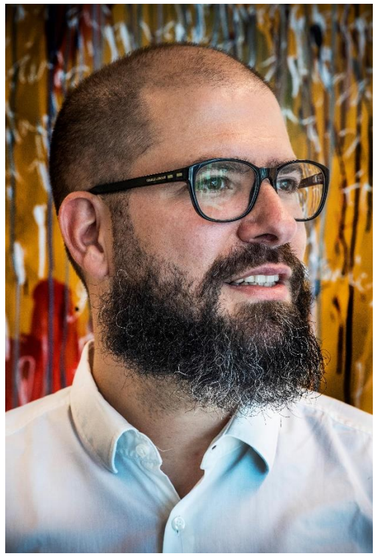
CYBER SECURITY COALITION.be

Privacy Focus Group

A.I. & Data Protection

Webinar – 9 November 2021
11:00 a.m. - 12:30 p.m.

KU LEUVEN



Guest Speakers:

Ellen Wauters
Koen Vranckaert
Brahim Bénichou

Knowledge Centre
Data & Society

AI & the GDPR

Ellen Wauters, Brahim Bénichou & Koen Vranckaert
KU Leuven Centre for IT and IP Law

Cyber Security Privacy Focus Group - AI and Data Protection
9 November 2021

Kenniscentrum
Data & Maatschappij

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone."[4] Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons;[5] and the evil of the

"The right to privacy", Warren and Brandeis, Harvard Law Review 1890

Overview

Kenniscentrum Data & Maatschappij

- **Introduction**
  - Recap: a few GDPR principles to keep in mind GDPR
  - Main challenges GDPR & AI
  - Risks when not complying with the GDPR
  - It’s all about data
- **Practical application of a number of specific GDPR requirements on AI systems**
  - Data Protection by Design
  - Data Minimisation
  - Data Security
  - Automated Decision Making
  - DPIA
  - Research & statistical purposes
  - Transparency
  - Data Retention
  - Data subject Rights
- **Conclusion**
- **Q&A**

RECAP: A FEW GDPR PRINCIPLES TO KEEP IN MIND

Kenniscentrum
Data & Maatschappij

GDPR Principles (art. 5 GDPR)

Kenniscentrum Data & Maatschappij

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

- Risk based approach

Data controller or data processor

Kenniscentrum Data & Maatschappij

Data controller

- Determines the purposes and means of the processing
- Is in charge of the processing

Data processor

- Processes on behalf/on instruction of the data controller
- Data processing agreement
- Cannot define means and purposes

