David Brown Santasalo

Data Protection Policy

This document 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 Group Limited (Company Number: 02432631)
- David Brown Santasalo UK Limited (Company Number: 06624684)
- David Brown Santasalo UK (Industrial) Limited (Company Number: 06677806)
- David Brown Santasalo France SARL (Company Number: B 790 806 129)
- David Brown Santasalo (Proprietary) Limited (Company Number: 1947/025759/07)
- David Brown Santasalo South Africa (Proprietary) Limited (Company Number: 2013/092642/07)
- David Brown Santasalo Australia Pty Ltd (Company Number: ABN 15 000 008 640)
- David Brown Santasalo USA West Inc (Company Number: EIN: 85-2301732)
- David Brown Santasalo USA Inc (Company Number: 55959-59)
- David Brown Santasalo Canada Inc (Company Number: 1390236-6)
- David Brown Santasalo Finland Oy (Company Number: 2646194-8)
- David Brown Santasalo Sweden AB (Company Number: 5561169607)
- David Brown Santasalo South America SA (Company Number: 76.130.276-0)
- David Brown Santasalo Peru SAC (Company Number: 13340406)
- David Brown Systems Teknoloji Ve Diş Ticaret Anonim Şirketi (Company Number: 148401-5)
- David Brown Santasalo Gears (Changshu) Co Ltd (Company Number: 320581000202302000000)
- Santasalo Gears (Suzhou) Co Limited (Company Number: 320594400023102)
- David Brown Systems Malaysia SDN BHD (Company Number: 1204448A)
- PT David Brown Putra Mas (Company Number: 360/1/IU/I/PMA/PERDAGANGAN/2012)
- David Brown Santasalo India (Private) Limited (Company Number: U29220PN2011PLC139832)

The policy explains when and why we collect personal data about individuals, how we keep it secure and what your rights are in relation to your personal data. DBS wants to ensure that employees handling personal data recognise the risks involved and fully understand the steps which they need to take in order to minimise those risks and comply with the law.

For the purposes of General Data Protection Regulations (“GDPR”) each site acts as a data controller for the personal data in which they collect and process as part of their operations.

If you have a query regarding your personal data or would like to contact the data controller you may do so by email at compliance@dbsantasalo.com or by post using the following addresses:

David Brown Group Limited	1 Mariner Court, Durkar, Wakefield, United Kingdom, WF4 3FL
David Brown Santasalo UK Limited	Park Works, Park Road, Lockwood, Huddersfield, United Kingdom, HD4 5DD
David Brown Santasalo UK (Industrial) Limited	Prospect Works, Park Road, Crosland Moor, Huddersfield, United Kingdom, HD4 5DD
David Brown Santasalo France SARL	2 Place de l'Eglise, 33310, Lormont, France
David Brown Santasalo (Proprietary) Limited	12 Birmingham Street, Industrial Sites, Benoni, Gauteng, South Africa

David Brown Santasalo South Africa (Proprietary) Limited	12 Birmingham Street, Industrial Sites, Benoni, Gauteng, South Africa
David Brown Santasalo Australia Pty Ltd	13-19 Franklin Avenue, Bulli, New South Wales 2516, Australia
David Brown Santasalo USA West Inc	998 South 3200 West, Salt Lake City, Utah 84104
David Brown Santasalo USA Inc	380 Business Parkway, Greer, South Carolina 29651, USA
David Brown Santasalo Canada Inc	20375 Clark Graham, Baie d'Urfe Quebec, H9X 3T5, Canada
David Brown Santasalo Finland Oy	Eteläportintie 7, 40530 Jyväskylä, Finland
David Brown Santasalo Sweden AB	Norra Langebergsgatan 4, Göteborg, SE-421 32, Sweden
David Brown Santasalo South America SA	Pudahuel Poniente, #1107 Commune of Pudahuel, Noviciado, Santiago, Chile
David Brown Santasalo Peru SAC	Avenida Ejercito 101, Efificio Nasya 1, Oficina 603, Distrito de Yanahuara, Arequipa, Perú
David Brown Systems Teknoloji Ve Diş Ticaret Anonim Şirketi	Sanayi Mah, Teknopark Bulvari, No:1, 1C/1410, 34906 Pendik / Istanbul, Turkey
David Brown Santasalo Gears (Changshu) Co Ltd	Block B&D, No. 15 Dian Chang Road, Bi Xi Street, Changshu City, Jiangsu Province, P.C. 215500, China
Santasalo Gears (Suzhou) Co Limited	Workshop 7, Jingling Industrial Park, No. 88 East Jingling Road, 215121 SIP, Suzhou, Jiangsu Province, China
David Brown Systems Malaysia SDN BHD	Unit 32-1, Level 32 Menara Prestige, No. 1 Jalan Pinang 50450, Kuala Lumpur, Malaysia
PT David Brown Putra Mas	Pergudangan Tanrise Southgate C-18, Jl. Nangka, Sruni – Gedangan, Sidoarjo 61254, Indonesia
David Brown Santasalo India (Private) Limited	#99, SIPCOT Industrial, Complex, Phase I, Hosur - 635126, Tamil Nadu, India

