This Privacy and Data Protection Policy is established on the 1st day of January 2025

By: N3 Technologies Limited

Applicable to: All employees, contractors, and third-party providers who handle personal data on behalf of the Company

Parties

(1) **N3 Technologies Limited**, a company incorporated under the laws of England and Wales, company registration number 14501106, with its registered office at Seymour House 15a Frederick Road, Edgbaston, Birmingham, England, B15 1JD (the "**Company**"), acting as data controller.

(2) All **employees** of the Company, including full-time, part-time, temporary, and seasonal employees.

(3) All **contractors and consultants** engaged by the Company who have access to personal data or the Company's systems.

(4) All **third-party service providers** and **data processors** who process personal data on behalf of the Company.

(5) **Directors and senior management** of the Company with specific data protection governance responsibilities.

Background

(A) N3 Technologies Limited operates a software as a service package serving clients in the construction, consultancy, and development finance sectors, employing between 1 and 50 people.

(B) The Company processes personal data in the course of its business operations, including sensitive client data, project details, employee information, and financial records relating to construction projects and consultancy services.

(C) The Company is subject to the UK General Data Protection Regulation and the Data Protection Act 2018, which impose strict obligations regarding the processing of personal data.

(D) The construction and consultancy industries involve unique data processing requirements, including the handling of confidential project information, multi-party collaborations, and sensitive commercial data.

(E) This Policy is necessary to ensure compliance with applicable data protection laws, protect the rights of data subjects, and establish clear guidelines for all personnel who handle personal data.

(F) The Company recognises its responsibility as a data controller to implement appropriate technical and organisational measures to ensure lawful, fair, and transparent processing of personal data.

(G) This Policy is governed by the laws of England and Wales and establishes the framework for the Company's data protection compliance programme.

1. Definitions

1.1. **Company** means N3 Technologies Limited, a company incorporated under the laws of England and Wales.

1.2. **Contractor** means any independent contractor, consultant, freelancer, or temporary worker engaged by the Company.

1.3. **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.

1.4. **Data Controller** means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

1.5. **Data Processor** means a natural or legal person which processes personal data on behalf of the data controller.

1.6. **Data Protection Impact Assessment** or **DPIA** means a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.

1.7. **Data Subject** means an identified or identifiable natural person to whom personal data relates.

1.8. **Employee** means any person employed by the Company under a contract of employment, whether full-time, part-time, temporary, or seasonal.

1.9. **ICO** means the Information Commissioner's Office, the UK's independent authority set up to uphold information rights.

1.10. **Lawful Basis** means one of the six legal grounds specified in Article 6 of the UK GDPR that permits the processing of personal data.

1.11. **Personal Data** means any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, by reference to an identifier or factors specific to that person.

1.12. **Policy** means this Data Protection Policy and any amendments or updates made from time to time.

1.13. **Processing** means any operation performed on personal data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, restriction, erasure, or destruction.

1.14. **Special Category Data** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation.

1.15. **Standard Contractual Clauses** means the standard data protection clauses adopted by the European Commission for the transfer of personal data to third countries.

1.16. **Third Party** means any natural or legal person, public authority, agency, or body other than the Company, its employees, contractors, and data processors acting under direct authority of the Company.

1.17. **UK GDPR** means the UK General Data Protection Regulation as retained in UK law following Brexit, together with the Data Protection Act 2018.

2. Purpose and Scope

2.1. The purpose of this Policy is to ensure that the Company complies with its obligations under the UK GDPR and the Data Protection Act 2018 in respect of all Processing of Personal Data undertaken by or on behalf of the Company.

2.2. This Policy applies to and is binding upon:

(a) all Employees of the Company;

(b) all Directors and senior management of the Company;

(c) all Contractors and consultants engaged by the Company;

(d) all Third Party service providers who Process Personal Data on behalf of the Company; and

(e) all Data Processors acting under the instructions of the Company.

2.3. This Policy covers all Personal Data Processed by the Company, including but not limited to:

(a) client data and project information relating to construction and consultancy services;

(b) Employee personal data and employment records;

(c) financial data relating to development finance activities;

(d) commercial and contractual information involving multiple parties; and

(e) any Special Category Data handled in the course of business operations.

2.4. The scope of this Policy extends to all Processing activities undertaken in connection with the Company's software as a service operations, including data collection, storage, analysis, sharing, and disposal across all business sectors served by the Company.

2.5. All persons covered by this Policy must comply with its provisions and maintain awareness of their data protection responsibilities under applicable law.

2.6. This Policy establishes the minimum standards for data protection compliance and may be supplemented by additional procedures, guidelines, or contractual obligations as required by the nature of specific Processing activities.

3. Data Protection Principles

3.1. The Company shall process all Personal Data in accordance with the data protection principles established under UK GDPR and shall ensure that all Employees, Contractors and Third Parties comply with these principles.

3.2. **Lawfulness, Fairness and Transparency**

(a) All Processing of Personal Data must have a valid Lawful Basis under UK GDPR and shall be conducted in a fair and transparent manner.

(b) The Company shall provide clear and accessible information to Data Subjects about how their Personal Data is processed, including the purposes of Processing and the legal basis relied upon.

(c) Privacy notices shall be provided to clients, employees, and other Data Subjects at the point of data collection and shall be regularly reviewed and updated.

3.3. **Purpose Limitation**

(a) Personal Data shall only be collected and processed for specified, explicit, and legitimate purposes related to construction, consultancy, and development finance services.

(b) Personal Data shall not be further processed in a manner incompatible with the original purposes for which it was collected.

(c) Any new Processing purposes shall require a separate Lawful Basis and appropriate notification to Data Subjects.

3.4. **Data Minimisation**

(a) The Company shall ensure that Personal Data processed is adequate, relevant, and limited to what is necessary for the specified purposes.

(b) Regular reviews shall be conducted to identify and eliminate unnecessary data collection and Processing activities.

