ACI UNIVERSAL PAYMENTS℠

PCI AND DATA PRIVACY UPDATE

October 17, 2018
NEbraskaCERT CSF

Lisa McKee, CISA, ISA, PCIP, MSSL
Lmmckee1979@yahoo.com
https://www.linkedin.com/in/lisammckee/

ANY PAYMENT,
EVERY POSSIBILITY.™

Agenda

- PCI Standards Updates from 2017-2018
- PCI Community Meeting Assessor Session
- Emerging US Data Privacy and Cybersecurity Landscape
- Exploding International Data Privacy Laws
- Periodic Table of Data Privacy
- Need for a holistic compliance program
- News from the Standards

PCI Standards Updates

Released 2017 - 2018

STANDARD	VERSION	RELEASE DATE	NOTES
PCI DSS	• v3.2.1	• May 2018	• Updated ROC Template • Updated SAQ templates
PTS PIN	• v3.0	• Aug 2018	• Merged with ANSI TR39 • Jan 1, 2023 TDES disallowed
PTS POI	• v5.1	• Mar 2018	
PCI 3DS CORE **PCI 3DS DATA MATRIX** **PCI 3DS SDK**	• v1.0 • v1.0 • v.1.0	• Oct 2017 • Oct 2017 • Nov 2017	• Core set of Standards for CDEs that process EMV transactions. NOTE: validation is determined by card brands • Set of standards for applications that process EMV payments (mobile); also requires EMV Co.
SPOC SECURITY REQUIREMENTS **SPOC TEST REQUIREMENTS**	• v1.0 • v1.0	• Jan 2018 • Feb 2018	• NEW Software-Based PIN Entry on Custom off the Shelf (COTS) • Currently no PCI approved solutions listed; per PCI SSC there are solutions in approval process • Will include contactless pyaments

PCI North American Community Meeting

Assessor Session

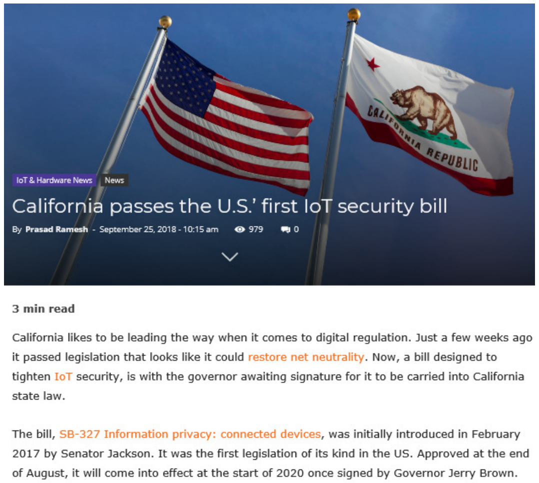
- PA-DSS
  - Validate applications until 2020; program retired around 2022
  - Framework & Standard
- P2PE
  - Major update to v3.0 coming in late 2020
  - Will have greater flexibility and simplicity
- ISO 11568 Standard for DUKPT
- ASV Program Guide Update v3.1 July 2018
  - Updated for SSL/TLS, includes FQDN this is not a false positive
- **Coming in 2019…**
  - PIN Assessor
  - Card Production Assessor
  - PCI DSS v4.0
  - Contactless
  - SPOC
  - P2PE

Emerging US Data Privacy and Cybersecurity Landscape

Fighting to have the Toughest Laws

- EU GDPR (May 2018)
  - Started motion for recent laws and regulations
- US California Data Privacy (Jan 2020)
- Colorado Data Privacy (Sept 2018)
- California IoT (Jan 2020)
- Illinois Biometric Privacy Act (2008)
- NY Cybersecurity Regulation (Aug 2017)

- As of May 18, 2018 at least 36 states, D.C and Puerto Rico introduced/considered more than 265 bills or resolutions related to cybersecurity.
- http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx



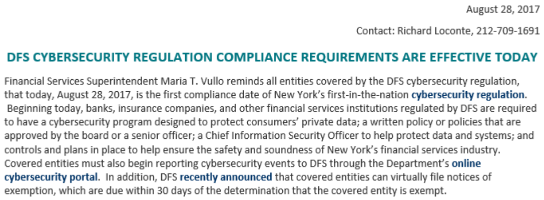
California passes the U.S.' first IoT security bill

By **Prasad Ramesh** - September 25, 2018 - 10:15 am 979 0

3 min read

California likes to be leading the way when it comes to digital regulation. Just a few weeks ago it passed legislation that looks like it could restore net neutrality. Now, a bill designed to tighten IoT security, is with the governor awaiting signature for it to be carried into California state law.

