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*

<table>
<thead>
<tr>
<th>STANDARD</th>
<th>VERSION</th>
<th>RELEASE DATE</th>
<th>NOTES</th>
</tr>
</thead>
</table>
| 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              | v1.0    | Oct 2017     | • Core set of Standards for CDEs that process EMV transactions. NOTE: validation is determined by card brands |
| PCI 3DS DATA MATRIX       | v1.0    | Oct 2017     | • Set of standards for applications that process EMV payments (mobile); also requires EMV Co. |
| PCI 3DS SDK               | v.1.0   | Nov 2017     |                                                                       |
| SPOC SECURITY REQUIREMENTS| v1.0    | Jan 2018     | • NEW Software-Based PIN Entry on Custom off the Shelf (COTS)       |
| SPOC TEST REQUIREMENTS    | v1.0    | Feb 2018     | • Currently no PCI approved solutions listed; per PCI SSC there are solutions in approval process  
|                           |         |              | • Will include contactless payments                                   |

**Note:** Updated ROC Template

**Note:** Updated SAQ templates

**Note:** Merged with ANSI TR39

**Note:** Jan 1, 2023 TDES disallowed

**Note:** Core set of Standards for CDEs that process EMV transactions. NOTE: validation is determined by card brands

**Note:** Set of standards for applications that process EMV payments (mobile); also requires EMV Co.

**Note:** NEW Software-Based PIN Entry on Custom off the Shelf (COTS)

**Note:** Currently no PCI approved solutions listed; per PCI SSC there are solutions in approval process

**Note:** Will include contactless payments
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.
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

<table>
<thead>
<tr>
<th>Category</th>
<th>Ac</th>
<th>Co</th>
<th>L</th>
<th>Ri</th>
<th>Vi</th>
<th>‘Com’</th>
<th>S</th>
<th>PbD</th>
<th>Pe</th>
<th>Pr</th>
<th>IT</th>
<th>DPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consent</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Right to be forgotten</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purpose</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lawfulness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fairness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Necessary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accuracy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local regulators</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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
  – 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/)
    ▪ [https://x9.org/history-of-x9/](https://x9.org/history-of-x9/)
    ▪ [https://x9.org/committees/international-committees/](https://x9.org/committees/international-committees/)

• NIST
  – 2<sup>nd</sup> 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 1<sup>st</sup> draft)
  – Updated ciphers for RSA
  – Comment period open until Nov 16, 2018

• ISO
  – DUKPT Standard
    ▪ [https://www.iso.org/standard/34937.html](https://www.iso.org/standard/34937.html)
Questions