Sub-processor

- Processes on instruction of the data (sub-) processor

Main challenges

Kenniscentrum
Data & Maatschappij

Data use

Kenniscentrum Data & Maatschappij

Transparency, fairness and accountability

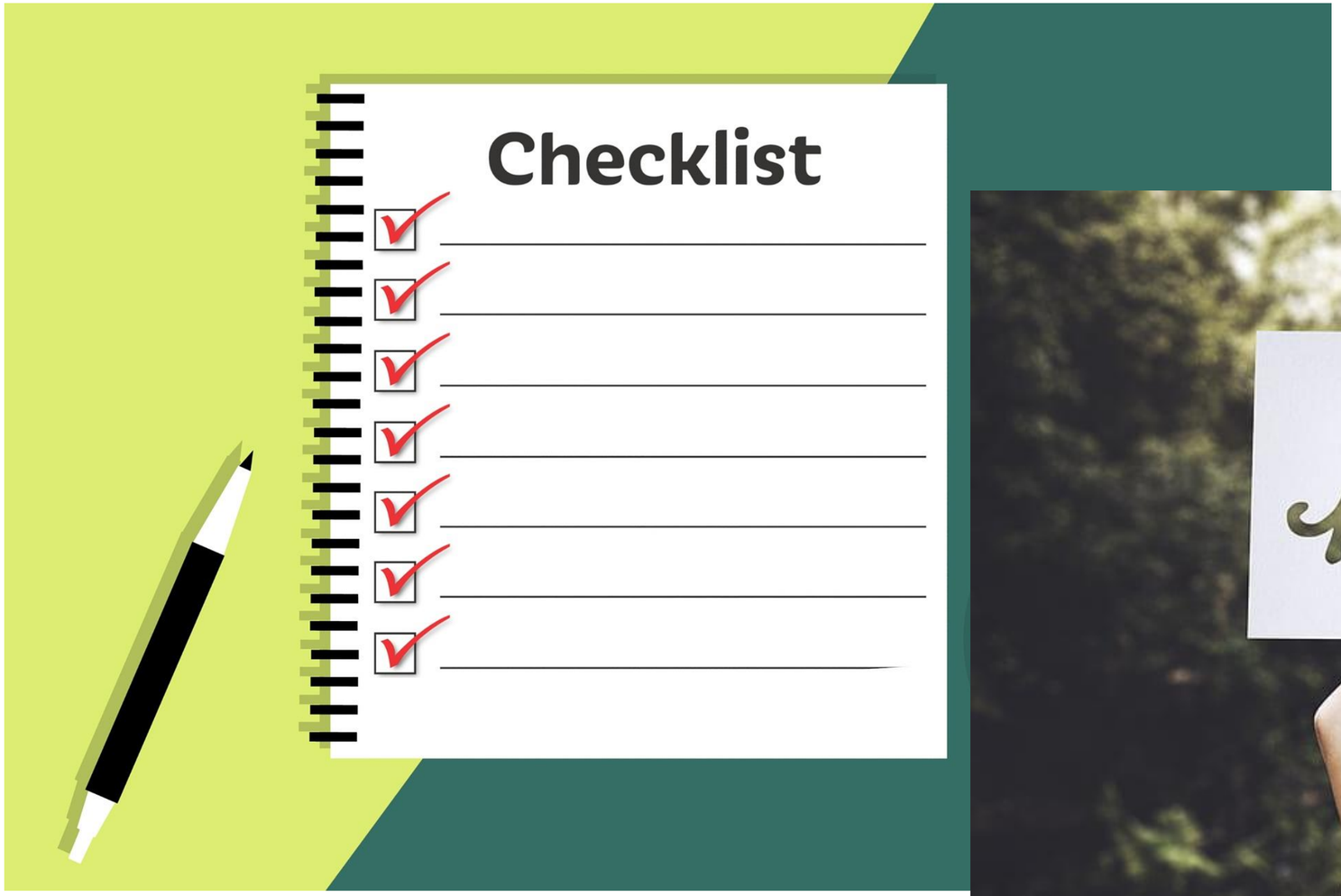
Kenniscentrum
Data & Maatschappij

Automated Decision Making

Kenniscentrum
Data & Maatschappij

Beware of a 'check-the-box' approach

Kenniscentrum
Data & Maatschappij



Most important GDPR risks related to AI

Kenniscentrum
Data & Maatschappij

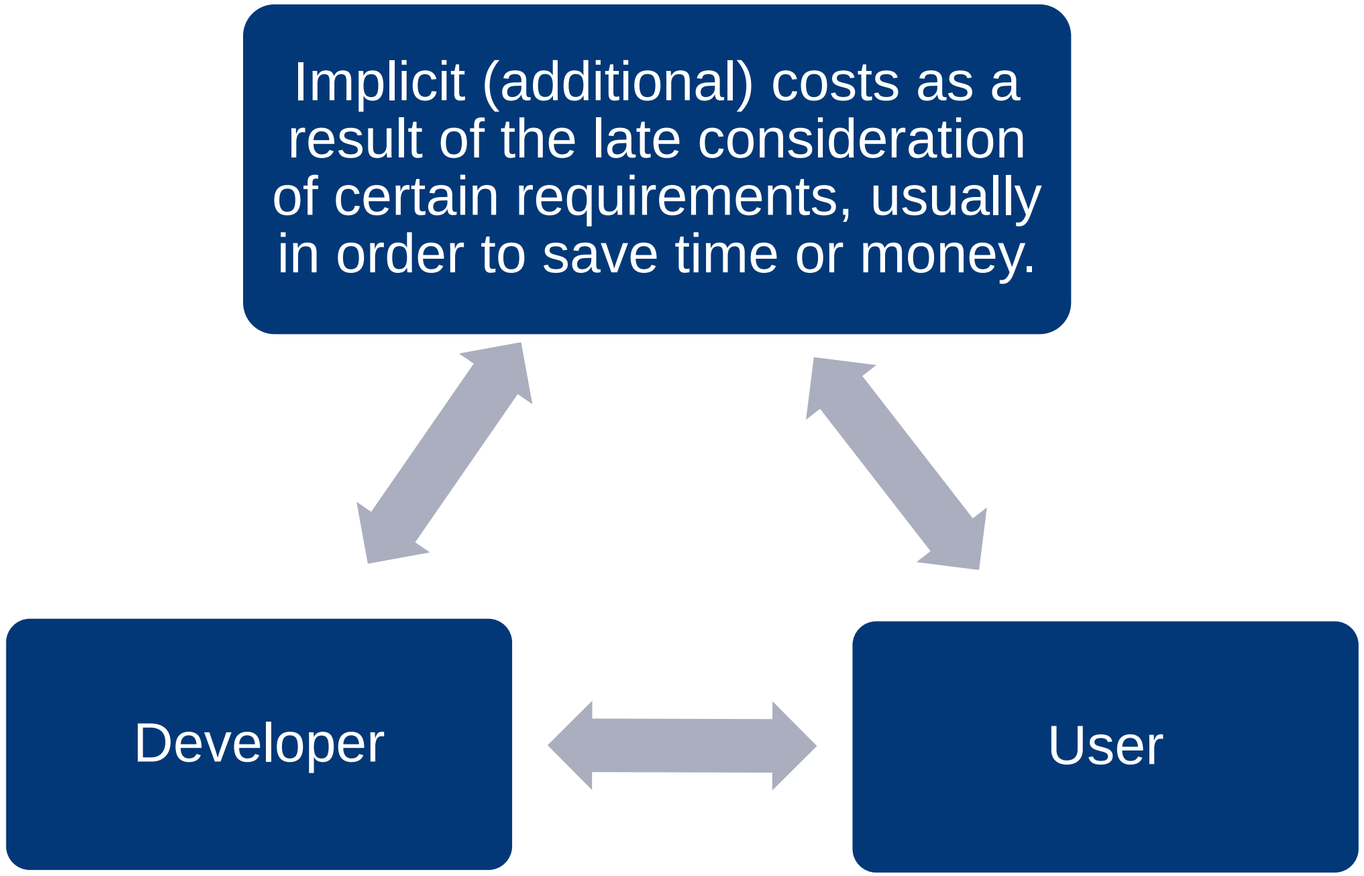
Non-compliance with the GDPR

Kenniscentrum Data & Maatschappij

- Commercial
- Sanctions
  - » Such as fines up to up to 20 Mio EUR or up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Art. 83 GDPR)
- Reputation
- Loss of useful data / business intelligence
- Data breaches
- Loss of sensitive information, trade secrets and know-how

Technical (privacy) debt

Kenniscentrum Data & Maatschappij



Quality / functioning of the AI-system

Kenniscentrum Data & Maatschappij

- Data quality is essential for the functioning of the AI system
  - » ‘Garbage in, garbage out’
- ‘Hidden failures’

IT’S ALL ABOUT DATA

Kenniscentrum
Data & Maatschappij

Know Your Data

Kenniscentrum Data & Maatschappij

- Origin and sources
- Age
- Types of data, characteristics and attributes
- Legal processing bases
- Limitations
- Sensitive data
- Etc.

