Economic and Social Commission for Asia and the Pacific
Second Ministerial Conference on Civil Registration and Vital Statistics in Asia and the Pacific
Bangkok and online, 16–19 November 2021
Items 7 and 11 of the provisional agenda*

The relationship between civil registration, identity management and vital statistics, and their role in ensuring legal identity in Asia and the Pacific
The importance of civil registration and vital statistics and legal identity for all to accelerate progress on the 2030 Agenda

Privacy and confidentiality in the context of civil registration and vital statistics systems**

Summary

The present information document provides an overview of privacy and data confidentiality issues as they occur in the context of civil registration and vital statistics practice. Furthermore, the document reviews current international standards and presents principles and emerging practices for countries and development partners to consider as they embark on strategies for incorporating privacy and data confidentiality measures into the continued development of civil registration and vital statistics systems.

The document also suggests options to be taken into consideration by countries as they work to implement the recommendations of the Regional Action Framework on Civil Registration and Vital Statistics in Asia and the Pacific.
I. Introduction

1. The phrase ‘right to privacy’ generally denotes the fundamental right of individuals to create boundaries limiting access to their person, communications or personal information, including data protection. Confidentiality, on the other hand, generally refers to the ethical guidelines responsible authorities should follow when collecting personal information, as well as how that information should be treated while in their possession.

2. Technology with its ever-increasing abilities to transmit data, as well as invade privacy, is entangled with personal choices in new and challenging ways. It is therefore important for agencies and ministries tasked with collecting personal information to adhere to and emphasize data confidentiality rules and guidelines to complement personal privacy choices and protect the information collected.

3. The coronavirus disease (COVID-19) pandemic highlights the importance of collecting highly sensitive personal information with new mechanisms for health tracking and reporting implemented. Many public health officials have acknowledged “the collection, use, sharing and further processing of data can help limit the spread of the virus and aid in accelerating the recovery, especially through digital contact tracing”, underscoring the heightening significance of data protection and privacy in this crisis.

4. When an individual decides to disclose personal information, data confidentiality should be the next logical step in securing individual rights and minimizing potential harm from abuse of personal information. Moreover, this shifts the burden from the individual to the entity managing the personal data.

II. Background

5. The purpose of civil registration is to collect and record personal information pertaining to vital events, which in turn, will be used to generate the legal documents necessary for establishing a person’s legal identity. Many of the privacy concerns at this point revolve specifically around “personal privacy”; i.e., the limits on accessing personal information. Questions typically include: who is entitled to collect personal information (either the agency itself or specific workers within the agency); what type of personal information should be collected for the specific purpose of the agency; and what are the privacy policies and other related guidance within the United Nations Organization and other selected bodies of the international development community.

---


3 United Nations Development Programme (UNDP), Data protection and privacy policies and other related guidance within the United Nations Organization and other selected bodies of the international development community (2021).

4 Ibid.


6 UNDP, Data protection and privacy policies and other related guidance within the United Nations Organization and other selected bodies of the international development community.
least invasive methods for securing only the information necessary for adequate record keeping and generating legal documents?

6. Recommendations from the United Nations Statistics Division stress there is also a need to protect the privacy of individuals and their families when issuing certificates. Requests for certificates of birth, death or other vital events should be granted only to interested parties – such as the registrant, a spouse, parent, or child of the registrant, or next of kin – or their legal representatives. Legislation should clearly define an ‘interested party’ for purposes of requesting a certificate.

7. To further protect privacy, certificates need not include some or all the statistical information captured in the civil register about a particular vital event. For example, a death certificate need not include information on causes of death, which can be sensitive information, especially if the death is due to a stigmatized cause. Similarly, a birth certificate need not include information on the marital status of the parents. While some of the information related to birth or death registration may be in the public domain, such as full name, name of parents, sex, and place and date of birth or death, additional information provided, such as that related to paternity and wedlock, may be sensitive and disclosure to the wrong person could violate the right to privacy. Only the immediate family, spouses, heirs, or their legal representatives, and third parties with a legitimate interest, should have access to such sensitive information. Government agencies may also require such information for legitimate purposes. The local registrar should have authority to determine the legitimacy of requests for information not in the public domain, in accordance with guidelines issued by the national registrar.\(^7\)

8. Subsequently, the purpose of vital statistics is to aggregate the collected data, analyse the data to identify trends, including population and health trends, and publish the analysis to inform policy and programmatic development. To do so, the national registrar must be required to share vital event registration data with the national statistics authority on a timely basis. This data sharing must be conducted in accordance with law to protect personal privacy and the security of data.\(^8\)

9. At this stage, privacy concerns focus on data confidentiality issues such as the transfer, storage and dissemination of information. Pertinent questions may include: which policies or standards govern data transfer and how do they apply to various types of data; who is responsible for data storage, the collector or the recipient; and finally, how can the data be publicized or disseminated to achieve stated policy goals without violating data confidentiality?

