PDPA PROCEDURES IN PROSEC

Every day, our Officers collect, use, disclose and store personal data in the course of their everyday duties. Because PROSEC is PDPA-compliant, we therefore request our clients to comply with relevant data protection principles covered in our Data Protection Governance Policies.

Our policies cover the Collection, Use, Disclosure, Disclosure and Disposal of personal information that our Officers encounter in the performance of their duties. They are summarized as follows:

.

Collection

- When collecting personal data, our Officers collect only what is necessary for security purposes proportionate with the relevant security requirements
- All visitors or members of the public are notified before or at the point of collection that their personal data is being collected for the purposes of safety and security
- Our officers avoid collecting the physical NRICs card unless it is a requirement to enter high-security areas
- All personal information collected are secured – whether it is entered into a visitor management system, or into a security logbook
- Only authorized devices or systems are used to collect personal information
- CCTV surveillance is conducted with due care for the specific purpose of safety and security
- Officers are not permitted to collect any personal information via photos, audio or camera video using a mobile device without consent or authorization
- Handling of personal data during registration, management of CCTV footage, and management of body camera surveillance footage and images are governed by Prosec's PDPA Code of Conduct.

Use

- Personal data can only be used for the purposes of security and safety and NOT for any other purposes – unless the relevant person gives consent for that particular purpose
- Our Officers are NOT allowed to use the personal data being processed for any other purpose
- Personal data is *accurately* recorded, especially when transcribing from hand-written notes or in the course of investigation
- Where relevant, our Officers will verify the accuracy of any personal information provided such as checking NRIC numbers against the actual NRIC card

Disclosure

- Our Officers do not reveal or disclose personal data to any unauthorized persons, channels or media (such as Youtube)
- Security log books are never be left open or exposed in full public view
- Any request for personal data (e.g. CCTV footage) should be channeled to Prosec's Data Protection Officer.
- Our officers ensure that CCTV camera surveillance is not intrusive and be positioned away from public view
- Before returning or releasing any "lost and found" item (in particular NRIC card or driving license), our Officers take reasonable care in verifying the identity of the individual.
- Any requests from individuals involving their own personal data (eg request of how their data is being processed or used, CCTV footage) etc should be directed to the Data Protection Officer

Storage / Disposal

- Our Officers ensure that all documents, books, systems or devices that contain personal information area secured especially when personnel are away from the security counter
- Our Officers do not write any personal information on scraps or pieces of paper.
- Only authorized containers or storage boxes are used by our Officers to store storing of sensitive data
- Our Officers do not permit unauthorized persons or any member of the public to enter any security room, FCC, or counters.
- Our Officers will take extra care and measures needed if any sensitive data is stored whether physically or electronically (e.g. biometrics related records, NRIC cards)

Thank you for your cooperation. If you have any questions, please contact our Data Protection Officer at dpo@prosegur-prosec.sg (6389 5154).