Chapter

10

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.

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. Generally, processing of data is lawful if it is by consent or pursuant to a legal obligation. To comply with the "fair and legitimate processing" principle, CRVSID legislation or regulations should specify the data to be collected and processed through civil registration and identity registration, so that the data to be collected is collected subject to the law.[2]

Guidance: Describe whether the laws that govern civil registration and identity registration (if applicable) clearly specify the data to be collected and processed. Explain whether in practice, this data and only this

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

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

data is collected. Note that the law does not need to detail every data element contained in civil registration forms or ID registration forms. However, it should set out the type of data to be collected; e.g., biographical information, information regarding characteristics of vital events, or biometric data (in the case of ID). If an ID law authorizes collection of biographical data, for example, but ID systems now collect biometric data without the law being amended to reflect this, this practice would violate the fair and legitimate use principle. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

_____

a. Does the law comply with the fair and legitimate processing principle? I.e., does it specify the type of data to be collected and processed?

Citation:

Comments:

2. Purpose Specification

Best practice: The purpose specification principle requires that data be processed only for its specified purpose. Legislation should clearly define the purposes - legal, statistical, administrative and other research purposes - for which the data will be used. This serves to notify the population of the purposes and uses of the data collected, in line with the purpose specification principle. If data is to be used for other purposes in the future, laws should be promulgated or amended to reflect these uses.[3]

Guidance: Describe whether the laws that govern civil registration and identity registration (if applicable) clearly specify the purpose for which data is processed. The law should be written broadly enough to cover all legitimate purposes for which data is used. For example, if civil registration or vital statistics micro-data is allowed to be used by private researchers, the law should state that data may be used for private research purposes (subject to privacy laws and confidentiality agreements) as well as government legal, statistical and administrative purposes. Note that this type of data should never be used for commercial purposes. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

_____

a. Does the law comply with the purpose specification principle? I.e., does it specify the purpose for which data is collected and processed?

Citation:

Comments:

[3] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 502.

3. Proportionality and Necessity

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. While a wide array of information is collected during registration of vital events, this information is necessary in order to carry out the legal, statistical and administrative functions of civil registration. Therefore, the collection of this information complies with the principle of proportionality and necessity. For identity registration, experts recommend that information collected for purposes of an identity credential be kept to the minimum needed to register, validate and authenticate an identity - for example, name, limited biographical information, and any biometrics (if provided for by law).[4]

Guidance: Describe whether the laws that govern civil registration, vital statistics, and identity registration (if applicable) meet the proportionality and necessity principle; i.e. is the data that is collected limited to what is relevant and adequate for the specified purpose (see principle 2). Generally, a wide variety of data may be collected for CRVS purposes, but only limited data may be collected for ID purposes. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

_____

a. Does the law comply with the proportionality and necessity principle? I.e. is the data collected limited to what is relevant and adequate for the specified purpose?

Citation:

Comments:

4. Retention

Best Practice: The retention principle requires that data be retained only for the time that is necessary for the specified purposes. Civil registration, vital statistics, and identity records (including population registers) are, by law, permanently maintained, even after a person's death. Therefore, the retention principle permits permanent retention of civil registration, vital statistics, and identity records. The retention principle is closely related to "the right to be forgotten"; a right contained in some countries' data protection laws. This concept maintains that a person has a right to erasure of their personal data if the data is no longer needed. However, this right generally does not apply where there is a legal obligation to retain the data, such as with CRVSID systems. Accordingly, countries do not delete civil registration, vital statistics, and identity records. They are kept and archived permanently.[5]

Guidance: Describe whether the laws that govern civil registration, vital statistics and identity registration (if applicable) meet the retention principle. For civil registration, vital statistics, and identity systems, data should be permanently maintained and archived after a person is deceased. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

---

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

[5] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 504.

a. Does the law comply with the retention principle?

Citation:

Comments:

5. Accuracy

Best practice: The accuracy principle requires that data be accurate and, where necessary, up to date to fulfill the specified purposes. The continuous and permanent nature of civil registration and identity management helps ensure that personal data is accurate, complete and kept up to date, in line with this principle.[6]

Guidance: Describe whether the laws that govern civil registration and identity registration (if applicable) meet the accuracy principle; i.e., is personal information in these systems kept accurate and up to date. This could mean, for example, that a person's death registration is linked to their birth registration, and that a person's divorce registration is linked to their marriage registration, so that individuals' records are up to date and accurate. This principle also requires that if a person contests any data in their record as inaccurate, there is a means to verify and correct that data. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

a. Does the law comply with the accuracy principle? Are personal records kept up-to-date and accurate?

