# Chapter

# 13

# Personal Privacy and Data Protection

**Why it is important:** Civil Registration, Vital Statistics, and Identity Management Systems contain a wealth of personal information. Protection of this data from accidental and unauthorized access, loss, destruction, and tampering is critical for public confidence, as well as the efficient and effective functioning of these systems.

**Introduction**

Civil Registration, Vital Statistics, and Identity Management Systems contain a wealth of personal information. While privacy principles have always applied to personal data stored in paper-based civil registration, vital statistics and identity management systems, digitization of data has given rise to new concerns due to the volume of personal data collected, used and stored; the range of analytics involving personal data; the value and global availability of personal data; and threats to personal privacy from hacking and other unauthorized access and use. With the linking of national ID systems, many of which contain biometric information, to civil registration systems, the protection of personal data becomes even more crucial.

Due to these concerns, in recent years many countries and organizations have adopted data protection laws and principles. In 2013, the Organization for Economic Co-operation and Development (OECD) adopted *Privacy Guidelines*, which updated previous guidelines from 1980. These *Privacy Guidelines* are applicable to public and private data collectors. In April 2016, the European Union adopted the *General Data Protection Regulation* (*GDPR*), which came into force in May 2018 and applies to all public and private data collectors in EU member countries, including CRVSID systems. The World Bank and key partners developed *Principles on Identification for Sustainable Development*, centred around the themes of inclusion, design and governance, that frame their work on identification for development. Recognizing the need for protection of personal data, the UN adopted *Personal Data and Privacy Principles* in October 2018, which apply to all personal data stored or processed by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities.[1]

The *OSCE Privacy Guidelines*, *EU GDPR* and *UN Personal Data and Privacy Principles* have much in common; they contain similar broad data protection and personal privacy concepts. Ideally, a country has a general data protection law that embodies these concepts. If such a law exists, CRVSID legislation or the general data protection law should state how the provisions of a general data protection law specifically apply to records in the CRVSID systems; as the application of these concepts to public, legally mandated databases (such as CRVSID systems) may differ from private data collection systems and other government systems. If a general data protection law does not exist, CRVSID legislation should contain provisions that apply these concepts in a way that provides for the protection of personal information contained in CRVSID records while still allowing for authorized administrative uses.

Below are set forth the *UN Personal Data and Privacy Principles*, with an explanation on how they may be applied to CRVSID systems to ensure the protection and privacy of personal data, while still allowing CRVSID systems to function effectively and fulfill their intended purposes.

This chapter covers the following topics:

1. Fair and Legitimate Processing
2. Purpose Specification
3. Proportionality and Necessity
4. Retention
5. Accuracy
6. Confidentiality
7. Security
8. Transparency
9. Transfers
10. Accountability

[1] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 51-52, 498.

**UN Principles of Data Protection and Privacy**

### 1. Fair and Legitimate Processing

**Best Practice:** Fair and legitimate processing means that data should be processed in a fair manner, on the basis of consent by the person whose data is collected or based on established rules.

Civil registration and identity registration systems comply with the fair and legitimate processing principle when data is collected based upon established laws. These laws should specify the data to be collected and processed through civil registration and identity registration.[2] Note that the data fields to be collected are usually contained in forms authorized under the law, rather than the law themselves. This aligns with good practice.

Biometric should only be collected if authorized by law. For example, if an ID law authorizes collection of biographical data, but the ID system now collects biometric data without the law being amended to authorize this, this practice would violate the fair and legitimate use principle.

**Guidance:** Describe whether data during civil registration and identity registration is collected based on established law or rules. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

**a. Does the collection of civil registration and identity data comply with the fair and legitimate processing principle?** In other words, is the data collected based on established law or rules?

Citations:

Comments:

### 2. Purpose Specification

**Best practice:** The purpose specification principle requires that data be processed only for its specified purpose.

To comply with the purpose specification principle, legislation should clearly define the purposes for which the data will be used, such as legal, statistical, and administrative purposes. The law should be written broadly enough to cover all legitimate purposes for which data is used. Use of data beyond these purposes violates the purpose specification principle.

**Guidance:** Describe whether laws that govern civil registration and identity registration clearly specify the purpose for which data is processed. In the comments section, note whether the use of data in practice goes beyond those purposes specified in law.

**a. Do the civil and identity registration laws clearly specify the purpose for which the data will be used?** Is the data used for any purposes other than those specified?

Citations:

Comments:

### 3. Proportionality and Necessity

[2] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 501.