(c) Data collection forms and systems shall be designed to capture only essential information required for business operations.

3.5. **Accuracy**

(a) The Company shall take reasonable steps to ensure that Personal Data is accurate and, where necessary, kept up to date.

(b) Inaccurate Personal Data shall be erased or rectified without delay upon identification or notification.

(c) Regular data quality checks shall be implemented, particularly for client project data and employee records.

3.6. **Storage Limitation**

(a) Personal Data shall not be kept for longer than necessary for the purposes for which it is processed.

(b) The Company shall establish and maintain clear data retention schedules specifying retention periods for different categories of Personal Data.

(c) Personal Data shall be securely deleted or anonymised when retention periods expire, subject to legal and regulatory requirements.

3.7. **Integrity and Confidentiality**

(a) The Company shall implement appropriate technical and organisational measures to ensure adequate security of Personal Data against unauthorised or unlawful Processing and accidental loss, destruction, or damage.

(b) Security measures shall include encryption, access controls, regular security assessments, and staff training on data security practices.

(c) Confidentiality obligations shall be imposed on all persons who have access to Personal Data through employment contracts, confidentiality agreements, or professional codes of conduct.

3.8. **Accountability**

(a) The Company shall be responsible for and able to demonstrate compliance with all data protection principles.

(b) Appropriate documentation, policies, procedures, and records shall be maintained to evidence compliance with UK GDPR requirements.

(c) Regular compliance audits and assessments shall be conducted to monitor adherence to these principles and identify areas for improvement.

3.9. The Company shall ensure that these principles are embedded in all business processes, system designs, and decision-making procedures that involve the Processing of Personal Data.

4. Lawful Basis for Processing

4.1. The Company will only process Personal Data where there is a valid **Lawful Basis** under Article 6 of the UK GDPR.

4.2. The Company relies on the following lawful bases for processing Personal Data:

(a) **Consent** where the Data Subject has given clear and specific consent to the processing for one or more specific purposes.

(b) **Performance of a contract** where processing is necessary for the performance of a contract to which the Data Subject is party, or to take steps at the request of the Data Subject prior to entering into a contract.

(c) **Legal obligation** where processing is necessary for compliance with a legal obligation to which the Company is subject.

(d) **Legitimate interests** where processing is necessary for the purposes of legitimate interests pursued by the Company or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

4.3. The Company applies these lawful bases to specific data processing activities as follows:

(a) **Client contract data** (names, contact details, project specifications): processed under performance of contract for service delivery and project management.

(b) **Employee data** (contact details, employment records, performance data): processed under performance of contract for employment administration and legal obligation for statutory reporting.

(c) **Construction project data** (site information, progress reports, safety records): processed under performance of contract for project delivery and legal obligation for health and safety compliance.

(d) **Financial data** (invoicing, payment records, development finance information): processed under performance of contract for billing purposes and legal obligation for accounting and tax requirements.

(e) **Marketing communications**: processed under legitimate interests for business development, subject to opt-out rights.

(f) **CCTV and security monitoring**: processed under legitimate interests for premises security and asset protection.

4.4. For **Special Category Data**, the Company relies on the following additional conditions under Article 9 of the UK GDPR:

(a) **Explicit consent** for processing health and safety information where required.

(b) **Employment obligations** for processing necessary for employment, social security, and social protection law obligations.

(c) **Substantial public interest** where processing is necessary for regulatory compliance in construction and financial services.

4.5. The Company maintains a **Record of Processing Activities** documenting the lawful basis for each processing activity and regularly reviews these bases to ensure continued compliance.

4.6. Where the Company relies on **legitimate interests**, a balancing test has been conducted and documented to ensure that the Company's interests do not override the Data Subject's rights and freedoms.

4.7. Data Subjects have the right to object to processing based on legitimate interests, and the Company will cease processing unless it can demonstrate compelling legitimate grounds that override the Data Subject's interests.

5. Data Categories and Processing Activities

5.1. The Company processes the following categories of Personal Data in connection with its business operations:

(a) **Employee Data**: Personal Data relating to current, former, and prospective employees, including contact details, employment records, payroll information, performance evaluations, training records, and disciplinary records.

(b) **Client Data**: Personal Data relating to clients and their representatives, including contact information, project requirements, commercial preferences, financial information, and communication records.

(c) **Project Data**: Personal Data embedded within construction and consultancy project documentation, including site records, contractor details, planning applications, technical specifications, project financials, project programme and project correspondence.

(d) **Financial Data**: Personal Data relating to invoicing, payments, credit assessments, and financial transactions involving clients, suppliers, and contractors.

(e) **Contractor and Consultant Data**: Personal Data relating to third-party contractors, consultants, and their personnel engaged in Company projects, including professional qualifications, insurance details, and performance records.

(f) **Visitor and Contact Data**: Personal Data relating to visitors to Company premises, website users, and individuals who make enquiries about Company services.

5.2. The Company undertakes the following Processing activities in relation to Personal Data:

(a) **Collection and Recording**: Gathering Personal Data through application forms, contracts, correspondence, website interactions, and direct communications.

(b) **Storage and Organisation**: Maintaining Personal Data in electronic databases, filing systems, and cloud-based platforms used for project management and business operations.

(c) **Use and Analysis**: Utilising Personal Data for service delivery, project management, financial administration, performance monitoring, and business development purposes.

(d) **Disclosure and Sharing**: Sharing Personal Data with clients, contractors, regulatory authorities, legal advisors, and other third parties as necessary for business operations and legal compliance.

(e) **Combination and Linking**: Combining Personal Data from different sources to create comprehensive project files and client profiles for effective service delivery.

(f) **Retention and Archiving**: Maintaining Personal Data for specified retention periods and transferring to archive systems where appropriate.

(g) **Deletion and Destruction**: Securely deleting or destroying Personal Data when retention periods expire or when no longer required for business purposes.

