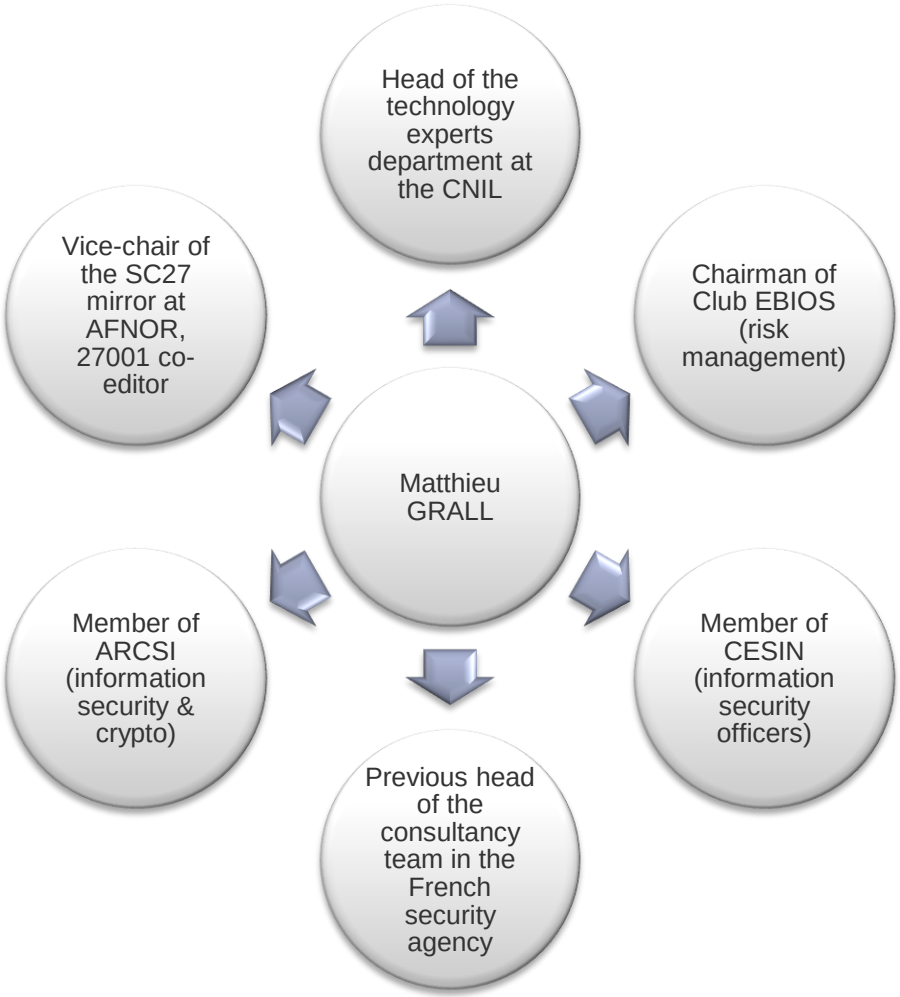
CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

Involvement of the Data Protection Authorities (DPAs) in standardization

2017-09-19

Who am I?


Head of the technology experts department at the CNIL
Vice-chair of the SC27 mirror at AFNOR, 27001 co-editor
Chairman of Club EBIOS (risk management)
Matthieu GRALL
Member of ARCSI (information security & crypto)
Member of CESIN (information security officers)
Previous head of the consultancy team in the French security agency


Cybersécurité
Objets connectés
Règlement européen
Véhicules connectés
Tracking sur le web & cookies
Big Data
Identité numérique
Collectivités
Énergie
Enfants et objets connectés
Privacy by design
Cloud computing
Alerte
Publicité ciblée
Anonymisation
PIA / DPIA / EIVP
Mots de passe
Biométrie
HADOPI
Réseaux sociaux
DLP
Billetique
BYOD
Banque
Vote électronique
Smartphones et tablettes
Smart cities
ANSSI
Santé
Drones
ARCEP
Travail
INVS
Téléservices
OTAN
TV connectée
Authentification
Robotique (IA)
Social
ASIP santé
Usages d'internet
Génétique
Smartgrids
Droit à l'oubli
Technologies sans contact

