CCTV and ANPR Policy

1. Ownership

Midi plc, a company registered in Malta, bearing company registration number C 15836 and having its registered address at North Shore, Manoel Island, Malta ("the Company") operates a CCTV surveillance system ("CCTV") and an Automatic Number Plate Recognition system ("ANPR") (the CCTV and ANPR systems shall be referred to as the "Systems") throughout the Tigne Point Car Park. The Systems are owned, managed and operated by the Company.

Webcams, covert installations and any other systems are in place to capture images of identifiable individuals for the purpose of viewing and or recording the activities of such individuals. CCTV images and ANPR data are monitored and recorded in strict accordance with this policy.

The ANPR system was designed to enhance the overall experience of Car Park users by implementing the following:

i. Each number plate is memorised at time of entry into the Car Park and a picture of the vehicle number plate is taken;
ii. The number plate is matched with the specific entry ticket and printed on the entry ticket of the user;
iii. The system facilitates exiting the Car Park without the need to insert the ticket at the exit barrier;
iv. The system assists in determining the exact length of the stay in the Car Park in case of a lost ticket;
v. The system eliminates abuses, for instance where customers procure a second entry ticket to simulate a shorter stay at the Car Park; or where customers that have parked for several days claim that a ticket has been lost; thus incurring only a lost card fee.

2. Compliance

Images obtained from the Systems which include recognisable individuals and number plates of vehicles, constitute personal data and are protected by data protection legislation including the Data Protection Act, Chapter 440 of the Laws of Malta as may be amended from time to time, and the General Data Protection Regulation (Regulation (EU) 2016/679) (the "Applicable Law").

In processing personal data in terms of this Policy, the Company is considered a data controller under data protection legislation.

3. Purpose of Processing

The Company's purpose for processing personal data through use of the Systems is for security, crime prevention, management of employment relations (including use of CCTV footage for disciplinary purposes) and to ensure the safety of staff, contractors, clients, passengers, and all visitors.

Our legitimate interest for processing such personal data through the Systems arises from the following:

- The Systems are used to maintain public safety, the security of property and premises
- for preventing and assisting authorities in investigating crimes;
- to ensure the safety of staff, clients, contractors, passengers and visitors;
- to ensure the quality of staff conduct and performance when carrying out work duties;
- to ensure that our legitimate financial interest in the correct measurement of parking duration is preserved.

For these reasons the information processed may include visual images, personal appearance and behaviours. The ANPR system collects the number plate image of vehicles accessing the Car Park and the date and time of entry.

This information may be about staff, guests, visitors, suppliers, business partners and clients, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Any monitoring of staff will be carried out in accordance with applicable legislation.

4. Description

The Systems are intended to produce images as clear as possible and appropriate for the purposes stated in this policy. The Systems are operated to provide, when required, information and images of evidential value.

CCTV system cameras are located at strategic points throughout the precincts of the Car Park, principally at the perimeters, entrance and exit points of buildings, public and non-public collection spaces.

ANPR system cameras are located at the entrance to the camera.

Signage is prominently placed at strategic points at the car park to inform staff, visitors and members of the public that the CCTV and ANPR Systems are in use.

5. Operation

Images captured by the system are recorded continuously and may be monitored in the following areas:

- Entry and Exit barriers of the carpark;
- On the Automatic Paying Machines (APMs);
- Info Point.

Images displayed on monitors are not visible from outside the Info Point control room and access to the Control Room is strictly limited to Car Park staff on the specific shift.

Only our Infopoint personnel and our ICT administrator have access to the Systems are made aware of the sensitivity of handling images and recordings. Authorised staff is also obliged to sign a Confidentiality and Non-Disclosure Agreement. The Company ensures that authorised staff is fully briefed and trained in all aspects of the operational and administrative functions of the system.

Furthermore, the number plate data is stored only specifically for the purpose of number plate with entry tickets and not used or stored for any other purpose.

6. Information retention

No more images and information shall be stored than is required for the stated purpose.

The general retention period for CCTV footage is 3 days whilst that of the ANPR systems if 4 days.

However, in certain instances, the retention period of images captured by some cameras may be extended further if a legal obligation is imposed on us at law.

Images will be deleted once there is no longer a necessity to keep such information.

7. Third Party Access to Personal Data

Skidata is our processor; they provide us with general software maintenance service with respect to the car park management software. The system provides for an access gateway – we control access rights to Skidata and this is strictly on a "need to know" basis to conduct software repairs and upgrades.

We will share the information collected by the Systems with other third parties only if there is a legal obligation imposed on us to do so, and in accordance with this policy.

8. Rights of Data Subjects

Anyone who believes that they have been filmed or their data recorded by the Systems, can request a copy of the recording, subject to any restrictions covered by Applicable Law.

Data subjects also have the right to request that inaccurate data be corrected or erased and to seek redress for any damage caused. Access requests should be submitted on gdpr@midimalta.com or by letter to 'Midi, North Shore, Manoel Island, Gzira GZR3016, Malta'.

Other data subject rights include the:

Right to Lodge a Complaint - Data subjects have the right to lodge a complaint regarding the processing of their personal data with the supervisory authority for data protection matters. In Malta this is the Information and Data Protection Commissioner on https://idpc.org.mt/en/Pages/contact/complaints.aspx

Right to Erasure – in certain circumstances data subjects may request that We delete the Personal Data that we hold about them;

Right to Object – data subjects have a right to object and request that We cease the processing of their personal data where we rely on our, or a third party's legitimate interest for processing personal data;

Right to Portability – data subjects may request that We provide personal data provide by the data subject in a structured, commonly used and machine-readable format. Where technically feasible, data subjects may also request that we transmit their personal data to a third party controller indicated by the data subjects;

Right to Restriction – data subjects have the right to request that We stop using their personal data in certain circumstances, including if they believe that We are unlawfully processing their data;

Data subjects' rights are not absolute and we may not be able to entertain the above requests if we are prevented from doing so in term of the applicable law.

Data subjects may exercise the rights indicated in this section by contacting Us on gdpr@midimalta.com. Alternatively Our Data Protection Officer may be contacted on +356 20655500.

9. Keeping Personal Data Secure

We shall implement and maintain appropriate and sufficient technical and organisational security measures, taking into account the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to protect personal data against any unauthorised accidental or unlawful destruction or loss, damage, alteration, disclosure or access to personal data transmitted, stored or otherwise processed and shall be solely responsible to implement such measures.

We shall ensure that our staff who process your data are aware of such technical and organisational security measures and we shall ensure that such staff are bound by a duty to keep personal data confidential.

The technical and organisational security measures in this clause shall mean the particular security measures intended to protect your personal data in accordance with any privacy and data protection laws.