5.3. The Processing activities specified in clause 5.2 are undertaken for the following purposes:

(a) **Contract Performance**: To fulfil contractual obligations to clients and manage construction and consultancy projects.

(b) **Employment Management**: To manage the employment relationship, including recruitment, payroll, performance management, and health and safety compliance.

(c) **Legal Compliance**: To comply with statutory and regulatory requirements applicable to the construction and consultancy industries.

(d) **Legitimate Interests**: To pursue the Company's legitimate business interests, including business development, risk management, and maintaining professional standards.

5.4. Special Category Data is processed only where strictly necessary and with appropriate additional safeguards, including:

(a) Health and safety information relating to employees and site personnel.

(b) Diversity and equality monitoring data for employment purposes.

(c) Criminal conviction data for roles requiring security clearance or regulatory compliance.

5.5. All Processing activities are conducted in accordance with the Data Protection Principles set out in this Policy and the applicable Lawful Basis identified in section 6.

6. Data Subject Rights

6.1. **General Rights**: Data subjects have the following rights under UK GDPR in relation to their Personal Data processed by the Company: the right of access, rectification, erasure, restriction of processing, data portability, objection, and rights relating to automated decision making and profiling.

6.2. **Right of Access**:

(a) Data subjects may request access to their Personal Data and information about how it is processed by submitting a subject access request to the Company.

(b) The Company shall provide the requested information within one month of receipt of a valid request, which may be extended by a further two months where requests are complex or numerous.

(c) The Company may request additional information to verify the identity of the data subject making the request.

(d) No fee shall be charged for subject access requests unless they are manifestly unfounded, excessive, or repetitive, in which case a reasonable administrative fee may be applied.

6.3. **Right to Rectification**:

(a) Data subjects may request rectification of inaccurate Personal Data or completion of incomplete Personal Data.

(b) The Company shall rectify inaccurate Personal Data without undue delay and within one month of receipt of a valid request.

(c) Where Personal Data has been disclosed to third parties, the Company shall inform such parties of the rectification where possible.

6.4. **Right to Erasure**:

(a) Data subjects may request erasure of their Personal Data where processing is no longer necessary, consent is withdrawn, processing is unlawful, or erasure is required for compliance with legal obligations.

(b) The Company shall consider each erasure request against applicable legal bases for continued processing and data retention requirements.

(c) Where erasure is granted, the Company shall take reasonable steps to inform third parties who have received the Personal Data.

6.5. **Right to Restrict Processing**:

(a) Data subjects may request restriction of processing where they contest the accuracy of Personal Data, processing is unlawful, or they require the data for legal claims.

(b) Where processing is restricted, the Company shall only process such Personal Data with the data subject's consent or for specific legal purposes.

6.6. **Right to Data Portability**:

(a) Where processing is based on consent or contract performance and carried out by automated means, data subjects may request their Personal Data in a structured, commonly used, and machine-readable format.

(b) Data subjects may request direct transmission of their Personal Data to another controller where technically feasible.

6.7. **Right to Object**:

(a) Data subjects may object to processing based on legitimate interests, direct marketing purposes, or scientific/historical research purposes.

(b) The Company shall cease such processing unless it can demonstrate compelling legitimate grounds that override the data subject's interests, rights, and freedoms.

6.8. **Automated Decision Making**:

(a) Data subjects have the right not to be subject to automated decision making, including profiling, which produces legal effects or similarly significant effects.

(b) Where automated decision making occurs, data subjects may request human intervention, express their point of view, and contest the decision.

6.9. **Request Procedures**:

(a) All data subject rights requests must be submitted in writing to the Company's designated contact address or email specified in this Policy.

(b) Requests may be made by the data subject directly or through an authorised representative with appropriate proof of authority.

(c) The Company may request reasonable information to verify the identity of the requestor and locate the relevant Personal Data.

6.10. **Response Requirements**:

(a) The Company shall acknowledge receipt of all data subject rights requests within 48 hours where practicable.

(b) Responses shall be provided in writing and include clear information about any action taken or reasons for refusal.

(c) Where requests are refused, the Company shall inform the data subject of their right to complain to the ICO and seek judicial remedy.

6.11. **Record Keeping**: The Company shall maintain records of all data subject rights requests, including the nature of the request, action taken, and response provided, for audit and compliance purposes.

7. Data Security Measures

7.1. The Company shall implement appropriate **technical and organisational measures** to ensure a level of security appropriate to the risk of Processing, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing.

7.2. **Technical Security Measures** shall include:

(a) **Encryption** of Personal Data both in transit and at rest using industry-standard encryption protocols (minimum AES-256 for data at rest and TLS 1.2 for data in transit).

(b) **Access controls** implementing role-based permissions ensuring Personnel can only access Personal Data necessary for their specific job functions.

(c) **Multi-factor authentication** for all systems containing Personal Data, particularly project management platforms and client databases.

(d) **Data loss prevention** systems to monitor, detect and prevent unauthorised transmission of Personal Data outside the Company's network.

(e) **Regular security updates** and patch management for all systems and software used in Processing Personal Data.

(f) **Network security** measures including firewalls, intrusion detection systems, and secure Wi-Fi protocols.

7.3. **Physical Security Measures** shall include:

(a) **Restricted access** to server rooms and data storage facilities through key card systems and biometric controls.

(b) **Secure disposal** of physical storage media containing Personal Data through certified destruction services.

(c) **Clean desk policy** requiring all physical documents containing Personal Data to be secured when not in use.

(d) **Visitor access controls** to premises where Personal Data is processed, including visitor logs and escort requirements.

7.4. **Organisational Security Measures** shall include:

(a) **Security policies** covering password management, remote working, bring-your-own-device usage, and data handling procedures.

(b) **Regular security training** for all Personnel on data protection and cybersecurity best practices.

(c) **Incident response procedures** for identifying, containing, and reporting security incidents.

(d) **Background checks** for Personnel with access to Special Category Data or sensitive client information.