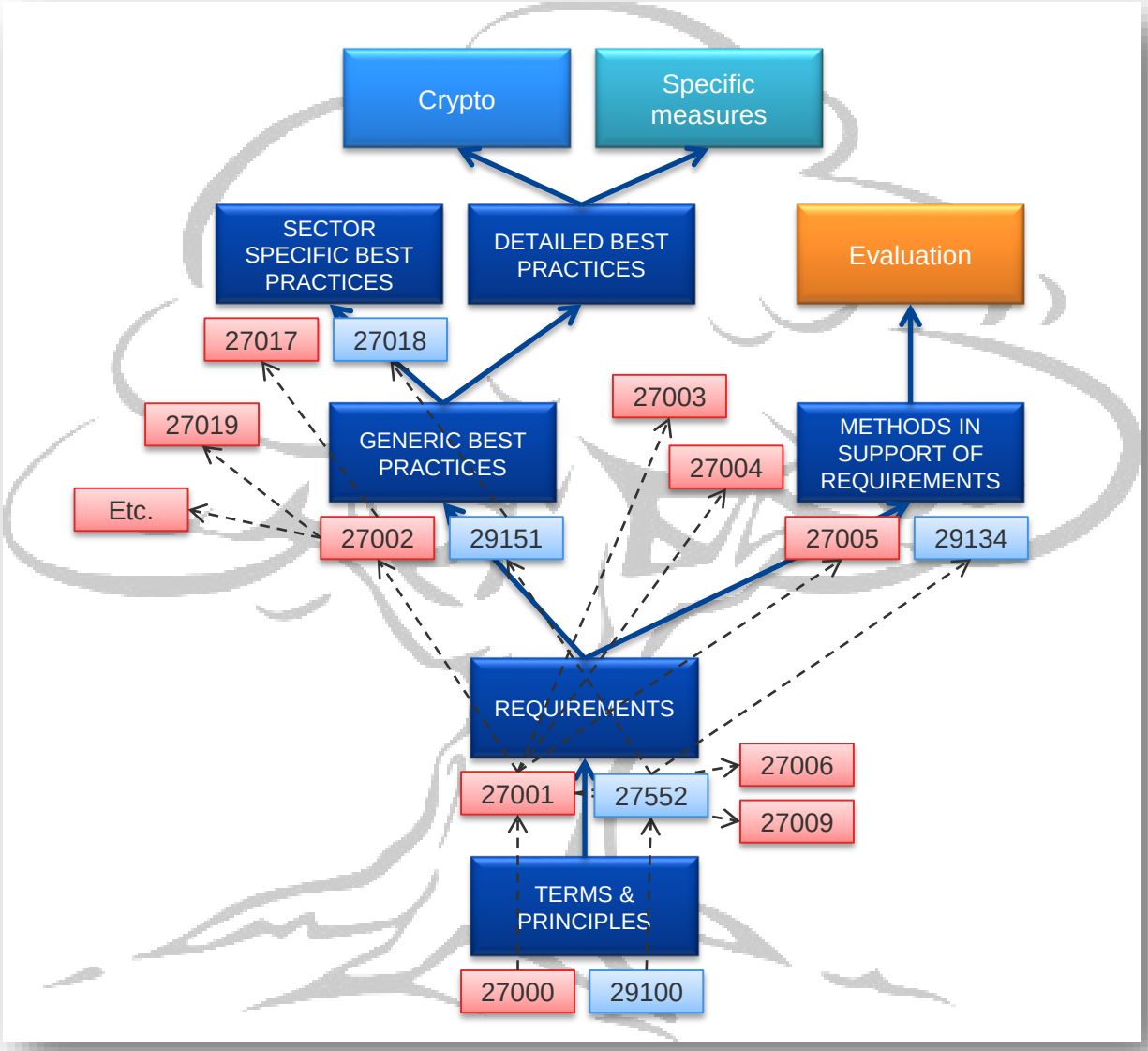
Involvement of the DPAs in standardization

