Data Protection Policy 0.9
21st May 2018

Policy information	
Organisation	**Quintadena Ltd** 412W Bizhub Castle Mill Dudley DY4 7UF Registered in England No. 5444953 Registered Office 97 Mushroom Green Dudley DY2 0EE
Scope of policy	Aspire Technologies Inc of Orlando, Florida, USA, ITMicroscope Ltd of Braintree, Essex and B C Stockford (Chartered Accountants) of Dudley, West Midlands act as Data Processors under certain circumstances. Peninsula Business Services of Manchester, UK are processors of our HR / Employment / Salary personal data for Directors and Staff.
Policy operational date	25th May 2018.
Policy prepared by	M. O. Checkley Data Protection Officer **Quintadena Ltd** 412W Bizhub Castle Mill Dudley DY4 7UF.
Date approved by Board/ Management Committee	
Policy review date	24th May 2021

Introduction	
Purpose of policy	The purpose of this policy is to:- • comply with the law • follow good practice • protect clients, staff and other individuals • protect **Quintadena Ltd.**
Types of data	Quintadena holds personal data (but not *sensitive* personal data) relating to prospects, customers and suppliers. The data consists of people's names, business email addresses and business telephone numbers and business addresses. This data is processed for the following purposes:- 1. Providing quotations and invoices for new and repeat business. 2. Placing orders with suppliers. 3. Sales Order Processing. 4. Project Management and Project fulfilment. 5. Discussing and resolving technical issues submitted by customers. 6. Notifying prospects and customers of technical developments. 7. Notifying prospects and customers of new products which appear relevant to their established business need. 8. Notifying prospects, customers and suppliers of changes to Quintadena business processes and / or Terms and Conditions of trading, as relevant and appropriate. Quintadena holds personal data (which may, on occasion, be *sensitive* personal data) relating to its own Directors and Staff. This includes names, personal addresses, personal telephone numbers, salary details, bank account details, NI numbers and all data necessary for the purposes of employment. This may, on occasion, include data relating to physical and / or mental health, and disciplinary data.
Policy statement	**Quintadena Ltd** is committed to:- • comply with both the law and good practice • respect individuals' rights • be open and honest with individuals whose data is held • provide training and support for staff who handle personal data, so that they can act confidently and consistently. • Notify the Information Commissioner of any Data Breach or suspected Data Breach when this is required by Law. • Notify the Information Commissioner of any Data Breach or suspected Data Breach voluntarily, even if this is not required by Law, other than in circumstances where the Board of Directors has determined that such would not be appropriate and

	recorded a board minute to that effect, stating the reason(s). • Quintadena is not obliged, due to the nature of our data processing, to register with the ICO as a Data Controller, nor to appoint a Data Protection Officer; see the below output from the ICO online assessment tool:- *"You are under no requirement to register. You are only processing personal data for the core business purposes. You therefore do not have to register with the ICO." ……. "You can still register voluntarily if you wish."* • The above notwithstanding, Quintadena has *registered voluntarily* with the ICO and will endeavour to adhere to the principles of GDPR as being generally good business practice.
Key risks	The key areas of risk of Data Breach are as follows:- 1. Breach of prospects / customers / suppliers electronically held personal data due to a "bad faith" action by a Director or Member of Staff. 2. Data Breach for reasons of malware / hacking / ransomware / malware regarding on-site systems. 3. Data Breach for reasons of malware / hacking / ransomware / malware regarding Cloud systems. 4. Breach of the above data by inappropriate forwarding or CCing of emails. 5. Breach of (possibly *sensitive*) personal data concerning individual Directors and Staff, resulting in potential reputational or other damage to the individual by the making available of data which might be adversely interpreted (e.g. someone's sickness record) by an outside party. 6. *Internal* breach of the above data by colleagues who are aware of other colleagues' personal data because of personal contact / friendship outside the work environment, disclosing that data to third-party colleagues in casual conversation without realising that they require the permission of the Data Subject.

