TRUST. WELL EARNED.	BRUSH Group Data Protection Policy	**Document Number**	BRUSH-LE/BPL/0006
		Issue	C

Department	Legal	**Approver**	D Jordan	**Signature**		**Date**	11/11/2022

THIS PAGE IS INTENTIONALLY BLANK

TRUST. WELL EARNED.

BRUSH Group
Data Protection Policy

The BRUSH Data Protection Policy must be followed by anyone who works for or represents BRUSH, including directors, officers, employees, agents, distributors, and business associates working for or on behalf of any BRUSH entity, including, but not limited to:

BRUSH Group Ltd., BRUSH Transformers Ltd., Hawker Siddeley Switchgear Ltd., Aprenda Ltd., Kirkman Utility Services Ltd., Eta Projects Ltd. and Hawker Siddeley Switchgear Pty Ltd.

Employees must gain an understanding of the Data Protection Policy and ensure that its principles are fully applied in relevant areas of their job role

Principle

This Policy sets out the obligations of BRUSH Group ("the Group" or "the Company) regarding data protection and the rights of its employees (in this context, "employee data subjects") in respect of their personal data under Data Protection Law. "Data Protection Law" means all legislation and regulations in force from time to time regulating the use of personal data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.

This Policy sets out the Group's obligations regarding the collection, processing, transfer, storage, and disposal of personal data relating to employee data subjects. The procedures and principles set out herein must be always followed by the Group, its employees, agents, contractors, and other parties working on behalf of the Group.

Compliance with data protection law is essential to ensure that personal data remains safe, the Group's business operations are secure, and the rights of individuals are respected. The Group's business units are data controllers under data protection law, meaning they decide how, why, and when they use personal data. This Policy explains the procedures for complying with data protection law in relation to personal data. It also sets out employees' obligations whenever they are processing any personal data in the course of their employment.

Who is responsible for data protection at BRUSH?

The Board is ultimately responsible for BRUSH's compliance with applicable data protection law.

All employees at BRUSH have responsibility for ensuring that personal data is kept secure and processed in a lawful manner although certain employees will have particular responsibilities, of which they will be aware and in respect of which they may receive specific instructions.

If an employee is in any doubt about how they should handle personal data, or if they have any concerns or questions in relation to the operation (or suspected breaches) of this Policy, they should seek advice from their line manager, the company's Data Privacy Manager or the Human Resources department

What is personal data?

Personal data means any personal or business-related information relating to any living individual (also known as a 'data subject'); who could be colleagues, consumers, members of the public, business contacts, etc. that identifies them directly or indirectly. Data may include but is not limited to:

- Name
- Address
- NI number
- Date of birth
- Employee number
- Email address

Personal data may be automated (e.g., electronic records such as computer files or in emails) or in manual records which are part of a filing system or are intended to form part of a filing system (e.g., structured paper files and archives).

Some personal data are deemed as 'Special Category' data because such information reveals high risk details of an individual's:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Physical or mental health;
- Sexual life or sexual orientation;
- Biometric or genetic data (if used to identify that individual); and
- Criminal offences or convictions.

Data Protection Obligations

BRUSH is responsible for and must be able to demonstrate compliance with data protection law. It is essential that employees comply with data protection law and any other Company policies, guidelines or instructions when processing personal data in the course of their employment.

Set out below are the key obligations under data protection law and details of how BRUSH expects employees to comply with these requirements.

What does "processing" personal data mean?

Processing personal data means any activity that involves the use of personal data (e.g., obtaining, recording, or holding the data, amending, retrieving, using, disclosing, sharing, erasing, or destroying). It also includes sending or transferring personal data to third parties.

Legal grounds for processing Data protection law allows the processing of personal data only where there are fair and legal grounds which justify using the information and at least one of these must be satisfied for each processing activity.

- Complying with a legal obligation (e.g., health and safety or tax laws);
- Entering or performing a contract with the individual (e.g., an employee's terms and conditions of emp'oyment, or a contract for services with an individual customer);
- Acting in BRUSH or a third party's legitimate interests (e.g., maintaining records of business activities, monitoring business productivity);
- Obtaining the consent of the individual (e.g., for sending direct marketing communications).
- To ensure the vital interest of the individual; and
- To carry out and administer justice

Where consent is relied upon, it must be freely given, specific, informed, and unambiguous, and BRUSH must effectively demonstrate that consent has been given. In line with Information Commissioners Office (ICO) guidance regarding the employer/employee relationship, BRUSH will not use consent as a legal ground for processing employee data unless the data processing activities concerned are genuinely optional.

