Supporting data controllers on assessing the risk of a personal data breach

A DPO’s perspective
Discussion points

1. How controllers perceive the notion of the risk (to the rights and freedoms of data subjects)?

2. Which are the processes a controller needs to have in place to perform a risk assessment?

3. What is the role of the DPO?
How controllers perceive the notion of the risk (to the rights and freedoms of data subjects)?

- Due to their position, controllers have experience in understanding risks.
- Data protection risk assessment is challenging for controllers because it is considered as something new.
- Controllers recognise that a data breach could be damaging (monetary, reputation, social costs etc).
- Controllers changed their approach from a “tick the box” exercise to a holistic assessment due the potential impact of a data breach.
How controllers perceive the notion of the risk (to the rights and freedoms of data subjects)?

- Hence, controllers take measures to mitigate such risk by setting up “Data breach response” structures and processes.
- Controllers prefer to notify the authorities i.e. considering a personal data breach as a “risk” also for transparency.
- **Guidelines for threshold assessment** of a data breach (“risk” or “high risk”) are considered not clear enough.
- Hence, an over-reporting of data breaches could be observed.
Processes for internal risk assessment

- Regulation states that controllers shall notify breaches ‘*unless the personal data breach is unlikely to result in a risk*’.
- Based on the regulation wording, it is perceived that the notification is the **default** position.
- So the question is not if is a “risk” but if is it a “**High risk**”?
- The assessment is done on a ”**case-by-case**” basis and considers the **likelihood and severity** of the risk to the rights and freedoms of data subjects.
Processes for internal risk assessment

- WP 29 recommends to take into account:
  - type of breach
  - nature, sensitivity, and volume of personal data
  - ease of identification of individuals
  - severity of consequences for individuals
  - special characteristics of the individual
  - special characteristics of the data controller
  - the number of affected individuals.
Processes for internal risk assessment

- DPIA identified risks, if applicable.
- Data management classification risks, if available.
- Involvement of the “Data breach response team”.
- Examples of references that could assist the controller during assessment:
  - EDPS Guidelines
  - WP 29 Guidelines on Personal data breach notification under Regulation 2016/679
  - ENISA’s “Recommendations for a methodology of the assessment of severity of personal data breaches”
What is the DPO’s role?

- The DPO is informed when a data breach is detected.
- Advises the controller on how to proceed in an objective and impartial manner.
- Acts as a contact point for the supervising authority and data subjects.
- Supports the controller by providing advice and monitoring compliance prior, during and after the incident.
Thank you for your attention!