- A real involvement in international standardization
  - The vision: International Standards design the future
  - The stake: integrate the vision of the DPAs into ISO standards
  - Co-regulation thru national standardization bodies, WP29 (European DPAs) and attendees at the ISO meetings
- Results
  - WP29 positions taken into account in ISO/IEC 29100
  - Official liaison between WP29 and ISO, and cooperation within WP29
  - Legitimity in information security brougth bu editing ISO/IEC 27001
  - New projects: ISO/IEC 27009, ISO/IEC 29134, ISO/IEC 29151, ISO/IEC 27552, *etc*.
- Priorities
  - Sector specific management systems certification
  - Privacy risk management and (D)PIAs
  - Privacy best practices

The process

- DPAs are directly concerned and highly interested in ISO/JTC1/SC27/WG5 issues
- A liaison has been established between WP29 and WG5 in 2010
- The liaison officer coordinates the activities, with the help of other representatives of the Italian (Guarante) and the French DPA (CNIL)
- They participated to each ISO SC27 meetings to represent WP29
- Following the ISO meetings, the liaison officer has informed WP29 during its plenary meetings on the key projects of WG5, e.g.:
  - Enhancement to ISO/IEC 27001 for privacy management (ISO/IEC 27552)
  - Privacy Impact Assessment (PIA, ISO/IEC 29134)
  - Privacy controls (ISO/IEC 29151)
  - Privacy Enhancing Technologies for Data de-identification (ISO/IEC 20889)
  - Online privacy notices and consent (ISO/IEC 29184)
- At each meeting, an information note has been provided, key issues have been highlighted, and positions have been coordinated, in order to prepare comments and votes on the projects at the national level
- Comments have been sent to ISO through this liaison as well

A tree of standards



Legend :

