AutoRefs

Data Processing Agreement

Data Processing Agreement - To the extent International data protection laws apply to the processing of personal data between AutoRefs and Customer, the default **Data Processing Agreement (“DPA”)** and the **Master Services Level Agreement** found at AutoRefs are incorporated by reference and form a part of these Terms of Service, unless expressly provided otherwise in writing by both parties.

Company Registration: 10937843
VAT Registration: GB388644344
Registered Address: Moss Bridge House,
Moss Bridge Road, Rochdale, OL16 5EA
United Kingdom

19 07 22

AGREEMENT ON THE PROCESSING OF PERSONAL DATA
IN ACCORDANCE WITH ARTICLE 28 OF THE
UK GENERAL DATA PROTECTION REGULATION (UK GDPR)
- DATA PROCESSING AGREEMENT -

Preamble

This Data Processing Agreement ("DPA") forms a part of the Customer Terms of Service found at https://www.autorefs.com/website-terms-of-use or other written agreement between Creative Marketing (NW) Ltd T/A AutoRefs. and Customer for the purchase and/or use of AutoRefs, Inc.'s and/or its Affiliates (collectively, "AutoRefs") products and/or services (the "Agreement"), and reflects the parties mutual understanding and agreement related to the Processing of Customer's Personal Data (as defined herein) by PandaDoc on behalf of Customer.

If and to the extent that the Processor collects, processes or otherwise uses personal data in the context of performing the services, the provisions of this Data Processing Agreement (hereinafter also "DPA") shall apply. If and to the extent that the provisions of this Data Processing Agreement deviate from the provisions of the Main Agreement, this Data Processing Agreement shall prevail.

1. Subject matter and duration of the Data Processing Agreement

(1) Subject matter

The Processor provides the following services:

- Automated Reference Checking
- Cloud storage of reference reports
- Bulk reference checking

(2) Duration

This Data Processing Agreement is authorised for an unlimited period and can be terminated by either Party with a notice period of 30 Days.

(3) Termination

The Controller may terminate this Data Processing Agreement at any time without notice, if the Processor is in violation of applicable data protection law or violates the terms of this Data

Processing Agreement. In order to be legally effective, the termination shall be declared in writing within the meaning of respective applicable national laws. The parties are aware that any (further) processing of personal data may not be accomplished without a valid Data Processing Agreement.

2. Details of the data processing

(1) Nature of the data processing by virtue of this Data Processing Agreement personal data will be;

- collected (=creating of data about the data subject)
- recorded (=writing down / registering of collected data)
- organised / arranged (=structuring of data)
- stored (=preserving of data, in particular on data carriers)
- adapted / altered (=adjusting/amending the information content)
- retrieved (… from an existing data set)
- consulted (… from an external data base)
- used (=purposively used)
- disclosed (=transfer or making available to third parties)
- synchronised (… making several data systems consistent)
- combined / linked (=matching several data systems)
- restricted (=prevent further processing)
- erased (… of data on electronic data carriers)
- destroyed (= deleted of the physical data carrier)

by the Processor.

(2) Purpose of processing

- Provision of the automated reference checking service in order to obtain a reference from an applicant.

(3) Place of Processing

The contractually agreed services shall be carried out exclusively within the United Kingdom (UK). Any relocation of the services or parts thereof to a third country requires the prior written consent of the Controller and shall only take place if the specific conditions of Art. 44 et seq. UK GDPR are met.

(4) Types of Data;

Applicant Personal & Employment Data;
Applicant Name
Applicant Email
Applicant Phone

Applicant Designation
Applicant Message
Referee Name
Referee Company
Referee Address
Referee Number
Referee's reference
Applicant Employment Dates
Referee Employment Number
Relationship to Applicant
Questions asked by Employer

(5) Special categories of data

Not Applicable

(5) Categories of data subjects

- **Employers Representatives**
- **Applicants**
- **Referees**
- **Data Controllers Staff**

3. Responsibility and right of the Controller to issue instructions

(1) Personal data transferred by the Controller or collected on behalf of the Controller ("Controller Data") shall only be processed by the Processor in accordance with the concluded agreements and the documented instructions by the Controller. Any processing or use of Controller Data deviating or exceeding the definitions in this Data Processing Agreement or the documented instructions by the Controller is not allowed; this shall especially apply to the processing of Controller Data for own purposes of the Processor or purposes of third parties. This shall also apply to the use of anonymised data.