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

DBS will:

- always comply with General Data Protection Regulations;
- ensure staff and other individuals are fully aware of both their rights and obligations under General Data Protection Regulations; and
- implement adequate and appropriate technical and organisational security measures to ensure the security of all information handled by DBS or by third parties on their behalf.

What is Personal Data?

Personal data is any information relating to a living individual who is identified or could be identified from that data. In our case this includes (but is not limited to) information about:

- Employees, prospective employees and ex-employees;
- Volunteers, interns, agency workers and contractors;
- Third party visitors and partners; and
- Employees of our customers and suppliers.

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

Personal data covers names, identification numbers, location data, online identifiers or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject. Images (e.g. photos, video and CCTV) or recorded audio, which allow individuals to be identified, apply equally as written information under GDPR.

Personal data is used by **Data Controllers** and **Data Processors**. The data controller is a person or legal entity who, either alone or jointly with others, determines the purpose and manner in which personal data is processed or used. The data processor is any person (other than an employee of the data controller) or legal entity who processes and uses the data on behalf of the data controller.

Certain categories of personal data are referred to as **Special Category Data**. This is more sensitive information concerning an individual's race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data or data about someone's sex life or sexual orientation. This type of personal data is more sensitive and requires extra protection because the use of this information could create significant risks to the individual's fundamental rights and freedoms.

Certain categories of personal data are referred to as **Criminal Offence Data**. This is also more sensitive information about offenders or suspected offenders in the context of criminal activity. It includes details about allegations, investigations and criminal proceedings or convictions. This type of personal data is more sensitive and requires extra protection because the use of this information could create significant risks to the individual's fundamental rights and freedoms.

The Six Principles

There are six data protection principles that underpin GDPR. These principles are obligations that we must follow whenever we are collecting and processing personal data. The six data protection principles apply equally to all data subjects. DBS will also ensure that any customers, suppliers or third parties comply with these principles when working with us.

In accordance with the data protection principles, whenever we are collecting or processing your personal data, we will ensure that it is:

- used lawfully, fairly and processed in a transparent manner;
- used only for specific and valid purposes and not further processed in a manner which is incompatible with those purposes unless we have obtained your consent or are required by law to do so;

- adequate, relevant and limited to what is necessary in order to achieve the purposes for which it was obtained;
- kept accurate and up to date;
- kept for no longer than necessary for the purposes in which it was obtained unless there is an applicable law, regulation or dispute requiring us to retain the data for a longer period; and
- kept secure and protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

All DBS staff involved in the processing of personal data will apply these principles whenever they are collecting or handling your data.

Processing

Under GDPR we are required to identify the purposes and the lawful grounds for which we intend to collect and process any personal data. There is a Privacy Notice located on our website which fully and accurately reflects the types of personal data that we collect and process; the purposes for which it is needed and the applicable lawful grounds for the processing of such data.

The privacy notice also confirms who we may transfer or share your data with and whether it will be transferred or shared with anyone overseas. The notice is continually reviewed and kept up to date to reflect any changes in how we may process your personal data.

There are six lawful grounds for the processing of personal data. Under GDPR the processing of personal data will only be lawful if:

- the individual has freely given specific and unambiguous consent to the processing of their data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the individual is a party or in order to take initial steps at the request of the individual prior to entering into a contract;
- processing is necessary in order to comply with the law;
- processing is necessary in order to protect someone's life;
- processing is necessary for the performance of a task that is carried out in the public interest or to exercise an official authority vested in the data controller; or
- processing is necessary for the legitimate interests of the data controller provided their legitimate interest does not override the interests, fundamental rights or freedoms of the individual.