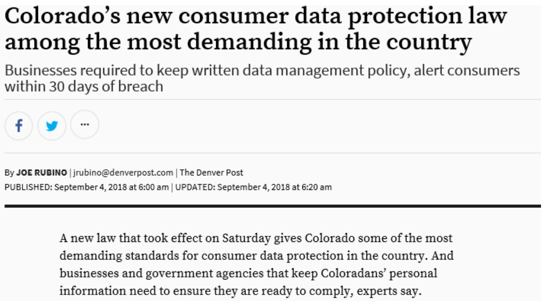
The bill, SB-327 Information privacy: connected devices, was initially introduced in February 2017 by Senator Jackson. It was the first legislation of its kind in the US. Approved at the end of August, it will come into effect at the start of 2020 once signed by Governor Jerry Brown.


August 28, 2017

Contact: Richard Loconte, 212-709-1691

DFS CYBERSECURITY REGULATION COMPLIANCE REQUIREMENTS ARE EFFECTIVE TODAY

Financial Services Superintendent Maria T. Vullo reminds all entities covered by the DFS cybersecurity regulation, that today, August 28, 2017, is the first compliance date of New York's first-in-the-nation **cybersecurity regulation**. Beginning today, banks, insurance companies, and other financial services institutions regulated by DFS are required to have a cybersecurity program designed to protect consumers' private data; a written policy or policies that are approved by the board or a senior officer; a Chief Information Security Officer to help protect data and systems; and controls and plans in place to help ensure the safety and soundness of New York's financial services industry. Covered entities must also begin reporting cybersecurity events to DFS through the Department's **online cybersecurity portal**. In addition, DFS **recently announced** that covered entities can virtually file notices of exemption, which are due within 30 days of the determination that the covered entity is exempt.


Colorado's new consumer data protection law among the most demanding in the country

Businesses required to keep written data management policy, alert consumers within 30 days of breach

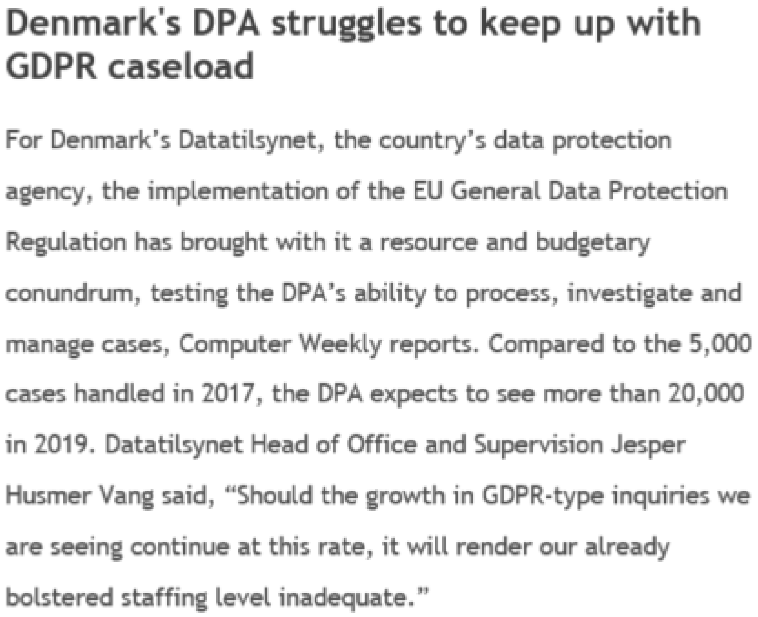
By **JOE RUBINO** | jrubino@denverpost.com | The Denver Post
PUBLISHED: September 4, 2018 at 6:00 am | UPDATED: September 4, 2018 at 6:20 am

A new law that took effect on Saturday gives Colorado some of the most demanding standards for consumer data protection in the country. And businesses and government agencies that keep Coloradans' personal information need to ensure they are ready to comply, experts say.

