Blanboz
Smart Renewables

01

Anti-Bribery-and-Corruption Policy Statement

Anti-Bribery-and-Corruption Policy Statement

1. Purpose

1.1 Blanboz Limited ("the Company") is committed to the practice of responsible corporate behaviour and to complying with all laws, regulations and other requirements which govern the conduct of our operations.

1.2 The Company is fully committed to instilling a strong anti-corruption culture and is fully committed to compliance with all anti-bribery and anti-corruption legislation including, but not limited to, the Bribery Act 2010 ("the Act") and ensures that no bribes or other corrupt payments, inducements or similar are made, offered, sought or obtained by us or anyone working on our behalf.

2. Bribery

2.1 Bribery is defined as the giving or promising of a financial or other advantage to another party where that advantage is intended to induce the other party to perform a particular function improperly, to reward them for the same, or where the acceptance of that advantage is in itself improper conduct.

2.2 Bribery is also deemed to take place if any party requests or agrees to receive a financial or other advantage from another party where that advantage is intended to induce that party to perform a particular function improperly, where the acceptance of that advantage is in itself improper conduct, or where that party acts improperly in anticipation of such advantage.

2.3 Bribery of a foreign official is defined as the giving or promising of a financial or other advantage which is intended to influence the official in order to obtain business or an advantage in the conduct of business unless the foreign official is required or permitted by law to be influenced by such advantage.

3. Consequences of Bribery

3.1 Anyone or any organisation found guilty of bribery under the Act may face fines and/or prison terms. In addition, high legal costs and adverse publicity are likely to result from any breach of the Act.

3.2 For employees of the Company, failure to comply with this Policy and/or with the Act may result in:

3.2.1 disciplinary action which may include dismissal; and

3.2.2 criminal penalties under the Act which may result in a fine and/or imprisonment for up to 10 years.

3.3 For the Company, any breach of this Policy by any employee or business associate may result in:

3.3.1 the Company being deemed to be in breach of the Act;

3.3.2 the Company being subject to fines; and

3.3.3 the Company suffering negative publicity and further associated damage as a result of such breach.

4. Responsibility for Compliance and Scope of Policy

4.1 This Policy applies to all employees, agents, contractors, subcontractors, consultants, business partners and any other parties (including individuals, partnerships and bodies corporate) associated with the Company or any of its subsidiaries.

4.2 It is the responsibility of all of the abovementioned parties to ensure that bribery is prevented, detected and reported and all such reports should be made in accordance with the Company's Whistleblowing Policy or as otherwise stated in this Policy, as appropriate.

4.3 No party described in section 4.1 may:

4.3.1 give or promise any financial or other advantage to another party (or use a third party to do the same) on the Company's behalf where that advantage is intended to induce the other party to perform a particular function improperly, to reward them for the same, or where the acceptance of that advantage will in itself constitute improper conduct;

4.3.2 request or agree to receive any financial or other advantage from another party where that advantage is intended to induce the improper performance of a particular function, where the acceptance of that advantage will in itself constitute improper conduct, or where the recipient intends to act improperly in anticipation of such an advantage.

4.4 Parties described in section 4.1 must:

4.4.1 be aware and alert at all times of all bribery risks as described in this Policy and in particular as set out in section 9 below;

4.4.2 exercise due diligence at all times when dealing with third parties on behalf of the Company; and

4.4.3 report any and all concerns relating to bribery to the Director or, in the case of non-employees, their normal point of contact within the Company, or otherwise in accordance with the Company's Whistleblowing Policy.

5. Facilitation Payments

5.1 A facilitation payment is defined as a small payment made to officials in order to ensure or speed up the performance of routine or necessary functions.

5.2 Facilitation payments constitute bribes and, subject to section 5.3, may not be made at any time irrespective of prevailing business customs in certain territories.

5.3 Facilitation or similar payments may be made in limited circumstances where your life is in danger but under no other circumstances. Any payment so made must be reported to the Director as soon as is reasonably possible and practicable.

6. Gifts and Hospitality

6.1 Gifts and hospitality remain a legitimate part of conducting business and should be provided only in compliance with the Company's Gifts and Hospitality Policy.

6.2 Gifts and hospitality can, when excessive, constitute a bribe and/or a conflict of interest. Care and due diligence should be exercised at all times when giving or receiving any form of gift or hospitality on behalf of the Company.