7.5. **Monitoring and Testing** requirements:

(a) **Continuous monitoring** of systems for unauthorised access attempts and suspicious activities.

(b) **Regular penetration testing** and vulnerability assessments conducted annually or following significant system changes.

(c) **Security audits** performed at least annually to assess the effectiveness of implemented measures.

7.6. **Construction and Consultancy Specific Measures**:

(a) **Project data segregation** ensuring client project data is logically separated and access-controlled by project team membership.

(b) **Secure collaboration platforms** for sharing sensitive construction drawings, financial models, and project documentation with Third Parties.

(c) **Mobile device management** for Personnel accessing project data on construction sites or client premises.

7.7. The Company shall **regularly review and update** security measures to address emerging threats and maintain compliance with UK GDPR requirements.

7.8. **Security incident reporting** procedures require immediate escalation to the Data Protection Officer and senior management for any suspected or actual security breaches.

8. Data Retention Schedule

8.1. The Company shall retain Personal Data only for as long as necessary to fulfil the purposes for which it was collected and processed, in accordance with the data minimisation principle under UK GDPR.

8.2. **Employee Data** shall be retained for a period of six (6) years following termination of employment, unless a longer retention period is required by law or for the establishment, exercise, or defence of legal claims.

8.3. **Client Project Data**, including construction project documentation, consultancy reports, and development finance records, shall be retained for a minimum period of seven (7) years following completion of the relevant project or termination of the client relationship.

8.4. **Financial Records and Transaction Data** shall be retained for a minimum of six (6) years in accordance with applicable tax and company law requirements.

8.5. **Marketing and Communications Data** shall be retained for a maximum of three (3) years from the date of last contact, unless the Data Subject has provided ongoing consent for marketing communications.

8.6. **CCTV and Security Footage** shall be retained for a maximum of thirty (30) days unless required for investigation of incidents or legal proceedings.

8.7. **Contract and Commercial Documentation** relating to client engagements shall be retained for a minimum period of six (6) years following expiry or termination of the relevant agreement.

8.8. The Company may extend retention periods where:

(a) Personal Data is required for the establishment, exercise, or defence of legal claims;

(b) Ongoing regulatory investigations or proceedings require retention of specific data;

(c) Statutory or regulatory obligations mandate longer retention periods.

8.9. **Automatic Deletion Procedures** shall be implemented to ensure Personal Data is securely deleted or anonymised upon expiry of the applicable retention period, unless an exception under clause 8.8 applies.

8.10. The Data Protection Officer shall maintain a **Data Retention Register** documenting all categories of Personal Data, applicable retention periods, and deletion schedules.

8.11. Annual reviews of retained Personal Data shall be conducted to ensure compliance with this retention schedule and to identify data eligible for deletion.

8.12. Where Personal Data is stored by Third Party processors, contractual provisions shall ensure compliance with the Company's retention requirements and secure deletion upon expiry of retention periods.

9. Data Breach Response Plan

9.1. The Company shall maintain procedures to detect, report, assess, and respond to any actual or suspected Data Breach affecting Personal Data processed by or on behalf of the Company.

9.2. Upon becoming aware of a Data Breach, any Employee, Contractor, or Third Party shall immediately notify the designated Data Protection Officer or, in their absence, a Director, without unreasonable delay and in any event within one hour of discovery.

9.3. The Company shall maintain a Data Breach response team comprising the Data Protection Officer, a Director, the IT administrator, and such other personnel as may be required depending on the nature and severity of the breach.

9.4. Upon notification of a suspected Data Breach, the response team shall immediately:

(a) assess whether a Data Breach has occurred and determine its scope and severity;

(b) take immediate steps to contain the breach and prevent further unauthorised access, disclosure, or loss of Personal Data;

(c) preserve evidence relating to the breach for investigation and regulatory purposes;

(d) document all actions taken in response to the breach.

9.5. Where a Data Breach is likely to result in a risk to the rights and freedoms of Data Subjects, the Company shall notify the ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach.

9.6. The notification to the ICO shall include:

(a) a description of the nature of the Data Breach including the categories and approximate number of Data Subjects and Personal Data records concerned;

(b) the name and contact details of the Data Protection Officer or other contact point;

(c) a description of the likely consequences of the Data Breach;

(d) a description of measures taken or proposed to address the Data Breach and mitigate its adverse effects.

9.7. Where the Data Breach is likely to result in a high risk to the rights and freedoms of Data Subjects, the Company shall communicate the breach to the affected Data Subjects without undue delay, unless:

(a) appropriate technical and organisational protection measures have been applied to the data affected by the breach, particularly encryption;

(b) subsequent actions have been taken to ensure the high risk is no longer likely to materialise; or

(c) it would involve disproportionate effort, in which case public communication or similar measure shall be used.

9.8. Communications to Data Subjects shall be in clear and plain language and shall include the information specified in clause 9.6, together with advice on steps the Data Subject may take to protect themselves from potential adverse effects.

9.9. The Company shall conduct a thorough investigation of each Data Breach to:

(a) determine the root cause and contributing factors;

(b) assess the effectiveness of existing security measures;

(c) identify lessons learned and recommendations for improvement;

(d) implement corrective actions to prevent similar breaches.

9.10. The Company shall maintain a register of all Data Breaches, whether or not notification to the ICO is required, recording:

(a) the facts relating to the breach;

(b) its effects and remedial action taken;

(c) evidence demonstrating compliance with notification obligations.

9.11. Following resolution of a Data Breach, the Company shall:

(a) review and update security policies and procedures as necessary;

(b) provide additional training to relevant personnel;

(c) implement technical or organisational measures to prevent recurrence;

(d) monitor for any ongoing effects or related incidents.

10. International Data Transfers

10.1. The Company shall only transfer Personal Data to countries or territories outside the United Kingdom where such transfer complies with the requirements of UK GDPR and applicable data protection laws.