IN PRACTICE

Kenniscentrum
Data & Maatschappij

Data Protection by Design and Data Protection by Default

Kenniscentrum Data & Maatschappij

1. …Controller shall, both at the time of determination of the **means of processing** and at the time of **the processing itself**, implement appropriate technical and organization measures … designed to implement DP principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing for data subject rights…
2. Controller shall … ensure that, **by default, only** personal data which are **necessary for each specific purpose** of the processing are processed. (data, processing, storage and accessibility)

Data Protection by Design and by Default

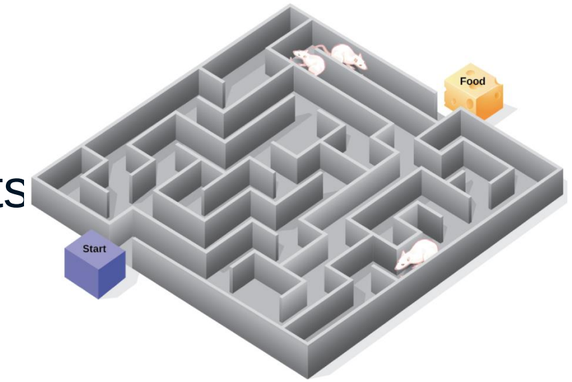
Kenniscentrum Data & Maatschappij

- Incorporate data protection in applications and processes
  - state-of-the-art, risks, costs,…
- Avoids technical debt!
- Nudges
- Relates to all obligations under the GDPR
- Risk based approach
  - Risk modelling (/threat modelling) – f.e. LINDDUN (linddun.org)
- Data Protection by default = Data Protection is the default
- Certification

Data Protection by Design and by Default

Kenniscentrum Data & Maatschappij

- Specific in an AI context
  - Explainability
  - Data subject rights
  - Use as little (personal) data as possible
  - Use encrypted and/or pseudonymized data
  - Avoid re-identification and derivation of sensitive data
  - Know your data
  - Data cleansing
    - » Redundant data? / Representative?/ Bias?
    - » Note: Article 10 AI Act Proposal imposes data quality requirements
- Document



Data Minimisation

Kenniscentrum Data & Maatschappij

- Article 5.1 (c) GDPR: Personal data shall be adequate, relevant and **limited to what is necessary for the purposes** for which they are processed.
- No personal data?
- As little data as possible
  - Lowest possible volume
  - Lowest amount of data subjects
  - Fewest types of data
- For the **purposes** : clear purposes give leeway

Data Minimisation

Kenniscentrum Data & Maatschappij

- Domain experts!
- Deployment and training of the AI system
- Limit internal access to data
- Benefits: clean data, less hassle

Data Minimisation

Kenniscentrum Data & Maatschappij

- Anonymisation / destruction
  - Attribute suppression
  - Record suppression
  - Character masking
  - Generalising
  - Swapping and shuffling
- Reduce readability/usability of personal data
  - Differential privacy and perturbation
  - Pseudonymisation
  - Make unreadable
  - Encryption and homomorphic encryption

Data Minimisation

Kenniscentrum Data & Maatschappij

- Data minimisation as product requirement

- Development and training phase
  - Federated learning
  - Generative adverserial networks (GANs)
  - Transfer learning