(2) In deviation of the preceding para. 3.1, a different processing of Controller Data by the Processor is only possible to the extent that the Processor is obliged thereto by applicable UK-law (Art. 28(3)(a), Art. 29, Art. 32(4) UK GDPR). In case of such an obligation, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(3) Instructions by the Controller shall be regularly made in writing or in text form (e-mail). When necessary, the Controller may render instructions also orally. Instructions made orally shall be confirmed by the authorised person within the meaning of para. 4 below in writing or in text form (e-mail) without undue delay. The Processor is obliged to document all instructions by the Controller. Modifications of the subject matter of the processing or its procedure shall be mutually coordinated by the Parties and shall be documented in writing.

(4) The Processor shall procure that the processing is accomplished in accordance with the provisions of this Data Processing Agreement and the instructions by the Controller. The Processor shall immediately inform the Controller if, in its opinion, an instruction by the Controller infringes data protection provisions. The Processor may suspend implementing the respective instructions until they are confirmed or modified by the Authorised Person of the Controller. When the respective instruction is confirmed by the Controller, the Processor shall comply therewith. In all other cases, the Processor shall carry out the instructions by the Controller without undue delay.

(5) The Parties agree that the Controller shall be solely responsible for the processing in accordance with the instructions given in context with this Data Processing Agreement.

2. Authorised persons

(1) Instructions shall be regularly given by the authorised person of the Controller and received by the person authorised for receipt on behalf of the Processor. However, in urgent cases the Controller may render instructions by virtue of this Data Processing Agreement to each employee of the

Processor if the authorised person is not available. The following persons are authorised to issue instructions on behalf of the Controller and, respectively to receive instructions on behalf of the Processor:

Authorised person on behalf of the Controller:

Owen Cannon
HR Information & Systems Manager
+44 (0) 77 6936 7252
owen.cannon@glhhotels.com

Authorised person on behalf of the Processor:

Kasim Javed
Director
kasim@creativemarketingltd.co.uk
01706 318200

(2) Any change in the authorised persons or their competence shall be communicated to the other party without undue delay in writing or in text form (e-mail).

3. Obligations of the Processor

(1) The Processor shall produce no copies or duplicates of the Controller Data or disclose such copies or duplicates to third parties without the Controller's prior written consent. This does not apply to backup or security copies that are required to ensure the proper processing of the data, or to any data required to comply with mandatory statutory retention periods.

(2) The Processor shall ensure that any personnel entrusted with the processing of personal data have been instructed on all the provisions provided by the UK GDPR and all other data protection requirements relevant for their work and have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(3) Without prejudice to any existing contractual arrangement between the parties, the Processor shall treat all personal data as confidential and shall inform its employees, agents and/or approved sub-processors engaged in processing the personal data of the confidential nature of personal data. The Processor shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

(4) The Processor shall assist the Controller in complying with its obligations concerning the notification of data breaches vis-à-vis the competent supervisory authorities. In particular, the Processor shall provide the Controller with any information necessary for the Controller to comply with his notification duties under Art. 33 et seq. UK GDPR. The notification shall contain a description of:

a. the nature of the breach of Controller Data, indicating, as far as possible, the categories and the approximate number of affected Data Subjects, the categories and the approximate number of affected Controller Data sets;

b. the likely consequences of the personal data breach;

c. the measures taken or proposed by the Party at whom the personal data breach occurred to remedy the breach of Controller Data and, where appropriate, measures to mitigate their potential adverse effects.

