PROTECTING PERSONAL DATA IN AN AI ERA: THE CASE OF CONFORMITY ASSESSMENT BODIES

Dr. Irene Kamara

Annual Privacy Forum 5 Sep 2024

Conformity assessment in EU Law

- Conformity assessment is the process of assessing whether legal requirements have been fulfilled
- Traditionally: product safety legislation
- But also: Radio Equipment Directive, AI Act, Cyber Resilience Act.

Two pillars:

- New Approach (1985)
  - Essential requirements in the law
  - Technical requirements in technical standards – 'harmonised European standards' by CEN, CENELEC, ETSI.

  - New Legislative Framework (2008)
    - Conformity assessment.
    - Aim: common rules for assessment of product harmonisation legislation
    - Different assessment modules depending on risk.

Tilburg Institute for Law, Technology, and Society

Personal data as a conformity assessment target

- The GDPR is NOT a New Approach/NLF law
- But: personal data aspects still assessed as part of conformity assessment procedures:
  - **AI Act Reg 1689/2024:** data governance (art. 10). – data collection processes, purpose of data collection, availability and quantity of datasets, special categories of personal data, records of processing.
  - **Radio Equipment Directive 53/2014**: Privacy, data protection as essential requirement

Art. 3(3) (e) RED *Radio equipment [..] shall be so constructed that it complies with the following essential requirements:*

*radio equipment **incorporates safeguards to ensure that the** personal data and privacy of the user and of the subscriber are protected*

See also: Commission Delegated Regulation (EU) 2022/30

Qualities and Liability of notified bodies

- Notified bodies under the AI Act, need to demonstrate:
  - Independence
  - Competence
  - absence of conflicts of interests and
  - suitable cybersecurity requirements

How about **liability** of notified bodies?
•Poly Implante Prothèse (PIP) breast implants scandal –
•Court of Justice EU C-219/15 - Schmitt case

•The manufacturer of those implants -- > **appointed TÜV Rheinland to assess its quality system**. Between 1998 to 2008 TÜV Rheinland made eight visits to the manufacturer's premises, all of which were announced in advance. During that period, TÜV Rheinland never inspected business records or ordered that the devices be inspected.

