Index

1. Introduction

1.1 We are committed to protecting the privacy and personal information of all our staff, contractors, and suppliers by striving to ensure we handle personal data fairly, lawfully, sensitively and with justification.

1.2 Personal data relates to any recorded information held by us from which a living individual can be identified. It will include a variety of information including names, addresses, date of birth, NI number, telephone numbers, photographs of people (including CCTV images) and other personal details. It will include any expression of opinion about a living individual or any indication of our intentions about that individual. Identification can be directly from the information alone or indirectly from any other information in the Data Controller's possession or likely to come into their possession.

1.3 The Data Controller is the person who decides how personal data is processed and for what purposes.

1.4 We will comply with The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) (the "Regulations") and this data protection policy covers the activities of:

1.4.1 Salisbury Workplace Services Limited

1.4.2 Salisbury Integrated Services Limited
1.4.3 Salisbury Engineering and Compliance Limited
1.4.4 Salisbury Security Services Limited
(together "Salisbury Group Companies").

1.5 Any breaches of this policy could have serious consequences for Salisbury Group and lead to reputational or financial damage to us. Breaches will be treated as a matter of serious gross misconduct and will be dealt with in accordance with Salisbury Group's disciplinary policy.

2 Purposes of the processing

2.1 Salisbury Group processes personal data to enable us to carry out building facilities management and services; promote and advertise our services, maintain our own accounts and records, support and manage our people. Our services include:

2.1.1 Energy
2.1.2 Cleaning
2.1.3 Engineering
2.1.4 Maintenance
2.1.5 Grounds maintenance
2.1.6 Catering
2.1.7 Mailroom Services
2.1.8 Facilities Management Services
2.1.9 Porterage
2.1.7 Security

3 How we collect personal data

3.1 Salisbury Group and their subcontractors handle a range of personal data relating to customers, suppliers, staff, and clients. Our collection and processing of personal data is subject to a variety of legal requirements. We process and retain personal data for purposes which include:

3.1.1 Recruitment, screening, vetting and identity checks
3.1.2 Contracts of employment, and payroll purposes including tax and National Insurance
3.1.3 Equal opportunities monitoring
3.1.4 Commercial contracts and compliance
3.1.5 Medical and health records
3.1.6 External supplier and customer relationships
3.1.7 Disciplinary and grievance procedures
3.1.8 Training/development records and performance information
3.1.9 Management purposes
3.1.10 IT services and management, computer records and e-mails

4 How we process personal data

4.1 The Data Controller is responsible for compliance with our obligations under the GDPR by ensuring that personal data is:

4.1.1 Processed lawfully, fairly and in a transparent manner
4.1.2 Collected for specified, explicit and legitimate purposes
4.1.3 Adequate, relevant and limited to what is necessary

4.1.4 Accurate and kept up to date
4.1.5 Retained only as long as necessary
4.1.6 Processed in an appropriate manner to maintain security

5 Legal basis for processing personal data

5.1 Salisbury Group will only process data in compliance with one of the following conditions:

5.1.1 Consent of the data subject – must be freely given, specific, informed and unambiguous by clear explicit means. A consent form exists for this purpose
5.1.2 Processing essential to the performance of a contract or steps required to enter into a contract
5.1.3 Compliance with a legal obligation
5.1.4 When necessary to protect the vital interests of a data subject
5.1.5 When necessary in the public interest or exercise of authority vested in the controller
5.1.6 Legitimate interests pursued by the Data Controller

6 Special categories of 'sensitive personal data'

6.1 Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

7 Legal basis for processing special categories of 'sensitive personal data'

7.1 As well as satisfying the 'legal basis for processing personal data' above, processing of 'sensitive personal data' is prohibited unless one of the following conditions is met:

7.1.1 Explicit consent – linked to a consent form
7.1.2 Processing is necessary for carrying out obligations under employment, social security, or social protection law, or a collective agreement
7.1.3 Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically incapable of giving consent
7.1.4 Processing is carried out by a foundation or not for profit organisation
7.1.5 Processing relates to personal data manifestly made public by the data subject
7.1.6 Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
7.1.7 Reasons of public interest in the area of public health
7.1.8 Processing is necessary for reasons of substantial public interest
7.1.9 Processing is necessary for reasons of preventative or occupational medicine, for assessing the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment/management of health

8. Record of processing

8.1 Salisbury Group will process data for the following purposes:

8.1.1 Property Management
8.1.2 Providing Facilities Services
8.1.3 Marketing and promoting FM Services

8.1.4 Managing accounts
8.1.5 Maintaining personnel records
8.1.6 Managing our people
8.1.7 Use of CCTV systems to monitor and collect visual images for the purposes of security, prevention and detection of crime, public safety and staff safety

8.2 Processing personal data as a contractual requirement for the purposes of security screening and vetting of staff, partner agencies and their sub-contractors in compliance with:

