Knowledge Hub on International Criminal Law: Protection of personal data

I. Regulatory framework

- Constitution of Ukraine.
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.
- Law of Ukraine "On Information"
- Law of Ukraine "On Access to Court Decisions".
- Law of Ukraine "On Access to Public Information".
- Law of Ukraine "On the Protection of Personal Data".
- Code of Judicial Ethics.

II. Terms

De-identification of personal data: removal of information that allows direct or indirect identification of a person. Types of de-identification include: **concealment, partial removal, pseudonymisation, data synthesis, data combination.**

- **Concealment** is the removal of direct information that identifies a person (e.g., name, address).
- **Partial removal** is the removal of some of the data that identifies a person (e.g., name and address) but retains other data (e.g., date of birth, gender).
- **Pseudonymisation** is the replacement of personal data with pseudonyms or coded references that allow information to be linked to a specific individual without naming them.
- **Data synthesis** is the mixing of data elements or the creation of new ones that retain meaningful data but without reference to specific individuals.
- **Data aggregation** is the replacement of exact values with general ones (e.g., replacing date of birth with age or years, addresses with regions).

Restricted access information is: 1) confidential information; 2) secret information; 3) official information.

Personal data processing is any action or set of actions, such as collection, registration, accumulation, storage, adaptation, modification, renewal, use and dissemination (distribution, sale, transfer), depersonalisation, destruction of personal data, including using information (automated) systems.

Personal data is information or a set of information about a natural person who is identified or can be specifically identified.

III. Information that is not subject to disclosure

1. **Personal data about a natural person:**
   - racial or ethnic origin;
   - political, religious or philosophical beliefs;
   - membership in political parties and trade unions;
   - criminal convictions;

- health status, sex life;
- biometric or genetic data.

2. Information that has become known as a result of criminal proceedings:

- place of residence or stay of individuals, including addresses, telephone numbers or other means of communication, email addresses, taxpayer identification numbers, details of identity documents, unique numbers in the Unified State Demographic Register;
- registration numbers of vehicles;
- bank account numbers, payment card numbers;
- information that makes it possible to identify a natural person;
- photographs of individuals or video recordings featuring individuals.

3. Information that makes it possible to identify a criminal case:

- unique number of the criminal proceeding in the Unified Register of Pre-trial Investigations;
- unique number of the criminal proceedings assigned by the Unified Judicial Information and Communication System;
- information that makes it possible to identify other participants in criminal proceedings;
- information with restricted access.

IV. Measures to anonymise information.

Measures to anonymise information are carried out by the portal user in accordance with the criteria for the list of information that is not subject to disclosure, with independent determination of the risk of disclosure of confidential information.

V. Working with information.

The information provided by the requester should be limited to achieving specific, predetermined legitimate purposes of this portal.

The main objective of the privacy policy when working with information that has become known in connection with the consideration of a specific criminal proceeding is to **prevent leaking information that allows the identification of the specific court case in which the question was asked**. This may include the data mentioned above, as well as information about the factual circumstances of the case, such as the specific place of commission, the exact time, and the method, if it contains unique features.

Judges and other users who have the right to ask questions to experts must be informed of the rules on confidentiality, in particular that **they must remove all unnecessary or confidential information themselves when formulating questions**.

VI. Rule on disclosure of information.

The key rule is that confidential information cannot be made public, so before publishing summaries of answers to questions, they shall be carefully reviewed.

At the same time, certain information may be important for the correct assessment of circumstances relevant to the case for example, the name of a city may indicate the proximity of events to the line of contact, etc.

However, this information should not be shared in any circumstances. In all cases, this type of confidential, identifying information, shall be replaced with letters or numbers. For example, City_X, which is located 3 km from the line of contact.

The recommended method of replacing information is to replace names with PERSON_X, other information with INFORMATION_X, and the settlement name with settlement X.

Facts should be abstracted to a higher level of generality.