Exploding International Data Privacy Laws

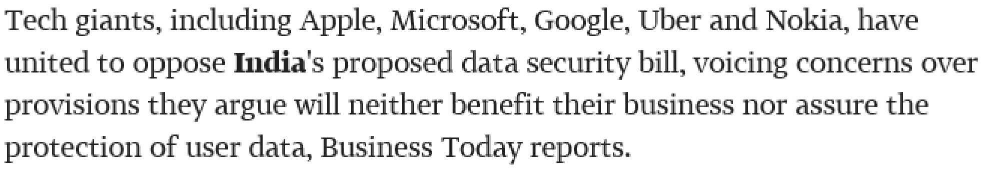
Where to Start…

- EU Data Protection Act 2018
- Vietnam Data Privacy (Jan 2019)
- China Cybersecurity Regulation (Nov 2018)
- New Zealand Customs and Excise Act (Oct 2018)
  - Imposes a NZ$5000 fine for travelers refusing to disclose their device passwords to customs official at the border
- Malaysia updating its data protections laws to prevent data breaches “on par” with GDPR



Denmark's DPA struggles to keep up with GDPR caseload

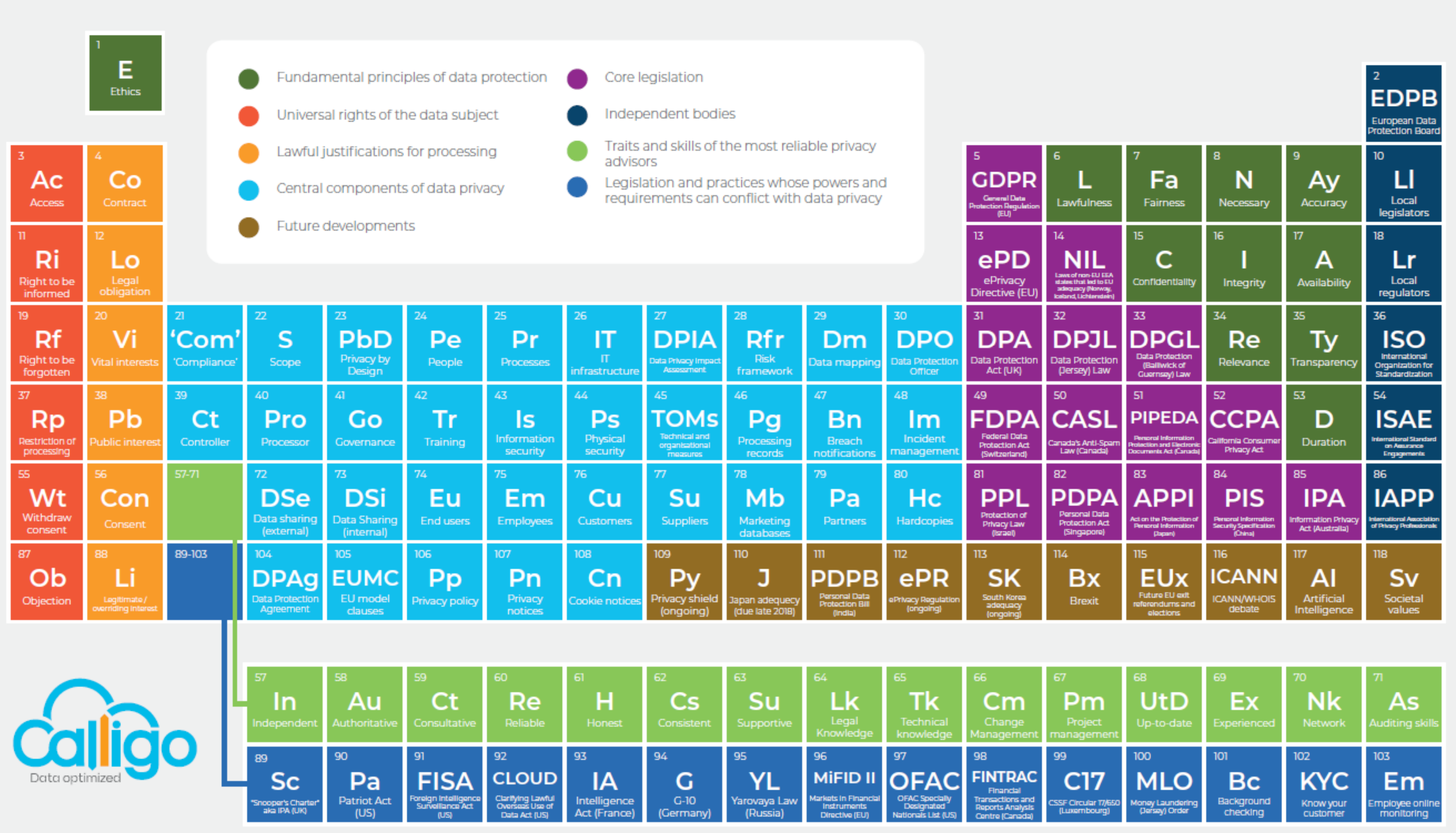
For Denmark’s Datatilsynet, the country’s data protection agency, the implementation of the EU General Data Protection Regulation has brought with it a resource and budgetary conundrum, testing the DPA’s ability to process, investigate and manage cases, Computer Weekly reports. Compared to the 5,000 cases handled in 2017, the DPA expects to see more than 20,000 in 2019. Datatilsynet Head of Office and Supervision Jesper Husmer Vang said, “Should the growth in GDPR-type inquiries we are seeing continue at this rate, it will render our already bolstered staffing level inadequate.”



