Head Office and Sales
Building 3
Workwell Office
Selby Road, LeedsLS15 4LG

Privacy and Security

Smarta Energy is committed to ensuring the privacy and confidentiality of customer data through the adoption of comprehensive privacy and security policies. These policies are designed in alignment with industry standards such as GDPR, ISO 27001, and NIST guidelines. Key responsibilities for data protection are clearly defined, with a dedicated Data Protection Officer (DPO) overseeing compliance, managing data protection measures, and ensuring that all staff are trained and aware of their obligations. Regular audits and policy reviews are conducted to ensure ongoing compliance and address any areas of improvement.

Data Access Control and Monitoring

Smarta Energy enforces strict and granular data access processes, based on the principle of need-to know. Access to sensitive data is restricted to authorized personnel only, using multi-factor authentication and role-based permissions. Access logs are monitored regularly, and any unauthorized access attempts are investigated promptly. Periodic audits are conducted to validate access controls, and violations of data access policies are subject to disciplinary measures, reinforcing the importance of maintaining data confidentiality.

Data Security Standards

Smarta Energy adheres to stringent data security standards, employing best practices from international standards such as ISO 27001 for Information Security Management and NIST Cybersecurity Framework. These standards guide our approach to data encryption, secure data storage, and transmission, as well as vulnerability management. Our systems are regularly tested for security vulnerabilities, and our infrastructure is designed to minimize risks of data breaches.

Regular Review and Assurance

Internal privacy and security policies are reviewed regularly to assess the effectiveness of the implemented security measures. These reviews include assessments against evolving threats, new regulatory requirements, and emerging best practices. Smarta Energy employs a continuous improvement approach, where findings from these reviews inform updates to our security posture, ensuring that our measures remain robust and effective in protecting client data.

Operations Centre
Redwood House, Brotherswood Court
Almonds- bury Business Park, Bristol, BS3 4QW
Registration: 12403001

Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. The group policies and procedures are designed to ensure compliance with the principles.

Personal data must be processed lawfully, fairly and transparently. The GDPR has increased requirements about what information should be available to data subjects. Transparently – the GDPR includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

It is also the responsibility of the data subject to ensure that data held by the group is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

Staff should be required to notify the company of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the business to ensure that any notification regarding change of circumstances is recorded and acted upon. The Organisation Data Protection Officer / GDPR Owners are responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

On at least an annual basis, the organisation Data Protection Officer / GDPR Owners will review the retention dates of all the personal data processed by the group, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered
purpose. This data will be securely deleted/destroyed.

The Organisation Data Protection Officer / GDPR Owners are responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing. Personal data will be retained in line with the organisation Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

The organisation Data Protection Officer / GDPR Owners must specifically approve any data retention that exceeds the retention periods defined in Retention of Records Procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation.

Personal data must be processed in a manner that ensures the appropriate security in determining appropriateness, the organisations Data Protection Officer / GDPR Owner should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or students) if a security breach occurs, the effect of any security breach on the group itself, and any likely reputational damage including the possible loss of customer trust.

Security of Data

All Staff are responsible for ensuring that any personal data that the company holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the company to receive that information and has entered into a confidentiality or data sharing agreement.

All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security and must be kept: in a lockable room with controlled access; and/or in a locked drawer or filing cabinet; and/or if computerised, password protected in line with corporate requirements

Care must be taken to ensure that staff PC screens and terminals are not visible except to authorised staff of the company. Manual records may not be left where they can be accessed by unauthorised personnel.

Personal data may only be deleted or disposed of in line with the organisation Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required before disposal.

Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off site.