(5) Upon request, the Processor shall provide the Controller with all information reasonably necessary to comply with his obligation to accomplish a data protection impact assessment under Art. 35 and 36 UK GDPR and – if applicable – supporting the Controller with regard to prior consultations of the supervisory authority.

(6) In addition, the Processor shall assist the Controller pursuant to Art. 28(3)(f) UK GDPR with complying to the obligations provided in Art. 32 UK GDPR taking into account the nature of processing and the information available to the Processor.

4. Confidentiality

(1) Each party must keep this Data Processing Agreement and any information it receives about the other party and its business in connection with this Data Processing Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other party except to the extent that:
(a) the relevant information is or becomes a part of the public domain through no act or omission of the receiving Party;
(b) was in n the receiving Party's lawful possession without confidentiality obligation prior to the disclosure and had not been obtained by the receiving Party either directly or indirectly from the disclosing Party; or (c) is lawfully disclosed to the receiving Party by a third party without restriction on disclosure; or
(d) is independently developed by the receiving Party by employees or agents without access to the disclosing Party's Confidential Information (e) is required to be disclosed by the receiving Party as a matter of law or by order of a competent court or by a competent regulatory body, provided that the receiving Party promptly notifies the disclosing Party (where lawfully permitted to do so) so that disclosing Party may intervene.

5. Notification and information requirements

(1) The Processor shall notify the Controller without undue delay in the event of a serious disruption of the data processing operations, suspected data protection violations and other irregularities in connection with the processing of Controller Data.

(2) Where required by applicable law, the Processor shall appoint a reliable expert as data protection officer. The Processor shall provide the Controller with the contact details of the data protection officer. If the Processor is located outside the UK, he shall appoint a representative pursuant to Art. 27 UK GDPR and shall provide the Controller with the respective contact details.

Contact details of the data protection officer:

DataCo International UK Limited
C/O One Peak Limited 2nd Floor
41 Great Pulteney Street
London
W1F 9NZ
Telephone: +442035146557

Email: privacy@dataguard.co.uk

The Processor shall inform the Controller immediately in the event of any change in the person of the data protection officer or the representative in the UK.

(3) The Processor shall inform the Controller immediately in the event of an inspection or any other regulatory activity by a supervisory authority, insofar related to this Data Processing Agreement. The Processor is obliged to inform the Controller about the results of such inspection in relation to this Commissioned Data Processing. The Processor shall correct any noncompliance as outlined in the inspection report without undue delay. Apart from that, the Controller and the Processor and, where applicable, their representatives shall cooperate, on request, with the supervisory authority in the performance of its tasks (Art. 31 UK GDPR).

(4) Insofar as the Controller for his part is subject to an inspection by a supervisory authority, administrative or criminal offence proceeding, liability claims by data subjects or third parties or any other claim in relation to the Commissioned Data Processing rendered by the Processor, the Processor shall assist the Controller to the best of his ability.

(5) The Processor shall inform the Controller immediately if Controller Data becomes subject to seizure or confiscation, insolvency or settlement proceedings or any other event or measures of third parties. The Processor shall notify all pertinent parties to such action that the sovereignty of the personal data lies with the Controller.

6. Employment of further Processors (Subcontractors)

(1) Subcontractors may only be instructed with the Controller’s prior written authorisation. This also applies to the change of existing subcontractors. The following provisions shall apply to subcontractors as well as (by way of analogy) to all further instructed (sub-) subcontractors. Subcontractors are to be selected with due diligence and taking particular account of the appropriateness of the specific technical and organisational measures implemented by the respective subcontractor. Upon request, the relevant documents shall be made available to the Controller. Controller Data may only be forwarded to the subcontractor and the subcontractor may only begin processing if all requirements have been fulfilled. The Processor shall remain responsible vis-à-vis the Controller for compliance with this Data Processing Agreement and the applicable data protection law by the subcontractor.