In most cases, consent is not required for other standard business activities involving use of customer or supplier data, but it may be needed for activities which are not required to manage the main business relationship, such as direct marketing activities.

Transparency

Data protection law also requires BRUSH to process personal data in a transparent manner by providing individuals with appropriate, clear, and concise information about how their personal data is processed.

BRUSH provides individuals with basic information about how their data is processed on forms which collect data (such as application forms or website forms), and in the Employees Privacy Notice, setting out details including: the types of personal data that is held about them, how it is used, the legal grounds for processing the information, who it might be shared with and how long it is kept for.

BRUSH supplements these notices, where appropriate, with reminders or additional information at the time particular processing activities take place or become relevant for an individual (for example when they sign up for a new service or event).

The standard privacy notices and statements that are issued, for example, to employees, customers, and the public, should normally be sufficient to ensure that individuals have appropriate information about how their personal data is handled in the course of employment. However, consideration should be given as to whether reminders or additional information may be appropriate at the time particular processing activities take place. This is particularly important if it is considered that individuals may need further assistance to understand clearly how their data will be used as part of such activities.

Any new forms which collect personal data, and any proposed consent wording must be approved in advance by the Data Privacy Manager and Human Resource department.

Any concerns about the legal grounds for processing personal data or whether individuals have been provided with appropriate information (in particular in relation to any new processing activities), should be checked with the Data Privacy Manager or the Human Resource department.

Handling sensitive or special category personal data

In addition to the legal grounds to process personal data an additional legal ground, from the list below, must exist to justify using sensitive information.

- Complying with a legal obligation/exercising a legal right in the field of employment;
- Assessing working capacity (based on expert medical opinion, and subject to obligations of confidentiality);
- Carrying out equalities monitoring in relation to racial or ethnic origin, religious beliefs, health or sexual orientation;
- Exercising, establishing, or defending legal claims;
- Preventing or detecting unlawful acts; or
- Explicit consent of the individual. This requires an express statement from the individual that their special category of data may be used for the intended purposes.

When handling special category personal data in the course of employment, employees must ensure:

- Any processing activities are strictly in accordance with their lawful job duties and the Company's instructions;
- Individuals have received adequate information regarding how their data is being handled. In some cases, an existing privacy notice may need to be supplemented with more specific information regarding special category data (e.g., when BRUSH is managing sickness absence and/or making adjustments to job duties for employees with disabilities or serious illness.
- Additional security and confidentiality measures must be applied, considering that the impact on individuals of loss or misuse of their special category data may be greater than with other types of data; and
- When relying on consent as a legal ground for processing data, advance approval of any consent wording must be obtained from the Data Privacy Manager.

Processing purposes

BRUSH will only process personal data in accordance with legitimate purposes to carry out its business operations, to administer employment and other business relationships and that the data is adequate, relevant for its purpose, limited to what is necessary for those purposes and is accurate and up to date.

Employees must:

- Only process personal data in the course of their duties for BRUSH's legitimate and authorised purposes,
- Not process personal data for any purposes which are unrelated to their job duties,
- Be able to justify why each specific category of data is being requested on any forms being created,
- Adhere to the BRUSH's Data Retention policy to ensure that personal data is only kept for as long as it is needed for any intended purpose, and
- Ensure that the HR department is informed of any changes to an employee's personal circumstances.

Processing personal data for any incompatible or unauthorised purposes could result in a breach of data protection law. This may have potentially damaging consequences for all parties concerned, including disciplinary action against the employee.

If an employee find that they need to process personal data for a different purpose from that for which it was originally collected, they must check whether the individuals have been informed and, if not, consider whether the additional purpose is legitimate (in the context of BRUSH's business activities) and compatible with the original purpose.

Document Retention

Records containing personal data should only be kept for as long as they are needed for the identified purposes. BRUSH has in place a Data Retention Policy that includes the retention limits for each type of data held by the Group.

Employees should familiarise themselves with the Data Retention Policy, processes, guidelines, and instructions that are relevant to their job. Ensure that, where it falls within their responsibility, employees destroy or erase all information that they no longer require in accordance with the instructions in the Data Retention Policy.

Data Security

Keeping personal data safe and complying with BRUSH's security procedures to protect the confidentiality, integrity, availability, and resilience of personal data is a key responsibility for BRUSH and its workforce.

BRUSH has IT policies which set out its organisational and technical security measures to protect information, including personal data. The policies set out protocols for employees on use of technology and communications systems to ensure appropriate security of personal data stored or communicated using such systems. These systems are regularly reviewed and tested to assess the effectiveness of these measures to ensure the security of its personal data processing activities.

