Data Protection Policy

This policy is intended to define the policy and principles adopted by the following companies in the David Brown Santasalo Group (each severally referred to as “DBS”, “we”, “us” or “our” throughout this policy document) to govern the processing of personal data:

- David Brown Systems UK Limited (Registered number SC341775 Scotland)
- David Brown Group Limited (Registered number 2432631 England)
- David Brown Gear Systems Limited (Registered number 6624684 England)
- David Brown UK Holdings Limited (Registered number 6677806 England)
- DB Union Pension Trustees Limited (Registered number SC 343362 Scotland)
- Santasalo Gears OY (Registered number 2646194-8 Finland)
- David Brown France Engrenages SAS (Registered number RCS Mulhouse 397 799651 France)
- Santasalo Gears AB (Registered number 556116-9607 Sweden)
- Santasalo Gears GmbH (Registered number HRB 3458 Germany)
- Santasalo Gears France Sarl (Registered number B790 806 129 France)

The policy explains when and why we collect personal data about individuals, how we keep it secure and the data subject’s rights in relation to the personal data processing. DBS wants to ensure that employees handling personal data recognise the risks involved when dealing with personal data and fully understand the steps which need to be taken to minimise such risks and take appropriate steps to ensure that DBS complies with the law.

DBS are a data controller for the purposes of the GDPR and are registered with the Information Commissioner. The DBS companies can be contacted by email at: **compliance@dbsantasalo.com**, or by post to the following addresses**:**

David Brown Systems UK Limited	3 Redwood Crescent, East Kilbride, G74 5PA, Scotland
David Brown Group Limited	Park Works, Park Road, Huddersfield, HD4 5DD, England
David Brown Gear Systems Limited	Park Works, Park Road, Huddersfield, HD4 5DD, England
David Brown UK Holdings Limited	Park Works, Park Road, Huddersfield, HD4 5DD, England
DB Union Pension Trustees Limited	3 Redwood Crescent, East Kilbride, G74 5PA, Scotland
Santasalo Gears OY	Vesangantie 1, 40100 Jyväskylä Finland
David Brown France Engrenages	33 Rue Henri Lebert, 68800 Thann, France
Santasalo Gears AB	Norra Långebergsgatan 4 SE-421 32 Göteborg, Sweden
Santasalo Gears GmbH	Otto-Hahn-Str. 51 42369 Wuppertal Germany
Santasalo Gears France Sarl	2 Place de l'Eglise, 33310 Lormont, France

DBS regards the lawful and correct treatment of personal data as crucial to the delivery of the highest quality of service and recognises that everyone has rights in relation to how their personal data is handled.

DBS will:

- always comply with the General Data Protection Regulation ("the GDPR");
- ensure staff and other individuals are fully aware of both their rights and obligations under the GDPR; and
- implement adequate and appropriate physical and technical security measures and organisational measures to ensure the security of all information contained in or handled by DBS including all computer systems and manual or paper systems managed by DBS or by other parties on their behalf.

What is Personal Data?

Personal data is all recorded information about living individuals who are or could be identified from that data. In DBS's case this includes (but is not limited to) information about: -

- DBS's employees, prospective employees and ex-employees, volunteers and interns;
- Parents, carer's guardians and children who use DBS's services;
- Individuals working for DBS or volunteering with them; and
- Individuals working for DBS's suppliers or referral partners

These individuals are referred to as **Data Subjects**.

Personal Data covers names, identification numbers, location data, or an online identifier such as an email address, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the Data Subject. As well as written information the GDPR applies equally to images (e.g. photos, video or CCTV footage) or recorded audio information that allows individuals to be identified.

Personal Data is used by **Data Controllers** and **Data Processors**. The Data Controller is a person or entity who either alone or in common with others determines the purposes for which and manner in which personal data is processed. "Processed" simply means used.

The Data Processor is any person other than an employee of the Data Controller who processes the data on behalf of the Data Controller.

Certain categories of personal data are referred to as **Special Personal Data** (or Sensitive Personal Data). This is information concerning an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data (both in relation to physical and mental wellbeing), sex life or sexual orientation and past or spent criminal convictions. Sensitive Personal Data requires stricter protection than Personal Data and the loss or breaches of such data rightfully carries stricter punishment.