Before we process your personal data we must identify at least one lawful ground for processing. If none of these grounds apply then any processing that is carried out will automatically be unlawful.

Individual's Rights

Where we collect personal data directly from an individual we will inform them about the purposes for which we intend to process that data and the types of third parties, if any, with whom that data may be shared with or disclosed to. Whenever we are collecting or processing personal data will always ensure that we maintain individual's rights under GDPR and in particular their right to:

- be informed about the collection and use of their personal data;
- request access to any data held about them;

- have data corrected where it is inaccurate, incomplete or not up to date;
- have data deleted or erased where the individual believes that it is no longer required for the purposes for which it was obtained, withdraws their consent on which processing was based or they have validly objected to our use of that information;
- restrict our use of their data if it is inaccurate, no longer required to achieve the purposes for which it was obtained or where there is no lawful basis for processing;
- request the transfer of their data to a third party or to receive it in a commonly used machine readable format so that it is easily accessible across systems and devices;
- object to processing their data unless there are compelling legitimate grounds for us to continue doing so which overrides the interests, rights and freedoms of the individual; and
- 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).

Individual's may also withdraw their consent to the processing of personal data where the lawful grounds of processing was 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 must be made in writing to the DBS Compliance Officer at their registered office address. Requests from employees must be in writing and addressed to the relevant site HR Manager.

DBS will respond to requests for access to personal data within 30 days of the request. If the request is unclear or complex then we may need additional time in order to consider and comply with the request. If we need additional time to consider and comply with your request then we will write to you to confirm why within one month of receiving the request.

There is no fee or charge for dealing with a Data Subject Access Request however we may charge you a reasonable fee to cover administrative costs where the request is unfounded or excessive.

Disclosures

DBS will share personal information with third parties only where this is necessary in relation to the purposes for which the information was obtained and where 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 fully compliant with GDPR and will maintain your individual rights and freedoms.

Procedures are also in place to share personal data with appropriate authorities to enable them to fulfil statutory duties e.g. when it is 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 General Manager directly before any disclosure is made.

DBS also shares anonymised statistical data with third parties such as funding bodies. 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 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 their DBS site 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 lawfully and in accordance with the rights of the individual.

The Chief Executive Officer 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 a manner consistent with the spirit of the policy and 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 which may result in criminal prosecution.

Data Security & Breaches

DBS place great importance on the security of all personal data that we hold and we will always try to take appropriate precautions to protect it. We will ensure that there are appropriate technical controls such as firewall and anti-virus measures in place and that we 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 to personal information will be role-based and on a need to know basis. Any third party processors will only process personal data on our documented instructions and are subject to a duty of confidentiality.

GDPR requires us to put in place procedures to deal with any actual 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 in place to deal with any actual or suspected breaches which all staff are required to comply with. A copy of this is available on the Ethics & Compliance section of the DBS Intranet and electronic copies are available on request.

Data Retention

DBS only retain personal data for as long as is 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 Data Retention Policy a copy of which can be made available on request.

International Data Transfers

Countries outside of the European Economic Area ("EEA") do not always offer the same level of protection or safeguards for the processing personal data as countries within the EEA. GDPR strictly 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 written contract is in place with the overseas entity which gives the personal data the same level of protection that it has within the EEA; or
- where the entity is based in the United States and they are party to the EU-US Privacy Shield which requires them to provide a similar level of protection to the personal data that it has within the EEA.

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

Complaints

We take any complaints about the collection and use of personal data very seriously. Any complaints, concerns or questions about this policy should be made to the Group Head of Compliance in the first instance.

If we are unable to resolve your concerns to your satisfaction then you have the right to make a formal complaint at any time to your local supervisory authority.

All individuals and businesses within the UK have the right to lodge a complaint to the Information Commissioner's Office whose contact details are as follows:

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

Telephone: 03031 231 113
Email: casework@ico.org.uk
Website: https://ico.org.uk/make-a-complaint/

The contact details for the corresponding supervisory and regulatory bodies in the other countries in which we operate can be made available on request by emailing compliance@dbsantasalo.com.

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

Last updated: 20th March 2025