GDPR Impact on Incident Response

WISE@STFC - 2018-02-26

Urpo Kaila <urpo.kaila@csc.fi>
Data Protection Officer,
Security Officer

EUDAT receives funding from the European Union's Horizon 2020 programme - DG CONNECT e-Infrastructures. Contract No. 654065

Agenda

- Information Security vs Data Protection
- The EU General Data Protection Regulation GDPR
- GDPR on Incident Response
- Incident Response and Security
- Typical Data Protection Incidents vs Security Incidents
- Issues and Possibilities on Incident Response
- WISE and Data Protection Incidents
- Suggestions for discussion on next steps

Information Security vs Data Protection

Information Security means protecting assets (systems, data, services, and reputation) against risks with security controls to prevail their

- Confidentiality: To prevent intentional or unintentional disclosure
- Integrity: To prevent unauthorized modification and protect consistency
- Availability: To protect reliable and timely access

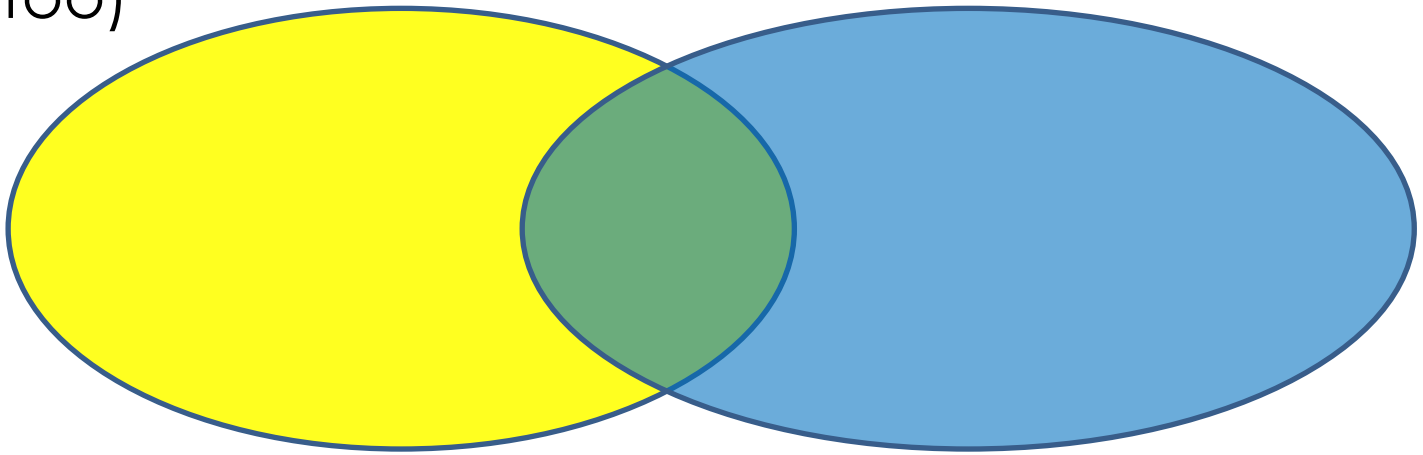
- Information security protects primarily the organisation or the community

Data Protection means protecting information relating to an identified or identifiable natural person

- Organisations are obliged to notify and ask for consent when personal data is collected or stored
- The scope of personal data must be restricted, some sensitive personal data must not be collected or stored
- Collected personal data must be protected against data leaks
- Data Protection is the legal right of the individual

Information Security vs Data Protection

- Information security is required for adequate data protection
- Information security doesn't cover all aspects of data protection
- There are many legal aspects in data protection (too)



The EU General Data Protection Regulation GDPR

- EU Regulation 2016/679 will strengthen data protection for individuals within EU
  - Obligations for Data Controllers and Data Processors
  - Enter directly into application 25 May 2018
- The Individual has the right to
  - Be informed – informed consent
  - Erasure of personal data
  - Restrict processing
  - Data portability
- Control of subcontractors
- Obligation to inform about security incidents and data breaches (72 h)
- Huge fines for misconducts
- Addresses export of personal data outside the EU
- Data protection to be embedded in services – privacy by design and by default

GDPR on Incident Response (Art, 33/34)

- In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority
- The processor shall notify the controller without undue delay after becoming aware of a personal data breach
- When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay

Incident Response and Security

- An proactive ability for incident response is basic requirement for governance on information security
- WISE-SCI*:
  - [IR1] A process to maintain security contact information for all service providers and communities
  - [IR2] A documented Incident Response procedure. This must address: roles and responsibilities of individuals and teams, identification and assessment of incidents, minimisation of damage to the infrastructure, response and recovery strategies to restore services, communication and tracking tools and procedures, and a post mortem review to capture lessons learned.
  - [IR3] The capability to collaborate in the handling of security incidents with affected service providers, communities, and infrastructures, together with processes to ensure the regular testing of this capability.
  - [IR4] Policies and procedures to ensure compliance with information sharing restrictions on incident data exchanged during collaborative investigations….

https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

Typical Data Protection Incidents vs Security Incidents

- Data Protection Incidents
  - Sensitive data
  - Access to information restricted on a need-to-know basis
  - Legal risks
- Security incidents
  - Availability issues/downtime
  - 'A scramble'
  - Information shared widely between CSIRT Teams
  - Vendors, media and other players trying to exploit the incident

Issues and Possibilities on Incident Response

- Huge risks on failing to comply on requirements to inform parties on data breaches
- A process to be created to cope with the requirements
- No reliable non-disclosure agreement between CSIRT teams
- CSIRT teams partly a professional network between individuals, unclear legal relations to constituents
- A tradition to exploit incidents is negative for trust
- The DLP protocol does not count as a NDA-agreement
- But,,, CSIRT should be obliged to inform DPO's for relevant risks,,,
- Better cooperation, trust and alignment can produce remarkable benefits for all interested parties

WISE and Data Protection Incidents

- WISE could now take a role to create a mature and secure operational procedures to exchange information between CSIRTs and DPO's
- Attempts to exploit GDPR for resourcing in a non-sustainable way must be avoided
- Planning could start with use cases and WP29 CoC's

Suggestions for discussion on next steps

- Should WISE form a WG covering Data Leak Protection and Handling affecting Personal Data?