(2) Subcontractors in third countries outside the UK may only be instructed if the specific requirements under Art. 44 et seq. UK GDPR are fulfilled. The parties agree that only the Controller is authorised to enter into contracts within the meaning of Art. 46(2)(c) or (d) and Art. 46 (3)(a) UK GDPR with subcontractors in third countries and that the Processor has no proxy or authority to do so on his own. Subject to the condition that the Processor ensures that the subcontractor complies with his duties as data-importer under the relevant contract, the Processor already undertakes to enter into a contract in accordance with the preceding rules [including a contract based on the standard data protection clauses for the transfer of personal data to processors in third countries as provided by the EU Commission in its resolution as of February 5, 2010 (“Standard Data Protection Clauses” – “SCC”) between the Controller and the subcontractor located in a third country.

(3) Assessment. Processor shall prior to transferring personal data to third countries or processing personal Data in such third countries, provide the Controller with a written assessment conducted by Processor and, where appropriate, in collaboration with the data importer in the third country of destination according the SCC, on a case-by-case basis, whether the law of the third country of destination ensures adequate protection with European data protection law (GDPR) of personal data transferred pursuant to the SCC, by providing, where necessary, additional safeguards to those offered by those SCC.

(4) The assessment of the third country, or of a territory or specified sector within a third country, shall take into account

a. how the particular third country respects the rule of law, access to justice as well as international human rights norms and standards and its general and sectoral law, including legislation concerning public security, defence and national security as well as public order and criminal law, and

b. if and to which extent the Processor and/or Data Importer and/or Sub-processor in the third country of destination and the processing of Personal Data, are subject to surveillance and disclosure laws and/or regulations (including, but not limited to Section 702 of the Foreign Intelligence Surveillance Act (FISA), the United States Foreign Intelligence Surveillance Court (FISC), US Executive Order 12333, Presidential Policy Directive 28 (“PPD-28”))", and
c. if Data Subjects concerned by the processing are provided with effective and enforceable rights and effective administrative and judicial redress.

(3) Subcontracts shall be in writing and shall impose the same obligations on the subcontractor as they are imposed on the Processor under this Data Processing Agreement. In particular and upon request, the Controller shall be entitled to reasonably inspect (including on site) the subcontractor or to have the subcontractor inspected by mandated third parties (contract for the benefit of third parties). The areas of responsibility of the Processor and the subcontractor shall be clearly separated from each other in the respective agreement between the Processor and the subcontractor. Upon request, the Controller shall be entitled to be informed about the content of the agreement and the implementation of the data protection relevant duties in the subcontractor relationship by inspecting the relevant contractual documents.

(4) The Processor shall monitor compliance of the duties of the subcontractor prior to subcontracting and periodically thereafter, however, at least once per year. The result of such review shall be documented and be made available to the Controller upon request.

(5) Subcontracting means services directly relating to the main performance. However, services which the Processor uses as mere secondary service at third parties for his business activities, shall not qualify as subcontracting. This includes, inter alia, cleaning services, mere communication services without a concrete reference to the main services rendered by the Processor on behalf of the Controller, postal and courier services, transportation and surveillance services. Nevertheless, the Processor shall, with regard to such secondary services by third parties, be obliged to ensure implementation of adequate precautions and technical and organisational measures safeguarding the protection of personal data. Maintenance and support of IT-systems or applications qualify as subcontracting subject to approval and as Commissioned Data Processing within the meaning of Art. 28 UK GDPR, if the maintenance and support concerns (i) systems also used in context with the services rendered on behalf of the Controller and (ii) allows access to personal data processed on behalf of the Controller.

(6) Currently approved subcontractors are listed in Appendix 2.

(7) The outsourcing by the subcontractor to further subcontractors is subject to the explicit prior consent of the Controller (at least in text-form); all contractual provisions in the chain of contract shall be imposed to the further contractors.

7. Technical and organisational security measures

(1) The Processor shall implement adequate technical and organisational measures for the protection of Controller Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed and maintains these measures for the duration of the Commissioned Data Processing.

