SECURITAL
GUARD | CASH | SYSTEMS
a kdm. group company

DATA PROTECTION POLICY

Securital Solutions Ltd and Securital Aviation Ltd provide security and security-related services in Malta and are committed to protecting the privacy and personal data of individuals in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and applicable Maltese data protection legislation, including the Data Protection Act (Cap. 586 of the Laws of Malta), as overseen by the Office of the Information and Data Protection Commissioner (IDPC).

This Policy explains how personal data is collected, used, stored, disclosed, and protected when individuals interact with Securital Solutions Ltd or Securital Aviation Ltd or make use of their services. It applies to all personal data processed by the Companies, regardless of format (electronic or paper), including data relating to employees, job applicants (including applicants processed through the Companies' Applicant Tracking System and related recruitment processes), clients, suppliers, contractors, and other third parties.

1. Data Controller and Data Protection Officer

- Data Controllers:
  Securital Solutions Ltd
  Securital Aviation Ltd

  The Data Controller is responsible for determining the purposes and means of processing personal data and for ensuring compliance with applicable data protection legislation.

- Data Protection Officer (DPO):
  Iria Rielo Rodriguez
  Email: iria.rielorodriguez@securital.mt
  Phone: +356 9971 4397

  The Data Protection Officer acts as a point of contact for data subjects and the Information and Data Protection Commissioner and oversees compliance with data protection obligations.

2. Types of Personal Data Collected

Depending on the nature of the relationship, Securital Solutions Ltd and Securital Aviation Ltd may collect and process the following categories of personal data:

- Identification and contact data:
  Name, address, email address, telephone number, identification details.

- Financial data:
  Bank account details, billing and payment information, where applicable.

- Transactional data:
  Invoicing details, payment records, service history.

- Technical data:
  IP address, browser type, device information, and website usage data (where applicable).

- Marketing and communication data:
  Communication preferences, correspondence, and feedback.

- Employee-related data:
  Employment records, payroll data, training records, performance-related information, and health and safety documentation.

- Recruitment-related data:
  CVs, résumés, cover letters, application form data, employment and education history, professional skills, qualifications and licenses, interview notes, assessments and test results, referee details, verification checks, background check information (only where legally permitted and subject to consent where required), and information from publicly available professional profiles (where relevant to the recruitment process).

3. Sources of Personal Data

Personal data may be collected directly from individuals; from publicly available sources (such as professional online platforms); through referrals from employees, partners, or recruitment providers; and from third-party recruitment or background-verification service providers, where applicable.

4. Legal Basis for Processing

Personal data is processed in accordance with Article 6 of the GDPR, based on one or more of the following lawful bases:

- **Consent**, where explicitly provided by the data subject, including consent given by job applicants to be considered for future employment opportunities (talent pools).
- **Contractual necessity**, where processing is required to perform a contract or take steps prior to entering into a contract.
- **Legal obligation**, where processing is required by law.
- **Legitimate interests**, where processing is necessary for the Companies' legitimate business interests and does not override the rights of the data subject.
- **Vital interests**, where processing is necessary to protect life or health.

The Companies do not carry out automated decision-making that produces legal or significant effects on individuals.

5. Purposes of Processing

Personal data may be processed for the following purposes:

- Delivering services and managing contractual relationships.
- Managing employment and human resources processes.
- Managing recruitment processes, including evaluating applications, arranging interviews, carrying out assessments, conducting legally-permitted background checks, and maintaining applicant profiles within the Applicant Tracking System.
- Complying with legal, regulatory, and statutory obligations.
- Managing billing, accounting, and financial processes.
- Improving services, operational performance, and customer experience.
- Communicating with clients, employees, applicants, and other stakeholders.
- Sending marketing communications, where consent has been provided.

6. Data Sharing and Disclosure

Personal data may be shared only where necessary and appropriate with:

- **Service providers and processors** acting on behalf of the Companies (e.g., IT providers,

payroll providers, ATS providers, external assessors, and consultants), subject to appropriate safeguards.

- **Regulatory and public authorities** where required by law.
- **Third parties in corporate transactions**, such as mergers or acquisitions, subject to confidentiality and legal safeguards.

The Companies do not sell or rent personal data to third parties for marketing purposes.

7. International Data Transfers

The Companies do not transfer personal data outside the European Economic Area (EEA).

Where recruitment-related or operational service providers rely on infrastructure or support services outside the EEA, the Companies ensure that such transfers may only take place subject to GDPR-compliant safeguards, including adequacy decisions or Standard Contractual Clauses.

8. Data Retention

Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected or to comply with legal and contractual obligations.

- Specific recruitment-related retention:
  - Unsuccessful applicants: retained for 12 months following the conclusion of the recruitment process.
  - Talent pool candidates: retained for 12 months from the date of inclusion.
  - Successful applicants: data is transferred to the employee file and retained in accordance with this Policy and internal HR requirements.

Individuals may request deletion of their personal data at any time, subject to legal and regulatory obligations.

9. Rights of Data Subjects

Under the GDPR, data subjects have the right to:

- Access their personal data.
- Request rectification of inaccurate or incomplete data.
- Request erasure of personal data, where applicable.
- Request restriction of processing.
- Request data portability.
- Object to processing, including for direct marketing.
- Withdraw consent at any time, where processing is based on consent.

Requests to exercise these rights should be directed to the Data Protection Officer using the contact details above.

10. Security of Personal Data

Securital Solutions Ltd and Securital Aviation Ltd implement appropriate technical and organizational measures to protect personal data against unauthorized access, loss, alteration, or disclosure. These measures include access controls, authentication procedures, data minimization, secure systems, encryption, regular monitoring, and staff awareness training.

Access to recruitment-related data stored within the Applicant Tracking System is strictly limited to authorized Human Resources personnel and hiring managers, and processed under confidentiality obligations

11. Cookies and Website Data

Where applicable, cookies and similar technologies may be used on the Companies' websites to enhance functionality and analyze usage. Users may manage cookie preferences through browser settings.

12. Children's Data

The Companies do not knowingly collect or process personal data relating to children under the age of 16. Any such data identified will be deleted without delay.

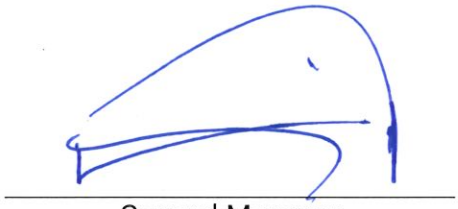
13. Complaints

Data subjects have the right to lodge a complaint with the Information and Data Protection Commissioner (IDPC) if they believe their personal data is being processed unlawfully.

IDPC Contact Details:
Information and Data Protection Commissioner
Level 2, Airways House
Triq Dun Karm
Birkirkara BKR 9034, Malta
Email: idpc.info@idpc.org.mt
Phone: +356 2328 7100

14. Policy Review and Updates

This Policy is reviewed periodically and updated as necessary to reflect changes in legal requirements or organizational practices. The most current version will be made available through appropriate channels.



General Manager
Elton Debattista