Citation:

Comments:

6. Confidentiality

Best practice: The confidentiality principle requires that data be processed with due regard for confidentiality. This principle is closely related to the "security principle" below, and confidentiality partly is maintained by complying with the security principle. In addition, confidentiality of civil registration data is maintained by permitting only persons with a legitimate interest to obtain vital event certificates or certified extracts of civil registration records. Identity management officials should also ensure that identity credentials do 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. Legislation should also define what information in the population register is available to the public. When information is shared with the statistics authority, procedures should provide for confidentiality while not causing excessive barriers to data linkage for verification purposes and research activities in the public interest. For example, procedures may require that individual records be anonymized, except perhaps for any

[6] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 505.

unique identification code used for data verification and cleaning purposes, before submission to the statistics agency.[7]

Guidance: Describe whether civil registration, vital statistics, and identity management data are collected, processed, transferred, stored and maintained in line with the confidentiality principle? Note whether: 1) only persons with a legitimate interest may obtain vital event certificates, 2) whether identity credential contain on their face, or digitally embedded, any confidential data that could be seen or accessed by unauthorized persons, 3) whether the law specifies what information is public, and 4) whether confidentiality procedures are followed when transferring data to statistics authorities. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

_____

a. Does the law comply with the confidentiality principle?

Citation:

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 have diverse needs for access and use of data from CRVSID systems. In keeping with the "security" principle, legislation should address the diverse needs for all those who may be able to access the records, in order to prevent unauthorized or accidental access. This includes civil registration and identity management officials, vital statistics officials and independent researchers, other government officials, vendors and contractors, and non-governmental and private institutional users.[8] The different users are discussed individually below.

7A. Access by civil registration and identity management officials

Best practice: The law should allow access to vital event and identity records for official legal, administrative and statistical purposes only. Access to civil registration and identity records should be limited to only the necessary officials. Regulations or instructions should establish a hierarchy for allowing different levels of access to the records, limiting this access to only that which is necessary for the specific legal, authorized administrative or statistical purpose in question.[9]

Guidance: Describe whether the law or internal operating procedures limit access to civil registration and identity records to only the necessary officials and for only official legal, administrative and statistical purposes. Describe whether laws or procedures establish a hierarchy allowing different levels of access. In

---

[7] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 506.

[8] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 507.

[9] *Handbook on Civil Registration and Vital Statistics Systems: Management, Operation, Maintenance, Revision 1*, United Nations Publication, Sales No. XXX, 2018, paragraph 485 - 488.

the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

---

a. Is access to civil registration and identity records restricted to only necessary officials? For only legitimate legal, administrative and statistical purposes? Is a hierarchy of officials established?

Citation:

Comments:

7B. Access by national statistics authority officials and independent researchers

Best practice: Individual records submitted from the civil registration agency to the statistics agency should be submitted with identifying information, such as name removed. While in some countries a unique identifying number may be available to statisticians, this only so that errors and inconsistencies can be identified in the processing, editing and aggregating of records; procedures should be in place to prevent the identification of individuals. This prevents unauthorized access to personal information and ensures that statistical data is used for its intended purpose. Access to civil registration records may be provided to certain users, such as academic and independent researchers, for legitimate research purposes. However, access to individual records (micro-data) should be subject to a user agreement on confidentiality and the use of data between the statistical agency and users (See Section 9, Transfers Principle). Identifying information should be removed from the file to protect the privacy of individuals.[10]

Guidance: Describe how national statisticians have access to civil registration data and whether that data is anonymized? Describe any arrangements for providing micro-data to outside researchers. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

---

a. Describe access to civil registration data by national statisticians:

Citation:

Comments:

b. Describe access to civil registration data by independent researchers:

Citation:

Comments:

[10] *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.

7C. Access by other government officials

Best practice: Other government agencies - such as health, social services, planning departments, and law enforcement - may have a need to access civil registration and identity records. Regulations or instructions should establish procedures for sharing of records or data with other government agencies for official government purposes, and should provide that any disclosure of information that might identify a person has been specifically authorized by law or consent.[11] As with access by civil registration and identity officials, access should be permitted only to the extent necessary for the specific administrative purpose and levels of access should be established.[12]

Guidance: Describe the procedure and rules regulating sharing of civil registration and identity records with other government officials. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

_____

a. Procedures for access to civil registration and identity records by other government officials:

Citation:

Comments:

7D. Access by vendors and contractors

Best practice: 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. For example, the identity management agency may contract with a vendor to provide authentication services, including point-of-service equipment and platform software; or enrolment in the program might be sub-contracted to a variety of entities, as with India's Aadhar system. Vendors' and contractors' access to data should be limited to only that which is essential to carry out the task required. Contracts between the government agency and vendor should contain provisions that explicitly set out what data may be accessed, how it may be accessed and used, and limit the ability of the vendor/contract to store and retain that data to only that which is necessary for the specified task. As with government officials, contractors should have protocols that establish a hierarchy of levels of access.[13]

Guidance: Describe law, rules and procedures that regulate access by vendors and contractors to civil registration and identity records. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

_____

a. Access by vendors and contracts to civil registration and identity records:

---

11 *Principles and Recommendations for a Vital Statistics System, Revision 3,* United Nations Publication, Sales No.E.13.XVII.10, United Nations, 2014, paragraph 417.

