19/11/2018

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

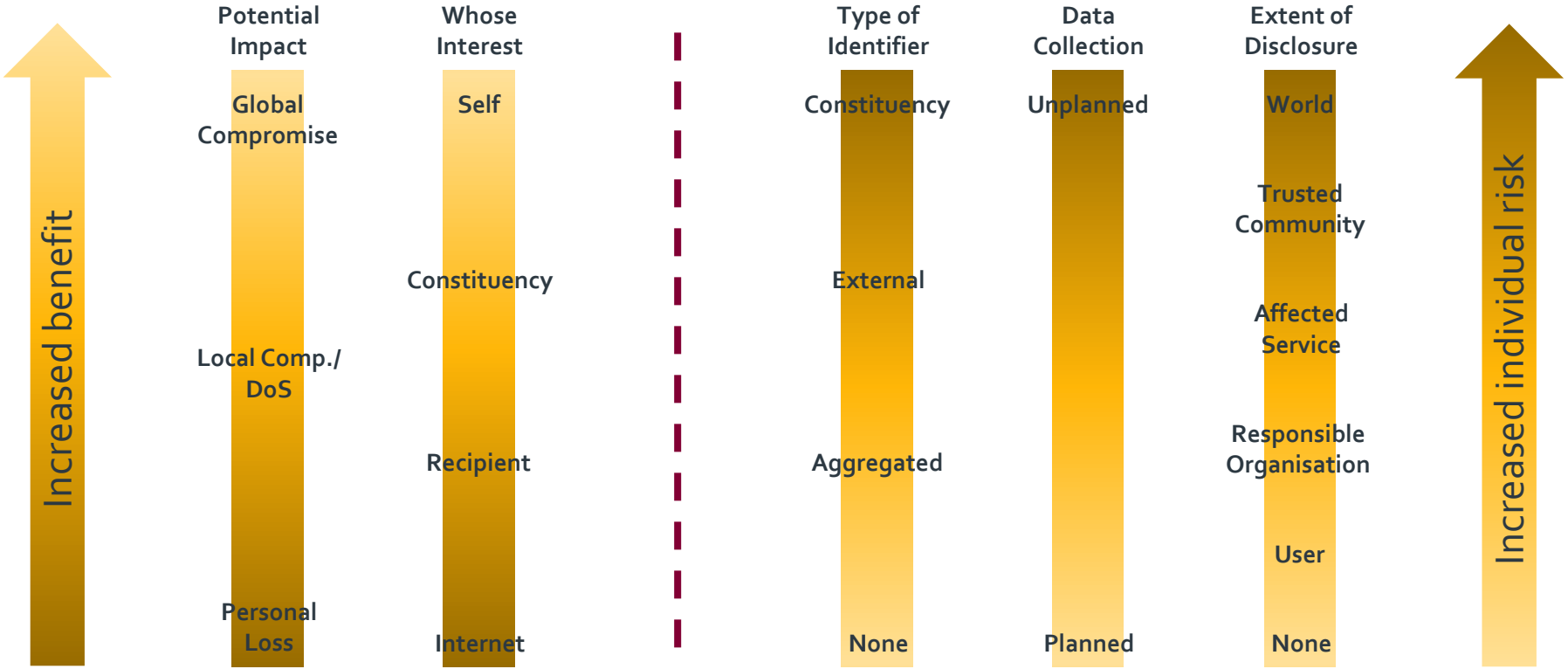
Benefit factors

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

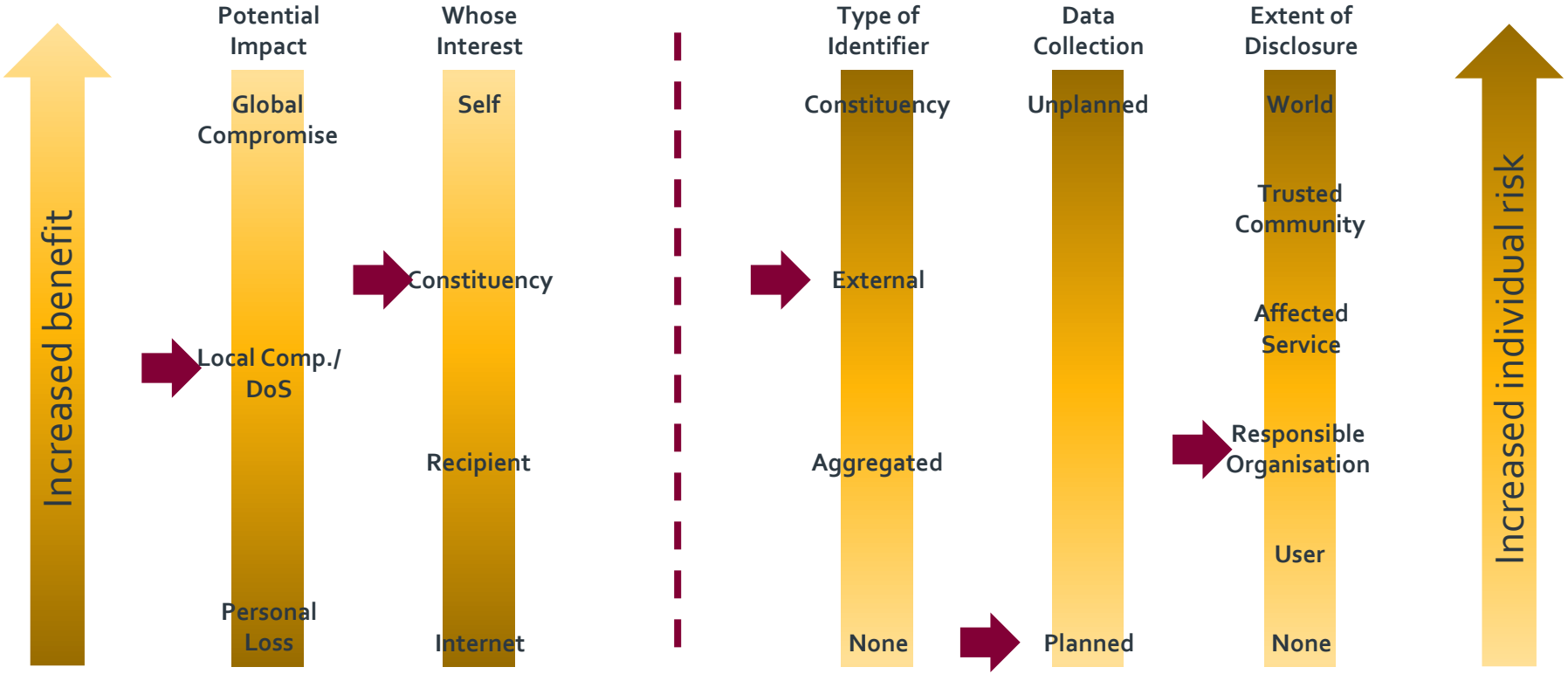
Harm factors

- 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

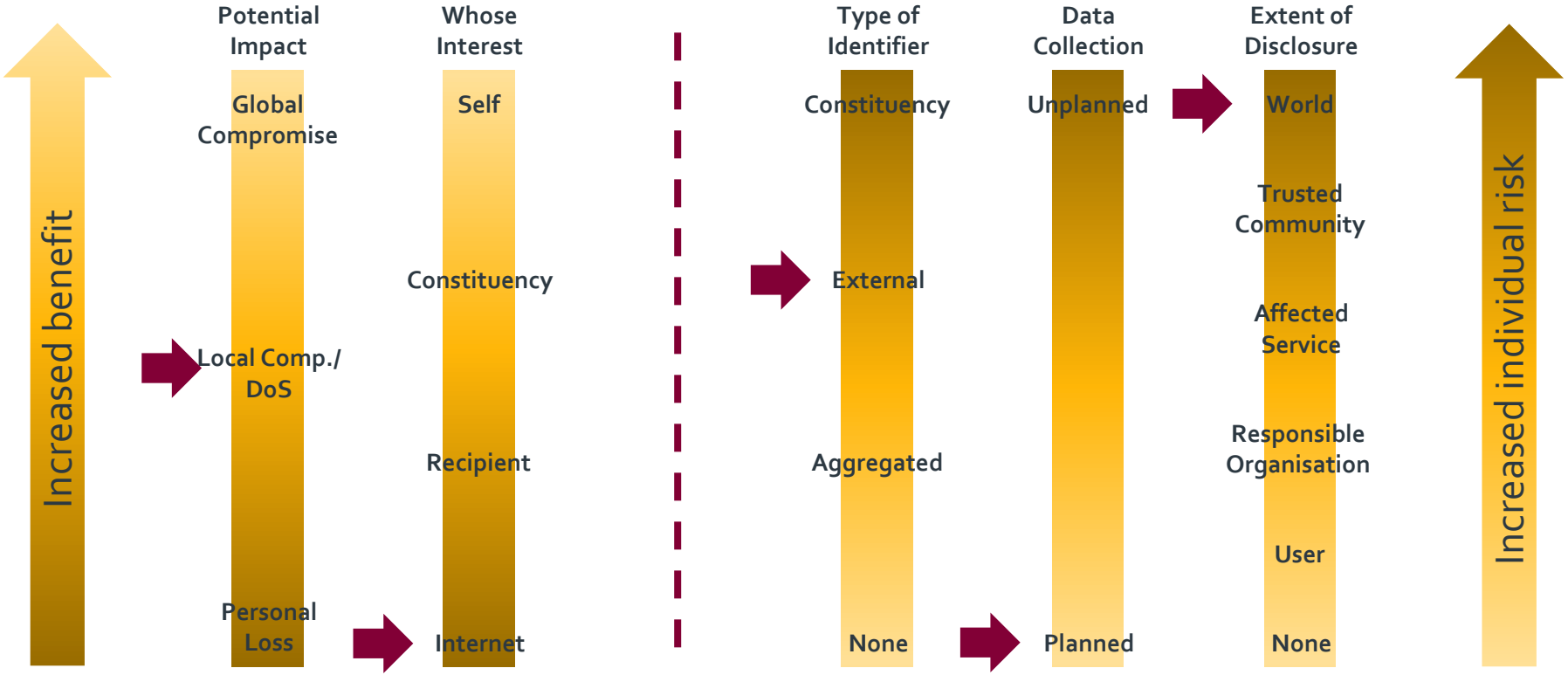
Or in Pictures…



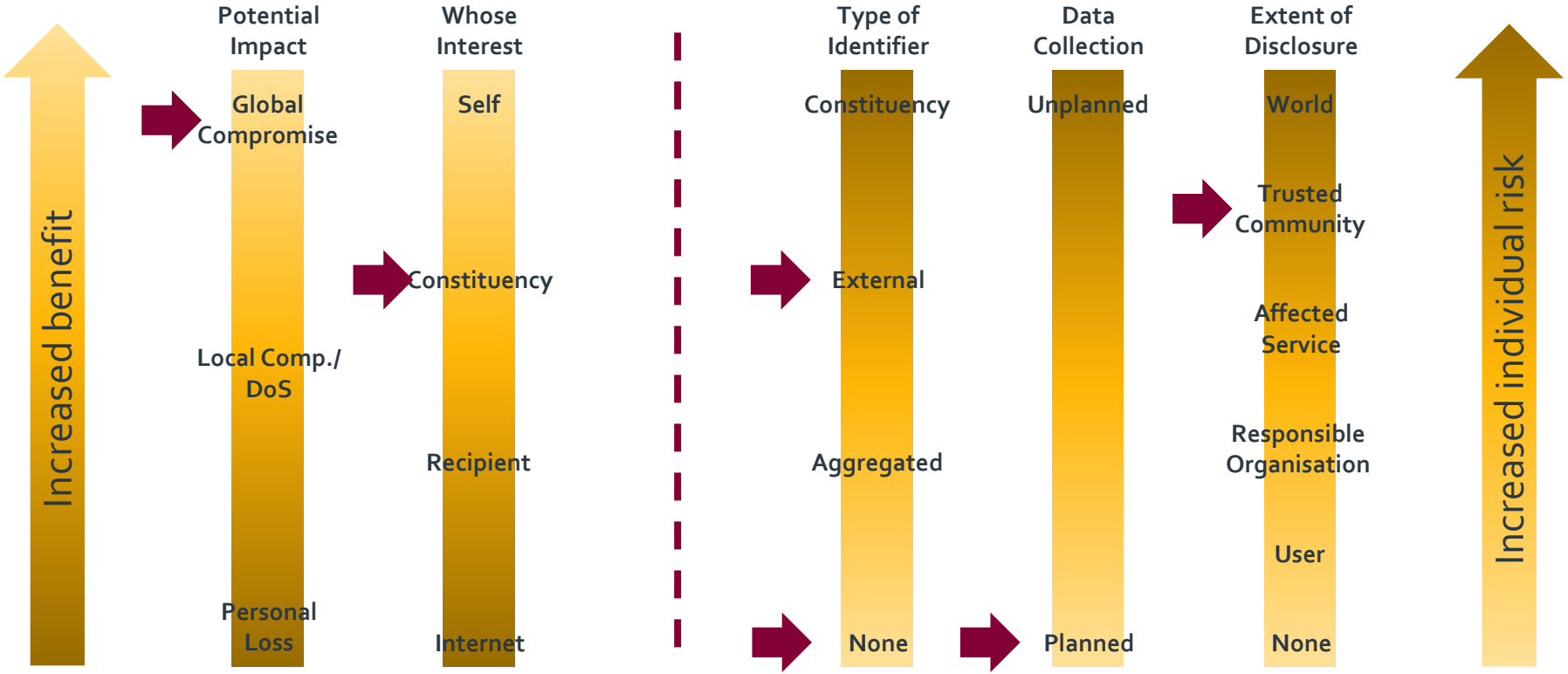