**Best Practice:** The principle of proportionality and necessity requires that processing of personal data be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal data processing.

A wide array of information is collected during registration of vital events in order to carry out the legal, statistical and administrative functions of civil registration. The legal information is stored and maintained in the civil register, and this information should be limited to that which is necessary for the legal functions of civil registration. In other words, the civil register should contain basic information regarding the vital event and the persons concerned. As discussed in the Vital Statistics Chapter, Section 6, a much larger amount of information is collected for the generation of vital statistics. This information is sent anonymized to the statistics agency and should not be stored in the civil register.

For identity credential registration, the information collected should be kept to the minimum needed to register, validate and authenticate an identity - for example, name, limited biographical information, and any biometrics (if authorized for by law).[3]

**Guidance:** Answer the questions below regarding whether data collected and stored for civil registration and identity registration aligns with the principle of proportionality and necessity. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

**a. Is the data collected and stored in the civil register limited to only the information needed for legal purposes?**

Citations:

Comments:

**b. Is the data collected during identity registration limited to only that which is relevant and necessary for identity registration, validation, and authentication purposes?**

Citations:

Comments:

### 4. Retention

**Best Practice:** The retention principle requires that data be retained only for the time that is necessary for the specified purposes.

It is best practice to maintain civil registration and identity registration records (including records in the population register) permanently, even after a person's death, as this is necessary for the legal purposes of civil and identity registration. Therefore, law should authorize the permanent archiving and retention of these records. This aligns with the retention principle.

**Guidance:** Describe whether the laws that govern civil registration and identity registration authorize the permanent retention of records. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

[3] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 503.

a. **Do civil registration and identity registration laws authorize the permanent retention of records?**

Citations:

Comments:

## 5. Accuracy

**Best practice:** The accuracy principle requires that data be accurate and, where necessary, up to date to fulfill the specified purposes.

This principle requires that laws permit individuals to correct or or amend their personal data in civil registration and identity registration records through authorized processes. These processes should be easy to access and swift and efficient, as this enables records to be kept up to date and accurate. Accordingly, laws should establish administrative process, rather than court processes, to the extent possible (See Chapter 3, Section 12, on corrections and amendments).

**Guidance:** Describe whether the laws that govern civil registration and identity registration allow for efficient and swift correction and amendment of personal data. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

a. **Do civil registration laws allow for efficient and swift correction or amendment of personal data?**

Citations:

Comments:

b. **Do identity registration laws allow for efficient and swift correction or amendment of personal data?**

Citations:

Comments:

## 6. Confidentiality

**Best practice:** The confidentiality principle requires that data be processed with due regard for confidentiality.

Civil and identity registrars should be required, by law, to protect the confidentiality of personal data. In addition, for civil registration, only those with a legitimate interest should be permitted to obtain vital event certificates or certified extracts of civil registration records. Further, identity credentials should not contain on their face, or digitally embedded, any confidential information in a manner that permits persons without a legitimate interest to access this information.

**Guidance:** Answer the questions below. In the comments section, describe whether the law aligns with best practice and note any recommendations for regulatory reform.

**a. Are civil and identity registrars required, by law to protect the confidentiality of personal data?**

Citations:

Comments:

## 7. Security

**Best practice:** The security principle requires that appropriate organizational, administrative, physical and technical safeguards and procedures be implemented to protect the security of personal data, including against or from unauthorized or accidental access, damage, loss or other risks presented by data processing.

Different categories of government officials and non-government persons –including civil registration, identity management and other government officials; vendors, contractors and independent researchers; and private institutional users - have diverse needs for access and use of data from CRVSID systems. Laws (including SOPs) should allow for the legitimate use of data to meet government needs while protecting the security of that data.[4]

*Government Officials*: To protect against unauthorized or accidental access by government officials – including civil and identity registrars and others - procedures should be put in place, or the system should be designed, to limit access to only the data necessary for the specific function or task in question.[5] To ensure that only authorized personnel access data, some systems are designed in such a manner as to automatically and continuously keep a log of personnel that access records.[6] This helps ensure that the policies put in place are complied with.