The Six Principles

There are six Principles included in the GDPR. These Principles are obligations that DBS must follow in any processing of personal information. These apply equally to employees, volunteers and any secondees, students or interns working for DBS. DBS will also ensure that any suppliers (including individual consultants) comply with these Principles when working with DBS. The GDPR says that personal data (i.e. information about living individuals held on computerised record systems or manual filing systems) must be: -

- used fairly and lawfully and processed in a transparent way;
- used for the valid purposes which we have advised you about and not used in any manner which is incompatible with those purposes (unless we have notified you and explained);
- used only to the extent necessary for the purposes we have advised you about;
- kept accurate and up to date;
- kept for no longer than necessary for the purpose which we have told you about; and
- kept secure and not be subject to unauthorised or accidental access, loss or damage or disclosure.

All DBS staff involved in processing personal data will apply these principles.

Processing

The GDPR requires DBS to specify the reason(s) for processing any personal data. There is a privacy statement on DBS's website which fully and accurately reflects DBS's processing. The Privacy Statement states the types of personal data processed; the lawful grounds for the processing; sources who it is disclosed to including any third-party processors used; and the geographic reach of any processing. Changes or additional uses of personal information are discussed with DBS's Head of Business & Finance to ensure that the privacy statement is kept up to date.

The GDPR states that there are six lawful grounds at least one of which must apply before personal data can be processed. These are that: -

- the individual has freely given specific and unambiguous consent to processing;
- processing is necessary for performance of a contract to which the individual is a party;
- processing is necessary to comply with a legal obligation;
- processing is necessary to protect the individual's vital interest (for example, providing emergency medical treatment in a life or death situation);
- processing is necessary for a task in the public interest or in the exercise of official authority; or
- processing is in the legitimate interests of the data controller provided their legitimate interest do not override the interests of the individual.

If none of these grounds apply any processing carried out will automatically be unlawful.

Individual's Rights

Where DBS collects personal data directly from an individual DBS must inform them about the purpose for which it intends to process that personal data, the types of third parties, if any, with whom that data may be shared or to which it may be disclosed. Processing will always be in line with the individual's rights under the GDPR and in particular their right to: -

- be informed about what information DBS collects about them;
- request access to any data held about them;
- have data corrected where it is inaccurate, incomplete or not up to date;
- object to processing their data unless there are overriding legitimate grounds for us to continue doing so;

- object to decisions being taken by automated means or profiling (which largely pertains to data used for the purposes of advertising, marketing and behavioural analysis);
- have data deleted or erased where the individual believes it is no longer required for the purpose for which it was obtained, or they have validly objected to our use of that information (sometimes referred to as the right to be forgotten);
- restrict our use of their personal data, for example, where there is no longer a basis for using the information, but they don't want us to delete it; and
- request the transfer of their data to a third party (sometimes referred to as the right of portability).

Individual's may also withdraw their consent to processing personal data where the grounds of processing is based on their consent (whereupon we will stop using it for the purpose for which consent was given).

Data Subject Right of Access

Any request by an individual for access to their personal data should be made in writing to DBS's Compliance Officer at their registered office address. Requests from employees should be addressed in writing to the relevant site HR Manager. DBS will respond to requests for access to personal data within the 30 days' time limit specified in the legislation. There is no fee or charge for dealing with a Data Subject Access Request.

Disclosures

DBS will share personal information with third parties only where this is necessary in relation to the purpose for which the information was obtained and we have notified the individual that we will do so (where there is a legitimate right to do this) or where the individual has consented to us doing so. However, DBS will ensure that the third-party processor is compliant with the GDPR. Procedures are also in place to share personal data with appropriate authorities where required to enable them to fulfil statutory duties, e.g. when necessary to prevent or detect crime or fraud and researchers where required for research purposes, if relevant conditions are met.

Disclosure can be unlawful even if a request comes from an individual's family member, local authority, government department or the police. If an employee receives any new requests for access to personal information from third parties outside of DBS they should contact their site Information Champion or General Manager directly before any disclosure is made.

DBS also shares anonymised statistical data with third parties such as funding bodies. The GDPR does not apply to this type of sharing as long as individuals cannot be identified from the personal data and provided that DBS ensures that any detailed information that could allow individuals to be identified is being withheld and that it is complying with the ICO's anonymisation code of practice.

