of the observation of the obser	n harved oger 191 og perste och døre 1912 in der tregenet er de Tala der und at die der de tregenet och Tala der und at die net de tregenet och Tala der effektive der personen och Tala der veder alle den m	 Beitingun ochsekteren Beitingun ochsekteren Beitingungs ochsekteren Beitingungs ochsekteren Beitingungs ochsekteren 	ore only both fills along the block institute from the second sec	Constantina de la constantia de la la guara constitución de la de la constitución de la constitució	A particular distance of weather distance of the second distance of the second of the second distance of the second distance of the second distance of the second of the second distance of the second distance of the second distance of the second distance of the second distance of the second distance of the second distance of the second distance of the second distance of the second distance of the second distance of the second distance of the second distance of the second distance of the second distance of the second dist	An faith are	ngintang tang tang ang disang sa Bartan di Ang ang Bartan di Ang Tang Laka katan di Ang	الحاوية بويادات تحيا خطاب	1999,9992 0	e ja za na kologi - Santa Santa - Santa Santa	n et fok peparatik (genori er nyose fo dis fan de elle en fok it peparatik (genorite organiz ff dis iteratio	Nik konservator 1. februar ogsater konserva _k te	 A first and the advances of advances of a strategy advances of the advances of th	an de Begegen an Beislady? Ar (1. Table Begerin de Santa Santa Terpej fan Person (Santa Santa
nghin big ana ping Ajara bin Inghin big Indating Anatolia	and the endpoint of the endpoint age on the endpoint of the endpoint interaction of the endpoint of the and the endpoint of the analysis and the endpoint of the analysis of the endpoint of the analysis the term of the constraint of the term of the constraint of the analysis the term of the constraint of the analysis the term of the constraint of the analysis		το του μότου αρχά καλ τομάζι κάται τη στο του του ΤΟ Πουρχουρία δια. το	n har om de pe 191 geperte och der 1912 de der tempeni trek Filipier weite soln her a n har och te pe 191 geperte och der 1912 de der tempeni trek Filipier	 Britispage schere Herrice 	ne adap bir All dala daala bir Kanada ka	Conditionen de la condition de la grane production de la de la condition de norma de la conditionen de la constructionen de la	Control of the second secon	6 1.0 st	ng terdap han di kang ang di kang ang di kang ang di kang dikang dikang dikang di kang di kang di kang di kang di kang di kang	falqo: qarlab Laur Cador	1999,9992 0	La (La na Mala) (1997) 	n e tre à page chicigen et un part de fair faith	This is an argument of the	n sin Course provide Mania II n Departy for adaptive start particulation to believe allow as associated	an de Begegen an Beislady? Ar (1. Table Begerin de Santa Santa Terpej fan Person (Santa Santa
Explose tog mean string align or the local control of the local of the backward of the backwar				na teres and a part of a part of a spectra dynamic of the large set of the	 Edupped Adalam and Adalam Adalam and Adalam and Adal		E see a second see in province of second sec	Control C	in face of the second s		dangan agantan terden terden dangan agantan terdenter dangan dara terdenter dangan dara terdenter	519300 F	- -		Yan kan na na na na 19 kan jar gundra a kan siga n 19 kan jar gundra a kan siga 19 kan jar jar jar jar jar jar jar na na jar jar jar jar jar jar jar jar na na jar jar jar jar jar jar jar na na jar jar jar jar jar jar jar jar na na jar jar jar jar jar jar jar jar na na jar jar jar jar jar jar jar jar na na jar jar jar jar jar jar jar jar jar ja	 A for any series of the Additional Office of the Additional Offi	Init Lange on a black (h) 41 Share (h) Share (h) 42 Share (h) Share (h) 43 Share (h) Share (h) 44 Share (h) Share (h) 45 Share (h) Share (h) 46 Share (h) Share (h) 47 Share (h) Share (h)





Demonstrate In	egrity of Session
----------------	-------------------



Provide Support to	End-User		
Dees Saljeens 🗧 🧮 📰		Name Report	
Data Controller			
Ders Pressor		-	
En 🌆 😑	ė,		(jj)

Data Sub-Pro

Data Sub-Processa



Conducting Privacy "Risk Assessments"

Privacy Impact Assessment (PIA)