(2) The measures shall guarantee a protection level appropriate to the risk concerning the confidentiality, integrity, availability and resilience of the processing systems. In choosing the measures, the Processor shall take into account the state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons. As a minimum, the Processor shall implement the technical and organisational measures as documented in Appendix 1 prior to the commencement of processing Controller Data and ensure compliance of such processing with the measures undertaken.

(3) Prior to the commencement of processing, the Processor shall document the technical and organisational measures, and shall present the relevant documentation to the Controller for inspection. Upon acceptance by the Controller, the documented measures become the foundation of this Data Processing Agreement. Insofar as the inspection by the Controller shows the need for amendments, such amendments shall be implemented by mutual agreement.

(4) Technical and organisational measures are subject to technological progress and further development. To this end, the Processor may further develop and adjust the existing measures to the state of the art, provided that such amendments do not fall short of the protection level of the measures defined in this Data Processing Agreement. Substantial changes must be agreed upon in writing by the parties.

(5) The Processor shall periodically monitor and control its internal processes and its technical and organisational measures to ensure adequate protection of the rights and freedoms of data subjects and ongoing compliance with applicable data protection requirements and the provisions of this Data Processing Agreement.

(6) Upon Controller’s request, the Processor shall demonstrate compliance with the technical and organisational measures defined in Appendix 1. The proof thereof can be produced by the submission of a current certificate or a report of an independent party (e.g. by auditors, revisors, internal or external data protection officers) or by a suitable certification. The inspections rights by Controller pursuant to para. 9 of this Data Processing Agreement shall remain unaffected.

8. Inspection Rights

(1) Prior to the start of the processing activities and regularly thereafter, the Controller shall have the right to verify or to have verified by mandated third parties the Processor’s compliance (including on site) with the implemented technical and organisational measures, the provisions of this Data Processing Agreement and the relevant data protection rules; The Processor shall provide the Controller with all information reasonably required by the Controller to comply with his inspections obligations.

(2) The Processor shall allow the Controller or third parties instructed by the latter to enter the business premises, in which the Controller Data is physically or electronically processed, during usual business hours. In particular, this also includes the data processing devices and the data processing programs of the Processor. With regard to on-site inspections, the Controller shall take into consideration the Processor’s business operations and shall notify him at least two weeks in advance. This obligation to notify shall be reduced to 24 hours (if necessary) in cases of controls by an order of the competent supervisory authorities or of an infringement by the Processor of data protection regulations or of this Data Processing Agreement. The Processor shall adequately assist the Controller with accomplishing the control measures.

9. Data Subject Rights

The Controller shall be responsible to preserve the data subject rights. However, taking this into consideration and depending on the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller’s obligation to respond to requests for exercising the data subject’s rights laid down in Chapter III of the UK GDPR, including the information obligations vis-à-vis the data subjects, with responding to their information requests, their rights to rectification, erasure, restriction, and data portability (including the relevant disclosure obligations) as well as their right to object and their right not be subject to automated individual decision-making including profiling, if the data subject asserts one of the data subject rights. Where a data subject directly addresses the Processor in asserting a respective data subject right and such request is apparently aimed toward the Controller only, the Processor forwards such request without undue delay to the Controller. The Processor may rectify, erase, or restrict the processing of personal data only upon instruction of the Controller. Information to third parties or data subjects may only be given by the Processor after prior written consent of the Controller.

10. Deletion and return of personal data

(1) Upon termination of the agreed processing activities, or earlier upon request of the Controller but upon termination of the Main Agreement at the latest, the Processor shall, at the choice of the Controller, return the Controller Data as well as any copies thereof to the Controller, or shall securely destroy the Controller Data. The Processor may not retain any Controller Data including copies (if any). Upon request, the Processor shall provide the Controller with written confirmation of the erasure or destruction of the data.

(2) Documentation intended as proof of proper data processing shall be kept by the Processor beyond the end of this Data Processing Agreement in accordance with relevant retention periods. For the purpose of discharge, the Processor may hand such documentation over to the Controller after the end of this Data Processing Agreement.

11. Liability

(1) The Controller and the Processor shall be liable vis-à-vis third parties pursuant to Art 82(1) UK GDPR for material and immaterial damages which an individual is suffering because of a violation of the UK GDPR.

