Information Sharing and GDPR
Andrew Cormack, Chief Regulatory Adviser (@Janet_LegReg)
GDPR: NIS is a Legitimate Interest

For processing personal data (including IP addresses, etc.):

“The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.” (GDPR, Rec.49)

For exporting personal data to “unsafe” countries (new under GDPR):

“For example, this might be the case if a data controller is compelled to transfer the personal data in order to protect its organization or systems from serious immediate harm or from a severe penalty which would seriously affect its business.” (EDPB, p.15)
So must ensure
See GDPR Art.6(1)(f)

Interest is legitimate (done, thanks to Recital 49)
Processing is necessary for that interest
  » i.e. no less intrusive way to achieve it
  » So only share what the recipient needs to fix their problem
Benefits of processing not overridden by risk to data subject (“balancing test”)
  » Noting that security done right should benefit system users, etc.
Factors in deciding to share information

Benefit factors
» Potential impact of the issue
  › Global compromise (vuln) > Local compromise (pwd)/DoS > Personal loss
» Who benefits
  › Self > Constituency > Recipient > Internet

Harm factors
» Type of Identifier being shared
  › Constituency > External > Aggregated > None
» How was information obtained?
  › Unplanned process > Planned process
» Extent of disclosure
  › World > Trusted Community > Affected Service (eg bank) > Responsible Org. (eg ISP) > User
Or in Pictures...

- **Potential Impact**
  - Global Compromise
  - Local Comp./DoS
  - Personal Loss

- **Whose Interest**
  - Constituency
  - Recipient
  - Internet

- **Type of Identifier**
  - Constituency
  - External
  - Aggregated
  - None

- **Data Collection**
  - Unplanned
  - Planned
  - None

- **Extent of Disclosure**
  - World
  - Trusted Community
  - Affected Service
  - Responsible Organisation
  - User
  - None

- **Increased benefit**

- **Increased individual risk**
e.g. your host is scanning me...

Increased benefit

- Global Compromise
- Local Comp./DoS
- Personal Loss

Increased individual risk

- World
- Trusted Community
- Affected Service
- Responsible Organisation
- User

Potential Impact

- Constituency
- Constituency
- Recipient

Whose Interest

- Constituency
- Internet
- Self

Type of Identifier

- Constituency
- External
- Aggregated
- None

Data Collection

- Unplanned
- Planned
- None

Extent of Disclosure

- None
e.g. published list of SSH brute-forcers

- Potential Impact
  - Global Compromise
  - Local Comp./DoS
  - Personal Loss

- Whose Interest
  - Constituency
  - Self
  - Recipient

- Type of Identifier
  - Constituency
  - External
  - Aggregated

- Data Collection
  - Unplanned
  - Planned

- Extent of Disclosure
  - World
  - Trusted Community
  - Affected Service
  - Responsible Organisation
  - User
  - None

Increased individual risk
Increased benefit
Extent of Disclosure
Data Collection
Type of Identifier
Whose Interest
Potential Impact
e.g. new IoC for malware email...

- **Potential Impact**: Global Compromise, Local Comp./DoS, Personal Loss
- **Whose Interest**: Constituency, Self, Recipient, Internet
- **Type of Identifier**: Constituency, External, Aggregated, None
- **Data Collection**: Unplanned, Planned
- **Extent of Disclosure**: World, Trusted Community, Affected Service, Responsible Organisation, User, None

Increased benefit

Increased individual risk
e.g. contributing to a pDNS archive
e.g. you tell me...
References


Thanks

Andrew Cormack
Chief Regulatory Adviser, Jisc Technologies

Andrew.Cormack@jisc.ac.uk

https://community.jisc.ac.uk/blogs/regulatory-developments/tags/Data-Protection-Regulation