10.2. **Adequacy Decisions**

(a) Personal Data may be transferred to countries or territories that have been subject to an adequacy decision by the Secretary of State or retained EU adequacy decisions recognised under UK law.

(b) The Company shall maintain a current list of countries with adequacy decisions and review this list regularly to ensure ongoing compliance.

10.3. **Standard Contractual Clauses**

(a) Where no adequacy decision exists, the Company shall implement Standard Contractual Clauses approved by the ICO or retained EU Standard Contractual Clauses recognised under UK law.

(b) All Third Party processors located outside the United Kingdom must execute Standard Contractual Clauses before any Personal Data transfer occurs.

(c) The Company shall ensure that Standard Contractual Clauses remain current and compliant with any updates or replacements issued by the ICO.

10.4. **Transfer Risk Assessment**

(a) Before transferring Personal Data internationally, the Company shall conduct a transfer risk assessment to evaluate the protection afforded to Personal Data in the destination country.

(b) The assessment shall consider local laws, government access rights, judicial systems, and any other factors that may impact data protection.

(c) Where the assessment identifies risks, the Company shall implement additional safeguards or suspend the transfer until adequate protection can be ensured.

10.5. **Documentation and Records**

(a) The Company shall maintain comprehensive records of all international data transfers, including the legal basis, destination country, categories of Personal Data, and safeguards implemented.

(b) Transfer documentation shall be reviewed annually and updated when circumstances change.

10.6. **Construction and Consultancy Specific Transfers**

(a) International transfers of project data, client information, or commercial data relating to construction or consultancy services shall be subject to additional contractual protections with overseas partners or subcontractors.

(b) Client consent shall be obtained where required for international transfers of confidential project information.

10.7. **Employee Responsibilities**

(a) Employees, Contractors, and consultants are prohibited from transferring Personal Data internationally without prior approval from the designated data protection contact.

(b) Any unauthorised international transfer shall be reported immediately as a potential Data Breach.

10.8. **Monitoring and Review**

(a) The Company shall regularly monitor the adequacy of international transfer safeguards and update procedures in response to changes in law or Data Subject rights.

(b) International transfer arrangements shall be reviewed annually or when material changes occur to the processing activities or destination country circumstances.

11. Data Protection Roles and Responsibilities

11.1. The Company shall appoint a **Data Protection Officer** who shall be responsible for monitoring compliance with this Policy and UK GDPR requirements, providing advice on data protection matters, and serving as the primary contact point for data protection inquiries.

11.2. **Directors and senior management** are accountable for ensuring that adequate resources are allocated for data protection compliance and that this Policy is effectively implemented throughout the organisation.

(a) Directors shall approve annual data protection budgets and resource allocations.

(b) Senior management shall ensure that data protection considerations are integrated into business decision-making processes.

11.3. All **Employees** have a responsibility to comply with this Policy and shall:

(a) Process personal data only in accordance with their job responsibilities and this Policy.

(b) Report any suspected data breaches or policy violations immediately to the Data Protection Officer.

(c) Complete mandatory data protection training within 30 days of commencement of employment and annually thereafter.

(d) Maintain confidentiality of personal data and implement appropriate security measures when handling such data.

11.4. **Contractors and consultants** engaged by the Company shall:

(a) Comply with all provisions of this Policy when processing personal data on behalf of the Company.

(b) Sign appropriate data processing agreements before accessing Company systems or personal data.

(c) Notify the Company immediately of any data security incidents or breaches.

11.5. **Third-party service providers** and **data processors** shall be subject to contractual obligations requiring:

(a) Processing of personal data only on documented instructions from the Company.

(b) Implementation of appropriate technical and organisational security measures.

(c) Assistance with data subject rights requests and regulatory compliance.

(d) Deletion or return of personal data upon termination of services.

11.6. The Data Protection Officer shall maintain a register of all data processing activities and ensure regular reviews of data protection compliance across all departments.

11.7. Department heads are responsible for ensuring their teams understand and comply with data protection requirements relevant to their specific roles and the construction and consultancy projects they manage.

12. Training and Awareness Programme

12.1. The Company shall provide **mandatory data protection training** to all Employees, Contractors, and Third Parties who process Personal Data on behalf of the Company.

12.2. **Induction Training** shall be provided to all new Employees and Contractors within **thirty (30) days** of commencement of employment or engagement.

(a) Induction training shall cover the fundamental principles of UK GDPR, this Policy, and role-specific data handling requirements.

(b) New personnel shall not be granted access to Personal Data systems until completion of induction training and acknowledgment of this Policy.

12.3. **Annual refresher training** shall be provided to all personnel handling Personal Data to ensure ongoing compliance and awareness of regulatory updates.

12.4. Training programmes shall include but not be limited to:

(a) UK GDPR principles and Data Subject rights;

(b) Identification and classification of Personal Data and Special Category Data;

(c) Lawful Basis requirements for Processing activities;

(d) Data security measures and breach prevention;

(e) Data Breach response procedures and reporting obligations;

(f) Data Subject request handling procedures;

(g) International data transfer requirements;

(h) Industry-specific requirements for construction and consultancy data handling.

12.5. **Role-specific training** shall be provided to personnel with enhanced data protection responsibilities, including senior management, IT administrators, and project managers handling client data.

12.6. The Company shall maintain **comprehensive training records** documenting:

(a) Training attendance and completion dates;

(b) Training content delivered;

(c) Assessment results where applicable;

(d) Refresher training schedules.

12.7. Training delivery methods may include face-to-face sessions, online modules, workshops, and distribution of guidance materials appropriate to the Company's size and resources.

12.8. The Company shall implement **ongoing awareness initiatives** including regular communications, policy updates, and sharing of relevant data protection guidance.

12.9. **Additional training** shall be provided when:

(a) Significant changes occur to data protection legislation;

(b) New systems or processes involving Personal Data are implemented;

(c) Data Breaches or compliance incidents occur;

(d) Personnel assume new roles with different data handling responsibilities.