BRUSH also outlines other organisational methods of protecting personal data as detailed in the IT Security Policy, IT Security User Password Standard, BRUSH Group Electronic Information and Communication Systems Policy and other associated policies.

Sharing Personal Data

The sharing or disclosure of personal data is a type of processing, and therefore all the principles described in this policy need to be applied.

Internally

Employees must ensure that personal data is only shared internally on a 'need to know' basis with authorised employees, and specific to the purpose for which they are intended. It must be shared via a secure method or if shared by email, it must be password protected with a robust password disclosed via a different method.

Externally

BRUSH will only share personal data with other third parties (including group entities) where there is a legitimate purpose, and an appropriate legal ground under data protection law which permits the sharing. This could include situations where there is a legal obligation to provide the information (e.g., to HMRC for tax purposes), where necessary to perform contractual duties to individuals (e.g., provision of information to the Group's occupational pension providers) and to appointed third party service providers who will handle information on the Group's behalf, for example to provide payroll, data storage or other technology services.

Details of the recipients or categories of recipients of personal data (including processors and other third parties) will be set out in privacy notices.

Employees may only share or disclose the personal data held internally with an employee, agent, or representative of BRUSH if the recipient has a job-related need to know the information.

Equally, employees may only disclose the personal data held to service providers or other third parties (including group entities) where:

- There is a legitimate purpose and an appropriate legal ground for doing so (e.g., it is necessary for them to process the personal data to provide a service to BRUSH such as payroll, or when legally obliged to do so);
- The individuals whose personal data is being shared have been properly informed (e.g., in an appropriate privacy notice);
- If the disclosure is to a service provider, BRUSH has checked that adequate security and data protection measures are in place to protect the personal data concerned;
- The service provider or third party has entered a written contract with BRUSH that contains the provisions required by data protection law; and
- The transfer complies with any overseas transfer restrictions, if applicable.

Routine disclosures of personal data to established recipients (e.g., payroll providers or group entities) which form a normal and regular part of an employees' role and job duties will ordinarily satisfy the above requirements.

Transfer of personal data outside of the UK and European Economic Area (EEA)

There may be occasions whereby data needs to be processed (e.g., transmitted, sent, viewed, accessed) or otherwise processed in a different country outside of the UK and EEA (this is the European Union plus Norway, Liechtenstein, and Iceland). Those countries outside of the UK and EEA may not have the same level of data protection, therefore the Company is obligated to ensure that adequate data protection measures are put in place and agreed upon before personal data is shared.

Before any data is shared with any organisations outside the UK and EEA countries, the below information must be established: This is particularly important in situations where employees are deployed outside of the UK and EEA for the purposes of performing work to fulfil their contract of employment with the Company.

- A detailed understanding of what data is required, who it is to be shared with, its intended purpose and appropriate safeguards followed as outlined in Appendix A;
- Assess the risks considering the principles in this policy and consider the restrictions on transfers outside the UK and EEA. Put in place additional appropriate safeguards where required;

- Insert a completed Appendix A into the commercial contract that is being entered, along with the appropriate data protection language; and
- Obtain approval to share the data from the Data Privacy Manager and retain a copy with the project paperwork
- When sending data to organisations and/or individuals, inside or outside of the UK and EEA, data must always be contained within an encrypted file with the password sent via alternative methods to avoid the data being compromised.

Data breaches and reporting

BRUSH takes any data protection breaches very seriously. Examples of a data breach can include:

- Lost or mislaid equipment or data,
- Use of inaccurate or excessive data,
- Failure to address an individual's rights,
- Accidental sending of data to the wrong person,
- Unauthorised access to, use of or disclosure of data,
- Deliberate attacks on the Company's systems;
- Theft of records, and
- Any equivalent breaches by BRUSH's service providers.

If an employee becomes aware of any breach (or suspected and potential breach) of this Policy, they must report it to the Data Privacy Manager immediately.

Where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to individuals' personal data the Company will take immediate steps to:

- Identify the breach, causes and impacts;
- Contain and remedy the breach;
- Notify all appropriate parties (see below).;
- Put in place mechanisms to avoid the breach reoccurring;
- Document all actions taken; and
- Record the breach and measures regardless of their effect and whether they should be reported to the ICO

If BRUSH discovers that there has been a personal data security breach that poses a risk to the rights and freedoms of individuals, the Data Privacy Manager will report it to the ICO within 72 hours of discovery.

If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the Company will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures BRUSH has taken.

