Data Protection Policy

David Brown Santasalo UK Limited (trading as DB Defence) (referred to as "DBD" or "we", "our" or "us") is a data controller for the purposes of the GDPR and are registered with the Information Commissioner. We can be contacted by post at C/o the Head of Compliance, David Brown Defence, Park Works, Park Road, Huddersfield, HD4 5DD, West Yorkshire, England or by email (For the Attention of the Head of Compliance) at: Compliance@db-def.com

This document is intended to define the policy and principles adopted by us to govern the control and processing of personal data.

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. DBD 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.

We are committed to protecting personal data in accordance with all applicable data protection and privacy laws. Depending on the location of our operations and the individuals whose data we process, this includes data protection laws outside of the UK as well as applicable laws in other jurisdictions where we operate, including Turkey.

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

DBD will: -

- always comply with UK GDPR;
- ensure staff and other individuals are fully aware of both their rights and obligations under UK GDPR;
- implement adequate and appropriate physical and technical security measures and organisational measures to ensure the security of all information contained in or handled by DBD including all computer systems and manual or paper systems managed by DBD or by other parties on their behalf; and
- publish our Protection of Third Party Data policy on our website.

DBD 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.

What is Personal Data?

Reference to personal information or data means all forms of personal data including special category data as defined by the UK GDPR.

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**.

What Does Personal Data Cover?

- Names;
- identification numbers;
- location data;
- online identifiers;
- 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)

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 Seven Principles

There are seven data protection principles that underpin UK GDPR. These principles are obligations that we must follow whenever we are collecting and processing personal data. The seven data protection principles apply equally to all data subjects. DBD 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:

1. used lawfully, fairly and processed in a transparent manner;
2. 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;
3. adequate, relevant and limited to what is necessary in order to achieve the purposes for which it was obtained;
4. kept accurate and up to date;
5. 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
6. kept secure and protected against unauthorised or unlawful processing, accidental loss, destruction or damage;
7. maintained in the appropriate filing for record keeping.

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

Processing

Under UK 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:

1. the individual has freely given specific and unambiguous consent to the processing of their data for one or more specific purposes;

2. 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;
3. processing is necessary in order to comply with the law;
4. processing is necessary in order to protect someone's life;
5. 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
6. 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 UK 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 DBD Head of Compliance. Requests from employees must be in writing and addressed to the Head of HR.

DBD 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

DBD 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, DBD will ensure that the third-party processor is fully compliant with UK 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 DBD they should contact their site Manager directly before any disclosure is made.

DBD also shares anonymised statistical data with third parties such as funding bodies. UK GDPR does not apply to this type of sharing as long as individuals cannot be identified from the personal data and provided that DSD 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 Manager as soon as possible. If there is any doubt, employees should immediately cease to process the information.

Responsibilities

Everyone who works for DBD (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 DBD works towards compliance with relevant laws and regulations. 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 Managers 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 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 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 Manager. Quick action can be crucial in mitigating the negative effects of a breach. DBD 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

DBD 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.

UK 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.

DBD 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 DBD Intranet and electronic copies are available on request.

Data Retention

DBD 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

Personal data may be transferred between our office in the United Kingdom and Turkey where necessary for business operations and employee administration.

Where personal data is transferred outside the United Kingdom or Turkey, we will ensure that appropriate safeguards are in place to protect personal data in accordance with the UK GDPR, the Data Protection Act 2018 and the Law on the Protection of Personal Data no. 66698.

Such safeguards may include contractual protections, such as Standard Contractual Clauses or the UK International Data Transfer Agreement (IDTA), to ensure that personal data receives an appropriate level of protection.

Where personal data is transferred between the Uk and Turkey, we will ensure that appropriate legal and organisational safeguards are implemented in accordance with applicable data protection laws in both jurisdictions.

Where we use cloud-based services or third-party providers, personal data may also be processed on systems located outside the United Kingdom or Turkey. In such cases, we will ensure appropriate safeguards are implemented to protect personal data.

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 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/

This 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: 24th March 2025