Custodial Institutions Agency
Ministry of Justice and Security

Privacy @ Europris

Let’s make it happen!

25 May 2017

PEBKAC

https://www.joe.ie/tech/watch-coffee-shop-prank-shows-the-dangers-of-sharing-your-data-online-551976

Link required to actual movie!

Content

- Content:
  - Introduction
  - Case discussions
  - Wrap up
  - Q&A
- Questions: feel free to interrupt and/or at the end

Why does privacy matter?

- Prisons process large quantities of sensitive data (medical, penal) of a vulnerable group: data loss has significant impact
- Incidents in prisons attract media attention
- Prisons cooperate with many partners inside and outside of the central government and exchange information
- Reliability of prisons is important for trust of society
- External threats are rising: hacking as a service, lively trade in information, professional tooling
- Business use of consumer products: focused on adding new functionalities not on security
- Flexible working conditions: any place, any time, any device
- Shadow IT: easy access to ‘free’ internet services

Privacy: more than 'just' the GDPR

Complex legal environment:

- Privacy requirement from several laws, regulations, standards, operational guidelines: medical, penal, telecom
- Purpose of processing from several laws: specific laws (e.g. the Dutch prison law), regulations concerning personnel, financial laws
- Legitimacy: balancing these two

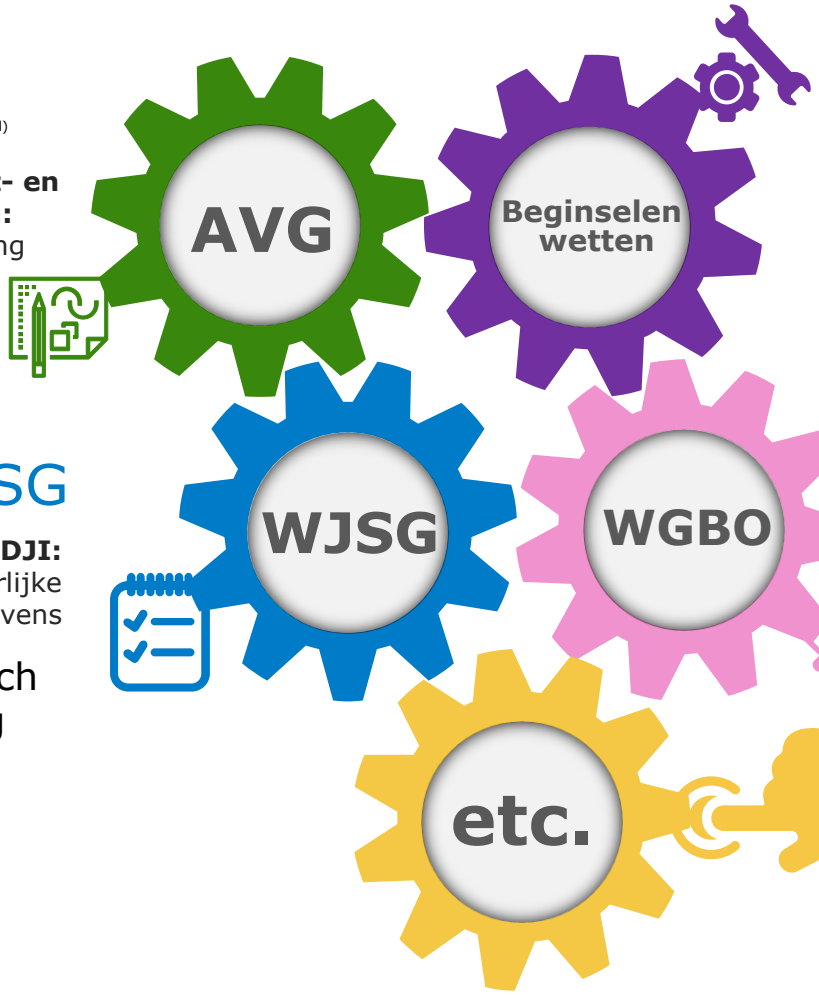
Privacy: more than ‘just’ the GDPR

Same as slide 4, but in Dutch

Is niet het enige wat aandacht vraagt !