Data Security

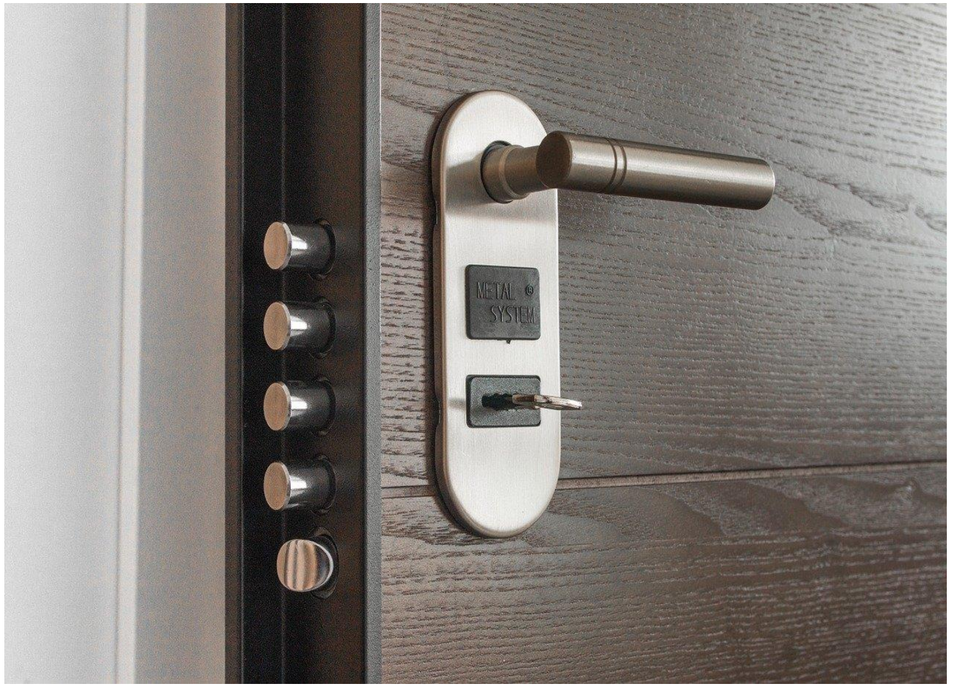
Kenniscentrum Data & Maatschappij

- Article 32 GDPR: *"… The controller and the processor shall implement **appropriate** technical and organizational measures to ensure a level of security **appropriate to the risk**…*

Data Security

Kenniscentrum Data & Maatschappij

- Technical and organisational security
- Risk-based approach
- Data security policy
- Data management and data mapping
- Awareness-raising and training
- Agreements with suppliers and processors
- Document



Automated decision-making & profiling

Kenniscentrum Data & Maatschappij

- **Profiling** = automated processing of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning a natural person (work, economic situation, health, personal preferences, reliability, behavior, location or movements)

- **ADM** = decisions based solely on automated processing, including profiling, producing legal effects or similarly significantly affecting a person

Automated decision-making & profiling

Kenniscentrum Data & Maatschappij

- **Profiling** = allowed if GDPR-principles are respected, incl. an appropriate legal basis

- **ADM** = prohibited unless 3 situations
  - necessary for performance of a contract between user and controller;
  - authorised by Union or national law which applies to the controller (incl. measures to safeguard the user's rights and freedoms)
  - the user's explicit consent (which can be withdrawn)
- However – scope!
  - ➢ solely automated decisions
  - ➢ that have a legal effect or otherwise significantly affect the person

Automated decision-making & profiling

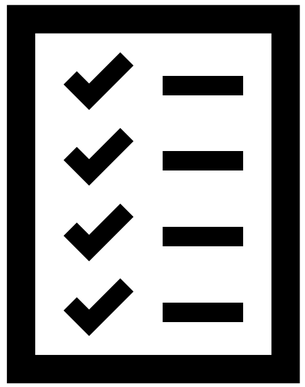
Kenniscentrum Data & Maatschappij

- Applying ADM?
  - Transparency-obligations (cfr. supra) and additional DSR:
    - » right to obtain human intervention, to express their point of view and to contest the decision.
- **In practice:**
  - ADM: Be aware of legal restrictions
    - » Consult your DPO/privacy manager when designing/developing a potential ADM-system
    - » Technical feasibility of human intervention,…
  - Importance of training operators of ADM-systems, quality monitoring, third party auditing,…

Data Protection Impact Assessment

Kenniscentrum Data & Maatschappij

- **What & why?**
  - Maps data protection risks in advance → corrective measures



- **What kind of processing activity?**
  - In theory: ‘high risk to the rights and freedoms of natural persons’, ‘new technologies’
    - » Further specified in GDPR and in guidance by BE DPA
  - In practice: AI-systems = new technology + often complex and not entirely transparent outcomes
    - » Consider to complete DPIAs even if not strictly mandatory