10. The answers matter because not only are they important for protecting privacy, but crucially, because confidentiality provisions in legislation and their implementing regulations should not be so rigid as to exclude the use of vital event registration records for properly authorized research purposes, or to inhibit the application of modern statistical approaches such as data linkage and small area analyses. Confidentiality provisions should be drafted to ensure records can be used for such purposes without publicly disclosing the identity and characteristics of the parties involved.\(^9\) Further, while privacy protections

---


\(^8\) Ibid.

\(^9\) Ibid.
must apply to the entire system, they must also provide specificity enough for
governing different procedures, as well as the overlapping, or sometimes even
discordant, operational purposes of various agencies or ministries.

III. Key international principles and guidelines

11. At the national level, local laws and regional agreements provide
theoretical and operational frameworks for implementing privacy and personal
data protection standards. However, there are several relevant international
principles and guidelines to help inform the national processes.

12. The United Nations has set out a basic framework, the Principles on
Personal Data Protection and Privacy, for the processing of personal data by,
or on behalf of, the United Nations System Organizations in carrying out their
mandated activities which are also relevant to personal data collected by
Governments. These Principles aim to: (a) harmonize standards for the
protection of personal data across the United Nations System; (b) facilitate the
accountable processing of personal data; and (c) ensure respect for the human
rights and fundamental freedoms of individuals, in particular the right to
privacy. These Principles apply to personal data, contained in any form, and
processed in any manner.10

13. The Principles include the following relevant points in regard to the
discussions in the present document:

    (a) Fair and legitimate processing. Personal data should be
        processed in a fair manner and with either the consent of the data subject and/or
        in the best interests of the data subject;

    (b) Purpose specification. Personal data should be processed for
        specified purposes and consider the balancing of relevant rights, freedoms and
        interests. Personal data should not be processed in ways that are incompatible
        with such purposes;

    (c) Proportionality and necessity. The processing of personal data
        should be relevant, limited and adequate to what is necessary in relation to the
        specified purposes of personal data processing;

    (d) Retention. Personal data should only be retained for the time that
        is necessary for the specified purposes;

    (e) Accuracy. Personal data should be accurate and, where
        necessary, up to date to fulfil the specified purposes;

    (f) Confidentiality. Personal data should be processed with due
        regard to confidentiality;

    (g) Security. Appropriate organizational, administrative, physical
        and technical safeguards and procedures should 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;

    (h) Transparency. Processing of personal data should be carried out
        with transparency to the data subjects, as appropriate and whenever possible.

10 See www.unsceb.org/sites/default/files/imported_files/UN-Principles-on-Personal-
Data-Protection-Privacy-2018_0.pdf.
14. These Principles are at the core of most international guidelines on data privacy, as far back as the General Assembly Resolution 45/95 on Guidelines for the Regulation of Computerized Personal Data Files,¹¹ and should be applied to civil registration and vital statistics systems and legal identity systems.

15. The Fundamental Principles of Official Statistics also iterates under Principle 6 that individual data collected by statistical agencies for statistical compilation, whether they refer to natural or legal persons, are to be strictly confidential and used exclusively for statistical purposes.¹²

16. The United Nations Statistics Division has further developed Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management Systems,¹³ which are intended to complement the Principles and Recommendations for Vital Statistics System, Revision 3.¹⁴ They offer a tool for developing a strong rights-based legal framework for civil registration, vital statistics and identity management systems. The legal framework is critical since it guarantees the privacy and security of records and gives the system an essential foundation to be able to operate successfully throughout the country. These Guidelines provide overarching principles as well as detailed elaboration on the legislative framework critical for implementing international recommendations, with a focus on ensuring a holistic, integrated approach to civil registration, vital statistics and identity management.

17. Finally, the United Nations Development Programme conducted a recent study “to review the current normative framework, as well as advisory and technical assistance activity, of the United Nations and other selected bodies within the international development community in support of data protection and privacy legislative and institutional governance frameworks”.¹⁵ The United Nations Development Programme study emphasizes key principles from subsidiary United Nations organizations, as well as non-United Nations institutions.

18. Digitization in particular has renewed attention on privacy and has fostered the issuance of standards to guide countries in the collection and use of personal data. The United Nations Roadmap for Digital Cooperation, published in 2020, acknowledges the potential a “good” digital identity can have for citizen’s empowerment, while warning of the privacy risks in case it is not properly managed.¹⁶

---

¹¹ See www.refworld.org/pdfid/3ddcafaac.pdf.
¹² See A/RES/68/261.
¹⁵ UNDP, Data protection and privacy policies and other related guidance within the United Nations Organization and other selected bodies of the international development community (2021).
19. The Economic Commission for Africa, for example, worked with the African Union Commission on a Digital Identity, Digital Trade and Digital Economy Initiative which contains “Principles of Digital ID”. The principles underline national digital identity implementations while affirming inclusive, secure and interoperable systems and providing a principled framework for developments. Many of the principles outlined emphasize foundations of previously drafted documents, especially from the Economic Commission for Africa Framework of Good Digital Identity. These principles cover inclusion to ensure no one is left behind, interoperability among member States with respect and recognition for different national systems, ownership of systems, the need to build security and safeguards into systems, and periodic and systematic assessments of quality to ensure accountability.