AVG
(nog 48 **werk**dagen Wbp|Mpd)

Privacy wet- en regelgeving:
- Verordening
- Richtlijn



Beginselenwetten

Verblijf in een penitentiaire inrichting of een tbs-instelling
- Penitentiaire beginselenwet
- Beginselenwet verpleging ter beschikking gestelden
- Beginselenwet justitiële jeugdinrichtingen

WJSG

Vanuit de taakstelling van DJI:
Wet justitiële en strafvorderlijke gegevens

Richtlijn vertaalt zich naar WJSG en Wpg

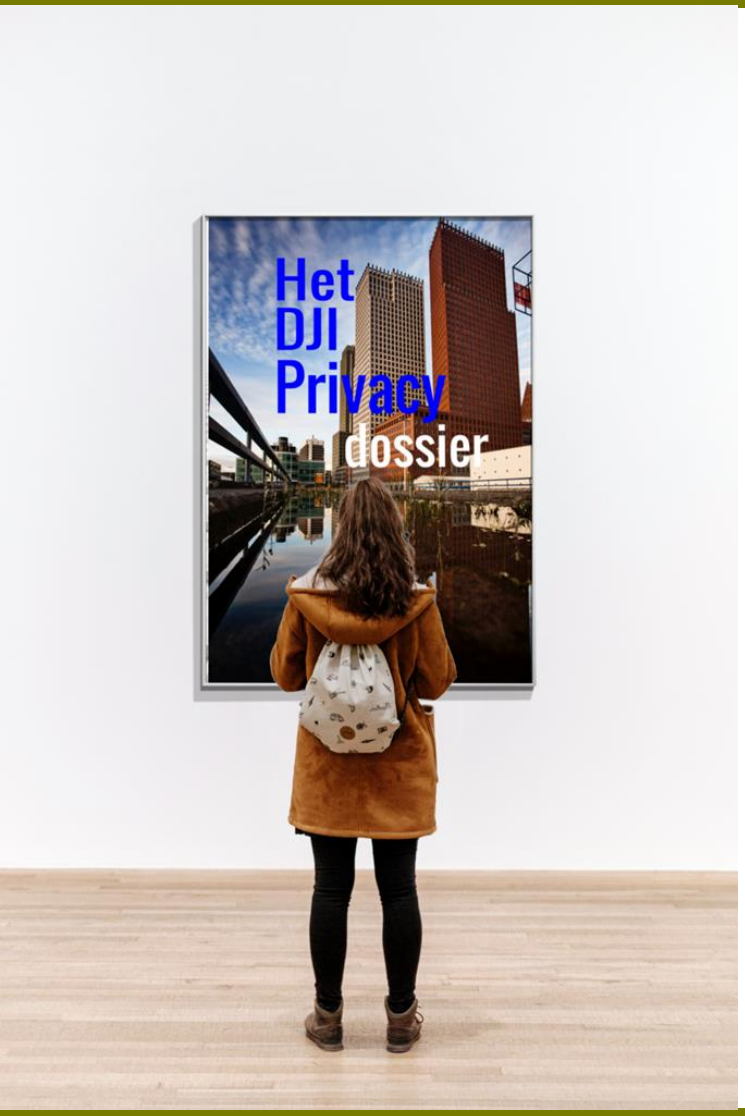
WGBO

Vanuit DJI als zorgaanbieder:
De Wet op de geneeskundige behandelingsovereenkomst (WGBO) beschrijft de rechten en plichten van cliënten in de zorg

