Gantner
technologies

Information:

Process description for the Biometric Reader GAT Access 6100 F with Biometrics Module Gantner Electronic GmbH

The following measures were taken to meet the specific European Privacy Laws regarding Personal Biometric Data:

• Biometric Data will be extracted at the GANTNER Enrollment Station. The GANTNER Enrollment Station is not connected to any PC or external Data Base.

• The Biometric Data is stored solely on the Data Carrier, e.g. Member Card, Wristband, or Key Fob, issued to the members.

• The Biometric Data is stored as vectors in designated sectors in the memory of the Data Carrier's Internal Chip. These sectors are secured with Crypt Keys to ensure no external readers can read or access this data.

General:

All Biometric Data is at all times with the Club Member. There is no link between the Club Management Software and the Biometric Data stored solely in the memory of the Chip.

The Biometric Data is stored as vectors in designated sectors in the memory of the Chip. These sectors are secured with Crypt Keys to ensure no external readers can read or access this data.

We, as Gantner Electronic GmbH, guarantee that the Biometric Data is safe in the Members Hand and not stored in any other media or database.