DPIA

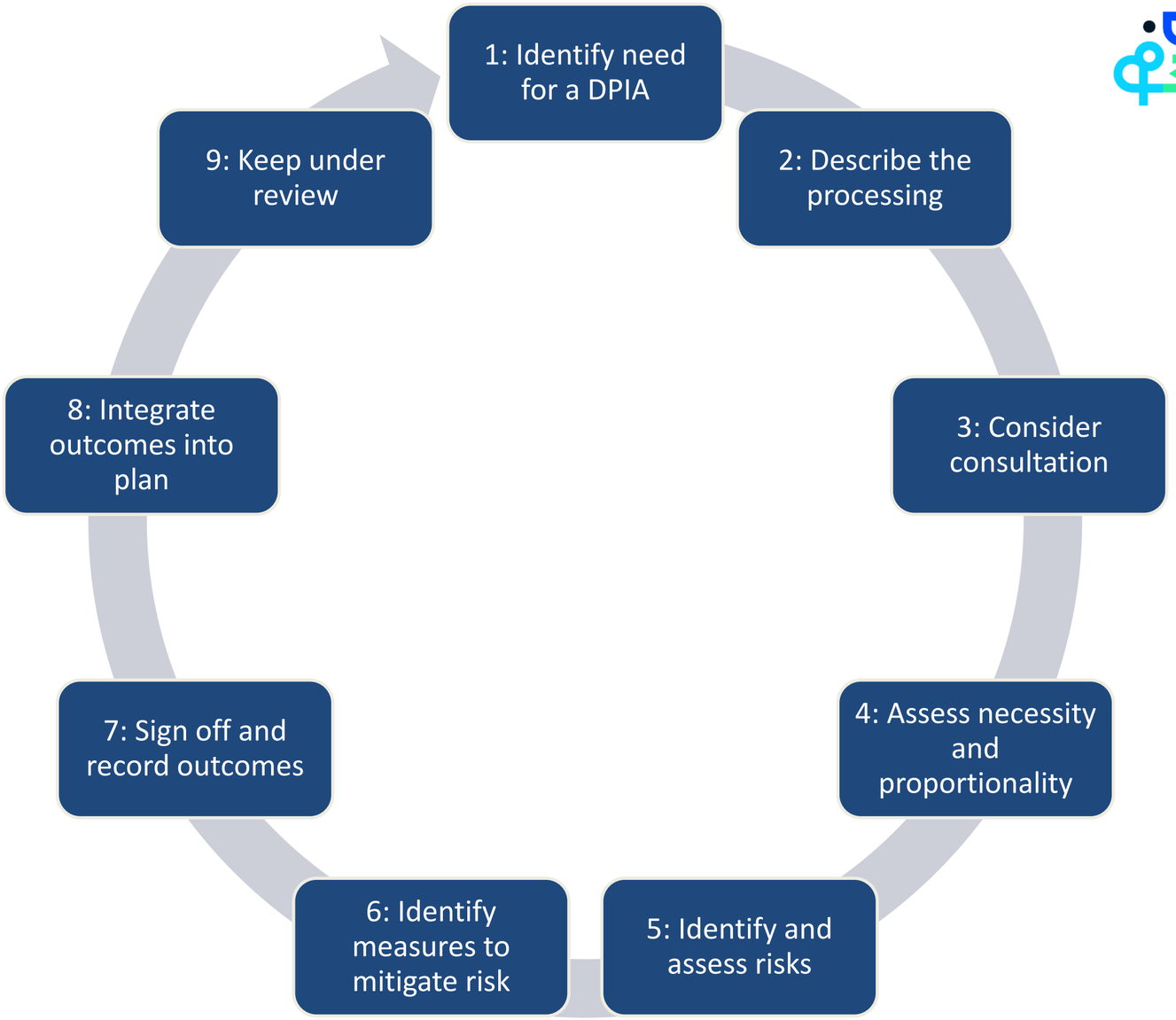
Kenniscentrum Data & Maatschappij

- **When?**
  - At the earliest possible moment
  - DPIA ≠ one-off exercise ➔ continuous exercise
    - » If risk of processing activity changes (e.g. due to societal context): complete DPIA