Responsibilities	
The Board / Company Directors	R J Edwards. P W Hodgetts. M O Checkley. They have overall responsibility for ensuring that the organisation complies with its legal obligations.
Data Protection Officer	The Data Protection Officer is M. O. Checkley (Director of Marketing and Development). He is responsible for:- • Briefing the Board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Delivering Data Protection training as scheduled by department heads / team leaders. • Notification to the ICO • Handling subject access requests. • Handling subject erasure requests. • Ensuring any unusual or controversial disclosures of personal data are brought before the Board. • Ensuring contracts with Data Processors are brought before the Board.
Specific Department Heads	Mr. P. W. Hodgetts (in his capacity as Technical Director). Mrs. P. A. Hodgetts (in her capacity as Financial Controller). Mr. R. J. Edwards (in his capacity as HR Director). Mrs. V. M. Wilby (in her capacity as Delivery Manager / Support Desk Manager).
Employees & Volunteers	All directors and staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.
Enforcement	Any infringement of the Data Policy will be handled through the formal disciplinary procedure which, if repeated and / or sufficiently serious, would have the potential to result in dismissal.

Security	
Scope	Data Security is not wholly a Data Protection issue. Business Continuity is included below but you may want to move this to a separate policy
Setting security levels	The consequences of a breach of confidentiality where the data subject is an "outside" person, such as a customer, are relatively light and for the overwhelming most part purely commercial. Quintadena Ltd does not hold the private contact details of its customers and suppliers, except in those cases where it is dealing with micro-businesses where people are working from home. There are essentially two levels of confidentiality within Quintadena Ltd. 1. Directors and Managers have access to all parts of all systems. 2. Other staff are restricted from viewing / printing Management reports which would include personal data. 3. All employees are contractually obligated to observe appropriate confidentiality. 4. Data, whether in hard copy or electronic form, may not be taken off-site without the permission of a Director. The consequences of a breach of confidentiality regarding the personal data of Directors and Members of Staff have the potential to be more damaging. The data held includes medical data, financial data, disciplinary data, and can include data relating to marital status and family membership. Because of the potentially sensitive nature of this data it is not held on-site at the trading address, but is held in hard-copy at the Company Registered Office and only available to the Managing Director and / or Financial Controller. Others requiring access to the data due to "need-to-know" must obtain it from that source.
Security measures	For each confidentiality level it may be worth setting out the security measures to be followed, such as password protection, clear desk policy, entry control This section should include your technical and organisational security measures **PH / SJ to provide this.**
Business continuity	This would include backup procedures (both for data and for key employee availability) and emergency planning. As noted above, it may be worth a separate policy. **PH / SJ to provide this.**

Specific risks	In this section the numbers referenced are those from the "Key Risks" section above. 1. This risk is mitigated (but can never be wholly eliminated) by restricting access to that which is necessary for the carrying out of each individual's job function. The Risk of Harm to individuals outside the organisation in the event of Data Breach is minimal-to-zero because the data in question is exclusively business related and does not include private addresses / contact details. The Risk of Harm lies primarily on Quintadena Ltd, associated with the possibility of such data falling into the hands of competitors, resulting in damage to the commercial interests of Quintadena Ltd. **2. Mitigation of this risk is in the hands of The Technical Director and the Network Administrator, PH / SJ.** **3. Mitigation of this risk is in the hands of The Technical Director and the Network Administrator, PH / SJ.** 4. This risk can only be mitigated by Training. 5. This risk is mitigated by the data being held in hard copy off-site at the Company Registered Office Address, in the custody of the Company Secretary who discloses it only on a need-to-know basis. 6. This risk can only be mitigated by Training.

