NATIONAL PRIVACY COMMISSION

The NPC is an attached agency of the Department of Information and Communications Technology

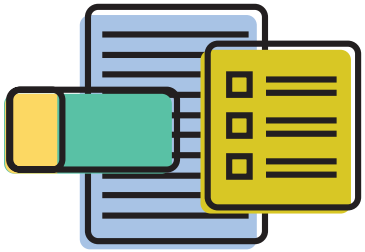
Security of Personal Data in Government Agencies

Data security means protecting data from destruction and any unwanted or unauthorized actions through the implementation of appropriate technical and organizational measures.

The Commission recommends ISO/IEC 27018 as the most appropriate certification for the service or function provided by a service provider, in relation to data security.

General obligations of government agencies engaged in the processing of personal data

1. Through its head of agency, designate a Data Protection Officer;
2. Conduct a Privacy Impact Assessment for each program, process or measure within the agency that involves personal data;
3. Create privacy and data protection policies;
4. Conduct an annual mandatory, agency-wide training on privacy and data protection policies, and a similar training during all agency personnel orientations.
5. Register its data processing systems with the National Privacy Commission, subject to the conditions under the Data Privacy Act, its IRR, and other issuances of the Commission.
6. Cooperate with the Commission when its privacy and data protection policies are subjected to review and assessment, in terms of their compliance with the requirements of the Act, its IRR and all issuances by the Commission.



Personal data being processed by a government agency shall be stored in a data center, which may or may not be owned and controlled by such agency. A **data center** refers to a centralized repository, physical or virtual, analog or digital, used for the storage, management, and dissemination of data, including personal data.

All personal data that are digitally processed must be encrypted, whether at rest or in transit. The Commission recommends Advanced Encryption Standard with a key size of 256 bits (AES-256) as the most appropriate encryption standard.

Passwords or passphrases used to access personal data should be of sufficient strength to deter password attacks. A password policy should be issued and enforced through a system management tool.

An agency personnel with the appropriate security clearance has restricted access to personal data being stored in a data center. This must be enforced by an access control system that records when, where, and by whom the data centers are accessed.

The Commission reserves the right to audit a government agency's data center, or, where applicable, that of its service provider. Independent verification or certification by a reputable third party may also be accepted by the Commission.

Only programs developed or licensed by a government agency shall be allowed to access and modify databases containing the personal data under the control or custody of a government agency.

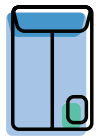
A government agency shall adopt and utilize technologies that prevent personal data accessible online from being copied to a local machine. It shall also provide for the automatic deletion of temporary files that may be stored on a local machine by its operating system.

Where possible, agency personnel shall not be allowed to save files to a local machine. They shall be directed to only save files to their allocated network drive. Drives and USB ports on local machines may also be disabled as a security measure. A government agency may also consider prohibiting the use of cameras in areas where personal data is displayed or processed.

Personal data may be transferred or stored in the following formats and media:

Portable media that utilize full disk encryption.

Removable physical media Only when unavoidable.



Mail or Post Delivered only to the addressee

Emails Encrypted or sent via a secure email facility

Security requirements

For the online access of personal data: Agency personnel who access personal data online shall authenticate their identity via a secure encrypted link and must use multi-factor authentication. Their access rights must be defined and controlled by a system management tool, or a software system that facilitates the administration of user passwords and access rights.

For paper-based filing systems: If personal data is stored in paper files or any physical media, the government agency shall maintain a log, from which it can be ascertained which file was accessed, including when, where, and by whom. Such log shall also indicate whether copies of the file were made. Agency management shall regularly review the log records, including all applicable procedures.

Can a third-party service provider be engaged in the disposal of personal data?

Yes. Note however that the service provider shall contractually agree to the agency's data protection procedures and ensure that the confidentiality of all personal data is protected.

Are there penalties for violation/s of the provisions of NPC Circular No. 2016-01?

Upon notice and hearing, violations are subject to compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing of personal data, or payment of fines, in accordance with a schedule to be published by the Commission.

Failure to comply with the provisions of the circular may be a ground for administrative and disciplinary sanctions against any erring public officer or employee.