Automated decision making

Profiling, or automated decision-making, occurs where an individual's personal data is processed and evaluated by automated means resulting in an important decision being taken in relation to that individual. This poses particular risks for individuals where a decision is based solely on that profiling or other automated processing.

The Group does not currently undertake this activity.

Privacy by design

Data protection law requires BRUSH to build data protection considerations and security measures into all its operations that involve the processing of personal data, particularly at the start of a new project or activity which may impact on the privacy of individuals.

At the beginning of any project, in conjunction with other project stakeholders, employees must give due consideration to all the principles of data protection set out in this policy and detailed within a **Data Protection Impact Assessment** ('DPIA').

A DPIA will ensure consideration is given to all aspects and potential risks to data protection within the project at the beginning and throughout its lifecycle with the intention of assessing the necessity and proportionality of a processing operation, the risks to individuals and the measures that can be put in place to mitigate those risks. The following factors must be considered:

- The risks (and their likelihood and severity) posed by the processing for the rights and freedoms of individuals;
- Technological capabilities;
- The cost of implementation; and
- The nature, scope, context, and purposes of the processing of personal data.

A copy of the DPIA form can be obtained from the Data Privacy Manager.

Individual rights and requests

Under data protection law, employees have certain rights when it comes to how the Group handles their personal data. For example:

- **The right to make a 'subject access request'.** This entitles an individual to receive a copy of the personal data held about them, together with information about how and why it is processed and other rights which they have (as outlined below). This enables them, for example, to check their data is being lawfully processed and to correct any inaccuracies.
- **The right to request that the Company corrects incomplete or inaccurate** personal data that is held about them.
- **The right to withdraw any consent** which they have given.
- **The right to request that the deletion or removal of** personal data that is held about them where there is no good reason to continue to process it. Individuals also have the right to request deletion or removal of their personal data where they have exercised their right to object to processing (see below).
- **The right to object to the processing** of their personal data for direct marketing purposes, or where the Company is relying on its legitimate interest (or those of a third party), where a compelling reason to continue the processing cannot be given.
- **The right to request the restriction in processing of** their personal data. This enables individuals to ask the Company to suspend the processing of personal data about them, for example if they want to establish its accuracy or the reason for processing it.
- **The right to request the transfer** to them or another party, in a structured format, their personal data which they have provided to the Company (also known as the right to 'data portability'). The applicability of this right depends on the legal grounds on which it is processed.
- **The right to challenge a decision** based solely on profiling/automated processing, to obtain human intervention, and to express their point of view.

The Company is required to comply with these rights without undue delay and, in respect of certain rights, within a one-month timeframe. Each request is considered upon its own merits and also considered against the Company's lawful basis for processing the data in question.

Individuals also have the right to complain about the Company's practices in relation to their rights by submitting their complaint in writing to the Data Privacy Manager and/or to the ICO/

Data processing map

To comply and demonstrate compliance with data protection law, BRUSH keeps various records of its data processing activities. These include a Data Process Map which contains, as a minimum, the purposes of processing; categories of data subjects and personal data; categories of recipients of disclosures of data; information about international data transfers; envisaged retention periods; general descriptions of security measures applied; and certain additional details for special category data. This map allows for a transparent view of how data flows through the Company as well as providing clear guidelines for all processors when processing personal data.

Employees must also comply with applicable processes/guidelines and any specific instructions given concerning the keeping of records about the processing of personal data.

If an employee is processing individuals' personal data in the course of their employment and any new types of personal data are collected, or any new types of processing activities undertaken, either through the introduction of new systems or technology or by amending existing ones, please inform the Data Privacy Manager so that records can be kept up to date.

Training

Employees are required to undergo training to enable them to comply with data protection law and this policy. Additional training may be required for specific roles and activities involving the use of personal data.

To this end, the Company provides training for new joiners to BRUSH and refresher training to existing employees. Attendance at such training is mandatory and is documented.

APPENDIX A – DATA TRANSFER CONSIDERATIONS FOR OUTSIDE OF EEA

What data, relating to the individual(s), do you intend to collect, process, store, use, view, share?	
What are the individual (categories) you are requesting the data about?	
Who in your organisation will have access to share, use and process this data?	
What are your reasons for needing this data? (Please be as specific as possible)	
What systems do you intend to use to process this data?	
What security measures will you put in place to ensure the data is securely protected, processed, stored, deleted, and not shared with individuals other than with those individuals mentioned above?	
What other individuals / organisations will you be sharing this data with (both inside and outside of your country) – please also detail the country and why?	
How have you ensured that the third-party individual / organisation will ensure the data is secured?	
How long will you keep the data before you destroy it by secure methods?	