(2) If one party must compensate a third party due to a negligently unlawful processing of personal data by the other party, the negligently acting party shall compensate the other party as provided under applicable law to the extent this corresponds to the quota of liability. The parties shall reasonably support each other with defending against unjustified claims.

(3) The Processor shall bear the burden of proof that damages and fines have not been caused by circumstances he is responsible for to the extent the relevant cause for the processing of the Controller Data is within the Processor's area of competence.

(4) Restrictions of liability agreed between the parties on other occasions (e.g. in the Main Agreement) shall not apply.

12. Final provisions

(1) If a provision of this Data Processing Agreement is or becomes invalid in total or in part or contains a gap, the validity of the other provisions shall not be affected. The parties shall replace the invalid or missing provision by a valid provision which comes closest to the purpose and intent of the parties and which is best complying with the requirements of Art. 28 and Art. 29 UK GDPR.

(2) All side agreements, modifications, and amendments of this Data Processing Agreement must be in writing which shall also apply to a waiver of this form requirement.

On behalf of the customer:

Company Name and Address:
____
____
____

Company Representative Details:
____
____
____

On behalf of Creative Marketing (NW) Ltd T/A AutoRefs

AutoRefs
Moss Bridge House,
Moss Bridge Road
Rochdale, OL16 5EA

Kasim Javed
Director
+44 (0) 1706 3182000
kasim@autorefs.com

Kasim Javed

07 / 23 / 2022

Appendix 1

Technical and organisational measures (Art. 32 UK GDPR)

1. Confidentiality (Art. 32(1)(b) UK GDPR)

✔ ID cards
✔ Electronic access code cards / access transponders
✔ Authorisation concept
✔ Alarm system
✔ Concept for handing over keys
✔ Visitor passes
✔ Accompanying visitors by own employees
✔ Recording of presence of visitor access
✔ Site security service also beyond common working hours
✔ Different levels of security areas and controlled access
✔ Special glazing
✔ Separate secured access to the computer centre
✔ Servers located in locked rooms
✔ Locked storage of data carriers (e.g. in locked rooms)
✔ Storage of back-up data (e.g. tapes, CDs) in a locked safe
✔ Instructions for handing over keys

✔ Password protection for computer workstations
✔ Functionally and / or timely restricted assignment of user authorisations
✔ Use of individualised passwords
✔ Automatic locking of user accounts after multiple wrong entries of password
✔ Automatic, password secured screen lock following inactivity (screensaver)
Password policy with minimum standards for password complexity
✔ at least 8 digits / uppercase and lowercase letters, special characters, numbers (at least 3 types thereof)
✔ preventing trivial passwords (e.g. dog1, dog2, dog3)
✔ password history (e.g. no re-use of the last 5 passwords)

Hashing of saved passwords

✔ hashes are “salted“ (Salt)
✔ hashes are “peppered“ (Pepper)

✔ Procedure for assignment of rights to new employees
✔ Procedure for withdrawal of rights due to changing department / position
✔ Procedure for withdrawal of rights concerning employees leaving the organisation
✔ Obligation to confidentiality
✔ Logging and analysis of the system use
✔ Controlled destruction of data carriers

✔ Definition of access rights, authorisation concept
✔ Rules for the restoration of data from backups (who, when, upon whose request)
✔ Regular review of access rights
✔ Restriction of free and uncontrolled retrieving of databases
✔ Regular evaluation of protocols (logfiles)
✔ Logging of access to data

Are corresponding security systems (software/hardware) used?

