Reference Measures for the Security of Any Personal Data Processing Operation[1]

Version 1.0

The present document contains a list of eleven domains of action relating to information security, for each of which any organisation keeping, processing or communicating personal data – be it a corporation[2], a company or a public authority – is to take measures.

Due to the extreme diversity of concrete situations, it is impossible to describe the actions to be undertaken for every single case.

The security controls described hereinafter should therefore be adapted to the context and the specific character of each organisation and should imply the application of practical solutions with a level of detail or complexity proportionate to the actual needs of the organisation.

In this process, the following must be taken into account:

- the nature of the personal data being processed and of the operations carried out on them, as well as requirements concerning confidentiality, integrity and availability;
- statutory or regulatory requirements which may be applicable;
- the size of the organisation (including the number of persons that may access the data);
- the importance and the complexity of the information systems, application programmes and computer systems involved;
- the organisation's degree of openness to the external world as well as the external world's level of access to the organisation's systems;
- the risks the organisation itself or the persons whose personal data are being processed are exposed to;
- and also the "state of technological development in this field and the cost of implementing measures"[3].

Information security being subject to constant evolution these reference measures shall be adapted systematically to the development of regulations, technology and other aspects.

---

[1] The present document is intended for data controllers in order to assist them in the implementation of reliable security in accordance with the duty imposed upon them by article 16 of the Belgian Law of 8 December 1992 on privacy protection in relation to the processing of personal data.

[2] This does not mean that natural persons shall be exempted from the duty imposed upon them by article 16 of the Belgian Law of 8 December 1992 on privacy protection in relation to the processing of personal data, which imposes duties relating to security upon any data processor.

[3] Belgian Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data (Art. 16).

1. Information security policy

Any organisation processing personal data should draw up a written document – the information security policy – giving a precise description of security strategies and protection features selected for data security.

Prior to determining these security strategies and protection features, the organisation must consider potential threats to the personal data being processed and assess the real risks the data are exposed to.

The information security policy should consist of:

- a clarification with regard to the analysis performed and to risk management of personal data;
- the priorities that have been set and the mechanisms that were or are introduced as a result of this analysis;
- a timesheet for the policy's taking effect;
- a description of the various responsibilities and organisational rules that were introduced;
- a description of how to manage security incidents;
- a description of the awareness-raising process for this policy within the organisation;
- the measures that were introduced to keep the security system up-to-date after installation.

The information security policy must be approved at the highest echelons of hierarchy and by the various persons in charge, and in order for this policy to be known to everyone, it must be sufficiently disseminated within the organisation.

The policy must be adapted at least once a year, or as a result of modifications or reassessment.

2. Organisation of information security

Depending on the nature of the personal data used/processed, an information security consultant must be appointed within the organisation, who is to be in charge of the implementation of the information security policy.

Reporting directly to the organisation's management, the information security consultant must receive sufficient resources (time, human resources, equipment and budget) and have free access to the information necessary for him to discharge his functions, to the extent that he does not operate outside the information security policy's framework.

He shall ensure that the various responsibilities with regard to information security (prevention, supervision, detection and processing) have been clearly defined and that the persons in charge of information security can operate autonomously and independently, and that they shall be safeguarded from pressurization as a result of personal or contradictory interests.

He must possess the necessary competences and be adequately trained, and cannot discharge any function nor take up any responsibility that is incompatible with that of an information security consultant.

3. Organisation and human aspects of information security

The organisation must clearly define the responsibilities and the management process regarding personal data security and properly integrate them in its general organisational structure and functioning.

To organise information security sufficient and adequate organisational, technical and financial resources must be made available.

To guarantee efficient data protection, the organisation should ensure that information classification[4] procedures are elaborated, so that an inventory can be drawn up and all personal data being processed can be localised, irrespective of the type of data carrier.

Successful protection of a computer system depends most highly on the correct provision of information to the different actors. Therefore, the organisation must take the necessary measures in order for all (internal or external) persons participating in the processing of personal information to be sufficiently and constantly informed about their duties and responsibilities during processing operations and for them to be sufficiently and adequately trained to discharge their functions and take up their information security responsibilities.

If necessary, disciplinary measures must be drawn up in case the rules are not observed, and whenever this is demanded by the risks, a declaration of confidentiality is required.

When a subcontractor is hired to process the entire set of personal data or a part of it, the organisation must ensure that the subcontract agreement includes the same security obligations as those in effect for the organisation itself.

4. Physical environment security

The organisation should take the necessary measures to guarantee physical security of personal data.

For this purpose, the organisation must ensure that carriers of personal data and computer systems processing the data, according to their classification, are positioned on clearly identified and adequately protected premises, and that the access to these premises is limited to the persons having the necessary authorization and to the hours in which these persons discharge their functions.

When continuity of service is necessary, equipment must be installed in order to prevent, detect and deal with physical threats such as fires or flooding. The equipment is to be inspected on a regular basis. The organisation must also provide the necessary safeguards (backups) in order to avoid the loss or accidental modification of personal data.

---

[4] Under this section the term "classification" is understood to mean the organisation of data, as it is generally used for computer security systems, i.e. information qualification, and it does therefore not refer to the meaning of security certificates and security recommendations as mentioned in the Belgian Law of 11th December 1998 on classification and security authorizations.

5. **Network security**

The organisation must make sure that the confidentiality and integrity of personal data are guaranteed if the equipment is connected to networks while/using processing the data.

If the organisation's internal network is connected to a public external network, the organisation must provide the necessary safeguards in order to protect the network(s) against any unwarranted access (intrusions, viruses and malware etc.) for the duration of the processing.

6. **Logical access security**

The organisation must ensure that personal data, based on their classification, are only accessible to persons and application programmes explicitly having the necessary authorisation.

The organisation shall keep an up-to-date list of the various persons authorised to access and process these data, as well as of these persons' respective authorisations.

The various authorisations should be reflected in technical dispositions and access controls for all computer-related elements (programmes, procedures, storage, telecommunication equipment,…) involved in the processing of personal data.

Technical dispositions must cover initial phase activities (development of application programmes) as well as final phase activities (backup management).

Should this be required by the level of security, the interveners' identification shall be completed with an authentication procedure.

7. **Access logging, audit trails and access analysis**

The organisation should implement logging and audit trail mechanisms.

If necessary, these mechanisms should allow for the identification of any person having accessed or processed personal data. Registration of this control information may relate to physical access, logical access or both, as the case may be.

The granularity of records, the localisation and the duration of storage thereof, the frequency and the type of processing depend on the context. Additional mechanisms for intrusion detection could be required. The information security counsellor must be able to justify the policy adopted.

Because detection data are also personal data, any operation performed on these data must be accompanied by adequate security measures.

8. **Monitoring, checks and maintenance**

The organisation must make sure that its technical or organisational measures have been

validated and that they are regularly checked.

Information security maintenance needs should be determined by monitoring processing operations, source evolution and logging analysis.

Since information systems and the risks they are exposed to are subject to permanent change, the organisation must regularly check (at least once a year) that the initial goals and the measures taken afterwards remain up-to-date, so that improvements can be made if necessary.

Every time the organisation is reorganised or its infrastructure is modified, security controls must be updated.

9. Security incident management and continuity

The organisation must have a security incident management plan.

In case of incidents representing a risk for the confidentiality and integrity of personal data, a rapid intervention is of primary importance to decrease the impact of such situation. For this purpose, the organisation must elaborate procedures giving a precise description of the steps to be taken when a security incident relating to personal data is detected, as well as of the persons in charge of dealing with the incident, in order to return to the normal situation as quickly as possible.

Moreover, the circumstances of the incident must be analyzed to elaborate preventive measures or make adaptations so as to avoid a repetition of this type of incident, or to return to the normal situation as quickly as possible.

Organisations having the duty to ensure the continuity of their services must:

- draw up a recovery and continuity plan when security incidents occur, in order to avoid an interruption of services exceeding an acceptable period of time;
- see to it in particular that the confidentiality and integrity of personal data are guaranteed during the implementation of the various plans.

10. Enforcement

Every organisation must apply all applicable rules and legislation regarding the processing and protection of personal data at all times. This legislation can always be consulted on the Privacy Commission in the "Legislation and Standards" section.

The Privacy Act very precisely determines the conditions and circumstances of a personal data processing operation or transfer. Prior to a processing operation, every organisation must check whether – taking into account the delicate nature of the data – carrying out the processing operation is not subject to an authorisation and it must always make sure that the authorisation's conditions are met.

11. Documentation

The organisation should have complete centralised documentation relating to information security, which is updated on a regular basis.

For proper management of protected personal data, the organisation should collect all the necessary documentation. This documentation should be complete and formalised, proportional to information security needs, up-to-date at any time, and accompanied by a directory available to properly authorised persons whenever necessary.

The documentation should at least contain the following elements:

- the identity of the information security counsellor;
- the information security policy;
- the implementation of security measures;
- an inventory of the personal data being processed, their localisation and the operations performed on them;
- a list with the names of the bodies or designated individuals having access to the data;
- the system and network configuration;
- technical documentation about the security controls that were introduced;
- a schedule of planned operations;
- the detection policy;
- security control test plans;
- incident reports;
- audit reports, if any.