- For new business systems, or changes to existing systems...
 - 1) Will any Personal Information (PI) or Personally Identifiable Information (PII) be impacted?
 - 2) If so, identify the potential "Risks to the Rights and Freedoms" of the relevant Data Subjects.
 - 3) Perform a Privacy Threshold Analysis (PTA)

Data Protection Impact Assessment (DPIA)

- Has each Risk identified (e.g., in PIAs) along the Data Flows, been assessed either Qualitatively, Quantitatively, or both?
- These Risk Assessments should consider existing...
 - a) Inherent Risk,
 - b) Existing Controls,
 - c) Residual Risk, and
 - d) whether that Residual Risk should be Accepted, Rejected, Further Mitigated, or Transferred (not easily done with Privacy issues).



Establishing Security & Privacy Controls

- For each Risk identified in your Assessments (PIA, DPIA)...
 - Have you identified a set of relevant Security & Privacy Controls to mitigate that Risk?
 - Administrative, Physical, Technical Controls
 - Preventative, Detective, *Corrective* Controls

For any/each Cross-Border Transfer of PI/PII

- Has an appropriate Control been established to ensure protection of the Privacy in the new geographic region?
- e.g., GDPR requires one of...
 - adequacy decisions,
 - Standard Contractual Clauses (SCC),
 - Binding Corporate Rules (BCR), etc.

Are you anonymizing or pseudonymizing PI/PII in any way?



Cyber Security Controls Landscape

© 2021 Phenomenati. All Rights Reserved.

Stage of Compromise

		Preventative	Detective	Corrective
/==	Technical	e.g., Authentication e.g., Authorization e.g., FWs, Gateways, Proxies e.g., Data Loss Prevention	e.g., Audit Trails (logs) e.g., Detection Analytics e.g., Honeypots/nets e.g., Canaries ("DRM")	e.g., Traffic Redirect e.g., Account Lock e.g., Software/System Quarantine e.g., System Restore
	Administrative	e.g., Policies & Procedures e.g., NDAs, Security Training e.g., Patch Management e.g., Principle of Least Privs	e.g., Auditing / Threat Hunting e.g., Separation of Duties e.g., Job Rotation e.g., Risk ID & Assessment	e.g., Disaster Recovery Plan e.g., Business Continuity Plan e.g., Cyber Insurance
Customer Management Bitandard Development Consistency Buinness Optimal	Physical	e.g., Guards, Gates, Badges e.g., Locks, Secure Areas e.g., Encryption	e.g., Audio/Video Surveillance e.g., RFID, GPS e.g., Heat Sensors	e.g., Fire Suppression e.g., Redundant Systems/Site e.g., Restore from Backup
		And and a second		Presenter Presen



Engaging with the Subjects of the Privacy Information

- Notice: Transparency of processing with the Data Subjects affected?
 - Are your Privacy Policies easily understood, and immediately accessible at the time/place of data collection?

• **Consent**: Is Consent needed? How/When is it obtained? Can it easily be revoked?

- Opt-In e.g., GDPR, and very likely all future legislation
- Opt-Out
 e.g., default in the U.S., and growing increasingly unpopular

• Establish a "Data Subject Requests (DSR) Program" to formally handle requests

- Ability for Data Subjects to restrict the processing of their PI/PII?
- Ability for Data Subjects to object to automated decision-making or profiling, based upon the PI/PII your organization collects on them?
- Access to the PI/PII for the Data Subjects affected?
- Ability to correct (rectify errors) PI/PII for the Data Subjects affected?
- Ability for the Data Subject to export their PI/PII for transfer to a similar system (where appropriate)?
- Right to be forgotten... ability to request PI/PII be erased... balanced with the legal or regulatory obligations for Data Retention.
- Breach Notification Obligation(s)
 - Has your organization prepared appropriate communications (content and services) for use in the event of a privacy data breach?

Trust Through Transparency

- 3rd Party Compliance Audits / Certifications
- Certification against Security & Privacy Standards
 - ISO/IEC 27001 requirements for an Information Security Management System (ISMS)
 - ISO/IEC 27017 security of cloud services
 - ISO/IEC 27018 data privacy in cloud services
 - ISO/IEC 27701 extends 27001 for Privacy Information Management
- Certification against Industry Regulations, Standards, and Frameworks
 - PCI DSS Payment Card Industry Data Security Standard
 - HIPAA, HITRUST CSF



Questions?