✔ virus scanners
✔ firewalls
✔ SPAM filters
✔ intrusion prevention systems (IPS)
✔ intrusion detection systems (IDS)
✔ software for security information and event management (SIEM)

Encrypted storage of data

- encryption algorithms in place (e.g. AES, RSA): please specify
- used hash functionality

✔ SHA2 (256, 384, 512 Bit)
✔ SHA3
✔ hashes are “salted“ (Salt)
✔ hashes are “peppered“ (Pepper)

✔ Separation of clients (multi-client capability of used system)
✔ Compartmentation of data files in databases
✔ Logical data separation (e.g. by virtue of client numbers)
✔ Storage of Controller Data on special data carriers (without data of other client)
✔ Authorisation concept taking into account separated processing of Controller Data from data of other clients

✔ Separation of functions
✔ Separation of development, testing and productive systems
✔ Dedicated system

2. Integrity (Art. 32(1)(b) UK GDPR)

Type of data transmission between the Processor and third parties:

✔ Citrix connection (128 bit encrypted)
✔ VPN connection (IP-Sec)
✔ email dispatch with encrypted ZIP files.
✔ data exchange via https connection
✔ encrypted email dispatch
✔ Secured entrance for delivering and dispatching
✔ Documented administration of data carriers, inventory control
✔ Definition of areas in which data carriers should be located
✔ Encryption of confidential data carriers
✔ Encryption of laptop hard drives
✔ Encryption of mobile data carriers
✔ Disposal of data carriers – secure erasure of data carriers:
✔ physical destruction
✔ overwriting of tapes and hard drives

Disposal of paper file – secure destruction of paper files:

✔ closed container made of metal (so called privacy containers)
✔ disposal by service providers
✔ shredder according ISO/IEC 21964-1
✔ Rules for making copies
✔ Backup copies of data carriers which must be transported
✔ Documentation of recipients to which transmission is envisaged
✔ Documentation of respective ways of transmission
✔ Rules for packaging and dispatching
✔ Completeness and accuracy control

✔ Marking of collected data
✔ Definition of user rights (profiles)

Differentiated user rights

✔ reading, modifying, deleting
✔ partial access to data or functions

✔ field access concerning databases
✔ Organisational definition of responsibilities for data entry
✔ Logging of data entries and deletions
✔ Log analysis system
✔ Log concept beyond OS-standard
✔ Dedicated log server
✔ Rules for access rights to log server (LogAdmin)
✔ Rules for retention periods for controlling and verification purposes

3. Availability and Resilience (Art. 32(1)(b) UK GDPR)

Data security and data backup concepts

✔ mirroring of hard drives
✔ online backups
✔ offline backups
✔ onsite backups
✔ offsite backups

Implementation data security and data backup concepts

✔ mirroring of hard drives
✔ online backups
✔ offline backups
✔ onsite backups
✔ offsite backups
✔ Fire alarm system in server rooms
✔ Smoke detector in server rooms
✔ Waterless fire-fighting system in server rooms
✔ Air-conditioned server rooms
✔ Lightning and surge protection
✔ Water sensors in server rooms
✔ Server rooms in separated fire compartments

Location of backup systems

✔ in separated rooms
✔ in separated fire compartments
✔ Ensuring future readability of backup data carriers
✔ Storage of archive storage data carriers under adequate conditions (air conditioning, protection level etc.)
✔ co2-fire extinguisher in the immediate vicinity of server rooms
✔ Agreement on handing over data backups
✔ Contingency plans (e.g. water, fire, explosion, terror attacks, crash, earthquake)
✔ Considering influence of adjacent structures (e.g. buildings)
✔ Vulnerability assessment (e.g. area protection, building protection, intrusion into computer systems and networks)

✔ Retention of data in data-security cabinet, safes
✔ UPS systems (Uninterruptible Power Supply)
✔ Electricity generator

Existence of a backup data centre?