8.2.1 Baseline Personnel Security Standard (BPSS)
8.2.2 Counter Terrorism Check (CTC)
8.2.3 Security Clearance (SC)

8.3 Processing personal data through vehicle tracking devices (Telematics) for the purposes of;

8.3.1 Safety and legal compliance – to increase driver safety and security, through safer and compliant driving as well as helping ensure the safety and consideration for other road users
8.3.2 Operational efficiencies – to provide data that supports operational improvements for example – start and finish times, and engineer availability
8.3.3 Vehicle cost efficiencies – to reduce maintenance costs, insurance costs, reduce the likelihood of accidents, and hire costs associated with vehicle downtime
8.3.4 Environmental – improve fuel efficiency, CO2 reduction, engine idling reduction

8.4 Processing personal data using telematics enabled smart devices for the purposes:

8.4.1 Legal compliance – Statutory Inspections of plant and safety equipment
8.4.2 Operational efficiencies – to provide data that supports operational improvements for example – start and finish times
8.4.3 Productivity – planned and reactive maintenance
8.4.4 Efficiencies – reduced time to respond and fix

8.5 Processing personal data for productivity and efficiency of staff in respect of effective planning and organisation of resources, travel time, overtime and budgetary management.

9. Sharing Of Personal Data

9.1 Salisbury Group will only share data with GDPR compliant organisations. Information is shared on a need to know basis and only the necessary information is shared. Typical examples where we are required to share data are:

9.1.1 HM Revenue and Customs
9.1.2 HM Government Screening and Vetting Unit
9.1.3 Payroll Bureau
9.1.4 Clients and customers who restrict access to their sites for security reasons
9.1.5 Training providers and accrediting bodies
9.1.6 Marketing
9.1.7 Travel and accommodation bookings

9.2 We also process and share personal data from the following sources as a direct consequence of our business:

9.2.1 Service partners, suppliers of services and sub-contractors
9.2.2 Consultants
9.2.3 Clients and customers

9.3 Legal Requirements

9.3.1 We may be required to share personal data in pursuance of sub-section 5.1. - legal basis for processing personal data above – 'compliance with a legal obligation' or 'when necessary in the public interest'. An example would be release of data when required by law such as legal proceedings or to law enforcement agencies in the course of a criminal investigation, matters of public health and substantial public interest.

10. Retention of personal data

10.1 We keep personal data for no longer than reasonably necessary, for retention periods please refer to – 'Salisbury Group Document Retention Policy' (SAL-PO-1032).

11. Security of personal data

11.1 Salisbury takes the security of its personal data very seriously. We have security procedures and a 'Salisbury Information Security Policy' (SAL-BM-5.2) to ensure we handle data appropriately and protect it from accidental loss or misuse. We only permit access to information with there is a legal basis to do so.

12. Data Breach's

12.1 Salisbury takes the security of its personal data very seriously and takes many measures to safeguard against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data. Please refer to 'Salisbury Information Security Incident Management Policy' (SAL-BM-C-16). Information security breaches should be reported on Information Security Incident Reporting Form 16.1A. (SAL-BM-C-R-16.1A).

13. Transfer of Data Abroad

13.1 Salisbury do not ordinarily transfer personal data outside of the European Community. On occasions personal data may be transferred to the USA under the protection of USA Privacy Shield agreement.

14. Automated Decision Making

14.1 Automated decision making is a decision made by automated means without any human involvement. Salisbury do not employ any such system or methods.

14.2 Profiling – processing of personal data to evaluate certain things about an individual can form part of automated decision making such as psychometric testing for recruitment purposes. Any use of such will be strictly governed by the Head of Human Resources and based upon explicit consent. Results will be restricted to those members of staff necessary in the recruitment process.

14.3 The GDPR only allows automated individual decision making and profiling on the following grounds

14.3.1 Necessary for the entry into or performance of a contract; or
14.3.2 Authorised by law
14.3.3 Based upon an individual's explicit consent

14.4 The Head of Human Resources will:

14.4.1 Follow ICO guidance
14.4.2 Conduct a Data Privacy Impact Assessment to identify the risks to individuals
14.4.3 Provide individuals with specific information about the processing and logic involved in the decision making
14.4.4 Introduce additional safeguards to prevent errors, bias or discrimination
14.4.5 Allow for challenging any findings or decision
14.4.6 Ensure the process is proportionate

14.5 No special categories of personal data will be processed.

15. Further Processing

15.1 If Salisbury wishes to process personal data for a new purpose, not covered by the privacy notice, then we shall provide you with a new notice explaining this new issue prior to commencing the processing and setting out the relevant purpose and processing conditions. Whenever necessary we will seek your prior consent to the new processing.