12.10. Training effectiveness shall be monitored through periodic assessments, compliance audits, and feedback mechanisms.

12.11. The **Data Protection Officer** shall be responsible for developing, coordinating, and overseeing the delivery of all data protection training programmes.

12.12. Directors and senior management shall demonstrate leadership in data protection compliance by participating in training programmes and promoting data protection awareness throughout the organisation.

13. Third Party Data Sharing

13.1. The Company may share Personal Data with Third Parties only where such sharing is necessary for legitimate business purposes and is conducted in accordance with UK GDPR and this Policy.

13.2. Prior to sharing Personal Data with any Third Party, the Company shall:

(a) Conduct appropriate due diligence to assess the Third Party's data protection capabilities and compliance standards.

(b) Verify that the Third Party has implemented adequate technical and organisational measures to protect Personal Data.

(c) Ensure the Third Party can demonstrate compliance with applicable data protection laws.

13.3. All Third Party data sharing arrangements shall be governed by written agreements that include:

(a) Clear specification of the categories of Personal Data to be shared and the purposes of Processing.

(b) Obligations requiring the Third Party to process Personal Data only in accordance with the Company's documented instructions.

(c) Confidentiality undertakings and restrictions on further disclosure without prior written consent.

(d) Implementation of appropriate security measures equivalent to those maintained by the Company.

(e) Procedures for handling Data Subject rights requests and notification of any Data Breach.

(f) Provisions for audit rights and compliance monitoring by the Company.

(g) Data retention and secure deletion requirements upon termination of the arrangement.

13.4. When engaging Data Processors, the Company shall ensure compliance with Article 28 of UK GDPR and execute formal data processing agreements containing all mandatory provisions.

13.5. For construction and consultancy projects involving multiple parties, the Company shall:

(a) Clearly define data sharing responsibilities and limitations in project agreements.

(b) Implement data sharing protocols that restrict access to Personal Data on a need-to-know basis.

(c) Ensure all project participants are bound by equivalent data protection obligations.

13.6. International data transfers to Third Parties shall comply with UK GDPR transfer mechanisms, including Standard Contractual Clauses where applicable.

13.7. The Company shall maintain records of all Third Party data sharing arrangements and regularly review their necessity and compliance status.

13.8. Any suspected or actual unauthorised disclosure of Personal Data by a Third Party shall be treated as a potential Data Breach and managed in accordance with the Company's breach response procedures.

14. Privacy by Design and Default

14.1. The Company shall implement data protection by design and by default in accordance with Article 25 of the UK GDPR, ensuring that appropriate technical and organisational measures are integrated into all data processing activities from the outset.

14.2. **Data Protection by Design Requirements**

(a) All new systems, processes, and services developed or procured by the Company shall incorporate data protection considerations from the initial design phase.

(b) The Company shall conduct privacy impact assessments during the planning stage of any new processing activities, system implementations, or business processes that involve Personal Data.

(c) Data minimisation principles shall be embedded into all system designs, ensuring that only Personal Data necessary for the specific purpose is collected and processed.

(d) Technical measures including pseudonymisation, encryption, access controls, and automated data deletion capabilities shall be built into systems where technically feasible and appropriate.

14.3. **Data Protection by Default Requirements**

(a) System default settings shall be configured to provide the highest level of data protection without requiring action from the Data Subject.

(b) Default configurations shall limit data collection to what is strictly necessary for the stated purpose and minimise data sharing with Third Parties.

(c) User interfaces shall be designed to present privacy-friendly options prominently and make data protection choices clear and accessible.

14.4. **System Development and Procurement**

(a) All software development projects shall include mandatory data protection requirements in project specifications and acceptance criteria.

(b) Third-party software and services shall be evaluated for privacy by design capabilities before procurement, with preference given to solutions that demonstrate strong built-in data protection features.

(c) Service level agreements with Data Processors shall include specific requirements for privacy by design implementation in their systems and processes.

14.5. **Documentation and Review**

(a) The Company shall maintain documentation demonstrating how privacy by design and default principles have been implemented in each system and process.

(b) Regular reviews shall be conducted to assess the effectiveness of privacy by design measures and identify opportunities for improvement.

(c) All Employees involved in system design, development, or procurement shall receive training on privacy by design principles and their practical application.

14.6. **Construction and Consultancy Specific Measures**

(a) Project management systems shall be configured by default to restrict access to project data based on the principle of least privilege and need-to-know basis.

(b) Client data sharing functionalities shall require explicit authorisation and shall not be enabled by default in collaboration platforms used for construction projects.

(c) Financial data processing systems shall incorporate automated data masking and role-based access controls as standard features.

15. Data Protection Impact Assessments

15.1. The Company shall conduct a **Data Protection Impact Assessment** before commencing any Processing operation that is likely to result in a high risk to the rights and freedoms of natural persons.

15.2. A DPIA shall be mandatory where the Processing involves:

(a) systematic and extensive evaluation of personal aspects relating to natural persons based on automated Processing;

(b) Processing of **Special Category Data** or personal data relating to criminal convictions on a large scale;

(c) systematic monitoring of publicly accessible areas on a large scale;

(d) new technologies that present high privacy risks;

(e) large-scale Processing of personal data in construction projects involving multiple **Third Parties**;

(f) automated decision-making systems affecting client project approvals or Employee performance evaluations.

15.3. Each DPIA shall contain:

(a) a systematic description of the envisaged Processing operations and the purposes of Processing;

(b) an assessment of the necessity and proportionality of the Processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of **Data Subjects**;

(d) the measures envisaged to address the risks and demonstrate compliance with the **UK GDPR**.

15.4. The **Data Controller** shall designate a responsible person to conduct each DPIA, who shall consult with relevant stakeholders including IT personnel, project managers, and affected departments.