✔ hot-standby
✔ Redundant power supply
✔ Redundant UPS system
✔ Redundant electricity generators
✔ Redundant air conditioning
✔ Redundant fire fighting
✔ Other redundant systems / procedures: please specify
✔ Computer Emergency Response Team (CERT)
✔ Load balancer
✔ Data storage on RAID systems (RAID 1 and higher)
✔ Definition of critical components
✔ Implementation of penetration tests
✔ System hardening (deactivation of unnecessary components)

Immediate and regular activation of available software and firmware updates

✔ identification of the specific devices which are part of the network and definition of their hardware version and the current software and firmware version
✔ communications channel with manufacturers to be informed about new updates and patches released for the operating devices
✔ definition of time periods for installations of updates (e.g. time periods with low operations, support times etc.)
✔ use of redundant systems to keep operations running during update times of main devices are
✔ progressive availability of updates/patches to identify problems at an early stage without interfering with several devices
✔ definition of a testing period to monitor the correct installing of updates and to ensure operations continuously running smoothly with new updates

During the implementation phase of the systems, security aspects are substantially taken into account
✔ definition of security measures for the protection and validation of communication between system components

✔ restriction of user rights in terms necessity and demand
✔ external service providers and maintenance staff receive specific access only activated during respective access times and deactivated at all other times

Regular security training and awareness-raising campaigns within the organisation
✔ awareness-raising campaigns to inform the users about the security concepts characteristic for specific systems as well as for traditional IT systems
✔ specific security training, teaching how to apply security measures and routines in everyday practice with minimal efforts

Cyber insurance

✔ identification of IT devices, assets and network systems in organisation's infrastructure
✔ performing a risk analysis taking into account all identified systems, devices, and assets for the assessment of risks including their likelihood and impact
✔ conclusion of a cyber insurance

4. Procedures for regular testing (Art. 32(1)(d), Art. 25(1) UK GDPR)

✔ Internal records of processing activities updated at least once a year
✔ Data protection officer notified of new / modified data processing methods
✔ Information security officer notified of new / modified data processing methods
✔ Documented processes regarding notification of new and modified data processing methods
✔ Data protection by default is used
✔ Implemented security measures are subject to regular internal control
✔ Relevant data processing with a high-risk potential is subject to a data protection impact assessment
✔ In case of negative outcome regarding aforementioned assessments, the security measures are adjusted to the relevant risks, renewed and implemented accordingly
✔ Process in preparation for security breaches (attacks), system interruptions and to identify, restrain, remedy and to recover from such incidents is in place (Incident Response Process)

5. Order / Contract Control (Art. 32(4) UK GDPR)

✔ Obligation of employees to codes of conduct
✔ Intra-corporate data protection policies
✔ Obligation of employees to adhere to relevant data protection provisions
✔ Training of all employees with access rights
✔ Appointment of contact persons and responsible project managers for concrete orders
✔ Contract management with service providers in line with legal provisions (Art. 28 UK GDPR)
✔ Centralised recording of instructed service providers (consistent contract management)
✔ Regular control at service providers after commencement of the contract (during the contract lifetime)
✔ On-site inspection of service providers
✔ Review of service providers’ data security concept
✔ Check of service providers’ IT security certificates

6. Pseudonymisation (Art. 32 (1) (a), Art. 25 (1) UK GDPR)

✔ Replacement of personal data by random codes
✔ Data masking

Appendix 2

LIST OF SUB-PROCESSORS

The Controller has authorized the following list of sub-processors:

Company	Sub-processing Activities	In what countries does AutoRefs store Customer Personal Data?	In what countries does AutoRefs process (e.g., access, transfer, or otherwise handle) Customer Personal Data?
Hetzner	Website Files & Database Hosting	Germany	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
PandaDoc	Cloud-based Sales Services	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Calendly	Meeting scheduler	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Google Analytics & Google Data Studio	Analytics & Business Intelligence	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States

Company	Sub-processing Activities	In what countries does AutoRefs store Customer Personal Data?	In what countries does AutoRefs process (e.g., access, transfer, or otherwise handle) Customer Personal Data?
Microsoft Office 365	Support Email Hosting	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Crisp Live Chat	Live Chat Support	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Mailgun Technologies, Inc.	Email API Processing	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Pipedrive	CRM System	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Twilio	Communication API	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States
Go Daddy	Domain Registration	United States	Asia-Pacific, Canada, Central America/ Caribbean/ Mexico, Europe (EEA), Europe (Non EEA), South America, United States