6.3 The following general principles apply:

6.3.1 Gifts and hospitality may neither be given nor received as rewards, inducements or encouragement for preferential treatment or inappropriate or dishonest conduct.

6.3.2 Neither gifts nor hospitality should be actively sought or encouraged from any party, nor should the impression be given that the award of any business, custom, contract or similar will be in any way conditional on gifts or hospitality.

6.3.3 Cash should be neither given nor received as a gift under any circumstances.

6.3.4 Gifts and hospitality to or from relevant parties should be generally avoided at the time of contracts being tendered or awarded.

6.3.5 The value of all gifts and hospitality, whether given or received, should be proportionate to the matter to which they relate and should not be unusually high or generous when compared to prevailing practices in our industry or sector.

6.3.6 Certain gifts which would otherwise be in breach of this Policy and/or the Hospitality and Gifts Policy may be accepted if refusal would cause significant and/or cultural offence, however the Company will donate any gifts accepted for such reasons to a charity of the Director's choosing.

6.3.7 All gifts and hospitality, whether given or received, must be recorded in the Hospitality & Gifts Register.

7. Charitable Donations

7.1 Charitable donations are permitted only to registered (non-profit) charities. No charitable donations may be given to any organisation which is not a registered charity.

7.2 All charitable donations must be fully recorded in Charitable Donation Register.

7.3 Proof of receipt of all charitable donations must be obtained from the recipient organisation.

7.4 Under no circumstances may charitable donations be made in cash.

7.5 No charitable donation may be made at the request of any party where that donation may result in improper conduct.

8. Political Donations

8.1 The Company does not make political donations and the Company is not affiliated with any political party, independent candidate, or with any other organisation whose activities are primarily political.

8.2 Employees and other associated parties are free to make personal donations provided such payments are not purported to be made on behalf of the Company and are not made to obtain any form of advantage in any business transaction.

9. Due Diligence and Risks

The following issues should be considered with care in any and all transactions, dealings with officials, and other business matters concerning third parties:

9.1 Territorial risks, particularly the prevalence of bribery and corruption in a particular country;

9.2 Cross-border payments, particularly those involving territories falling under section 9.1;

9.3 Requests for cash payment, payment through intermediaries or other unusual methods of payment;

9.4 Activities requiring the Company and / or any associated party to obtain permits or other forms of official authorisation;

9.5 Transactions involving the import or export of goods;

This Anti-Brivery-and-Corruption Policy Statement has been approved & authorised by:

Name: Andres Blanco

Position: Director

Date: 01 December 2025

Signature: 

Blanboz
Smart Renewables

02

Quality Statement Policy

Quality Statement Policy

Blanboz Limited is dedicated to providing world-class technical advisory and engineering support in the renewable energy sector, with a primary focus on Battery Energy Storage Systems (BESS) projects. Our mission is support our clients with deep technical knowledge and years of experience to accelerate their BESS projects as well as the clean energy transition to achieving sustainability. Provide a high-quality service and generate added value, ensuring not only our environmental and social contribution but also the human and professional development of the Blanboz team. Our vision is supporting companies and communities in the transition to clean energy, sharing the same goals of achieving net zero C02 eq emissions worldwide. Position ourselves as the leading consultancy in the BESS market in the United Kingdom.

Our commitment to quality is guided by the following core principles:

- **Customer-Centric Excellence:** We strive to understand and exceed the expectations of our clients, including developers, buyers, asset managers, and investors, by delivering tailored technical solutions, risk assessments, and project support that ensure performance, safety, and compliance with industry standards.

- **Technical Expertise and Safety:** With over 15 years of experience in renewable energy and a specialised focus on BESS, we prioritise safety through rigorous adherence to Health and Safety regulations in the UK and BS standards, ensuring the safety of our team, work and those working with us.

- **Continuous Improvement:** We maintain a robust Quality Management System (QMS) aligned with ISO 9001:2015, fostering continuous improvement in our processes, from site assessments and technical due diligence to factory and site acceptance testing (FATs and SATs), to deliver reliable and innovative solutions. We are in the process of obtaining the ISO 9001 certification, expected in Q2 2026.

- **Sustainability and Community Impact:** We are committed to advancing clean energy development and supporting communities through feasibility studies, training, and projects that promote accessible electricity, particularly in developing regions, aligning with our vision of "Electricity for all - Batteries lead the charge."

- **Employee Empowerment:** Our team of experts is empowered through ongoing training and clear communication to uphold the highest standards of quality, safety, and efficiency, ensuring every project reflects our values of respect, care, and simplicity.

- **Compliance with Requirements:** We commit to complying with all applicable statutory, regulatory, and customer requirements relevant to our services and operations.

- **Quality objectives:** This Quality Policy provides the framework for stablishing, reviewing, and improving quality objectives aligned with our strategic direction.

Top management at Blanboz Limited is responsible for establishing, implementing, and maintaining the QMS, ensuring resources are allocated to achieve our quality objectives. We conduct regular reviews to monitor performance, drive innovation, and address emerging challenges in the renewable energy sector. Our services, including pre-construction assessments, construction monitoring, and visual inspections in high-risk environments, are designed to meet stringent safety and performance standards, ensuring client confidence and project success.

This Quality Policy Statement is communicated to all employees, and shared with clients, partners, and stakeholders to demonstrate our unwavering commitment to quality, safety, and sustainability. Every member of the Blanboz team is responsible for contributing to the effectiveness of our QMS, supported by leadership and resources to achieve our objectives.

This Quality Statement Policy has been approved & authorised by:

Name: Andres Blanco

Position: Director

Date: 01 December 2025

Signature: 

Blanboz
Smart Renewables

03

Modern Slavery and Human Trafficking Policy Statement

Modern Slavery and Human Trafficking Policy Statement

Blanboz Limited is committed to preventing slavery and human trafficking in our business activities and supply chains. We have implemented processes to ensure that there is no slavery or human trafficking in our operations. All staff have a duty to remain vigilant to risks, however small, and are expected to report concerns so that management can act upon them promptly.

Organisational structure and supply chains

Blanboz Limited provides technical advisory services throughout the entire project life cycle for renewable energy projects, particularly those related to battery energy storage systems.

Our activities include acting as a contractor, and in some cases subcontracting to cover specific client scopes of work. In all circumstances, this policy must be adhered to.

The Company currently operates in the United Kingdom, with potential expansion to the continental shelves of the North Atlantic, North America, the Caribbean, South America, and Europe.

Risk Assessment Process

The Company has established a risk assessment process to evaluate whether particular activities or countries present a high risk in relation to modern slavery or human trafficking. This process includes:

- Reviewing international indices and reports (e.g., Global Slavery Index, Transparency International).
- Conducting supplier questionnaires and compliance checks.
- Performing due diligence on subcontractors, including background checks and contractual obligations.
- Monitoring geopolitical and socio-economic conditions in countries where we operate.
- Annual internal audits of supply chain practices.

High Risk Activities

The following activities are considered to be at high risk of modern slavery or human trafficking:

- Subcontracting arrangements in regions with weak labor protections, where oversight may be more challenging.
- Procurement of materials (such as metals and minerals used in battery storage systems) from countries with documented risks of forced labor.
- Construction and installation services in jurisdictions with limited enforcement of labor standards.

These activities are considered high risk due to the complexity of supply chains, reliance on manual labor, and the potential for exploitation in industries linked to renewable energy infrastructure.

Training

To ensure a good understanding of the risks of modern slavery and human trafficking in our business and supply chains, the Company requires all staff to complete an online training course on modern. This training is mandatory and will be refreshed annually to ensure that employees remain informed about evolving risks and best practices.

Policies

The Company is committed to ensuring that there is no modern slavery or human trafficking in our business or our supply chains. This Statement affirms our intention to act ethically in our business relationships.
The following items set down our approach to the identification of modern slavery risks and steps to be taken to prevent slavery and human trafficking in our operations:

- The Company encourages all its workers, customers, and other business partners to report any concerns related to its direct activities or its supply chains. Concerns may be reported directly to the Director or Through established internal communication channels and will be treated confidentially and without retaliation.
- The Code of Conduct and Ethics sets down the actions and behaviour expected of employees and suppliers when representing the Company, including compliance with human rights and labour laws.

Due Diligence Processes for Slavery and Human Trafficking

The Company undertakes due diligence when considering taking on new suppliers and regularly reviews its existing suppliers. The due diligence process includes:

- Building long-standing relationships with suppliers and making clear our expectations of business partners.
- Evaluating the modern slavery and human trafficking risks of each new supplier through questionnaires and audits.
- Requiring contractual commitments from suppliers to comply with anti-slavery standards.
- Invoking sanctions against suppliers that fail to improve their performance in line with an action plan provided by us, including the termination of the business relationship.

Performance Indicators

The Company uses the following key performance indicators (KPIs) to measure how effective we are in ensuring slavery and human trafficking is not taking place in any part of our business or supply chains:

- Requiring all relevant staff to have completed training on modern slavery by the set deadline.
- Monitoring labour practices through payroll systems to ensure compliance with wage and hour laws.
- Conducting annual supplier audits to verify adherence to anti-slavery commitments.
- Tracking the number of reported concerns and ensuring timely resolution.

Review and Endorsement

This Modern Slavery and Human Trafficking Statement will be regularly reviewed and updated as necessary. The Board of Directors endorses this policy statement and is fully committed to its implementation.

This Anti-Brivery-and-Corruption Policy Statement has been approved & authorised by:

Name: Andres Blanco

Position: Director

Date: 01 December 2025

Signature: 

Blanboz
Smart Renewables

04

Environmental Policy Statement

Environmental Policy Statement

The Environmental Policy of Blanboz Limited ("the Company") is to ensure so far as it is reasonably practicable that its operations will be carried out with a commitment to protecting and enhancing the environment by promoting low carbon and appropriate waste management systems in our business, contractors and suppliers.

The Company therefore seeks to comply with all relevant environmental legislation and regulation. It also aims to establish higher standards of environmental performance including low carbon and waste management where these are practicable and appropriate.

The Company employees are required to carry out their duties with concern for the environment. All Company employees must adhere to the aims and objectives of the Policy.

In the event of an environmental accident or incident at work, it is a Company requirement that the details are promptly and properly reported to the Director who will investigate and take prompt action to make good any damage and avoid recurrence.

All contractors working on behalf of the Company are required to adopt environmental standards fully consistent with those of the Company and they are expected to achieve comparable levels of performance.

As an office we are aware that we generate waste paper products, electricity consumption and transport emissions. However, as we strive for excellence in every aspect of our business we are committed to minimising the environmental impacts of the business operation.

This Environmental Policy provides the framework for setting and reviewing environmental objectives and targets and supports the continuous improvement of environmental performance across our activities and services.

The company considers environmental impacts associated with its activities, services and supply chain across their lifecycle, where relevant and practicable.

Our stated aims are to:

Aim to continuously improve our environmental performance particularly with regards to our reduce of CO2 emission by means of transportation, electricity consumption. Waste reduction by recycling and re-use of paper.

- Where possible we will use recycled or ecologically friendly paper.
- We will use 'waste' paper for notepads unless confidentiality may be compromised.
- Reduce our consumption of resources and improve the efficiency of those resources by printing double sided where practicable.
- Manage waste generated from my business operations according to the principles of reduction, re-use and recycling.

- Recycle all paper products, ink or toner cartridges.
- Transportation by use of electric car, where possible.
- Office electricity supply by renewable energy sources
- Comply as a minimum with all relevant environmental legislation as well as other environmental requirements.

This Environmental Policy Statement will be regularly reviewed and updated as necessary. The management team endorses these policy statements and is fully committed to their implementation.

This Environmental Policy Statement has been approved & authorised by:

Name: Andres Blanco

Position: Director

Date: 01 December 2025

Signature: 

Blanboz
Smart Renewables

05

Health and Safety Policy Statement

Health and Safety Policy Statement

It is the policy of Blanboz Limited ("the Company") to foster a positive health and safety culture throughout the Company because we believe that high standards of health and safety are a moral and commercial pre-requisite.

The Company is committed to:

- Consulting and involving workers, where applicable, in matters affecting their health and safety, and continually improving the occupational health and safety management system to enhance performance and prevent work-related injury and ill health.
- Providing adequate control of the health and safety risks arising from our work activities.
- Promote safe work against possible pandemic environment (e.g. COVID 19) following Government latest advice and guidance.
- Working to prevent accidents and work related ill health.
- Providing and maintaining safe plant and equipment.
- Ensuring that all of our on-site activities are evaluated under our risk assessments and method of works, de-risking any material risk to our personnel.
- Maintaining safe and healthy working conditions, and adequate welfare facilities.
- Ensuring safe handling and use of hazardous substances.
- Using and maintaining the proper safe plant and equipment needed for each task, including all Personal Protection Equipment where needed.
- Ensuring all employees are competent to do their tasks, and to give them adequate training.
- Ensuring the safety of our clients/customers at all times.
- Reviewing and revising this policy statement annually.

Our stated aims and objectives for the year 2025 are:

- To ensure all H&S documentation is up to date.
- To update all Risk Assessments and Method of Statement.
- To continue to work to ensure compliance.

Implementation, maintenance and review

The Director, Andres Blanco, accepts overall responsibility for all Health and Safety within the Company and is responsible for all policy implementation.

This Health and Safety Policy Statement has been approved & authorised by:

Name: Andres Blanco

Position: Director

Date: 01 December 2025

Signature: 

Blanboz
Smart Renewables

06

Privacy Policy

Privacy Policy

BACKGROUND:

Blanboz Limited understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of everyone who visits this website, www.blanboz.com ("Our Site") and only collect and use your personal data as described in this Privacy Policy. Any personal data we collect will only be used as permitted by law.

Please read this Privacy Policy carefully and ensure that you understand it. Your acceptance of this Privacy Policy is requested when you agree to our Privacy Policy by selecting the agree option.

1. Information About Us

Our Site is owned and operated by Blanboz Limited, a limited company registered in Scotland under company number SC713901.
Registered address: Office 1, Technology House, 9 Newton Place, Glasgow, G3 7PR. United Kingdom.
Address: Office 1, Technology House, 9 Newton Place, Glasgow, G3 7PR. United Kingdom.
Data Protection Officer: Andres Blanco.
Email address: info@blanboz.com.
Telephone number: 00447908686424.
Postal address: G3 7PR
We are regulated by Th Data Protection Legilsation.

2. What Does This Policy Cover?

This Privacy Policy applies only to your use of Our Site. Our Site may contain links to other websites. Please note that we have no control over how your data is collected, stored, or used by other websites and We advise you to check the privacy policies of any such websites before providing any data to them.

3. What Is Personal Data?

Personal data is defined by the UK GDPR and the Data Protection Act 2018 (collectively, "the Data Protection Legislation") as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'.
Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.

4. What Are My Rights?

Under the Data Protection Legislation, you have the following rights, which we will always work to uphold:

a) The right to be informed about our collection and use of your personal data. This Privacy Policy should tell you everything you need to know, but you can always contact us to find out more or to ask any questions using the details in Part 10.

b) The right to access the personal data we hold about you. Part 9 will tell you how to do this.

c) The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete. Please contact us using the details in Part 10 to find out more.

d) The right to be forgotten, i.e. the right to ask us to delete or otherwise dispose of any of your personal data that we hold. Please contact us using the details in Part 10 to find out more.

e) The right to restrict (i.e. prevent) the processing of your personal data.

f) The right to object to us using your personal data for a particular purpose or purposes.

g) The right to withdraw consent. This means that, if we are relying on your consent as the legal basis for using your personal data, you are free to withdraw that consent at any time.

h) The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in many cases.

i) Rights relating to automated decision-making and profiling. We do not use your personal data in this way.

For more information about our use of your personal data or exercising your rights as outlined above, please contact us using the details provided in Part 10.

It is important that your personal data is kept accurate and up-to-date. If any of the personal data we hold about you changes, please keep us informed as long as we have that data.

Further information about your rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau.

If you have any cause for complaint about our use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office. We would welcome the opportunity to resolve your concerns ourselves, however, so please contact us first, using the details in Part 10.

5. What Personal Data Do You Collect and How?

Subject to the following, we do not collect any personal data from you. We do not place cookies on your computer or device, nor do we use any other means of data collection.

Our Site collects certain information automatically, including your IP address, the type of browser you are using, Google Analytics and certain other non-personal data about your computer or device such as your operating system type or version, and display resolution.

If you send us an email, we may collect your name, your email address, and any other information which you choose to give us. For the purposes of the Data Protection Legislation, We are the data controller responsible for such personal data.

The lawful basis under the Data Protection Legislation that allows us to use such information is article 6(1)(f) of the UK GDPR which allows us to process personal data when it is necessary for the purposes of our legitimate interests, in this case, the proper operation and functionality of Our Site. If you contact us as described above, you will be required to consent to our use of your personal data to contact you. In this case, our lawful basis for using your personal data will be article 6(1)(a) of the UK GDPR, which allows us to use your personal data with your consent for a particular purpose or purposes.

6. How Do You Use My Personal Data?

Where we collect any personal data, it will be processed and stored securely, for no longer than is necessary in light of the reason(s) for which it was first collected. We will comply with our obligations and safeguard your rights under the Data Protection Legislation at all times. For more details on security see Part 7, below.

As stated above, we do not generally collect any personal data directly from you, but if you contact us and we obtain your personal details from your email, we may use them to respond to your email. The other technical data referred to above is necessary for the technical operation of Our Site and will not normally be used in any way to personally identify you.

Any and all emails containing your personal data will be deleted no later than 20 years after the subject matter of your email has been resolved. and no other personal data will be retained for any longer than is necessary.

We will not share any of your personal data with any third parties for any purposes other than storage on an email and/or web hosting server.

7. How and Where Do You Store My Data?

We will only store some of your personal data in the UK. This means that it will be fully protected under the Data Protection Legislation.

AND/OR

We will store some of your personal data within the European Economic Area (the "EEA"). The EEA consists of all EU member states, plus Norway, Iceland, and Liechtenstein. This means that your personal data will be fully protected under the EU GDPR and/or to equivalent standards by law. Transfers of personal data to the EEA from the UK are permitted without additional safeguards.

AND/OR

We store some or all of your personal data in countries outside of the UK. These are known as "third countries". We will take additional steps in order to ensure that your personal data is treated just as safely and securely as it would be within the UK and under the Data Protection Legislation as follows:

We ensure that your personal data is protected under binding corporate rules. Binding corporate rules are a set of common rules which all our group companies are required to follow when processing personal data. For further information, please refer to the Information Commissioner's Office.
OR

We will only store or transfer personal data in or to countries that are deemed to provide an adequate level of protection for personal data. For further information about adequacy decisions and adequacy regulations, please refer to the Information Commissioner's Office.
OR

We will use specific approved contracts which ensure the same levels of personal data protection that apply under the Data Protection Legislation. For further information, please refer to the Information Commissioner's Office.

Please contact us using the details below in Part 10 for further information about the particular data protection safeguard(s) used by us when transferring your personal data to a third country.
Personal data security is essential to us, and to protect personal data, we take the following measures:

- limiting access to your personal data to those employees, agents, contractors, and other third parties with a legitimate need to know and ensuring that they are subject to duties of confidentiality;

- procedures for dealing with data breaches (the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, your personal data) including notifying you and/or the Information Commissioner's Office where we are legally required to do so;

8. Do You Share My Personal Data?

We will not share any of your personal data with any third parties for any purposes, subject to the following exception(s).

If we sell, transfer, or merge parts of our business or assets, your personal data may be transferred to a third party. Any new owner of our business may continue to use your personal data in the same way that we have used it, as specified in this Privacy Policy (i.e. to communicate with you).

In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.
OR

We may contract with the following third party for hosting and data storage purposes:

- Google Analytics SaaS web analytic perform within Google Marketing platfotm.

If any of your personal data is transferred to a third party, as described above, we will take steps to ensure that your personal data is handled safely, securely, and in accordance with your rights, our obligations, and the third party's obligations under the law, as described above in Part 7.

If any personal data is transferred outside of the UK, we will take suitable steps in order to ensure that your personal data is treated just as safely and securely as it would be within the UK and under the Data Protection Legislation, as explained above in Part 7.

If we sell, transfer, or merge parts of our business or assets, your personal data may be transferred to a third party. Any new owner of our business may continue to use your personal data in the same way(s) that we have used it, as specified in this Privacy Policy (i.e. to communicate with you).

In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

9. How Can I Access My Personal Data?

If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a "subject access request".

All subject access requests should be made in writing and sent to the email or postal addresses shown in Part 10.

There is not normally any charge for a subject access request. If your request is 'manifestly unfounded or excessive' (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding.

We will respond to your subject access request within less than one month and, in any case, not more than one month of receiving it. Normally, we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully informed of our progress.

10. How Do I Contact You?

To contact us about anything to do with your personal data and data protection, including to make a subject access request, please use the following details (for the attention of Director):

Email address: info@blanboz.com.

Postal Address: Office 1, Technology House,
9 Newton Place, Glasgow, G3 7PR. United Kingdom.

11. Changes to this Privacy Policy

We may change this Privacy Policy from time to time. This may be necessary, for example, if the law changes, or if we change our business in a way that affects personal data protection.

Any changes will be immediately posted on Our Site and you will be deemed to have accepted the terms of the Privacy Policy on your first use of Our Site following the alterations. [We] OR [I] recommend that you check this page regularly to keep up-to-date. This Privacy Policy was last updated on 01 December 2025.

12. Attribution

This Privacy Policy has been created using a document template from www.simply-docs.co.uk.

07

Data Protection

Data Protection - Blanboz Limited

1. Introduction

This Policy sets out the obligations of Blanboz Limited, a company registered in Scotland under number SC713901, whose registered office is at Office 1 , Technology House, 9 Newton Place,Glasgow, G3 7PR, United Kingdom ("the Company") regarding data protection and the rights of customers, business information and sensible data in respect of their personal data under UK Data Protection Legislation (defined below).

This Policy sets out the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

2. Definitions

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they (by a statement or by a clear affirmative action) signify their agreement to the processing of personal data relating to them;
"data controller"	means the person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to customers, business information and sensible data used in our business;
"data processor"	means a person or organisation which processes personal data on behalf of a data controller;
"Data Protection Legislation"	means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder), and the Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation;
"data subject"	means a living, identified, or identifiable individual about whom the Company holds personal data;
"EEA"	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;

"personal data"	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
"personal data breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
"processing"	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"pseudonymisation"	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
"special category personal data"	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

3. Data Protection Officer & Scope of Policy

3.1 The Company's Data Protection Officer is Andres Blanco, a.blanco@blanboz.com. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies (including those referred to in this Policy), procedures, and/or guidelines.

3.2 All Blanboz's directors and managers are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

3.3 Any questions relating to this Policy, the Company's collection, processing, or holding of personal data, or to the Data Protection Legislation should be referred to the Data Protection Officer.

4. The Data Protection Principles

The Data Protection Legislation sets out the following principles with which any party handling personal data must comply. All personal data must be:

4.1 processed lawfully, fairly, and in a transparent manner in relation to the data subject;

4.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

4.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;

4.4 accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;

4.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of the data subject;

4.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

5. The Rights of Data Subjects

The Data Protection Legislation sets out the following key rights applicable to data subjects:

5.1 The right to be informed;
5.2 the right of access;
5.3 the right to rectification;
5.4 the right to erasure (also known as the 'right to be forgotten');
5.5 the right to restrict processing;
5.6 the right to data portability;
5.7 the right to object; and
5.8 rights with respect to automated decision-making and profiling.

6. Lawful, Fair, and Transparent Data Processing

6.1 The Data Protection Legislation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

6.2 If the personal data in question is special category personal data (also known as 'sensitive personal data'), at least one of the following conditions must be met:

a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);

b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;

e) the processing relates to personal data which is manifestly made public by the data subject;

f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

g) the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;

i) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or

j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

7. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

7.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

7.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

7.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

7.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

7.5 If special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.

7.6 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

8. Specified, Explicit, and Legitimate Purposes

8.1 The Company collects and processes the personal data set out in our services and products, and, or communication with clients and third parties. This includes:

a) personal data collected directly from data subjects; and

b) personal data obtained from third parties.

8.2 The Company only collects, processes, and holds personal data for the specific purposes set out in our services and products, and, or communication with clients and third parties (or for other purposes expressly permitted by the Data Protection Legislation).

8.3 Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.

9. Adequate, Relevant, and Limited Data Processing

9.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 8, above, and as set out in our services and products, and, or communication with clients and third parties.

9.2 Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

9.3 Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

10. Accuracy of Data and Keeping Data Up-to-Date

10.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 17, below.

10.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

11. Data Retention

11.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

11.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

11.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

12. Secure Processing

12.1 The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in the Company's Data Security Policy.

12.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

12.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

13. Accountability and Record-Keeping

13.1 The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

13.2 The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please refer to Part 14 for further information).

13.3 All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of the Data Protection Legislation, this Policy, and all other applicable Company policies.

13.4 The Company's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

13.5 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following:

a) the name and details of the Company, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);

b) the purposes for which the Company collects, holds, and processes personal data;

c) the Company's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;

d) details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

e) details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards;

f) details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy);

g) details of personal data storage, including location(s); and

h) detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

14. Data Protection Impact Assessments and Privacy by Design

14.1 In accordance with privacy by design principles, the Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

14.2 The principles of privacy by design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:

a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;

b) the state of the art of all relevant technical and organisational measures to be taken;

c) the cost of implementing such measures; and

d) the risks posed to data subjects and to the Company, including their likelihood and severity.

14.3 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

a) the type(s) of personal data that will be collected, held, and processed;

b) the purpose(s) for which personal data is to be used;

c) the Company's objectives;

d) how personal data is to be used;

e) the parties (internal and/or external) who are to be consulted;

f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

g) risks posed to data subjects;

h) risks posed both within and to the Company; and

i) proposed measures to minimise and handle identified risks.

15. Keeping Data Subjects Informed

15.1 The Company shall provide the information set out in Part 15.2 to every data subject:

a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

i) if the personal data is used to communicate with the data subject, when the first communication is made; or

ii) if the personal data is to be transferred to another party, before that transfer is made; or

iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

15.2 The following information shall be provided in the form of a privacy notice:

a) details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;

b) the purpose(s) for which the personal data is being collected and will be processed (as detailed in our services and products, and, or communication with clients and third parties) and the lawful basis justifying that collection and processing;

c) where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) where the personal data is to be transferred to one or more third parties, details of those parties;

f) where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see Part 25 of this Policy for further details);

g) details of applicable data retention periods;

h) details of the data subject's rights under the Data Protection Legislation;

i) details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

j) details of the data subject's right to complain to the Information Commissioner's Office;

k) where the personal data is not obtained directly from the data subject, details about the source of that personal data;

l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

m) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

16. Data Subject Access

16.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

16.2 Employees wishing to make a SAR should do so using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at a.blanco@blanboz.com or +44790 8686 4 24.

16.3 Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

16.4 All SARs received shall be handled by the Company's Data Protection Officer and in accordance with the Company's Data Subject Access Request Policy & Procedure.

16.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

17. Rectification of Personal Data

17.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

17.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

17.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

18. Erasure of Personal Data

18.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);

d) the personal data has been processed unlawfully;

e) the personal data needs to be erased in order for the Company to comply with a particular legal obligation.

18.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

18.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

19. Restriction of Personal Data Processing

19.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

19.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

20. Objections to Personal Data Processing

20.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing (including profiling).

20.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

20.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

21. Direct Marketing

21.1 The Company is subject to certain rules and regulations when marketing its products and services.

21.2 The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:

a) The Company may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from the Company.

21.3 The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.

21.4 If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.]

22. Personal Data Collected, Held, and Processed

Full details of the personal data collected, held, and processed by the Company are located in Blanboz's 365 Microsoft suite and Blanboz's computer. For details of data retention, please refer to the Company's Data Retention Policy.

23. Transferring Personal Data to a Country Outside the UK

23.1 The Company may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The Data Protection Legislation restricts such transfers in order to ensure that the level of protection given to data subjects is not compromised.

23.2 Personal data may only be transferred to a country outside the UK if one of the following applies:

a) The UK has issued adequacy regulations confirming that the personal data will receive an adequate level of protection (referred to as 'adequacy decisions', 'adequacy regulations', or 'partial findings of adequacy'). Such regulations may apply to a country as a whole, organisation(s), framework(s) or mechanism(s), or to data covered by specific legislation. Since 1 January 2021, transfers of personal data from the UK to EEA countries have continued to be permitted. Pre-existing EU Commission adequacy decisions in effect as at 31 December 2020 are also recognised, subject to ongoing review by the UK Government.

b) Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct, or an approved certification mechanism. Standard contractual clauses include the International Data Transfer Agreement issued by the Information Commissioner's Office and the International Data Transfer Addendum to the current EU Commission Standard Contractual Clauses (set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021), issued by the Information Commissioner's Office. (Contracts entered into on the basis of the old EU Commission Standard Contractual Clauses prior to 21 September 2022 will continue to provide appropriate safeguards until 21 March 2024.)

c) The transfer is made with the informed and explicit consent of the relevant data subject(s).

d) The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the data subject and the Company; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for the Company's legitimate interests.

24. Data Breach Notification

24.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

24.2 If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

24.3 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

24.4 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 26.3) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

24.5 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

25. Implementation of Policy

This Policy shall be deemed effective as of 01 December 2025. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name:	Andres Blanco
Position:	Director
Date:	01 December 2025
Due for Review by:	02 December 2026
Signature: