Procedure for review of disclosure risk in data

Purpose

It is crucial that data containing disclosure information is identified and handled properly to avoid this type of data being stored in the systems where data is freely available to the public.

This procedure describes how to identify disclosure risk in data and what measures to take to avoid storing disclosure data in inappropriate databases and systems at NMD.

Target group and Responsibility

Data managers responsible for receiving, handling and storing data at NMD.

Definitions

Data managers are employees at NMD, who receives and loads data to different databases and storage systems at IMR.

Private, confidential, or otherwise legally protected information (e. g., personal identifiable information) is regarded as disclosure data and must be identified.

Legally requirements for storage of disclosure data are those stated by Datatilsynet.

Description

The following stepwise procedure must be followed to review disclosure risk in data at NMD.

1. The data is delivered at NMD.
2. The data is classified by a Data manager either as IMR cruise data or other type. If the data is classified as IMR cruise data and it is not regarded as sensitive data (see procedure for sensitive data at IMR) it is not necessary to follow this procedure to review disclosure risk in data, because the IMR cruise data does not contain any private, confidential or otherwise legally protected information.
3. If the data is not IMR cruise data or sensitive data, the Data manager opens and reviews the files. To determine if the data contains disclosure information the Data manager visually inspects the files and looks for private, confidential or otherwise legally protected information. Such information could be any of the following types of information:
   - Name
   - Personal address
   - Date of birth
   - Telephone number
   - Email address
   - Dates directly related to individuals
   - Social security number
   - Bank account number
   - Certificate/license number
   - Vehicle identification/serial number
   - Device identification/serial number
   - Credit card number

    - Full face photographs and comparable images
    - IP address
    - URL

4. If disclosure data is discovered, the Data manager must work with the author to either
    a. Remove or obscure the disclosure information from the data, or
    b. Decide and agree on where to store the disclosure data to meet legally requirements for data storage of data with disclosure information.
5. Based on the step above one of the following must be done:
    a. If disclosure information in the data was successfully removed, the data is accepted and stored at NMD as ordinary data.
    b. If the disclosure data could not be removed and it is decided not to keep the data at NMD, the data is rejected by NMD and the files are securely removed from NMD’s systems.
    c. If it is decided to keep the data at NMD with the disclosure information the data is stored in appropriate systems for data with disclosure information.
6. The submission of the data is finalized by the Data manager through digital preservation steps and the creation of custom metadata for access, discovery and reuse (with restriction on disclosure data).

Kryssreferanser

Eksterne referanser