Tech giants, including Apple, Microsoft, Google, Uber and Nokia, have united to oppose **India**'s proposed data security bill, voicing concerns over provisions they argue will neither benefit their business nor assure the protection of user data, Business Today reports.

The Periodic Table of Data Privacy

An overview of the key elements of data privacy



- ● Fundamental principles of data protection
- ● Universal rights of the data subject
- ● Lawful justifications for processing
- ● Central components of data privacy
- ● Future developments
- ● Core legislation
- ● Independent bodies
- ● Traits and skills of the most reliable privacy advisors
- ● Legislation and practices whose powers and requirements can conflict with data privacy

	1 E Ethics																2 EDPB European Data Protection Board
3 Ac Access	4 Co Contract											5 GDPR General Data Protection Regulation (EU)	6 L Lawfulness	7 Fa Fairness	8 N Necessary	9 Ay Accuracy	10 Ll Local legislators
11 Ri Right to be informed	12 Lo Legal obligation											13 ePD ePrivacy Directive (EU)	14 NIL Laws of non-EU EEA states that led to EU adequacy (Norway, Iceland, Lichtenstein)	15 C Confidentiality	16 I Integrity	17 A Availability	18 Lr Local regulators
19 Rf Right to be forgotten	20 Vi Vital interests	21 'Com' 'Compliance'	22 S Scope	23 PbD Privacy by Design	24 Pe People	25 Pr Processes	26 IT IT infrastructure	27 DPIA Data Privacy Impact Assessment	28 Rfr Risk framework	29 Dm Data mapping	30 DPO Data Protection Officer	31 DPA Data Protection Act (UK)	32 DPJL Data Protection (Jersey) Law	33 DPGL Data Protection (Bailiwick of Guernsey) Law	34 Re Relevance	35 Ty Transparency	36 ISO International Organization for Standardization
37 Rp Restriction of processing	38 Pb Public interest	39 Ct Controller	40 Pro Processor	41 Go Governance	42 Tr Training	43 Is Information security	44 Ps Physical security	45 TOMs Technical and organisational measures	46 Pg Processing records	47 Bn Breach notifications	48 Im Incident management	49 FDPA Federal Data Protection Act (Switzerland)	50 CASL Canada's Anti-Spam Law (Canada)	51 PIPEDA Personal Information Protection and Electronic Documents Act (Canada)	52 CCPA California Consumer Privacy Act	53 D Duration	54 ISAE International Standard on Assurance Engagements
55 Wt Withdraw consent	56 Con Consent	57-71	72 DSe Data sharing (external)	73 DSi Data Sharing (internal)	74 Eu End users	75 Em Employees	76 Cu Customers	77 Su Suppliers	78 Mb Marketing databases	79 Pa Partners	80 Hc Hardcopies	81 PPL Protection of Privacy Law (Israel)	82 PDPA Personal Data Protection Act (Singapore)	83 APPI Act on the Protection of Personal Information (Japan)	84 PIS Personal Information Security Specification (China)	85 IPA Information Privacy Act (Australia)	86 IAPP International Association of Privacy Professionals