Data recording and storage	
Accuracy	1. Data provided directly from the data subject is checked with the data subject at time of recording. 2. Data provided by a referring agency is checked with the data subject at time of first contact.
Updating	1. CV's submitted for employment purposes are not retained after the selection process is complete, unless an unsuccessful applicant expresses a wish to be "kept on file". 2. Customer / Prospect / Supplier data is updates as and when new data is provided by the data subject.
Storage	1. Personal / potentially *sensitive* personal data regarding employees and staff is held in hard copy off-site at the Company Registered Office. 2. Customer / Supplier / Prospect
Retention periods	Data is retained indefinitely, other than on receipt of a Subject Erasure Request.
Archiving	Hard-copy data is shredded once it has served its purpose. Electronic data is **PH / SJ to provide this.**

Right of Access	
Responsibility	The responsibility for identifying a subject access / erasure / rectification etc. request rests with the Member of Staff receiving the request, and traini9ng has been delivered (9 5 2018) to facilitate this. The responsibility for ensuring that the request is addressed (including, where appropriate, declined) rests with the Data Protection Officer.
Procedure for making request	Right of access requests must be in writing. There is a clear responsibility on all employees to pass on anything which might be a subject access request to the appropriate person without delay, and appropriate training has been delivered (9 5 2018) to facilitate this.
Provision for verifying identity	Where the person managing the access procedure does not know the individual personally their identity will be appropriately verified before handing over any information. The standard of identification required will be determined by the level of potential harm that could be occasioned by inappropriate release of data. In the event that *sensitive* personal data is to be made available under a subject access request, rigorous standards of identification will be imposed.
Charging	Quintadena will provide information free of charge other than if a request is manifestly unfounded or excessive, particularly if it is repetitive. Quintadena will charge a reasonable fee to comply with requests for further copies of the same information. (But not for all subsequent access requests.) The fee will be based on the administrative cost of providing the information
Procedure for granting access	If the request is made electronically, Quintadena will provide the information in a commonly used electronic format. It will not be appropriate for Quintadena to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information.

Transparency	
Commitment	Quintadena Ltd is fully committed to ensuring that Data Subjects are aware that their data is being processed and • for what purpose it is being processed • what types of disclosure are likely, and • how to exercise their rights in relation to the data
Procedure	Data Subjects will be informed through appropriate channels, for example:- 1. The Company Handbook. 2. The welcome letter or pack for clients. 3. The Company website
Responsibility	Mr. M. O. Checkley is responsible for transparency of customer, prospect and supplier personal data. Mr. R. J. Edwards is responsible for transparency of Directors / Staff sensitive personal data.

Lawful Basis	
Underlying principles	The lawful base for the processing of data is a combination of "legitimate interest" and "consent". When we receive enquiries and requests for quotations from people who are interested in our goods and services, *consent* to process the data to the extend necessary to respond to those enquiries is implicit in the enquiry. When we become aware of "new information" relative to an enquiry we have received (e.g. technical software advances, new products directly relevant to the business need) we have a *legitimate interest* in communicating such matters to our external data subjects, and they have a *legitimate interest* to receive it. With the singular exception of the necessary processing of internal personal data in order to manage (and pay) our Staff those are the only purposes for which data is processed.
Opting out	Our documentation advises data subjects of their right to erasure and their right to restrict processing, which rights are inherent in our business processes.
Withdrawing consent	Quintadena Ltd acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where Quintadena Ltd has no choice other than to retain data for a certain length of time, even though consent for using it has been withdrawn.

Employee training & Acceptance of responsibilities	
Induction	All employees who have access to any kind of personal data have their responsibilities outlined during their induction procedures.
Continuing training	Opportunities to raise Data Protection issues are available during employee GDPR training and PPD appraisal meetings with line management.
Procedure for staff signifying acceptance of policy	Employees show acceptance of their responsibilities to Data Protection by their accession to the contents of the Company Handbook etc., which forms part of their Contract of Employment.

Policy review	
Responsibility	Mr. R. J. Edwards (Chairman) will instigate the next policy review by including it on the agenda of the Board of Directors.
Procedure	Mr. P. W. Hodgetts, Mrs. P. A. Hodgetts, Mr. S. J. Jeffs and Mrs. V. M. Wilby will be specifically consulted. All Members of staff will be advised that there is to be a review, and provided with the opportunity to input their suggestions.
Timing	The review will commence January 2021, unless circumstances dictate that it is appropriate to review sooner.