15.5. Where a DPIA indicates that Processing would result in a high risk in the absence of measures to mitigate the risk, the Company shall consult the **ICO** prior to commencing Processing.

15.6. DPIAs shall be reviewed and updated:

(a) when there is a change in the risk represented by Processing operations;

(b) at least annually for ongoing high-risk Processing activities;

(c) when new technologies or Processing methods are implemented.

15.7. All completed DPIAs shall be documented, retained for the duration of the relevant Processing activity, and made available to the ICO upon request.

16. Monitoring and Compliance

16.1. The Company shall establish and maintain a comprehensive monitoring programme to ensure ongoing compliance with this Policy and applicable data protection laws.

16.2. The Company shall conduct regular internal audits of data protection practices at least annually, including:

(a) Review of data processing activities and their lawful bases;

(b) Assessment of technical and organisational security measures;

(c) Evaluation of data retention practices and disposal procedures;

(d) Review of Third Party data processing arrangements and contracts.

16.3. The Company shall maintain records of Processing activities in accordance with Article 30 of the UK GDPR, including:

(a) The purposes of Processing;

(b) Categories of Data Subjects and Personal Data;

(c) Recipients of Personal Data;

(d) Details of international transfers;

(e) Time limits for erasure of different categories of data.

16.4. The Company shall monitor compliance with data subject rights procedures, including response times, accuracy of responses, and resolution rates.

16.5. The Company shall establish key performance indicators for data protection compliance, including:

(a) Number and nature of data subject requests received and processed;

(b) Data Breach incidents and response times;

(c) Training completion rates among Employees;

(d) Results of security assessments and penetration testing.

16.6. The Company shall conduct quarterly compliance reviews with senior management to assess the effectiveness of data protection measures and identify areas for improvement.

16.7. All Employees, Contractors, and Third Parties shall be required to report suspected non-compliance or data protection concerns immediately to the designated data protection contact.

16.8. The Company shall maintain documentation evidencing compliance efforts, including audit reports, training records, incident logs, and corrective action plans.

16.9. Non-compliance with this Policy may result in disciplinary action in accordance with the Company's employment policies and procedures.

16.10. The Company shall engage external auditors or consultants as necessary to conduct independent assessments of data protection compliance.

17. Budget and Resource Allocation

17.1. The Company shall allocate an annual budget of £10,000 for data protection compliance activities, software solutions, and security measures necessary to maintain adherence to UK GDPR requirements.

17.2. The allocated budget shall cover the following data protection expenditure:

(a) Data protection software licensing and subscription fees for security tools, encryption solutions, and compliance management systems.

(b) Technical security measures including data loss prevention software, access control systems, and monitoring tools.

(c) Professional services for Data Protection Impact Assessments, compliance audits, and legal consultancy relating to data protection matters.

(d) Staff training programmes, certification courses, and awareness materials for data protection education.

(e) Hardware and infrastructure costs relating to secure data storage, backup systems, and physical security measures.

17.3. The Directors shall approve the annual data protection budget as part of the Company's overall financial planning process.

17.4. Budget expenditure exceeding the allocated amount requires prior written approval from the board of Directors.

17.5. The designated Data Protection Officer or senior management representative shall maintain records of all data protection-related expenditure and provide quarterly budget reports to the Directors.

17.6. The Company shall review and adjust the data protection budget annually to ensure adequate resources are available to meet evolving compliance requirements and business growth.

17.7. Emergency expenditure for data breach response, regulatory investigations, or urgent security measures may be authorised by any Director without prior budget approval, subject to immediate notification to the board.

18. Policy Review and Updates

18.1. The Company shall conduct a comprehensive review of this Policy at least annually to ensure its continued effectiveness and compliance with applicable data protection laws.

18.2. The Policy shall be reviewed and updated immediately upon any of the following circumstances:

(a) changes to UK GDPR, Data Protection Act 2018, or other applicable data protection legislation;

(b) guidance issued by the ICO that affects the Company's data processing activities;

(c) material changes to the Company's business operations, data processing activities, or organisational structure;

(d) identification of compliance gaps through internal audits, data protection impact assessments, or breach investigations;

(e) changes in technology systems or data security measures that affect data processing procedures.

18.3. The Data Protection Officer shall be responsible for coordinating policy reviews and shall prepare a written assessment identifying any necessary updates or amendments.

18.4. All proposed amendments to this Policy must be approved by the Board of Directors before implementation.

18.5. Upon approval of any updates, the Company shall:

(a) implement a new version control system identifying the revision date and version number;

(b) communicate changes to all Employees, Contractors, and relevant Third Parties within 30 days of approval;

(c) provide additional training where updates materially affect data handling procedures;

(d) update all related documentation, procedures, and training materials to reflect the changes.

18.6. The Company shall maintain records of all policy reviews, including the date of review, personnel involved, findings, and any resulting amendments.

18.7. Emergency updates may be implemented immediately without the full review process where required for regulatory compliance, provided that formal approval is obtained within 14 days of implementation.

19. Contact Information

19.1. The Company's Data Protection Officer can be contacted regarding any data protection matters at:

(a) Email: dpo@n-3.co.uk

(b) Post: Data Protection Officer, N3 Technologies Limited, Seymour House 15a Frederick Road, Edgbaston, Birmingham, England, B15 1JD

(c) Telephone: 0121 262 3450 during normal business hours (9:00 AM to 5:00 PM, Monday to Friday, excluding public holidays)

19.2. For general data protection inquiries, data subject rights requests, or complaints, individuals may contact:

(a) Email: support@n-3.co.uk

(b) Post: Data Protection Team, N3 Technologies Limited, Seymour House 15a Frederick Road, Edgbaston, Birmingham, England, B15 1JD

19.3. The Company will acknowledge receipt of all data protection inquiries within **2 business days** and provide a substantive response within the timeframes specified in this Policy.