20. Some development partners involved in the digitization of civil registration and legal identity system have also issued guidance to help countries cross those steps. The Guidelines of the Identity for Development (ID4D) programme of the World Bank present Principles on Identification for Sustainable Development. Principle 3 relates to data protection and stands for establishing a robust—unique, secure, and accurate—identity. It is highlighted that the robustness of the identification system, including the uniqueness, accuracy, and security of individual identities, depends on quality of information collected during the registration, the frequency of updating, the strength of validation processes, and the procedures for storing and managing personal data.

21. Other guidelines address more specific concerns related to the privacy and confidentiality in civil registration and vital statistics systems. The United Nations Children’s Fund has published guidance on the use of biometrics in children-focused services to ensure both the privacy and security of children, as well as to prevent errors in systems conceived for adults which could lead to exclusion of children from certain services. Recommendations on the protection and use of health-related data were prepared by a taskforce under the United Nations special rapporteur on privacy, to serve as a common international baseline for minimum data protection standards. These recommendations function as a reference point in the ongoing debates, partly fuelled by scientific developments, about this highly sensitive topic, which includes civil registration and vital statistics data.

IV. Linkages with legal identity and identity management systems

22. Many of the same previous concerns related to civil registration also apply to identity management systems, although they may also relate further to biometric data. Indeed, the two systems are often integrated together.

23. As outlined by the World Bank, identification systems must be designed to prioritize and protect data and privacy as the default setting without requiring any additional special action on the part of an individual. Personal data, including any data that are linked or linkable to an individual, must be protected from improper use proactively and by default through a robust legal

---

18 Ibid.
19 Ibid.
20 Ibid.
21 Ibid.
and regulatory framework, system design, and the adoption of technical standards and operational controls.22

24. The World Bank goes on to further state that the design, policies, and technology used by identification systems should be in accordance with principles for data protection, including data minimization and proportionality, purpose specification, strict limits on data retention, data security, accountability, and transparency, among others. For example, identification systems should limit the collection and exposure of data—particularly sensitive personal information—including in credentials and the structure of identification numbers. Authentication protocols must disclose only the minimum data necessary to ensure appropriate levels of assurance.23

V. Digitization, new technologies and data integration

25. Since the inception of the Asia and Pacific Civil Registration and Vital Statistics Decade (2015–2024) in 2015, there has been significant progress made in digital identification, civil registration, and open government initiatives. For many countries in the region the persistent shift away from paper-based records, although necessary and inevitable, is likewise shifting the landscape of the security measures for data collection and storage.

26. This shift raises new concerns that some country-level agencies may be contemplating, for the first time, including restrictions on access to information for private companies, the use of new information technology, an increase in unlawful access, unethical targeted-marketing, data security, server storage and the release of information. Specialists and advocates for privacy and data protection must therefore be at the vanguard of this shifting landscape to inform the evolution of privacy and data confidentiality policies.

27. Countries have recognized the value of linking and integrating data across ministries for producing statistics as well as improving government processes. Building on this momentum, governments and stakeholders are presented with opportunities to use civil registration records and population registers for the issuance of universal identity documents and data sharing across governance departments in ways that are commonly referred to as ‘whole of government’ and ‘single window’ approaches. These opportunities can improve efficiency and better enable countries to utilize their resources to implement the 2030 Agenda for Sustainable Development.

28. Despite the benefits, the capacity to obtain personally identifying information from integrating previously separate databases also raises concerns. Further, security breaches in computer systems have inadvertently exposed valuable data to outside exploitation. Additionally, as is commonly seen in work at the policy level, unintended consequences have been identified, such as the use of biometric data to reinforce existing social and ethnic inequalities. These examples highlight the intersection of governmental policies, the benefits of technology, and the challenges encountered.

29. Further, considering the private sector is responsible for introducing new information technology solutions to the registration process, privacy protections and data confidentiality provisions must maintain the flexibility necessary for adapting to rapidly changing markets. For example, Plan

23 Ibid.
International notes this flexibility as particularly pertinent considering the expansion of mobile “registration outside of a controlled environment (a hospital or government office)” which can present new security risks for vulnerable children and families.\textsuperscript{24}

VI. Conclusion

30. Data integration, new technologies, digitalization and national identity management systems present opportunities to further leverage the civil registration records, going beyond just the production of vital statistics. With that, new challenges emerge, particularly with respect to data privacy and confidentiality.

31. As countries improve their registration coverage, the resulting data becomes more valuable. And as countries create interoperable data ecosystems, especially with national identity management systems, the potential to identify individual citizens becomes much greater. It is critical to balance the right of the individual to privacy, especially when providing information for a compulsory administrative service, with the societal good from being able to access that data, especially with regards to microdata access.

32. Over recent years, guidance has been developed to fill the new gaps resulting from these emerging areas although there is still unmet demand for support and assistance and much remains to be done. This paper has outlined some of the key considerations and guidelines available to help inform progress under the Asia and Pacific Civil Registration and Vital Statistics Decade (2015–2024).