EU cybersecurity regulation and the EU privacy, data protection and emerging digital legislation: considerations for the close future

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Massimo Attoresi
Technology and Privacy Unit (EDPS)

"Cybersecurity Collective Resilience through Regulation" conference

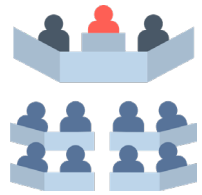
22 June 2023 - Maastricht University Campus Brussels

EDPS and Cybersecurity

- ✓ EDPS is **not directly** competent in Cybersecurity
  - ❖ cooperation with MSs & EUIs: ENISA
  - ❖ operational cybersec for EUIs : CERT-EU
- ✓ BUT: **Important interplay** Cybersecurity and DP/Privacy;
- ✓ **Article 42** of the EUDPR: we provide our formal comments/opinions on policy/legislative proposals (including on Cybersecurity)

- ❑ We focus on the **intersection/interplay** between DP/Privacy and Cybersecurity

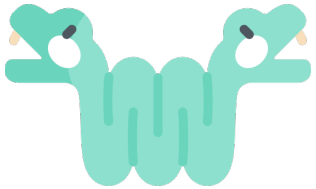
Just two recent news last week …



- ✓ Artificial Intelligence Act – EP position
  - ❖ Bans and stringent rules for High Risk systems
  - ❖ Growing role of AI in cybersecurity

- ✓ Pegasus file – EP resolution adopted
  - ❖ Illicit use of spyware puts democracy at stake
  - ❖ Authorised in exceptional cases for a pre-defined purpose and a limited time, within well-defined legal boundaries.

Cybersecurity and data protection (fundamental rights): a twofold relationship



- ✓ Cybersecurity protects communications and data, an **essential companion for the protection of fundamental rights**, including privacy and the protection of personal data.
- ✓ Operating **cybersecurity** implies more and more processing a trove of (personal) data and **might interfere with fundamental rights**, by building profiles of users and organisations as well as taking decisions on their communications and data

Some general elements for the close future

- ✓ Key to devote resources for a professional approach to foresight applied to cybersecurity
- ✓ Undoubtedly AI and quantum as main techno drivers, in a cat and mouse race. Cyberwarfare inevitably (and unfortunately) growing.

  So, innovation but with clear limits and purposes explicitly set by the legislation and hopefully supported by co- and self-regulation instruments (standards, codes of conducts, etc.) at global level

- ✓ Cybersecurity governance and structured interaction with regulators competent for digital/fundamental rights is essential

… more on governance for effective integration of fund. rights with cybersecurity

- ✓ Complexity in EU cybersecurity governance while…
- ✓ Even more complex pattern being designed in EU digital/fundamental rights regulation (e.g. DSA and AI Act, vs pre-existing privacy and data protection law)
- ✓ Current NIS provides for mandatory collaboration « to the extent possible » between competent authorities in NIS and GDPR/ePrivacy + comm. obligations if NIS infringements have DP effects
- ✓ Recital 66: NIS2 Cooperation Group « should consider » inviting … EDPB (and maybe the EDPS?)
- ✓ Presence of a strong DP and fundamental rights office in competente cybersec organisations is key

When cybersecurity and fundamental rights go hand in hand...

- ✓ NIS2 cybersecurity management obligations
  - ❖ A primer as horizontal obligations for organisations in scope
  - ❖ GDPR provides for a risk-based approach erga omnes if personal data are processed
- ✓ Integrated approach for data breach notifications, challenges but more advantages
- ✓ New EU Cybersecurity certification framework and the GDPR
- ✓ Protecting data spaces and AI systems, providing PETs

When cybersec operations challenge fundamental rights …

- ✓ The debate on the legal basis for cybersecurity operations in the GDPR
- ✓ Pegasus and spyware friends
  - ❖ Again, politicians and investigative journalists targeted
  - ❖ EDPS : ban or moratorium on spyware development and deployment
  - ❖ EDPS: in any case, stronger democratic oversight and real judicial review; strict implementation of CJEU judgements; stop to abuse of national security purpose; rule of law issues as fertile ground for abuse
- ✓ Same in the European Media Freedom Act proposal
- ✓ The AI Act, what about AI in cybersecurity
- ✓ Sandboxes and cybersecurity

A couple of key messages…

1. A legal, strategic and operational approach to cybersecurity that **integrates by design fundamental rights**, including privacy and personal data protection, is key to protect EU people, values and data from attacks and at the same time uphold our freedoms, rule of law and democracy when doing it. Differently, it will NOT work and can de facto impose a different value model.
2. In our digital and cyber context more intrusiveness in people's life is a reality. **Red lines should be clearly drawn**. Whenever necessary and proportionate in a democratic society, this processing needs always to be **counter-balanced by adequate safeguards and sufficient independent, democratically based oversight**. Authorities or offices dealing with fundamental rights within competent organisations to be granted the necessary resources. And this everywhere, in civil, law enforcement and military contexts

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

Image credits to free icons in www.flaticon.com

@EU_EDPS

European Data Protection Supervison

EDPS