Gewoon véél Wet- en regelgeving

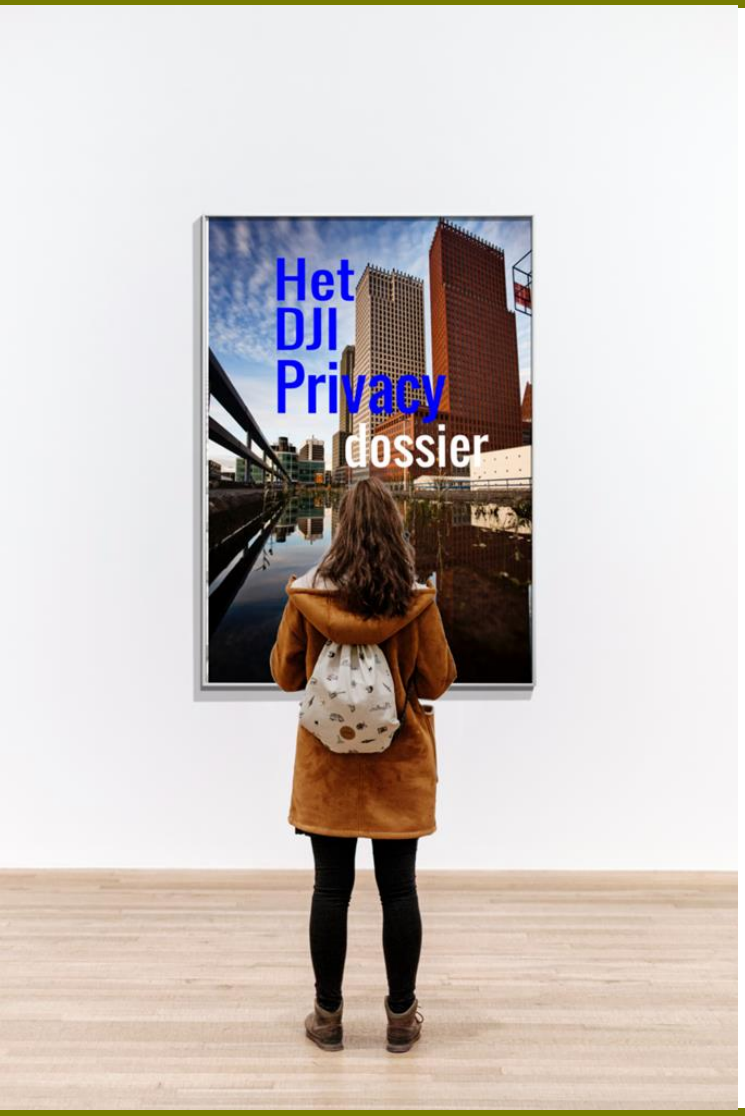
Binnen taakveld van DJI

Privacy … nothing new really….



- **Legitimacy/Just cause**
  Purpose limitation, Proportionality, Subsidiarity, Retention time, deletion
- **Quality**
  Data quality, data minimisation, currentness
- **Security**
  Situational & deliberate choices, minimisation of user access (authorizations)
- **Partners & information supply chain**
  Processing agreements, In control statements & ttp, anonymised testing
- **Transparency**
  Obligation to inform, written informed consent, documentation duty, privacy statements, PIA-reports
- **Rights of the individual stakeholder**
  Access/inspection, deletion, right to be forgotten, right to object, data portability → requires procedures
- **Privacy by design**
  Policies, begin with the end in mind, privacy awareness
- **Planning & Control**
  Privacy on management agenda, Privacy in Plan-Do-Check-Act-cycle

…. apart from



- **Demonstrable compliance**
  Documentation: in general: design & operating effectiveness & specifically: DPIA, Register
- **Rights of the individual stakeholder**
  Stronger position, shorter response times, answers of higher quality
- **Supervisory bodies**
  Strong position, wide array of measures
- **Fines**
  High fines and personal liability

A practical approach

- Educate personnel, focus on ‘how to’ & make it easy to comply
- Develop a compact privacy policy providing personnel with direction, e.g. ‘safety, security and health care take priority over privacy’
- Define a management system for privacy: translate privacy requirements to controls and link those to underlying documents
- Work risk-based: make DPIA’s, fill the register and implement controls for systems containing the most sensitive data
- Make it easy to manage: design a control plan tailored to the responsibilities of a prison director
- Include a privacy-KPI in the management control cycle
- Apply privacy by design: embed privacy (and security) in all activities, documents and products: post-documenting & -corrections → €€€ & 🕐
- Begin with the end in mind: exit-strategy, retention times, deletion
- Don’t dash on a marathon, make small and constant improvements
- Hatch onto projects and other initiatives and add a touch of privacy
- Document everything: privacy-analysis, designs, agreements, procedures, policies

Possible cases

May I use production data to evaluate operational policies and processes?

On the network share, our team has many many thousands of files. It is impossible to sort through them all. Is that sufficient reason to not take action?

I want to share information with a professional partner. Processing by this partner is covered by law. May I share this information?

I want to email a dossier containing penal data, is that allowed?

I want to run a pilot, do I need to comply to all privacy requirements?

I want to set up a data warehouse and correlate data from different sources and be able to drill down to the individual, is that allowed?

When investigating a technical error in the camera systems I caught personnel seriously misbehaving. I do not have a policy permitting or forbidding using the camera systems for that purpose. Can I take action?

Closing thoughts

https://www.youtube.com/watch?v=EjeZxySmYKA

Questions?