e.g. your host is scanning me…



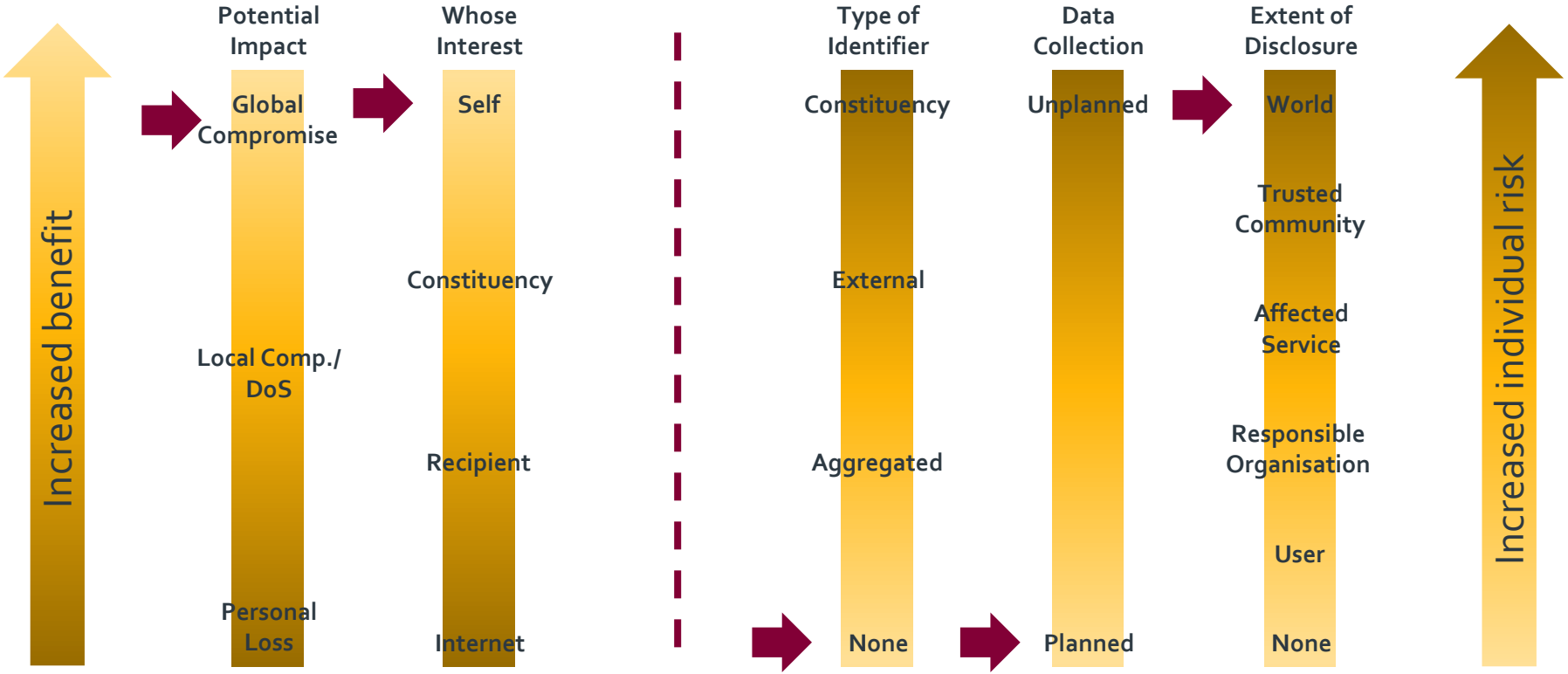
e.g. published list of SSH brute-forcers