12 United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 510.

13 United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 511.

Citation:

Comments:

7E. Access by non-governmental and private institutional users

Best practice: 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 authentication the individual at the time of request.[14]

Guidance: Describe the procedures used by non-governmental and private institutions for authentication of identity of individuals. Note whether those entities have the ability to access or store the data. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

_____

a. Access by non-government and private institutional users

Citation:

Comments:

7F. Tracking and Monitoring Access

Best Practice: To ensure that only authorized personnel access data, some countries have a system to monitor and track system users who access records. These systems are designed in such a manner as to automatically and continuously keep a log of personnel that access records.[15] This helps ensure that the policies put in place to address 7A - 7E are complied with.

Guidance: Describe whether a tracking and monitoring system is in place, if known. Note that this type of requirement is generally found in operating procedures rather than law. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

_____

a. Describe any tracking and monitoring procedures:

Citation:

Comments:

[14] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 512.

[15] United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 513.

7G. Protection of data during transmission and linking

Best practice: Data is particularly vulnerable during transmission and therefore measures should be put in place to safeguard data during transmission. Specific processes to protect data will differ for manual and digital systems. For manual systems, records should be physically protected from tampering and improper access and use when being transferred from local registrars to the central authority. Where registration records are transmitted electronically, end-to-end encryption should be used.[16]

Special consideration should be given to issues of privacy and security when record linking is used, as linking may provide opportunities for inadvertent and inappropriate disclosures.[17] If record linking is employed, regulations should address how access to information and data elements will be limited to only those officials with authorization and need to access that information.

Guidance: Describe measures that are in place to protect data during manual and/or electronic submission, sharing and/or linking of data. Note that these measures are likely contained in operating procedures, not laws. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

---

a. Measures to protect data during submission, sharing, and linking, if known:

Citation:

Comments:

7H. Protection of data from loss and destruction

Best Practice: Protection of data from loss and destruction during storage and archiving requires protocols for maintenance and backup systems. For digital civil registration and identity management systems (including a population register), procedures for storing and preserving records rely on current general practices for maintenance and backup. A common approach consists of having two servers simultaneously online and mirroring each other so that each interaction and input of a new record is recorded on both. Another common practice is to have daily backups from the main server maintaining the database/population register, thus ensuring the preservation of records. Frequently, the mirror or backup server is located in a different geographical area, even a different country, as a risk mitigation strategy. If this course of action is taken, data protection measures for the mirror server must be taken, particularly if the service is outsourced to a private company or the mirror server located abroad.[18]

---

16 United Nations, Guidelines for the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems, New York, 2019, Para. 515.

17 *Principles and Recommendations for a Vital Statistics System, Revision 3,* United Nations Publication, Sales No.E.13.XVII.10, United Nations, 2014, paragraph 425.

18 *Handbook on Civil Registration and Vital Statistics Systems: Management, Operation, Maintenance, Revision 1*, United Nations Publication, Sales No. XXX, 2018, paragraph 251.

Guidance: Describe measures that are in place to protect data from loss and destruction. Note that these measures are likely contained in operating procedures, not laws. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

---

a. Measures to protect against data loss and destruction:

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. All persons also have a right to correct and modify their own civil registration and identity records, subject to proper documentary or other evidentiary proof, and challenge improper use of data, in accordance with provisions of the law. Provisions in the law that address amendments and corrections of vital events records and identity documents, as well as provisions that allow for administrative and judicial appeal processes help ensure transparency rights.[19]

Guidance: Describe measures that are in place that help ensure transparency of data processing, including the ability of an individual to access, correct, and modify their civil registration and identity registration records, subject to proper procedures, as well as challenge any decisions in administrative or judicial proceedings. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

---

a. Describe procedures that allow for access, correction or modification of one's civil registration and identity records:

Citation

Comments:

b. Describe the process to challenge registrar decisions, including through administrative and judicial proceedings:

Citation:

Comments:

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

9. Transfers

Best practice: This 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 systems. This may be the case if a country does not have a general data protection law. In that case, CRVSID legislation should require that civil registration, vital statistic, and identity management records may be shared with other government agencies only subject to an enforceable confidentiality and data protection agreement.[20]

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. Data transfer policies, included rules requiring transferees to have adequate personal data protection policies:

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.[21]

Guidance: Describe any penalties or sanctions imposed for a violation of any of the above principles. In the comments section, describe whether the law aligns with good practice and note any recommendations for regulatory reform.

---

a. Penalties and sanctions:

---

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

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

Citation:

Comments: