

Wincent Investment Fund PCC Limited

Data Privacy Policy

Table of Contents

1. Introduction.....	2
2. Policy principles.....	2
3. Glossary.....	3
4. Data collection.....	4
5. Lawful Grounds and Purpose of Processing.....	5
6. Data retention.....	5
7. Breach response.....	6
8. Data security.....	6
9. Data accuracy and rectification.....	7
10. Data Protection Officer (DPO).....	7
11. Sharing and Transfers of Personal Data.....	8
12. Contact and Complaints.....	8
13. Conclusion.....	9
14. Policy Updates and approval.....	9

1. Introduction

- 1.1. Wincent Investment Fund PCC Limited, and its affiliated entities (together, '**Wincent**') is committed to ensuring full compliance with the General Data Protection Regulation (GDPR), adhering to its key requirements to protect the Personal Data of individuals in compliance with Regulation (EU) 2016/679, Gibraltar GDPR, and Data Protection Act 2004 (DPA)(together, the '**Privacy Legislation**') .
- 1.2. This policy applies to all individuals whose personal data is collected or Processed by Wincent, including but not limited to clients, investors, contractors, visitors to our websites, prospective employees, candidates and other business contacts.

2. Policy principles

- 2.1. In accordance with GDPR Article 5(1)(a), and DPA Articles 14(2) and 8(a), Wincent Processes Personal Data lawfully, fairly, and transparently, ensuring that individuals are informed about the collection and use of their Personal Data. In addition, in accordance with GDPR Article 6 and DPA Article 10, all Processing activities have a valid lawful basis.
- 2.2. Wincent collects and Processes Personal Data solely for specified, explicit, and legitimate purposes, as mandated by GDPR Article 5(1)(b) and DPA Article 43, ensuring that data collected is (i) adequate, (ii) relevant, and (iii) limited to what is necessary for the relevant business functions, in compliance with the principle of data minimisation under GDPR Article 5(1)(c).
- 2.3. Wincent acknowledges and is fully committed to upholding Data Subjects' rights, continuously monitoring compliance, rectifying inaccuracies, erasing data, and transparently communicating to Data Subjects their rights as stipulated in Chapter 3, Articles 15-21 of the GDPR and Articles 55, and 56 of DPA. These rights are enshrined in the Privacy Legislation and include, but are not limited to, the following:
 - a. Right to Be Informed: Transparency regarding data collection and Processing.
 - b. Right of Access: The ability to obtain a copy of Personal Data.

- c. Right to Rectification: Correction of inaccurate or incomplete data.
- d. Right to Erasure: Deletion of Personal Data under certain conditions.
- e. Right to Restrict Processing: Limiting the Processing of data.
- f. Right to Data Portability: Receiving data in a structured format for transfer to another party.
- g. Right to Object: Opposing data Processing based on legitimate interests or direct marketing.
- h. Right Not to Be Subject to Automated Decision-Making: Protection against solely automated Processing affecting legal or significant decisions.

3. Glossary

Controller	Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
Data subject	Means any identified or identifiable natural person whose Personal Data is Processed by the Controller or the Processor. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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 natural person.
Personal data	Means any information relating to a Data Subject;
Process (Processing, Processed and Processes)	Means any operation or set of operations which is performed on Personal Data, whether or not by automated means, including but not limited to the 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 of such data.
Processor	Means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.
Special Category Personal Data	Refers to specific types of Personal Data that are considered more sensitive and thus require higher levels of protection. The definition includes: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation.

4. Data collection

- 4.1. Wincent may collect and process personal information from individuals in various contexts, such as during recruitment, when establishing a trading relationship, or through other forms of engagement. This information may include personal and contact details (e.g., name, date of birth, ID/passport details, email address, physical address), records of our communications (e.g., via email or Slack), financial information (e.g., payment and bank account details, payroll details), employment information (e.g., references from previous employers, professional qualifications, educational background) and any other information that can identify you.
- 4.2. Additionally, we may Process special categories of Personal Data when required to meet legal and regulatory obligations, including Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) checks and Know Your Customer (KYC) requirements as required by GDPR Article 6(1)(c) and DPA Article 15.
- 4.3. Wincent primarily collects information directly from Data Subjects but may also gather data from other sources, including publicly available sources and third parties such as due diligence and sanctions screening providers. If Data Subjects provide Wincent with

Personal Data of individuals and/or entities other than themselves, data shall be Processed in compliance with current regulatory requirements.

5. Lawful Grounds and Purpose of Processing

- 5.1. Wincent commits to Processing Personal Data according to principles and procedures that are enshrined in the GDPR and DPA Article 53, including, but not limited to:
- A. Compliance with contractual duties: When Processing is necessary to comply with contracts with counterparties or when establishing a business relationship (GDPR Article 6(1)(b)) e.g. service providers, counter-parties and prospective employees.
 - B. Compliance with Legal and Regulatory Requirements: Wincent Processes Personal Data to meet legal obligations such as AML/CTF checks (GDPR Article 6(1)(c)) e.g. investors, counter-parties, OTC Clients, directors and ultimate beneficial owners.
 - C. Recruitment: Personal data of job applicants is processed based on our legitimate interests in recruitment, or where necessary to take steps prior to entering into a contract, in accordance with GDPR Article 6(1)(b) and (f).
 - D. Special Categories of Data: When necessary, Wincent Processes sensitive data only with explicit consent or in circumstances permitted by relevant legislations.

6. Data retention

- 6.1. Personal data is retained only for as long as necessary to fulfill the purposes for which it was collected, following Article 5(1)(e) GDPR¹. Typically, the timeframe for retention is up to five years post-termination of agreements unless a longer retention period is required by law or a competent authority has requested this via official communication to Wincent. For

¹ Unless data is the object of a Suspicious Activity Report, and has actively been escalated to the relevant authorities. In such a case, data will be treated in compliance with the instructions of the authorities, and in full compliance with regulatory requirements.

the avoidance of doubt, Wincent confirms that Personal Data is securely deleted or anonymised once it is no longer required for the purposes for which it was collected.

- 6.2. Additionally, in order to maintain accuracy and integrity of the Personal Data, Wincent commits to promptly rectify any inaccuracies in Personal Data as per GDPR Article 5(1)(d).

7. Breach response

- 7.1. In the event of a Personal Data breach, Wincent will, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data breach to the supervisory authority competent in accordance with GDPR Article 55 and DPA Article 76, unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons involved. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay, in compliance with GDPR Article 33.
- 7.2. Additionally, Wincent commits to notify a Personal Data breach to the Data Subject in accordance with GDPR Article 34 and DPA Article 77. Any such communication to the Data Subject shall be written in clear and plain language about the nature of the Personal Data breach and contain at least the information and measures referred to in points (b), (c) and (d) of GDPR Article 33(3).

8. Data security

- 8.1. To ensure the security of Personal Data, Wincent implements appropriate technical and organisational measures as required under GDPR Article 32 and DPA Article 75, protecting against unauthorised access, alteration, disclosure, or destruction. Where Processing activities are likely to result in high risks for individuals' rights and freedoms, Wincent commits to conducting Data Protection Impact Assessments (DPIAs) where required in accordance with GDPR Article 35 and DPA Article 73, in order to identify and mitigate related risks.

- 8.2. Wincent's systems and procedures are developed and maintained in accordance with DPA Article 65 and GDPR Article 25 to ensure that, by default, only Personal Data which is necessary for each specific Processing purpose is collected and Processed. This reflects the principle of data minimisation and the application of appropriate technical and organisational measures, consistent with the GDPR's requirement to implement '*data protection by design and default*'.
- 8.3. Wincent establishes clear agreements with Processors in order to ensure compliance with GDPR requirements, as stipulated in GDPR Article 28, ensuring that they are Processing Personal Data only on documented instructions and with appropriate safeguards. Wincent engages only Processors who provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing would meet the requirements of GDPR, and ensure the protection of the rights of the Data Subject, as per GDPR Article 28.

9. Data accuracy and rectification

- 9.1. Wincent also recognises and facilitates the rights of Data Subjects, including access, rectification, erasure, restriction of Processing, data portability, and the right to object to Processing, as granted by GDPR Articles 15-21 and DPA 56(3), 157(1)(a), and 157(3)(a).

10. Data Protection Officer (DPO)

- 10.1. Wincent has appointed a Data Protection Officer (DPO) who is in charge of periodically reviewing this policy to ensure ongoing compliance with regulatory requirements and overseeing Wincent's data protection strategy, in compliance with GDPR Article 37 and Chapter 4 Article 78-80 of DPA.
- 10.2. Wincent's DPO is registered with the Gibraltar Regulatory Authority. The DPO register may be viewed at the [Data Protection Officer Register](#).

10.3. The DPO may be contacted at:

10.3.1. **Email:** gdpr@wincent.co

10.3.2. **Address:** 120B Old Police Station, Irish Town, Gibraltar, GX11 1AA

11. Sharing and Transfers of Personal Data

11.1. Wincent does not sell Personal Data to any third parties.

11.2. Wincent may share Personal Data internally within the Wincent Group and externally with service providers, financial institutions, legal advisors, and, where legally required, government authorities. As Wincent is a global entity, Wincent might also transfer Personal Data outside the European Economic Area (EEA). In such cases, Wincent ensures appropriate safeguards are applied to the data transferred in compliance with Chapter V of GDPR (standard contractual clauses or adequacy decisions) and Article 82 - Article 85 of DPA.

12. Contact and Complaints

12.1. For any inquiries or to exercise the above-listed rights, including withdrawing consent where Processing is based on it, Data Subjects can contact the DPO at gdpr@wincent.co. Wincent will acknowledge receipt and respond within one calendar month, in accordance with GDPR Article 12(3). Withdrawal of consent will not affect the lawfulness of any Processing carried out prior to its withdrawal.

12.2. Wincent recognises and supports the right of Data Subjects to lodge a complaint with the Gibraltar Data Protection Commissioner, and will always inform the Data Subject of such a right.

13. Conclusion

- 13.1. By implementing this policy, Wincent commits to maintaining the highest standards of compliance and integrity in activities involving data collection, protection, security, retention, and sharing.
- 13.2. The Board of Directors approves this Policy in compliance with the regulatory requirements of the jurisdiction of Gibraltar and confirms its alignment with the GDPR and DPA. The Board of Directors acknowledges that this Policy adheres to all the regulations in force in the above mentioned jurisdiction at the moment of writing.

14. Policy Updates and approval

- 14.1. This Privacy Policy was last updated on March 26 2025 and will be reviewed annually or upon material change to the applicable data protection laws.

1. Version	2. Date of approval	3. Comments
1.0	9.4.2025	Minutes link here