Reference	POL 42
Version	5
Issue Date	05/11/2023
Approved	MD

PREMIUM SECURITY SERVICES
DATA PROTECTION POLICY

PRIVACY NOTICE West Club (Piccadilly) Ltd t/a Premium Security Services (Data Controller) treats the privacy of its employees (Data subjects) very seriously and we take appropriate security measures to safeguard your privacy.
This Policy explains how we collect and process your personal data to manage the employment relationship and to meet legal obligations.

The regulation contains 6 principles:
• Personal data should be processed fairly, lawfully and in a transparent manner.
• Data should be obtained for specified and lawful purposes and not further processed in a manner that is incompatible with those purposes.
• The data should be adequate, relevant, and not excessive.
• The data should be accurate and where necessary kept up to date.
• Data should not be kept for longer than necessary.
• Data should be kept secure.

All staff have a responsibility to ensure that their activities comply with the data protection principles. Line managers have responsibility for the type of personal data they collect and how they use it. Staff should not disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes. What information we collect

The organisation collects and processes a range of information about you.
This includes:- Your name, address, contact details, including email address, date of birth, NI number, bank details, gender and Next of Kin details; the terms and conditions of your employment; details of your qualifications, skills, experience; your employment and education history from previous employers, education establishments and job centres to complete your screening; information about your remuneration, including entitlement to benefits such as pensions or insurance cover in the event of a TUPE transfer; injury and accident information; information about your nationality and entitlement to work in the UK; details of your schedule (days of work and working hours) and attendance at work; details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave; details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence; assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence; information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments; details of trade union membership; and equal opportunities monitoring information, e.g. ethnic origin;

How we obtain your personal data
The organisation collects this information in a variety of ways: -
• Information provided by you, e.g., from your application form, induction or over the course of your employment.
• Information from ID, e.g., passports, address ID.
• We may also keep information contained in any correspondence you may have with us by telephone, post or by email.
• Information from interviews, meetings, or other assessments.

• Information we receive from other sources, e.g., previous employers, government departments, personal referees, and credit reference agencies to enable us to carry out employment screening to the BS 7858 Standard.
• Information provided by the out-going contractor in the event of a TUPE transfer.
• The SIA for licensing purposes.

How we use your personal data

We use information held about you in the following manner: -
• In the performance of a contract for the purposes of legitimate interests of the Company
• As part of the employment relationship and to meets its obligations under your employment contract.
• To pay you and make agreed deductions such as union membership and pension contributions
• To comply with the BS 7858 Standard and Company screening
• To comply with legislation, e.g., the Transfer of Undertakings (Protection of Employment) Regulations (TUPE), Right to Work in the UK checks, employment law and vital interests such as Health & Safety reasons
• To provide a reference for future employers
• For the purposes of audit and compliance monitoring
• For insurance and employment claim purposes
• Sensitive data for court or monitoring purposes
• We only transfer your personal data outside the EEA for screening purposes
• We may share your information with selected third parties if we are under a duty to disclose or share your personal data to comply with any legal obligation, i.e., regulatory authorities such as the SIA and fraud prevention agencies.

We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy. Unfortunately, the transmission of information via the internet is not completely secure and whilst we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site and therefore any transmission is at your own risk.

Cookies: Our website does not use cookies.

Links to other websites:

Our website may contain links to other websites of interest, e.g., accreditations. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy policy. You should exercise caution and look at the privacy statement applicable to the website in question.

Where we store your personal data.

Hard copies of your personal data are stored securely in your personnel file in HR and pay related information is held securely in the Payroll Department. Data is held on our computerised management system, SQL, with restrictive access levels and the information will be deleted in accordance with the timescales below: Data will be saved on an encrypted SQL server, backed up in the Cloud for emergency recovery purposes.

How long do we keep this information about you?

We hold your personal data for the duration of your employment/service and then for specific periods after the end of your employment/service as set out below. Our need to use your personal information will be reassessed on a regular basis and information which is no longer required will be disposed of.
The following timescales will be adhered to after your employment ends:
Payroll and sick pay details - 7 years for HMRC, NI and fraud detection purposes
Personnel files - 6 months for employment queries or potential tribunal claims
Employment contracts - 7 years for potential breach of contract claims
Screening and training records - 7 years for potential insurance claims
Employee Liability Information - for the duration of the contract
Injuries - indefinitely for potential insurance claims Tribunals - 7 years
Sensitive data - ethnic origin will be held for monitoring purposes but will be anonymous.
Rosters - 6 years for Working Time Directive purposes.
Employment dates and reason for leaving - 7 years for references.

Data subject rights

If you wish to exercise any of the following rights, please contact the HR Department. Subject access requests The General Data Protection Regulation (GDPR) grants you the right to access personal data that we hold about you. This is referred to as a subject access request. We shall respond promptly, and certainly within one month or 2 months if complex, from the point of receiving the request and all necessary information from you.

Right to rectification. You, the data subject, shall have the right to obtain from us, without undue delay, the rectification of inaccurate personal data we hold concerning you. You can help us by informing us of any changes to your personal data when they occur.

Right to erasure. You, the data subject, shall have the right to obtain from us the erasure of personal data concerning you without undue delay, where there is no compelling reason for its continued processing.

Right to restriction of processing. Subject to exemptions, you, the data subject, shall have the right to obtain from us restriction of processing where one of the following applies: a) the accuracy of the personal data is contested by you, the data subject, and is restricted until the accuracy of the data has been verified; b) the processing is unlawful and you, the data subject, oppose the erasure of the personal data and instead request the restriction in its use; c) we no longer need the personal data for the purposes of processing, but it is required by you, the data subject, for the establishment, exercise or defence of legal claims; d) you, the data subject, have objected to processing of your personal data pending the verification of whether there are legitimate grounds for us to override these objections.

Right to data portability. You, the data subject, shall have the right to receive your personal data, which you have provided to us and have the right to transmit this data to another controller, without hindrance from us.

Right to object. You, the data subject, shall have the right to object, on grounds relating to your situation, at any time to the processing of personal data concerning you, including any personal profiling; unless this relates to processing that is necessary for the performance of a task carried out in the public interest or an exercise of official authority vested in us. We shall no longer process the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of you, the data subject, or for the establishment, exercise, or defence of legal claims.

Right to not be subject to decisions based solely on automated processing. We do not carry out any automated processing, which may lead to an automated decision based on your personal data.

Changes to our Privacy Policy. Please check back frequently to see any updates or changes to our privacy policy. If you have any questions or queries which are not answered by this Privacy Policy, or have any potential concerns about how we may use the personal data we hold, please contact HR. Right to Complain If your complaint is not resolved to your satisfaction and you wish to make a formal complaint to the Information Commissioner's Office (ICO), you can contact them on 01625 545745 or 0303 123 1113. You also have the right to judicial remedy against a legally binding decision of the ICO where you consider that your rights under this regulation have been infringed because of the processing of your personal data. You have the right to appoint a third party to lodge the complaint on your behalf and exercise your right to seek compensation.