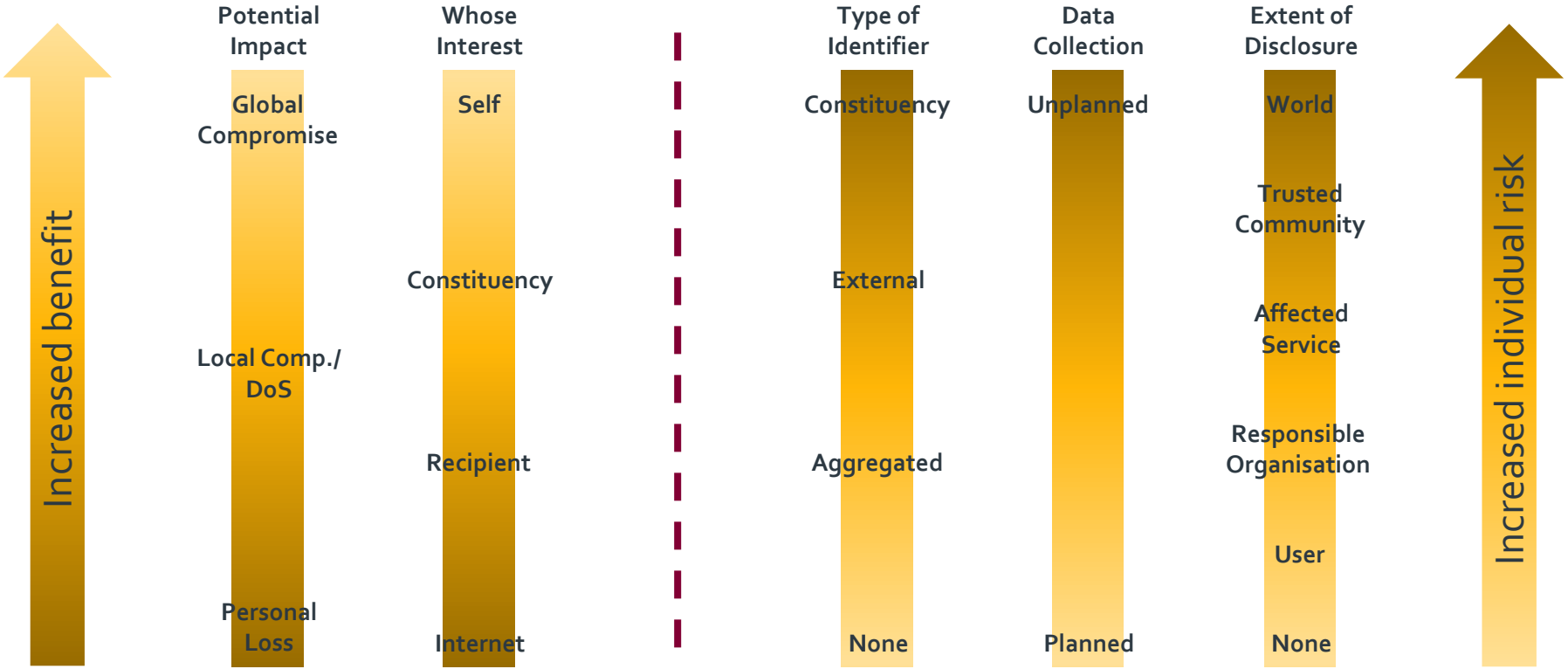
e.g. new IoC for malware email…



e.g. contributing to a pDNS archive



e.g. you tell me…



References

Original paper (with pictures): https://www.terena.org/activities/tf-csirt/publications/data-protection-v2.pdf

Peer-reviewed law journal paper: https://script-ed.org/article/incident-response-protecting-individual-rights-under-the-general-data-protection-regulation/

GDPR processing: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

EDPB exports: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

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