Information Sharing & Draft NIS2 Directive

Andrew Cormack, Chief Regulatory Adviser, Jisc @Janet_LegReg

Contains law…

But…

- Looking for law-maker thinking/motivation (Recitals)
  - Not actual law (Articles)
- Think of it like analysing artifacts
  - What has stayed the same?
  - What has changed?

Jisc

Incident Response in laws

GDPR Recital 49 (2016)

- "processing … for the **purposes of ensuring network and information security** … constitutes a legitimate interest [i.e. Art.6(1)(f)] of the data controller concerned"
- "This could for example, include, **preventing unauthorised access … and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems**"

- Covers public authorities, CERTs, CSIRTs, providers of electronic communications networks and services, providers of security technologies and services
  - Plus, by Regulator guidance, all data controllers

Draft NIS2D Recital 69 (2021)

- "processing … for the **purposes of ensuring network and information security** … constitutes a legitimate interest of the data controller concerned"

- "This should include measures related to the **prevention, detection, analysis and response to incidents** …

- "… to **raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated disclosure … voluntary exchange of information on those incidents, cyber threats and vulnerabilities, IoCs, tactics, techniques and procedures, cybersecurity alerts and configuration tools**"

- Covers GDPR list plus NIS-relevant entities
  - Plus, by Art.27, "entities falling outside the scope"

Jisc

Information sharing strongly linked to incident response

Whose legal framework (Legitimate Interest) is well known ☺

Why do legislators want this?

GDPR (2016) interested in IR because…

- "Unauthorised access, malware, DoS, damage to computer and electronic communication systems" (Rec.49)
- i.e. harms to **individual** or **service**
- **Legitimate interest** in preventing such harm [GDPR Art.6(1)(f)]

NIS2D (2021) interested in IR because…

- "network and information systems have developed into a central feature of everyday life … including cross-border exchanges" (Rec.3)
- "cyber incidents can impede the pursuit of economic activities …, generate financial losses, undermine user confidence and cause major damage to … economy and society" (Rec.3)

and

- "Given the importance of international cooperation … should be able to participate in international cooperation networks" (Rec.26)

Sounds a lot like…

- [International] "transfer is necessary for **important reasons of public interest**" [GDPR Art.49(1)(d)]

Possible framework for (international) sharing (1)?

When to share

- GDPR Art 49(1)(d)
- Necessary for “important public interest”…

…defined in

- NIS2D Rec.3
- Financial losses
- User confidence
- Damage to economy
- Damage to society
- …

What to share

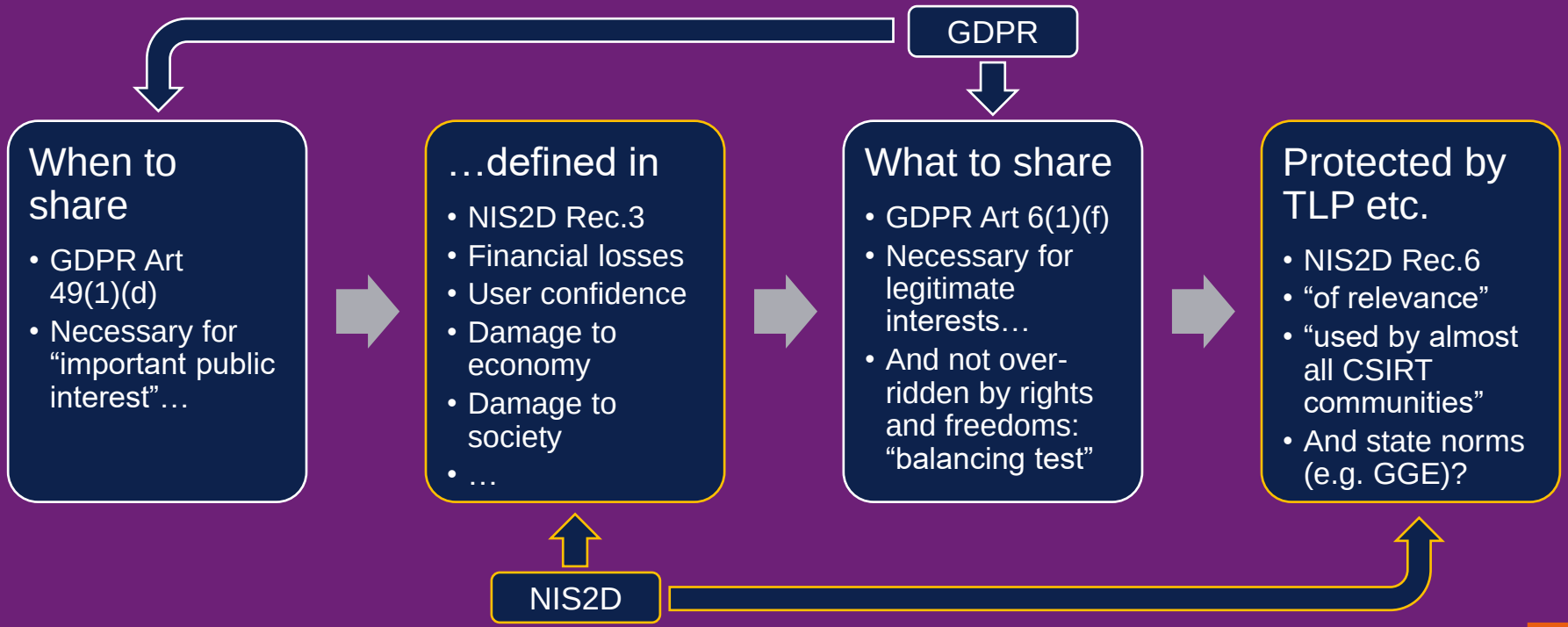
- GDPR Art 6(1)(f)
- Necessary for legitimate interests…
- And not over-ridden by rights and freedoms: “balancing test”

Protected by TLP etc.

- NIS2D Rec.6
- “of relevance”
- “used by almost all CSIRT communities”
- And state norms (e.g. GGE)?

Possible framework for (international) sharing (2)?

NIS2D glue adds safeguards/consistency to existing GDPR ☺



References

- Incident response and GDPR
  - https://regulatorydevelopments.jiscinvolve.org/wp/2012/06/06/privacy-and-incident-response/
  - https://regulatorydevelopments.jiscinvolve.org/wp/2018/11/19/information-sharing-and-gdpr/
  - https://script-ed.org/article/incident-response-protecting-individual-rights-under-the-general-data-protection-regulation/
- Information sharing and Draft NIS2D
  - https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union
  - https://regulatorydevelopments.jiscinvolve.org/wp/2021/02/23/nis2-directive-security-teams-should-be-collaborating/
  - **Paper** https://script-ed.org/article/nisd2-a-common-framework-for-information-sharing-among-network-defenders/
- My blog
  - https://regulatorydevelopments.jiscinvolve.org/wp/tag/incident-response/

Contact

Andrew Cormack

Chief Regulatory Adviser

@Janet_LegReg

Lumen House, Library Avenue, Didcot

OX11 0SG UK

Andrew.Cormack@jisc.ac.uk

jisc.ac.uk