**Workshop Title:** Revision of the EDPS Guidelines on personal data breaches

**Description:** The purpose of this workshop was to discuss with DPOs their experience with personal data breach handling and the EDPS Guidelines on personal data breach notification, with a goal to provide more specific guidelines and support in the future.

**Discussed topics:**

- EDPS experiences from the personal data breach handling process (differences in the way EUIs handle, assess and notify personal data breaches, differences in the cooperation of DPOs with IT management teams, different experiences with processors when it comes to personal data breach reporting).

- Areas in which guidelines will be introduced (e.g. High risk indicators based on categories of personal data and/or sensitive contexts; cases of unlikely risk to the data subjects (when there is not a need to notify); further elements to include in Data Breach Notifications (DBNs); clarifications for cases where the controller is not sure a personal data breach has taken place; examples of not usual cases).

- Expectations on EDPS feedback and proposals for statistics/publications.

(more details can be found in the presentation)

In both sessions, DPOs showed a common interest in receiving more clear and practical examples. The main common concerns were related to: when is there a need or not to notify (e.g: human error), when does the "deadline" of 72 hours start, how to understand when there is a risk/high risk; and what are the specific criteria to notify to data subjects.

**Main conclusions achieved:**

- There is need for a risk methodology to apply when assessing a personal data breach and there is also a need for specific criteria on when to notify (EDPS/data subjects). The EDPS approach for the moment is to provide criteria and examples, but the DPOs network could assist in developing such a methodology. In the meanwhile, methodologies of national authorities could be used.

- Sharing knowledge on personal data breaches could be enhanced by creating an anonymised database of personal data breaches notified to the EDPS.

- There is a need to create templates for quick handling of common personal data breach cases (criteria for assessment, mitigation measures, templates for the documentation of the incident), especially for cases that most likely would result in unlikely risks to the data subjects. Human error cases could be a good candidate for this.

- It was suggested to create a "whitelist" of data breaches that may lead to unlikely risk and to update it frequently.

- It was suggested that an Annex should be included in the "EDPS personal data breach notification guidelines" including/proposing the several mitigation measures for different personal data breach cases.

- There is need for further collaboration among DPOs. A form to exchange information on cases of personal data breaches could promote collaboration.

- There is need for guidance in personal data breach notifications in cases of joint-controllership.

- There is need for closer collaboration of DPOs with the IT management or security response teams in case of a personal data breach. For example, when there is a security incident, many times this is not considered as a personal data breach from IT colleagues.

- It was suggested (as a best practice) to give specific trainings on the topic (including theory and practice).

**Ways forward:**
DPOs are invited to provide the EDPS with suggestions on elements missing from the guidelines/areas where more support is needed (that were not discussed in the workshop) or concrete examples of unusual DBN cases to consider in the guidelines.
Proposals to be sent **by 18 June 2021 EOB**, via email to:
DATA-BREACH-NOTIFICATION@edps.europa.eu