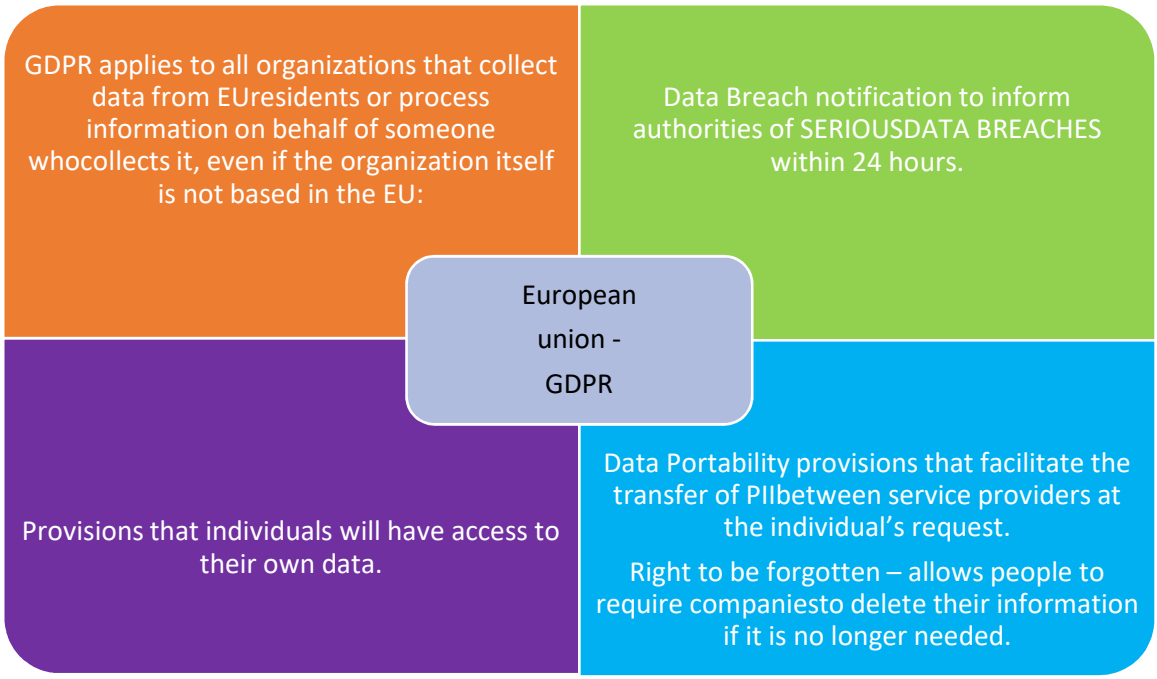
Unit 8: How to Evaluate and Apply Applicable Security Standards

We studied and covered regulations and standards during this unit with a greater focus on General Data Protection Regulation, PCI-DSS, and HIPPA.



PCI-DSS

- Payment Card Industry regulation – the Payment Card industry Self-regulates. Is not a Law, but a Data Security standard.
- All companies that accept, process, store or transmit credit-card information are subject to PCI-DSS Compliance.
- Requires disclosure by Merchants in case of Credit card data breach.

HIPAA-HITECH

- Applies to any organization that processes or stores private medical information of individuals such as Health-care providers, health insurance providers etc.
- HITECH 2013, also modifies this act to cover Business Associates of healthcare industry who work on PHI data to also be covered under HIPAA via Business Associate Agreement.
- HITECH also enforces Data Breach Notifications, requiring HIPAA covered entities notify affected individuals in theevent of a breach. Also notify Secretary of Health, and the media in case breach is higher than 500 individuals.