

Quality & Security

Standard Developing Organisations

World Wide Web Consortium
OpenID Foundation

Security Organisations (operational)

National Cyber Security Centre

- Threat mitigation
- Incident handling

Privacy Authority

- Monitor **proactively**
 - criminal investigation processes
 - exceptional data collection processes in case of emergency
- Transparent debriefing
- Ensure data deletion after
 - closure of criminal investigation
 - cancelling of state of emergency

Report proven GDPR violations

Certification Organisations
Certify

Authorizes

Certify

Ethical Hacking

Certified Ethical Hacking Services
 Determine vulnerabilities
 Get rewarded

[View this example](#)

Service Providers:

Governmental Organisations

Enterprises SME's

Non Governmental Organisations

- should comply to Privacy and Security by Design (GDPR)
 - Proactive not reactive; preventive not remedial
 - Privacy embedded into design
 - Positive sum of privacy & functionality
 - Full lifecycle protection e.g secure erasure
 - Visibility and transparency
 - User-centric
- provide a machine readable standard privacy policy p3p
- OpenID Authentication protocol (standard way to provide personal data to SP's)
- All entrusted data is stored under privacy-contract-number makes e.g. efficient erasure possible

Privacy Protectors (PP's):

Authenticate on behalf of individual and execute processes on request or unsolicited to **enforce GDPR rights:**
 to be informed | of access | of rectification | to erasure
 to restrict processing | to data portability
 to object processing personal information
 in the context of profiling and automatic decision making
Privacy Protectors have no other business model than giving of individuals control over access and use by third parties should therefore be funded by individuals

- Can offer additional services like
 - Password creation-retention change-services
 - Personal Data Stores: Automatic updates to service providers
 - Attribute verification services across Privacy Protectors like age or role
 - Translate privacy policies to human understandable language
 - Automatic content erasure requests

Individuals have **freedom of choice** to select **one or more** privacy protector services based on criteria that meet their need: quality, cost, usability or support of domain specific features (like the sensitive health domain)

Select PP's

Individuals

Life cycle: Pre borns | Children | Adults | Deceased | Donors

Role: Parents | Guardians | Legal

Legal state: Suspected | Accused | Detained

Personal Information categories to be protected

Physical Contact Information | Online Contact Information | Unique Identifiers | Purchase Information | Financial Information | Computer Information | Navigation Click- Stream Data Interactive Data | Demo - and Sociographic Data | Content | State Managements Mechanisms
 Political Information | Health Information | Preference Data | Location Data | Government-issued identifiers | Other Information p3p

Legislative Processes

Eerste kamer
Tweede kamer
Council of State

Appoint stakeholders

Recommendations

Internet board

Appointed stakeholders

Economy | Consumer | Advertisers | Health Justice | Secret Service | Lawyers

Elected members from internet parties
 Privacy First | Bits of Freedom | Piraten Partij and current political parties
Inspired by Dutch Water Authorities

Elect (in)directly

Elect (in)directly