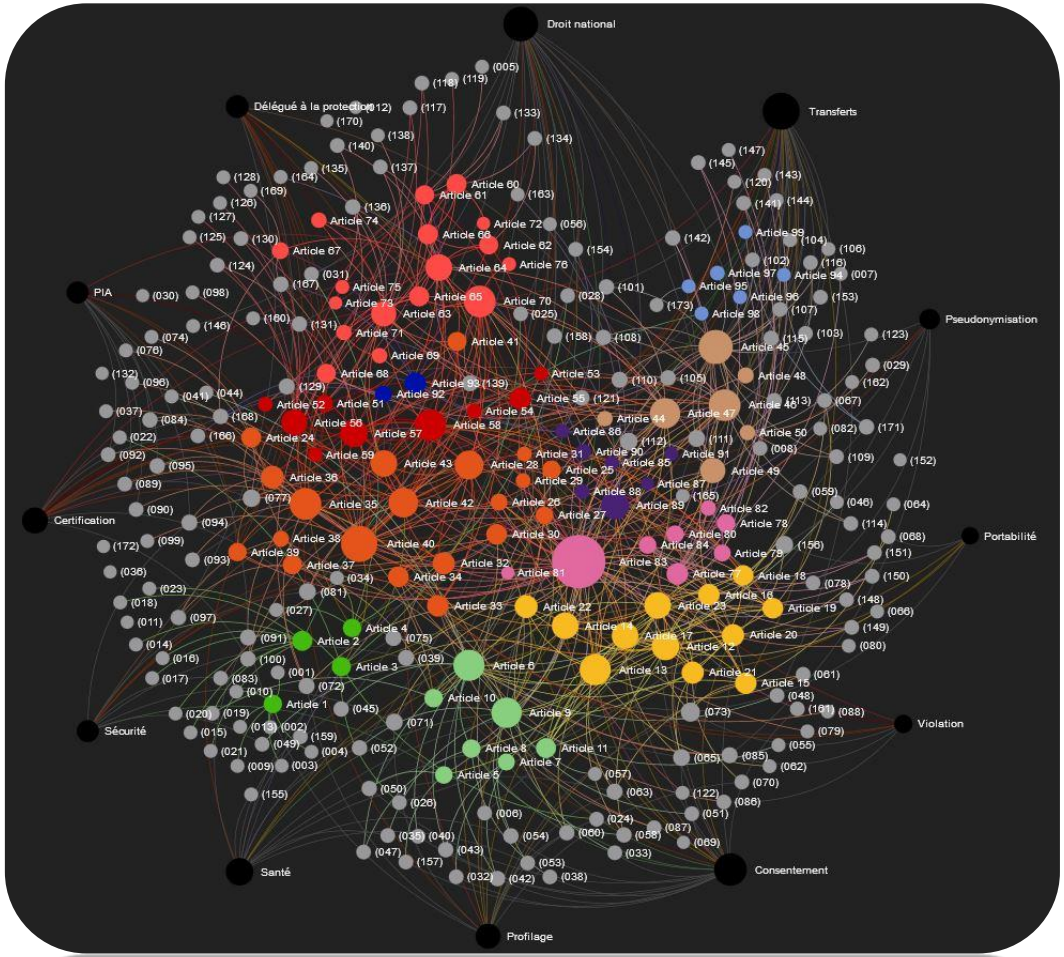
- TYPES
- WG1
- WG2
- WG3
- WG4
- WG5

(see annexes)

Conclusion

- Privacy related standards contribute to bring trust in processings of personal data
- They are a practical complement to international regulations
- The base is built (ISO/IEC 29100 for terminology and principles, ISO/IEC 29134 for PIA, ISO/IEC 29151 for privacy best practices)
- Specific standards have begun to emerge (cloud computing, notice and consent, de-identification, *etc*.)
- In the future, it’s going to be possible to carry out certification of management systems integrating the privacy