19.4. Individuals have the right to lodge a complaint with the Information Commissioner's Office (ICO) if they are dissatisfied with the Company's handling of their personal data:

(a) ICO Website: www.ico.org.uk

(b) ICO Helpline: 0303 123 1113

(c) ICO Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

19.5. The Company's ICO registration number is [Registration Number] and current registration details can be verified on the ICO's public register.

19.6. This contact information will be reviewed annually and updated as necessary to ensure accuracy and accessibility. This Policy has been approved and authorised by the undersigned on behalf of N3 Technologies Limited and shall come into effect on 1st January 2025.

20. PUBLIC PRIVACY NOTICE

20.1. This Privacy Notice explains how N3 Technologies Limited collects, uses, and protects your personal information when you visit our website, use our services, or interact with our company.

20.2. **Who We Are**

(a) N3 Technologies Limited is a software as a service company serving clients in construction, consultancy, and development finance sectors. We are registered in England and Wales (company number 14501106) with our registered office at Seymour House 15a Frederick Road, Edgbaston, Birmingham, England, B15 1JD.

(b) We act as a data controller for the personal information we collect about you. This means we determine how and why your personal data is processed.

20.3. **What Personal Information We Collect**

(a) We may collect and process the following personal information about you:

(i) **Contact Information**: Name, email address, phone number, and postal address when you contact us or request our services.

(ii) **Business Information**: Company name, job title, and professional details relevant to our construction and consultancy services.

(iii) **Project Information**: Details about construction projects, consultancy requirements, or development finance needs that you share with us.

(iv) **Website Data**: Information about your visits to our website, including IP address, browser type, pages viewed, and time spent on our site.

(v) **Communication Records**: Copies of correspondence and notes from meetings or phone calls with our team.

20.4. **How We Use Your Personal Information**

(a) We use your personal information for the following purposes:

(i) **Providing Services**: To deliver our software solutions and professional services in construction, consultancy, and development finance.

(ii) **Communication**: To respond to your enquiries, provide updates about our services, and maintain business relationships.

(iii) **Business Development**: To understand your needs and develop our services to better serve the construction and consultancy sectors.

(iv) **Legal Compliance**: To comply with our legal and regulatory obligations in the industries we serve.

20.5. **Legal Basis for Processing**

(a) We process your personal information based on the following legal grounds:

(i) **Contract Performance**: When processing is necessary to provide services you have requested or to take steps before entering into a contract.

(ii) **Legitimate Interests**: For business development, improving our services, and maintaining client relationships, balanced against your privacy rights.

(iii) **Legal Obligation**: When we need to comply with applicable laws and regulations.

(iv) **Consent**: Where we have obtained your explicit consent, which you can withdraw at any time.

20.6. **Who We Share Your Information With**

(a) We may share your personal information with:

(i) **Service Providers**: Third-party companies that help us deliver our services, such as IT support, hosting providers, and professional advisors.

(ii) **Project Partners**: Other professionals involved in construction or consultancy projects, where necessary for project delivery.

(iii) **Legal Authorities**: When required by law or to protect our rights and interests.

(b) We ensure all third parties are contractually bound to protect your personal information and use it only for the purposes we specify.

(c) **International Transfers**

(i) Your personal information may be transferred outside the UK where our service providers are located internationally. We ensure appropriate safeguards are in place, including Standard Contractual Clauses and adequacy decisions, to protect your information.

(d) **How Long We Keep Your Information**

(i) We retain your personal information only for as long as necessary for the purposes outlined above:

(A) **Client Information**: Up to 7 years after the end of our business relationship.

(B) **Marketing Information**: Up to 3 years from last contact, unless you opt out earlier.

(C) **Website Data**: Typically 12-24 months, depending on the type of data collected.

(e) **Your Rights**

(i) Under UK data protection law, you have the following rights:

(A) **Access**: Request a copy of the personal information we hold about you.

(B) **Rectification**: Ask us to correct any inaccurate or incomplete information.

(C) **Erasure**: Request deletion of your personal information in certain circumstances.

(D) **Restriction**: Ask us to limit how we use your information in certain situations.

(E) **Portability**: Receive your information in a portable format where technically feasible.

(F) **Object**: Opt out of processing based on legitimate interests or for marketing purposes.

(ii) To exercise any of these rights, please contact us using the details in the Contact section below.

(iii) **Cookies and Website Technology**

(A) Our website uses cookies and similar technologies to enhance your browsing experience and analyse website performance. You can control cookie settings through your browser preferences. Essential cookies necessary for website functionality cannot be disabled.

(iv) **Data Security**

(A) We implement appropriate technical and organisational measures to protect your personal information, including encryption, access controls, and regular security assessments. However, no internet transmission is completely secure, and we cannot guarantee absolute security.

(v) **Contact Us**

(A) If you have any questions about this Privacy Notice or wish to exercise your rights, please contact us:

(B) **Email**: support@n-3.co.uk

(C) **Post**: Data Protection Team, N3 Technologies Limited, Seymour House 15a Frederick Road, Edgbaston, Birmingham, England, B15 1JD

(D) **Phone**: 0121 262 3450

(f) **Complaints**

(i) If you are unhappy with how we handle your personal information, you have the right to complain to the Information Commissioner's Office (ICO):

(A) **Website**: www.ico.org.uk

(B) **Phone**: 0303 123 1113

(C) **Address**: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

(g) **Updates to This Notice**

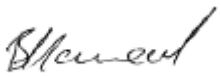
(i) We may update this Privacy Notice from time to time to reflect changes in our practices or applicable laws. The current version will always be available on our website with the date of last update clearly displayed.

(h) **Last Updated**: 1st January 2025

Company Director:

Name: Benjamin Harwood

Position: Chief Executive Officer



Signature:

Date: 1st January 2025

Data Protection Officer:

Name: Gareth Parker

Position: Data Protection Officer

Signature: 

Date: 1st January 2025

This Policy shall be binding upon all employees, contractors, consultants, third-party service providers, and data processors engaged by the Company from the effective date specified above.