

# Data Processing Norms and Standards

The measures which need to be complied with as a minimum are:

- a policy document that relates to the measures taken to safeguard the processing of personal data, as well as guaranteeing privacy is maintained. This policy document (hereafter: the privacy and information security policy) is based on applicable legislation and generally-maintained (security) standards.
- The responsibilities, both on a managerial and executive level, are clearly defined and allocated.
- The employees are bound by a confidentiality obligation and, if applicable, prior to entry into service, suitable screening will have been done.
- All employees and, where applicable, hired staff and external users are informed about the privacy and information security policy and procedures of the organization, where relevant for their position.
- IT provisions and equipment are physically protected from access by unauthorized persons and from damage and disruptions.
- There are procedures to give users authorized access to the information systems and services which they need to perform their tasks and to prevent unauthorized access to the network and information systems.
- When conveying confidential personal data, adequate security always needs to be applied.
- There are procedures for acquisition, development, maintenance and destruction of information systems.
- In all information systems, security measures are built in, including adequate access management.
- The network and the information systems are actively monitored and managed.
- A procedure is available for processing any Data Breaches.
- Software, such as browsers, virus scanners and operating systems are kept up-to-date. Timely solutions which the supplier issues for security breaches are installed in this software.
- There are procedures for the timely and targeted handling of privacy and information security incidents and weak points in security, as soon as they are reported.
- The limitation of the consequences of natural disasters, accidents, failure of equipment or deliberate action is covered by setting up continuity management, where a combination of preventative measures and restorative measures are used.

- The rights of data subjects and other measures ensuing from the privacy legislation and regulations are facilitated.