87 Ob Objection	88 Li Legitimate / overriding interest	89-103	104 DPAg Data Protection Agreement	105 EUMC EU model clauses	106 Pp Privacy policy	107 Pn Privacy notices	108 Cn Cookie notices	109 Py Privacy shield (ongoing)	110 J Japan adequecy (due late 2018)	111 PDPB Personal Data Protection Bill (India)	112 ePR ePrivacy Regulation (ongoing)	113 SK South Korea adequacy (ongoing)	114 Bx Brexit	115 EUx Future EU exit referendums and elections	116 ICANN ICANN/WHOIS debate	117 AI Artificial Intelligence	118 Sv Societal values
			57 In Independent	58 Au Authoritative	59 Ct Consultative	60 Re Reliable	61 H Honest	62 Cs Consistent	63 Su Supportive	64 Lk Legal Knowledge	65 Tk Technical knowledge	66 Cm Change Management	67 Pm Project management	68 UtD Up-to-date	69 Ex Experienced	70 Nk Network	71 As Auditing skills
			89 Sc "Snooper's Charter" aka IPA (UK)	90 Pa Patriot Act (US)	91 FISA Foreign Intelligence Surveillance Act (US)	92 CLOUD Clarifying Lawful Overseas Use of Data Act (US)	93 IA Intelligence Act (France)	94 G G-10 (Germany)	95 YL Yarovaya Law (Russia)	96 MiFID II Markets in Financial Instruments Directive (EU)	97 OFAC OFAC Specially Designated Nationals List (US)	98 FINTRAC Financial Transactions and Reports Analysis Centre (Canada)	99 C17 CSSF Circular 17/650 (Luxembourg)	100 MLO Money Laundering (Jersey) Order	101 Bc Background checking	102 KYC Know your customer	103 Em Employee online monitoring

https://iapp.org/news/a/introducing-the-periodic-table-of-data-privacy/

Holistic Compliance Program

What is that?

- Inventory of Compliance Regulations, Laws and Standards
  - Keelan Stewart (Boystown) has a great one that I used as a starting point
- What areas does your company do business
  - Insurance
  - Finance
  - Healthcare
  - PCI/Payment Card Brands
  - State Statutes
  - Data Privacy Laws
  - Cybersecurity Regulations
- Include Corporate Compliance Responsibilities
  - HR Laws
  - OSHA
  - GLBA
  - OFAC
  - Treasury
- Define an Industry Standard
  - ASC X9
  - ANSI
  - ISO
  - NIST
- Signup for Memberships and RSS Feeds
  - IAPP

News from the Standards

ASC X9, NIST, ISO

- ASC X9 is the USA vote to ISO and the ANSI appointed US Technical Advisory Group
  - New Standard for Securing and Managing Mobile Commerce (Sept 2018)
  - First AES DUKPT Key Management Implementation (April 2018)
  - New Financial and Personal Data Protection and Brach Notification Standard
  - Study Groups (PKI, TLS, Quantum Computing)
    - https://x9.org/
    - https://x9.org/history-of-x9/
    - https://x9.org/committees/international-committees/
- NIST
  - 2nd draft of TLS Guidance Oct 15, 2018
  - Extends deadline for support TLS v1.3 to Jan 1, 2024
  - TLS v1.3 coexist with TLS v1.2 rather than replace it, YEAH! (Update from 1st draft)
  - Updated ciphers for RSA
  - Comment period open until Nov 16, 2018
    - https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/draft
- ISO
  - DUKPT Standard
    - https://www.iso.org/standard/34937.html

Questions