*Independent researchers:* In some instances, academic or independent researchers may request access to civil registration or other data for legitimate research purposes. Any data transferred to independent researchers should have identifying information removed and the use of the data should be subject to a user agreement on confidentiality.[7]

*Contractors and Vendors:* Civil registration and identity management agencies may have need to contract with technology firms and other vendors to carry out specific functions of the system. Vendors' and contractors' access to data should be limited to only that which is essential to carry out the task required. In addition, access should be subject to a contract between the government agency and the vendor that sets out what data may be accessed, how it may be accessed and processed, and limiting the ability of the vendor/contract to store and retain that data.[8]

[4] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 507.
[5] *Handbook on Civil Registration and Vital Statistics Systems: Management, Operation, Maintenance, Revision 1*, paragraph 485 - 488.
[6] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 513.
[7] *Principles and Recommendations for a Vital Statistics System, Revision 3,* United Nations Publication, Sales No.E.13.XVII.10, United Nations, 2014, paragraphs 269, 299.
[8] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 511.

*Private Institutions*: Private institutions, such as banks, private hospitals, and others, may use the identity management system for authentication of individuals. The means for authenticating an identity should ensure that the private institution does not have the ability to collect and store identity data, but has only the ability to authenticate the identity of the individual at the time of request.[9]

*Transmission and Storage:* Data is particularly vulnerable during transmission (including linking) and therefore measures, such as end-to-end encryption, should be put in place to safeguard data during transmission.[10] To ensure against accidental loss of data during storage and archiving, there should be protocols for maintenance and backup systems.[11]

**Guidance:** Answer the questions below. In the comments section, analyze whether the law and procedures in place align with best practice and note any recommendations for reform.

---

**a. For government officials, is access to personal data restricted to only that which is necessary for the specific task in question?** Are access logs kept?

Citation:

Comments:

**b. For independent researchers, is data anonymized and subject to user and confidentiality agreements?**

Citation:

Comments:

**c. For contractors and vendors, is data access limited to only that which is necessary for the specified task and subject to user and confidentiality agreements?**

Citation:

Comments:

**d. For private institutions using identity authentication services, are systems designed to prevent the collection and storage of identity data?**

Citation:

Comments:

---

[9] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 512.
[10] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 515.
[11] *Handbook on Civil Registration and Vital Statistics Systems: Management, Operation, Maintenance, Revision 1*, 2018, paragraph 251.

e. **Describe measure to protect data during transmission and storage,** including encryption, back-up and storage, if known.

Citation:

Comments:

## 8. Transparency

**Best practice:** Processing of personal data should be carried out with transparency to the data subjects.

All persons have a right to know how their civil registration and identity data is collected, used, stored and shared. To help ensure transparency of personal data processing, the law should allow for administrative complaints and judicial appeals of decisions by government officials that infringe upon transparency.[12]

**Guidance:** Describe procedures that allow a challenge to any registrar's decision regarding personal data. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

a. **Describe any procedures that allow for administrative complaints and judicial appeal of decisions by civil registration and identity registration officials.**

Citation:

Comments:

## 9. Transfers

**Best practice:** The transfer principle mandates that data may be transferred to a third party only if the data collector satisfies itself that the third party affords appropriate protection for the personal data.

This principle has implications for cross-border data sharing of data, such as data sharing between national registrars, which is helpful in keeping civil registers, identity registers and population registers up to date. Legislation should mandate that CRVSID systems may share data with another country if that country provides for an adequate level of data protection. If a country is not deemed to have adequate data protection laws, the data should only be shared subject to appropriate safeguards, such as an enforceable confidentiality and data protection agreement.

This transfer principle may also have implications for data transfers within a country if other government agencies, or non-governmental or private sector entities, are not subject to the same data protection rules as the CRVSID system. This may be the case if a country does not have a general data protection law. In that case, the CRVSID laws should require that civil registration and identity management records may

[12] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 519-520.

be shared with other government agencies only subject to an enforceable confidentiality and data protection agreement.[13]

**Guidance:** Describe any laws, policies or rules that set standards regarding to whom data may be transferred and note whether these standards require transferees to have adequate data protection policies. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

**a. Describe data transfer policies, included rules requiring transferees to have adequate personal data protection policies in place.**

Citation:

Comments:

**10. Accountability**

**Best practice:** The accountability principle requires entities that collect data to have adequate policies and mechanisms in place to adhere to all of the above principles. To comply with the accountability principle, CRVSID systems should be subject to general data protection laws that reflect the above principles, or CRVSID laws themselves should reflect these principles. In addition, providing for sanctions and penalties for a breach of data protection principles ensures registrars and other government and non-governmental entities and persons are held accountable for compliance.[14]

**Guidance:** Describe any penalties or sanctions imposed on civil and identity registrars and others for breaching personal privacy and data security requirements. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

**a. Describe any penalties or sanctions imposed on civil and identity registrars for breaching personal privacy and data security requirements.**

Citation:

Comments:

[13] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 521.
[14] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 520, 522.