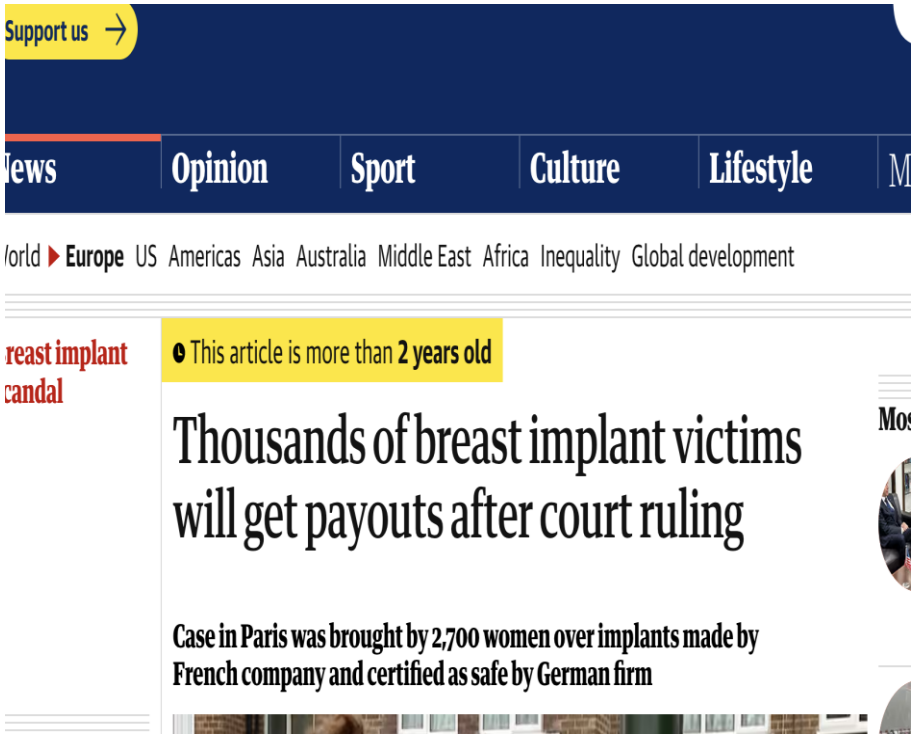
CJEU Ruling in PIP Scandal

- TUV was not under a general obligation to carry out unannounced inspections, to examine devices and/or to examine the manufacturer's business records.
- However, in the face of evidence indicating that a medical device may not comply with the requirements laid down the law → the auditor body must take all the steps necessary to ensure that it fulfils its obligations
- The procedure relating to the EC declaration of conformity, **the purpose of the notified body's involvement is to protect the end users of medical devices**.
  - The conditions under which culpable failure by that body to fulfil its obligations under the directive in connection with that **procedure may give rise to liability on its part vis-à-vis those end users are governed by national law,** subject to the principles of equivalence and effectiveness.

Tilburg Institute for Law, Technology, and Society

PIP Scandal – Liability of Auditors?

- "In 2021, the Paris Court of Appeal ruled that the auditing firm involved (TÜV Rheinland) negligently certified the producer of the implants due to a lack of impartiality on the part of its subcontracted auditor (TÜV France) and **was therefore liable under French tort law for the harm suffered by victims** who received faulty breast implants." [P. Verbruggen]



https://www.theguardian.com/world/2021/may/20/pay-compensation-to-victims-of-defective-breast-implants-rules-paris-court

P Verbruggen and B van Leeuwen, "Liability of Notified Bodies under the EU's New Approach: The Impact of the PIP Breast Implants Case (C-219/15)" (2018) 42(3) European Law Review 394. https://research.tilburguniversity.edu/en/publications/the-liability-of-notified-bodies-under-the-eus-new-approach-the-i

Liability of Notified bodies in the AI act?

- Art. 31(9) Notified bodies shall take out **appropriate liability insurance** for their conformity assessment activities, unless liability is assumed by the Member State in which they are established in accordance with national law or that Member State is itself directly responsible for the conformity assessment.

- *"Where the notified body is not satisfied with the tests carried out by the provider, the notified body shall itself directly carry out adequate tests, as appropriate."* Annex VII AI act

Recap

- Conformity assessment under New Approach/NLF as a regulatory technique for pre-market gatekeeping – AI, cybersecurity, and others
- Low expectations from self-assessment
- Questions about suitability of notified bodies in those new areas
- Liability of notified bodies is essential

Tilburg Institute for Law, Technology, and Society

Tilburg Institute for Law, Technology, and Society

WWW.TILT.NL

Tilburg University

Understanding Society

AI Act – conformity assessment

- Regulation (EU) 2024/1689
- Pre-market requirement:
  - Conformity assessment of high-risk AI based systems – Art. 43 AI Act.
- Aim: high level of trustworthiness of high-risk AI systems
- Self-assessment or third-party conformity assessment bodies (CABs)

Standalone AI systems: subject to self-assessment – internal control procedure (Art. 43(2)):

- Critical infrastructure
- Education & vocational training
- Employment worker's management
- Access & enjoyment of private/public services
- Law enforcement
- Migration, asylum, and border control management
- Administration of justice and democratic processes

Third party:
CABs: private for profit organisations -
Notified to the Commission --> 'notified bodies' (see also: Decision 768/2008/EC)

Systems that are already subject to conformity assessment under the New Legislative Framework - **but** following the process of the sectoral legislation!!

+ Standalone AI systems with Biometric identification and categorisation of natural persons

- “For high-risk AI systems **related** to **products which are covered by existing Union harmonisation legislation based on the New Legislative Framewor**k, the compliance of those AI systems with the requirements of this Regulation **should be assessed as part of the conformity assessment already provided for in that law.** The applicability of the requirements of this Regulation **should thus not affect the specific logic**, **methodology or general structure of conformity assessment** under the relevant Union harmonisation legislation.”
  - Recital 124 AI Act