- **By who?**
  - You, your team and your DPO/Privacy manager

- **Where?**
  - Contact your DPO/Privacy manager for template DPIA

Kenniscentrum Data & Maatschappij



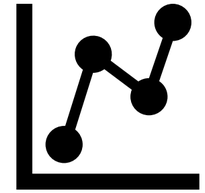
Source: ICO

Research and statistical purposes

Kenniscentrum Data & Maatschappij

- Various exceptions/additional rules apply: data subject rights, data retention,…

Scientific research	Statistical purposes
• Broad concept • Incl. technological development and demonstration, fundamental research, applied research,.. • Publicly or privately financed	• *“any operation of collection and processing of personal data necessary for statistical surveys or for the production of statistical results.”* • **!!** statistical purpose ➔result of processing for statistical purposes ≠ personal data, but aggregate data, not used in relation to any particular natural person.
Example: training AI-system during training-phase (⇔ operational phase?)	Example: aggregated user statistics/ accuracy analyses during training & operational phase



Research and statistical purposes

Kenniscentrum Data & Maatschappij

- Respect rights of data subjects
  - Data minimisation guaranteed through technological and organisational measures
- Further processing is deemed compatible
  - but: information obligation
- Longer retention period possible

Research and statistical purposes: BE

Kenniscentrum Data & Maatschappij

PRINCIPLE	The controller for processing for scientific research or statistical purposes uses anonymous data.
EXCEPTION	If it is not possible to achieve the research or statistical objective with anonymous data, the controller will use pseudonymised data.
EXCEPTION	If it is not possible to achieve the research or statistical objective with pseudonymised data, the controller will use non-pseudonymised data.

Research and statistical purposes: BE

Kenniscentrum Data & Maatschappij

- Exceptions/additional rules in connection to:
  - Obligations to anonymise/pseudonymize
    - 4 situations which stipulate who needs to anonymize/pseudonymize
  - Public dissemination of personal data
    - ban on dissemination of personal data, but 4 exceptions
  - Communication of data
    - obligation to communicate non-pseudonymised data in a non reproduceable manner in 3 instances
  - Transparency
  - Retention
  - Data subject rights

Transparency

Kenniscentrum Data & Maatschappij

- Internal vs. external transparency

- Internal transparency:
  - Understanding of AI-systems by other parties
  - Internal policies and guidelines
  - Accountability measures
  - Registry of processing activities

External Transparency

Kenniscentrum Data & Maatschappij

- Privacy statements: art. 12-14 GDPR

- Scientific research: additional obligations
  - Direct vs indirect data collection

A privacy reminder from Google

To be consistent with data protection laws, we're asking you to take a moment to review key points of Google's Privacy Policy. This is not about a change we've made - it's just a chance to review the key points below. **Click "I agree" when you're ready to continue, or explore other options on this page.**

External Transparency

Kenniscentrum Data & Maatschappij

- Art. 12: Form: information has to be
  - Concise
  - Transparent
  - Intelligible and easily accessible form
  - Using clear and plain language

External Transparency

Kenniscentrum Data & Maatschappij

- Art. 13: which information:
  - ✓ Who
  - ✓ Contact details
  - ✓ Purpose; why
  - ✓ Where
  - ✓ Recipients (if any)
  - ✓ (Transfer to third countries)
  - ✓ How long
  - ✓ Existence of rights
  - ✓ If based on consent => right of withdrawal
  - ✓ Right to lodge a complaint
  - ✓ Existence of automated decision-making

External Transparency

Kenniscentrum Data & Maatschappij

- Art. 14: when not directly obtained from the data subject:
  - which categories of personal data are collected (the person will probably not know which data about him/her was collected)
  - the source of the personal data and when applicable, if they came from public available sources
- When to provide this information
  - when collecting the data (art. 13)
  - within a reasonable timeframe, max. 1 month (art.14)

External transparency

Kenniscentrum Data & Maatschappij

- **FOCUS**: Automated decision-making – information about
  - the existence and use of automated decision-making, including profiling
    - » *Users need to be aware of ADM*
  - meaningful information about the logic involved
    - » *Not a complex but a specific, useful and clear explanation*
  - the significance and the envisaged consequences of such processing for the data subject.
    - » *The manner in which the ADM-process may influence/ have consequences for the user (e.g. by giving examples)*

- Technical counterpart: explainability (by design)

External Transparency

Kenniscentrum Data & Maatschappij

By placing an order via this web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions. We reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act. If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this sub-clause and proceed with your transaction.