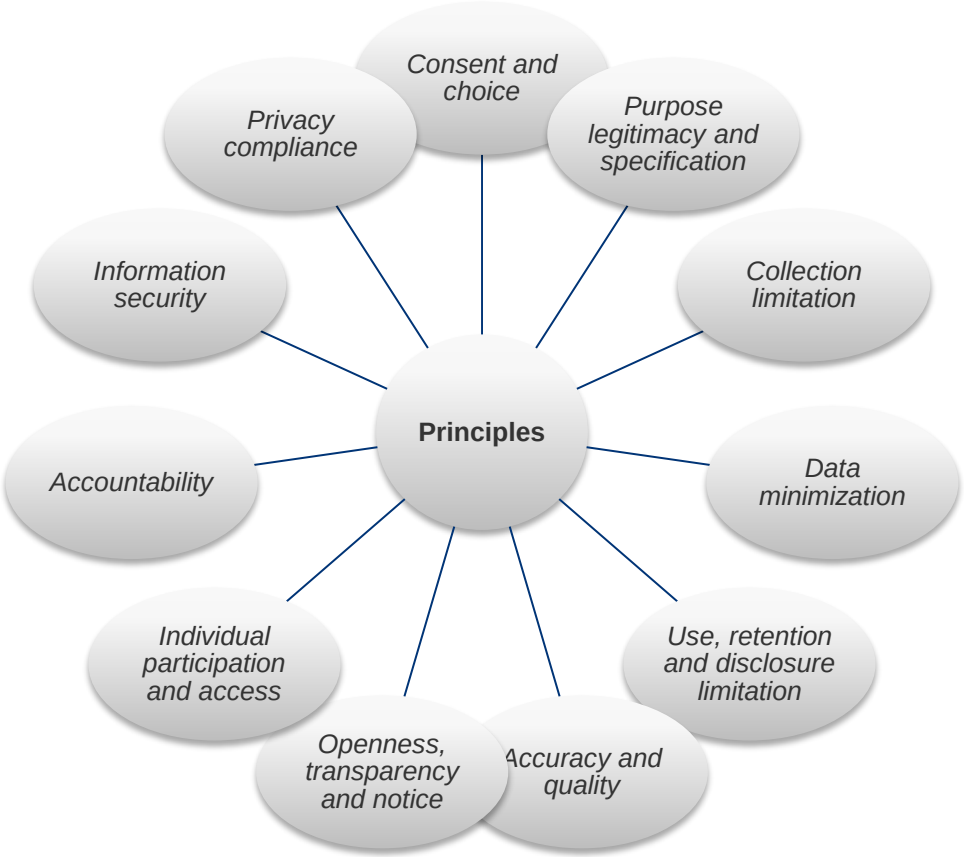
Going forward…



Annexes

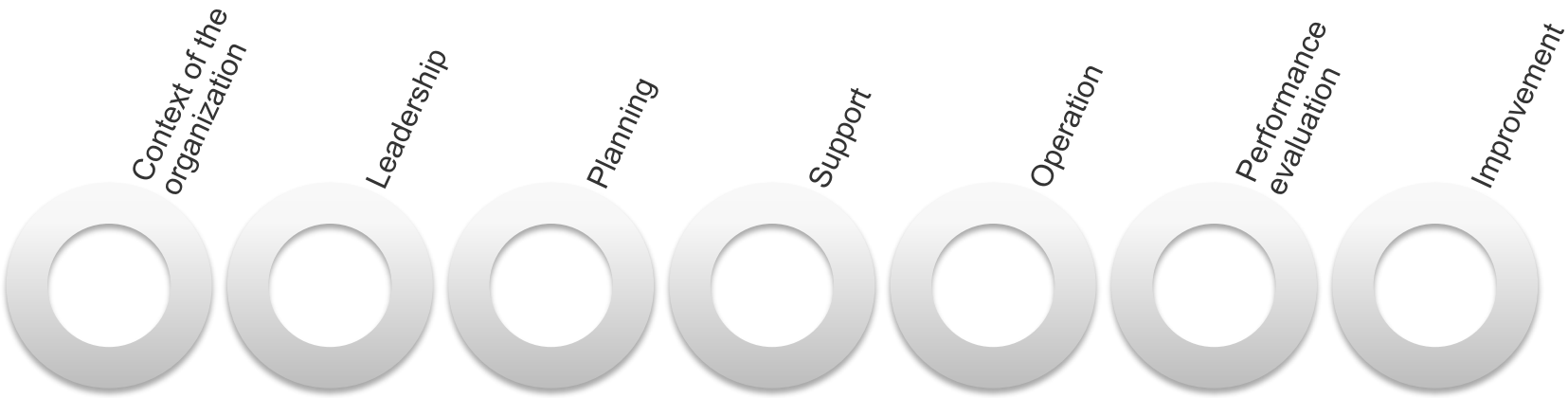
ZOOM ON EXISTING PRIVACY RELATED STANDARDS

Privacy terms and principles: ISO/IEC 29100



This standard is published free of charge:
http://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip

Requirements for an information security management system (ISMS): ISO/IEC 27001



Towards a management system integrating privacy? ISO/IEC 27009

- Requirements to create sector specific standards in the ISO/IEC 27001 framework
- A « sector » is means anything different from information security
- Two sector specific types of standards:
  - Additional requirements to ISO/IEC 27001
  - Additional controls to ISO/IEC 27001 Annex A / ISO/IEC 27002

How to carry out a PIA: ISO/IEC 29134

- Provides a framework to carry out « Privacy Impact Assessments » (PIA)
- Can help data controllers to implement legal requirements (GDPR art.35)
- Some DPAs already have their own method, that could be enriched by this standard, e.g. CNIL:

- WP29 (D)PIA guidelines will be adopted in October
- Could become a CEN standard

Generic privacy best practices : ISO/IEC 29151

- This standard is a generic set of controls

- Stakes
  - Implementation of the ISO/IEC 29100 principles
  - Determination of controls to treat the privacy risks
  - A privacy specific reference catalog in the ISO/IEC 27001 framework
  - A framework for ISO/IEC 27018 to rely on

Best practices for cloud computing processors: ISO/IEC 27018

- In a ISO/IEC 27001 framework, this set of controls should be used in addition to ISO/IEC 27002 (information security best practices)
- Containing technical and « legal » best practices
- Could be useful for a conformity process in the specific context of cloud computing