



Parliament of Sint Maarten

Staten van Sint Maarten

MEMO

Committee Kingdom Affairs and Interparliamentary Relations

The protection of Personal Data in relation to Convention 108+ - Sint Maarten

In preparation of the Interparliamentary Kingdom Consultations (IPKO) scheduled for June 2026 in the Netherlands, the Committee of Kingdom Affairs and Interparliamentary Relations (CKAIR) of the Parliament of Sint Maarten requested information from the Minister of Justice to assist in the inventory being conducted to assess the extent to which the countries within the Kingdom comply with the basic standards for the protection of personal data necessary for the free exchange of data in the context of essential cooperation, including in the area of security, as is indicated inter alia in Convention 108+ of the Council of Europe.

See below the responses of the Minister of Justice regarding this topic as it regards Sint Maarten.

1. Can the current legal and institutional safeguards for the protection of personal data in Sint Maarten be indicated? We acknowledge our current National Ordinance personal data protection.

Sint Maarten currently has a general statutory framework governing the protection of personal data through the National Ordinance on the Protection of Personal Data (Landsverordening bescherming persoonsgegevens – (hereinafter:LBP). The ordinance was introduced following the constitutional transition of 10 October 2010 and was enacted in implementation of Article 5 of the Constitution of Sint Maarten, which guarantees the protection of privacy and personal data.

The explanatory memorandum accompanying the ordinance expressly recognizes that modern society increasingly depends on the collection, storage and exchange of personal data, while at the same time acknowledging the significant risks such processing may pose to the privacy and fundamental rights of individuals. The legislative framework was therefore designed to establish legal safeguards within which personal data may be processed while ensuring adequate protection of the individual concerned.

The LBP applies to both the public and private sectors and contains general principles relating to lawful processing, purpose limitation, proportionality, data quality, security of processing, and the protection of sensitive personal data. The ordinance further provides data subjects with rights of access, rectification and objection and establishes both judicial and administrative remedies for violations of the law. These principles correspond substantially with the foundational principles reflected in Articles 5 through 10 of Convention 108+.

Institutionally, supervisory oversight is entrusted to the “Commissie Toezicht Bescherming Persoonsgegevens”, established under Chapter 7 of the ordinance. The supervisory

framework includes investigative and enforcement powers, including the authority to supervise compliance and impose enforcement measures where necessary. The supervisory authority is established by law, but has not yet been constituted/operationalized (e.g., appointments and operational resourcing/budget have not been completed and allocated).

The explanatory memorandum further makes clear that the legislative framework was intentionally modelled on internationally recognized standards and substantially based on the former Dutch Personal Data Protection Act (Wet Bescherming Persoonsgegevens).

2. Can the extent to which these safeguards align with the principles and requirements set out in Convention 108+ be indicated?

The current legal framework of Sint Maarten reflects many of the core principles contained in Convention 108 and the modernized Convention 108+ of the Council of Europe. This includes principles relating to legality, fairness, transparency, purpose limitation, proportionality, data security and the protection of data subject rights as reflected inter alia in articles 5, 7, 8 and 9 of Convention 108+.

At the same time, it must be underscored that the present framework does not yet fully satisfy all modernized standards introduced through Convention 108+. In particular, the current legislation does not yet comprehensively regulate modern accountability obligations, mandatory data breach notifications, data protection impact assessments, privacy-by-design obligations or the expanded supervisory requirements now associated with contemporary international data protection frameworks. Additionally, it also contains a basic safeguard regarding solely automated decision-making. The current legal framework of Sint Maarten reflects many of the core principles contained in Convention 108 and the modernized Convention 108+ of the Council of Europe. This includes principles relating to legality, fairness, transparency, purpose limitation, proportionality, data security and the protection of data subject rights as reflected inter alia in articles 5, 7, 8 and 9 of Convention 108+.

In practice, the implementation of modern data protection standards also requires significant institutional and technical capacity. This concerns not only legislation itself, but also the operational independence and resourcing of supervisory authorities, cybersecurity resilience, digital governance structures, and the ability of both government institutions and private entities to effectively comply with increasingly technical regulatory obligations. The LBP applies broadly across public and private sectors, subject to statutory carve-outs (e.g., intelligence/security services, police tasks, civil registry/population administration, VOG/JD, elections). In this respect, Article 15 of Convention 108+ requires supervisory authorities to operate independently and to possess adequate investigative, intervention and enforcement powers, as well as sufficient resources for the effective exercise of their function.

It should further be noted that Convention 108 was previously ratified for the Kingdom of the Netherlands, but was not extended to the former Netherlands Antilles. The explanatory memorandum to the LBP already recognized that, following the constitutional reform of the Kingdom, the desirability of extension or co-ratification would need to be reconsidered.

3. Can any existing or planned legislation, policy measures, or implementation processes in this area be indicated, including the status of the ongoing discussions and initiatives aimed at harmonizing personal data protection frameworks among Aruba, Curaçao, and Sint Maarten in the context of the Country Packages?

At present, the legal frameworks governing the protection of personal data within Aruba, Curaçao, Sint Maarten, the BES islands and the European part of the Netherlands differ considerably. As a consequence, the level of legal protection afforded to natural persons likewise differs throughout the Kingdom.

This fragmentation has both legal and practical implications. In particular, it complicates the exchange of personal data between governments, semi-public institutions such as healthcare providers and social security institutions, and private sector entities operating across multiple jurisdictions within the Kingdom. There is no uniform Kingdom-wide level of protection aligned with modern European standards; this can complicate EU–Caribbean data transfers and may require additional safeguards. This may hinder or complicate the transfer of personal data between Europe and the Caribbean parts of the Kingdom.

Against this background, the Ministers of Justice of the Kingdom countries jointly decided to pursue harmonization of personal data protection legislation through a Consensus Kingdom Act (Consensusrijkswet). The harmonization initiative was subsequently incorporated into the Country Packages, including Chapter 9.1 of the Country Package of Sint Maarten.

The proposed Consensus Kingdom Act serves three principal objectives. Firstly, it seeks to establish a higher and more modern level of protection for individuals whose personal data is processed in an increasingly digital society. Secondly, it aims to create a level playing field within the Caribbean parts of the Kingdom, thereby facilitating lawful and secure data exchange between jurisdictions. Thirdly, the proposed framework is intended to simplify and strengthen the transfer of personal data between Europe and the Caribbean parts of the Kingdom.

The proposed Consensus Kingdom Act is intended to serve as the implementation instrument for Convention 108+ of the Council of Europe and its accompanying protocol. Convention 108+ is internationally recognized as one of the leading global standards concerning the protection of personal data and is closely connected, both substantively and structurally, to the principles underlying the European Union General Data Protection Regulation (GDPR).

Formal drafting activities of the Consensus Kingdom Act commenced in early 2022. In April 2022, the second draft of Chapter 1 of the proposed Kingdom Act was prepared. This chapter contained the general provisions of the framework, including definitions, provisions concerning scope of application, principles governing lawful processing, obligations for controllers and processors, transparency obligations and storage limitation principles. During the drafting process, considerable attention was devoted to the institutional structure and financing of the supervisory authority responsible for enforcement and oversight under

the new framework. Discussions focused in particular on the authority's financing model, legal personality, governance structure, operational independence and the balance between centralized coordination and local operational presence.

In May 2022, agreement was reached regarding the financing model for the future supervisory authority, whereby Aruba, Curaçao, Sint Maarten and the Netherlands, acting on behalf of the BES islands, would each contribute proportionally twenty-five percent of the operational costs.

Subsequently, in June 2022, further agreement was reached concerning the organizational structure and legal status of the supervisory authority. The authority was designated as the "Gemeenschappelijke Autoriteit Gegevensbescherming". It was decided that the authority would possess public legal personality while simultaneously maintaining local presence within each jurisdiction through local service desk functions.

By the end of 2022, Chapter 1 of the proposed Kingdom Act had been finalized. The explanatory memorandum accompanying this chapter expressly emphasized the importance of alignment with Convention 108+ and identified the Convention as the principal international benchmark for the harmonization process.

Chapter 2 of the proposed Kingdom Act specifically concerns the processing of personal data by public and private legal entities. The objective of this chapter is to establish a uniform legal framework governing transparency obligation, rights of data subjects, lawful processing requirements, and the obligations of controllers and processors. Chapter 3 concerns the processing of personal data within the law enforcement chain. Chapter 4 contains transitional regulations.

The project group responsible for the development of the proposed Kingdom Act has furthermore informed the Judicial Four-Party Consultation (JVO) that implementation of the proposed framework will require substantial review and amendment of existing national legislation within the participating jurisdictions. As is customary when introducing overarching general legislation, existing legislation in each country will need to be reviewed for inconsistencies, conflicts, legal gaps and redundant provisions.

Finally, it is important to note that the proposed Consensus Kingdom Act does not extend to the processing of personal data by intelligence and security services, the processing of personal data in the context of elections, or the population administration and civil registry systems. Should the countries ultimately proceed toward ratification and implementation of Convention 108+, these separate legal regimes will likewise require independent assessment in order to determine whether the level of protection currently provided is sufficient or whether additional legislative amendments may be necessary.

4. Are there any challenges or points of concern relevant to international and or Kingdom-wide cooperation involving the sharing of data and security matters, considering the shared need?

The increasing digitalization of government services and cross-border cooperation has significantly increased the importance of secure and lawful data exchange both within the Kingdom and internationally. Effective cooperation in areas such as law enforcement, border control, customs, taxation, migration, healthcare, cybersecurity and financial supervision increasingly depends upon compatible legal frameworks and sufficiently secure digital infrastructures.

At the same time, important challenges remain. These include differences in legal standards between jurisdictions, limited implementation capacity, cybersecurity vulnerabilities, resource constraints and the need to balance privacy rights against legitimate national security and public safety interests.

Convention 108+ itself recognizes that restrictions relating to national security and criminal investigations may under certain circumstances be necessary, provided such restrictions remain lawful, proportionate within a democratic society and subject to independent oversight.