Click here to nulify your soul transfer.

GameStation 2010

Kenniscentrum
Data & Maatschappij

NOV.
23

Workshop: Legal Design

door Kenniscentrum Data & Maatschappij

50 volgers Volgen

Gratis

Uitverkocht

Details

Data retention

Kenniscentrum Data & Maatschappij

	**Principle**: PD cannot be stored longer than is necessary for the purposes for which the personal data are processed
	Exception: Scientific research or statistical purposes (+ appropriate technical and organisational measures)

- In practice?
  - Data retention policy/storage guidelines/…
- Advantages of deleting data?
  - Decrease the extent of possible data breaches, decrease risk of using inaccurate, excessive or irrelevant data,…
- Organisation-specific!

Data subject rights

Kenniscentrum Data & Maatschappij

- Various rights: access, rectification, erasure, data portability, object,…
  - If conditions are met ➔ obliged to respond (1 month)
  - Exception – Scientific research/statistical purposes: *“likely to render impossible or seriously impair the achievement of the purposes”*

- Practical consequences:
  - **Organisation**: Data subject rights policy/request procedure/…
  - **Product**: AI-systems need to allow for the exercise of such rights
    - » E.g. rectification/erasure of data: re-training? Unlearning?

Data subject rights

Kenniscentrum Data & Maatschappij

- What if you receive a DSR-request?
  - Follow DSRP or
  - Escalate to DPO/Privacy manager

- Don’t leave a request unanswered → Risk of DPA involvement

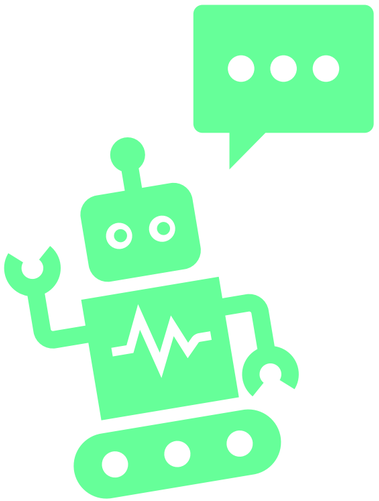
Conclusion

Kenniscentrum Data & Maatschappij

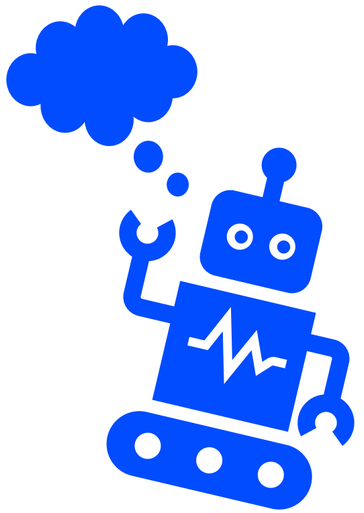
- Know your data
- Understand which internal policies apply on your activities
- Understand how your product/system may impact the private life of the persons concerned
- Consider the applicable legal requirements and take them into account when developing AI-systems or in your research
- Have an interdisciplinary mindset when applying data protection and product development
- Create legally correct but technically and practically applicable guidelines and advice

Kenniscentrum
Data & Maatschappij

Q&A



Ellen Wauters – ellen.wauters@kuleuven.be
Brahim Bénichou – brahim.benichou@kuleuven.be
Koen Vranckaert – koen.Vranckaert@kuleuven.be



CYBER SECURITY
COALITION.be

Follow us on Linkedin

Follow us on Twitter

www.cybersecuritycoalition.be

Thank you

Subscribe to our Cyber Pulse newsletter

Join our mailing list to receive updates from the Cyber Security Coalition.

Email Address

First Name

Last Name

I agree to receive Cyber Pulse and know that I can easily unsubscribe at any time.

SUBSCRIBE NOW!