If employees have any concerns or questions regarding the processing or use of personal data, they should contact DBS's site Information Champion or General Manager as soon as possible. If there is any doubt, employees should immediately cease to process the information.

Responsibilities

Everyone who works for DBS (whether employed or a contractor) has a responsibility to ensure that this Data Protection Policy is fully and properly observed, to actively respond to any concerns regarding confidentiality and to ensure that personal information is processed in accordance with the rights of the individual.

The Chief Executive and Board of Directors have overall responsibility for ensuring that DBS works towards compliance with GDPR. Recognising that this requires the active co-operation of all staff, they will ensure that training and guidance are provided, so that all staff are able to understand and apply good information handling practices in accordance with this policy.

Much of the day to day operation of the policy is delegated to the relevant site General Manager and their management team, who are responsible for making all managerial decisions in manner consistent with the spirit of the policy, for communicating the policy to all staff within their areas and supporting staff to understand their responsibilities. The site management team must promote the development of good practice and compliance with statutory legislation and ensure that individuals managing and handling personal information are appropriately trained to do so and appropriately supervised.

Managers and supervisors have an additional responsibility to: -

- set a positive example; and
- observe people and stop inappropriate practices immediately.

If a member of staff becomes aware of an actual or potential breach of security in relation to personal information, they should report it immediately to their line manager. Quick action can be crucial in mitigating the negative effects of a breach. DBS will conduct regular audits in relation to the nature and extent of the personal data that is being stored and the uses to which such data is being put with the aim of monitoring compliance with the data protection principles described above and will exercise sanctions in respect of any breaches.

A breach of this policy by any member of staff is a disciplinary offence and may constitute gross misconduct. It is also a criminal offence for any employee, secondee, intern, consultant or supplier to access, use or disclose personal data without being authorised to do so for the purpose of their role. This may result in criminal prosecution.

Data Security & Breaches

DBS place great importance on the security of all personal data that we hold and will always try to take appropriate precautions to protect it. We ensure that there are appropriate technical controls such as firewall and anti-virus measures in place and carry out regular security reviews on our network. We always ensure that only authorised staff have access to personal data and that they are appropriately trained to handle it. Access will be role-based and on a need to know basis. Any third-party processors will only process personal data on our instructions and are subject to a duty of confidentiality.

The GDPR requires us to put in place procedures to deal with any security breaches or suspected security breaches including reporting certain kinds of breaches to the Information Commissioner's Office within 72 hours of discovery, and in certain circumstances notifying data subjects affected of the breach. DBS has an Incident Reporting and Security Breach Policy and procedures in place to deal with any breaches which all staff are required to comply with. A copy of this is available on the Ethics and Compliance section of the DBS Intranet and electronic copies are available on request.

Data Retention

DBS only retain personal data for as long as necessary to fulfil the purposes for which it was collected, including for the purposes of satisfying any legal, accounting or reporting requirements. To determine the appropriate retention period for personal data we refer to our Records Management Policy and Data Retention Schedule a copy of which can be made available on request.

Overseas Transfers

Countries outside of the European Economic Area ("EEA") do not always offer the same level of protection or safeguards for processing personal data as countries within the EEA. The GDPR prohibits transfers outside of the EEA unless the transfer meets certain conditions, namely: -

- that the country to which the transfer is made has been deemed to provide an adequate level of protection by the European Commission; or
- a specific contract is in place with the overseas based service provider which has been approved by the European Commission as giving personal data the same protection it has within the EEA; or
- where the service provider is based in the United States they are party to the EU-US Privacy Shield which requires them to provide similar protection to personal data shared between EEA based service providers.

If none of the above conditions apply we may request the individual's explicit consent for the transfer but they are not obliged to give it and, if they do give it they have the right to withdraw consent at any time.

Complaints

Complaints, concerns or questions about this policy should be made to the Head of Compliance. However, all individuals within UK businesses have the right to lodge a complaint with the Information Commissioner's Office whose contact details are as follows: -

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113 or 01625 545745

Website: https://ico.org.uk/concerns

The contact details of the corresponding regulatory bodies in Finland, France, Germany and Sweden are available on request from the relevant site Information Champion or General Manager.

The policy will be made readily available, regularly and consistently enforced, and it will be made known to managers, supervisors, employees, volunteer workers. More detailed guidance will also be provided to staff. The Policy will be reviewed and updated regularly in response to legislative or organisational changes.