16. Right to be informed

16.1 If the personal data is not obtained directly from the data subject, the Data Controller will provide the data subject with the following additional items of information within 1 month of having received their personal data:

16.1.1 The categories of personal data we are processing

16.1.2 The source from where the personal data originates and whether it came from publicly accessible sources

17. Data subject rights

17.1 The right to request a copy of your personal data which Salisbury holds about you
17.2 The right to request that the Data Controller corrects any personal data that is found to be inaccurate or out of date
17.3 The right to request your personal data is erased where it is no longer necessary to retain such data
17.4 The right to withdraw consent to processing at any time – if consent is relied upon as a processing condition
17.5 The right to request that the Data Controller provide the data subject with their personal data and where possible to transmit that data directly to another Data Controller (Data Portability) – only applies where the processing is based on consent or is necessary for the performance of a contract with the data subject and where the Data Controller processes the data by automated means
17.6 The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing
17.7 The right to object to the processing of personal data – where processing is based on legitimate interests or performance of a task in the public interest/exercise of official authority, and direct marketing
17.8 The right to lodge a complaint with The Information Commissioners Office (ICO)

18. Subject Access Requests

18.1 The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) details rights of access to Data Subjects to their personal data held by Salisbury. A Subject Access Request (SAR) is a written request for personal information held about a data subject who generally has the right to see what personal data we hold about them. All requests for information must be directed to The Data Controller without delay and will be dealt with in accordance with 'Salisbury Subject Access Request Policy' (SAL-PO-1039).

19. Obligation of Salisbury Companies staff and contractor's

19.1 The Data Controller is the person who decides how personal data is processed and for what purposes. As part of Salisbury's control measures key individuals within our business will be formally appointed Data Processors and receive commensurate training. They will process data in accordance with this policy and under the direction of The Data Controller.

19.2 The Data Controller will maintain a register of persons responsible for data privacy for all contractors, service partners, clients and customers. Salisbury will only share data with GDPR compliant organisations.

19.3 The Data Protection Officer will effect 'day to day' operational controls over data processing.

19.4 All employees and contractors working for Salisbury Companies must be aware of the importance of handling personal data while working on Salisbury business and ensure:

19.4.1 They understand their responsibilities when handling or managing personal data;

19.4.2 That the only individuals authorised to access personal data are those who need it for their work

19.4.3 All personal data is kept secure by using strong passwords which should be kept confidential

19.4.4 Personal data is not disclosed to unauthorised people, either within the company or externally

19.4.5 Personal data is reviewed and updated if found to be out of date and if no longer required, should be deleted or safely disposed

20 Storage of Personal Data

20.1 Paper records

20.1.1 Personal data stored on paper should be kept in a secure place where unauthorised people cannot access it. Personal data printouts should be shredded and disposed of securely when no longer required.

20.1.2 Bulk confidential waste should be managed in accordance with 'Salisbury Confidential Waste Policy' (SAL-PO-1047).

20.2 Electronic records – Salisbury Information Security Policy (SAL-BM-5.2)

20.2.1 Personal data stored electronically must be protected from unauthorised access, accidental deletion and cyber-attack. The following safeguards shall apply:

20.2.2 Personal data should not be stored on removable media (like a disc, portable hard drive or memory stick) without the express permission of The IT Director and in accordance with Acceptable Use Policy (SAL-BM-C-8.1.3) and Mobile Device Policy (SAL-BM-C-6.2.1)any removable media devices should be kept locked away securely when not being used

20.2.3 Servers containing personal data should be sited in a secure location, not in general office space

20.2.4 Personal data should be backed up frequently

20.2.5 Personal data should never be stored on a laptop unless it is encrypted

20.2.6 Personal data should not be stored on mobile devices like tablets or smart phones unless they are encrypted

20.2.7 All servers and computers containing personal data should be protected by appropriate software and a firewall

21 Use of Personal Data

21.1 Personal data is of no value to us unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. When handling personal data, we must all ensure:

21.1.1 Compliance with 'Salisbury Group Clear Desk Policy' (SAL-PO-1043)

21.1.2 Computer screens are always locked when left unattended

21.1.3 Personal data should not be shared between individuals, unless it is necessary for work undertaken

21.1.4 Sensitive personal data should be password protected if being sent by email

21.1.5 Personal data should not be saved onto personal devices

22 Accuracy of Personal Data

22.1 It is the responsibility of all of us who work with personal data to take reasonable steps to ensure it is accurate and up to date. Data should be corrected when inaccuracies are discovered.

23 Salisbury Group's commitment to data protection

23.1 We will ensure that:

23.1.1 Everyone managing and handling personal data understands that they are responsible for following good GDPR practice

23.1.2 Methods of managing or handling personal data are regularly reviewed and evaluated

23.1.3 Any disclosure of personal data will comply with approved procedures

23.1.4 We take all necessary steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure

23.1.5 All contractors who are users of personal data supplied by us will be required to confirm that they will abide by the requirements of GDPR with regard to personal data supplied by us.

23.2 The Data Controller leads on data protection for Salisbury Group Companies. They are responsible for ensuring that this policy is effectively implemented. They will conduct an annual review to ensure compliance with GDPR and this policy. They will also review this policy regularly to ensure it remains fit for purpose.

24 Key Contacts

To exercise all relevant rights, queries or complaints please contact:

Data Controller - Nigel Davies Security Operations Director nigel.davies@salisburygroup.com

Data Protection Officer – Graham Hanson Compliance Manager graham.hanson@salisburygroup.com

Head of Human Resources – Angie Grace angie.grace@salisburygroup.com