Privacy in practice
EU legal framework for Privacy

- **General Data Protection Regulation** (GDPR) (EU) 2016/679
  - To replace Data Protection Directive 95/46/EC on 25 May 2018
  - Horizontal application

- **ePrivacy Directive** 2002/58/EC/
ePrivacy Regulation (ePD) (proposal)
  - Sector specific application (telecom): complements and particularises
ePD versus GDPR

- ePD particularises & complements Directive 95/46/EC regarding the protection of personal data for the electronic communications sector
- It relies on definitions GDPR (personal data, consent, processing of personal data)
- Relationship ePD vis-à-vis DPD and proposal vis-à-vis GDPR remains the same
Privacy H2020 Projects
privacy as a service: stores the users’ personal data securely to authorized Online Service Providers (OSPs), based on the individual User’s Privacy Policies (UPP);

effects management: module that ensures that OSPs have the required privileges to access the requested user data;

UPP: where all the user privacy data is stored; captures the access preferences (‘consent’) of the data subject.

demo: https://occowncloud.oxfordcc.co.uk/index.php/s/sKfEBSyMuB69uU5
consent management

Synchronous

Asynchronous

www.bpr4gdpr.eu
Data Access Rights Analysis module: support elicitation, modelling and analysis of data access rights scenarios by analysing potential access requests.

Consent Analyser: allows data subjects to define consent preferences and create Data Privacy Consent model, to manage, monitor and enforce data subject consent.

Graphical visualization gain in transparency and usability.
H2020 project POSEID-ON

https://www.poseidon-h2020.eu/

- implementation of dashboard by data controllers or processors enabling data subjects to safeguard/monitor/control (allow/revoke consent) the exposure of their private data;
- exploits the cutting-edge technologies of Smart Contracts and Blockchain, data management and processing while ensuring GDPR compliance.
More H2020 privacy projects on:
consent management, qualified anonymity, GDPR compliance in practice

<table>
<thead>
<tr>
<th>SMOOTH GDPR</th>
<th>PAPAYA</th>
<th>Future Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUNFISH</td>
<td>RECREO/INCOGNITO</td>
<td></td>
</tr>
<tr>
<td>PDP4E</td>
<td>CUREX</td>
<td>.............</td>
</tr>
</tbody>
</table>
Upcoming H2020 privacy topics
Open Calls in SC7 – Digital Security


- **SU-DS05-2018-2019**: Digital security, privacy, data protection and accountability in critical sectors (subtopic a) Transport, IA, budget: 10 MEUR; subtopic b) Healthcare, RIA, budget: 10 MEUR)

  - **Opening**: 14 Mar 2019
  - **Call deadline**: 22 Aug 2019
Cybersecurity Call in LEIT-ICT - SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems

Subtopics:
(a) Cybersecurity/privacy audit, certification and standardization;
(b) Trusted supply chains of ICT systems;
(c) Designing and developing privacy-friendly and secure software and hardware.

Type of Action: RIA, Budget: 47.00 MEUR
Opening: 25/07/2019; Deadline: 19/11/2019
LEIT-ICT - Other topics relevant for Cybersecurity & Digital Privacy

- **ICT-08-2019**: Security and resilience for collaborative manufacturing environments

- **ICT-13-2018-2019**: Supporting the emergence of data markets and the data economy

- **ICT-20-2019-2020**: 5G Long Term Evolution

...and more, as this is a cross-cutting issue
The future
Better and more EU cyber secure & privacy aware technologies

- **Privacy**
- **Security**
- **Accountability**

by design

- Robust
- Dynamic
- Resilient
- Autonomous

(independent of non EU components)

- Ethical,
- non bias
- human centric
- democratic

- Self-
- healing
- management
- recovery
Short term privacy research challenges

- Interoperable, dynamic, standardized privacy and security assessment methodologies and tools;
- GDPR and NIS impose strict obligations (e.g. data minimisation, accountability, transparency, security & privacy risk assessment); complementary, methodological approaches, check lists and self-assessment tools (especially for SMEs & MEs) need to be developed, which organisations can use to deal with these obligations;
- privacy-by-design in practice requires:
  Step-by-step system and software engineering methods that apply privacy principles to engineering designs
Privacy mid/long-term research challenges

- Assess and modify eIDAS’ current specifications and GDPR Art. 25 so the use of national eID schemes operating under eIDAS will extend to the private sector;
- Identification of privacy threats/requirements for the emerging technologies (e.g. AI, Big Data, HPC, Blockchain, 5G);
- Assess GDPR and eDP against the privacy challenges of the emerging technologies;
- Advance software engineering methods that apply privacy principles to engineering designs appropriate for AI/5G systems and applications.
Next MFF (2021-2027)

- **Horizon Europe** *(research programme)*

- **Digital Europe Programme** *(apply digital capabilities)*
Follow us on get involved:

On : https://twitter.com/Cybersec_EU

Subscribe to our newsletter: http://europa.eu/!yT68Jg
Thank you for your attention!

Nineta.POLEM1@ec.europa.eu