d.vinci

Individual Agreement
regarding the consignment processing of personal data

Between

Customer

- Principal -

And

d.vinci HR-Systems GmbH

Nagelsweg 37-39

20097 Hamburg

Germany

- Contractor -

1. Subject of the order

1) The Parties concluded a General Agreement regarding the consignment processing of personal data, which is now supplemented by this Individual Agreement.

2) Reason for the conclusion of this Individual Agreement is the assignment for the usage of the d.vinci Applicant Management, whereby the Contactor processes personal data on behalf of the Principal.

2. Subject and purpose of the processing

1) The subject of the processing of personal data is the provision of services specified in the General Agreement by the Contractor on behalf of the Principal.

2) The purpose of the respective processing of personal data is based on the General Agreement. Personal data from the Principal's domain is exclusively processed by the Contractor for the fulfilment of the purpose and in connection with the performances to be provided by the Contractor in this context according to Article 4 no. 2 GDPR (General Data Protection Regulations), specifically collected, stored, amended, read, retrieved, used, disclosed, compared, linked and erased. The purpose comprises the following tasks:

    a) Processing of job advertisements
    b) Receipt and management of applications
    c) Operation of the d.vinci Applicant Management in a data processing centre commissioned by the Contractor
    d) Maintenance and support of software in accordance with the contractual stipulations

3. Types of personal data affected by the processing

The following types of personal data are affected by the consignment processing:

a) Address data
b) Resumes
c) Reports (e.g. job references)
d) Applicant profiles, if applicable with the incorporation of data from suitability test
e) other applicant data and documentation, such as photos

A risk assessment by the Principal is required to determine whether the services to be provided by the Contractor and the respectively adopted agreements are suitable for the processing of special categories of personal data in accordance with Article 9 (1) GDPR.

4. Category of persons affected by the processing

The following categories of persons are affected by the consignment processing:

a) Applicants
b) Employees (users)

5. Technical and organisational measures

The Contractor shall take the technical and organisational measures specified in Annexures 1 and 2 for the personal data processed on consignment.

6. Persons authorised to issue instructions

1) The following persons are authorised by the Principal to issue instructions; the Principal can modify the list of authorised persons at any time by way of a unilateral declaration.

    a) The number of all persons authorised by the Principal to conduct legal transactions in accordance with the Commercial Register
    b) All specifically nominated key users of the Principal

2) The Contractor declares that the following persons are authorised to receive on behalf of the Contractor:

    a) The number of all persons authorised by the Contractor to conduct legal transactions in accordance with the Commercial Register
    b) All employees of d.vinci working in the Customer Service sector

7. Sub-processor

1) The Contractor utilises the following sub-processors for the processing of data:

    a) pop-interactive GmbH, Wendenstrasse 408, 20537 Hamburg
    b) Textkernel BV, Nieuwendammerkade 28/a17, 1022 AB, Amsterdam, NL (only for the usage of CV parsing)

2) Requirements for the sub-processor pop-interactive GmbH: pop-interactive GmbH is responsible for its own compliant usage of the data centre and all other required services such as network establishment, carrier links, internal wiring and rack construction. The data centre is operated in conjunction with Mr. net Group GmbH & Co at Wendenstrasse, Hamburg. Infrastructural contract matters for the operation of the data centre are executed by Mr. net Group GmbH & Co with the respective suppliers and service companies. This also includes an annual VdS audit.

3) Requirements for the subcontractor Textkernel BV: Textkernel provides a semantic search, sourcing and matching tool which is integrated in the d.vinci application management. The use of this tool permits the personnel managers to analyse CVs and jobs. In the course of processing, the documents, which contain the CV of the respective applicant, are transmitted to the subcontractor Textkernel BV. The information contained therein is transmitted to the Contractor. Following the transmission of the data, the documents are deleted on the Textkernel sites.

8. Place of data processing

The data is processed exclusively within the area of the Federal Republic of Germany, a member state of the European Union or another contracting state of the treaty concerning the European economic area. The data is not disclosed to third parties.

9. Return

1) Following the demand of the Principal, data, data carriers as well as all other materials with personal data subject to this Agreement have to be surrendered or erased upon the expiration of the Agreement. The Principal is responsible for any additional costs incurred by the Contractor based on instructions issued for the erasure of data which deviates from the previously agreed terms. The erasure has to be documented in a suitable manner. The Principal is entitled to verify the complete and contractually agreed return and erasure of the data with the Contractor. This can also be accomplished by inspecting the data processing systems.

2) The Parties agree that the plea of the right of retention by the Contractor in terms of Section 273 BGB (German Civil Code) with respect to the data processed for the Principal and the associated data carriers is excluded. This does not apply if the Principal is obligated to continue storing the personal data according to the laws of the European Union or the member states. In this case, this Agreement continues to apply for the duration of this obligation.

10. Term of the Agreement

The duration of this Individual Agreement is based on the term of the General Agreement. It can be terminated separately for an important reason.

d.vinci HR-SYSTEMS
d.vinci HR-Systems GmbH
Nagelsweg 37–39 · 20097 Hamburg

_____	_____
Customer	d.vinci HR-Systems GmbH

Annexures

Annexure 1: Technical and organisational measures – office premises

Annexure 2: Technical and organisational measures – data processing centre

Annexure 1 - Technical-organisational measures according to Article 32 GDPR

The measures described in this document refer to the **location Nagelsweg 37-39 in Hamburg, where the office premises are situated on levels 4 and 5.** As described in the operational concept, as a rule, applicant data is not processed on these premises. Applicant data can be processed in these premises in exceptional cases; this will always require an order by the customer.

1. Confidentiality (Article 32 (1) b GDPR)

a) Access control || The following implemented measures prevent unauthorised persons to access the data processing systems

- ☑ Key management / documentation of key distribution
- ☑ Alarm system
- ☑ Special protective measures for the storage of backups and/or other data carriers
- ☑ Irreversible destruction of data carriers
- ☑ Employee and authorisation IDs
- ☑ Visitor regulation (for example, pick-up at the reception, documentation of visiting times, visitor's ID, escorting the visitor to the exit)

b) Access control || The following implemented measures prevent unauthorised persons from accessing the data processing system.

- ☑ Personal and individual user log-in upon registering in the system and/or the company network
- ☑ Authorisation process for access authorisations
- ☑ Limitation of authorised users
- ☑ BIOS passwords
- ☑ Password process (specification of password parameters with respect to complexity and updating interval)
- ☑ Logging access (ADS and firewall logs)
- ☑ Additional systems log for certain applications
- ☑ Automatic blocking of clients after certain laps of time without user activity (also password-protected screen saver or automatic pausing)
- ☑ Firewall

c) Access control || The following implemented measures ensure, that unauthorised persons do not have access to personal data.

- ☑ Management and documentation of distinct authorisations
- ☑ Conclusion of data processing agreements for the external service, maintenance and repair of data processing systems, if the processing of pbD, i.e. the handling of personal data via remote maintenance is subject of the service
- ☑ Analysis / recording of data processing tasks
- ☑ Authorisation process for the authorities
- ☑ Approval routines
- ☑ Profiles/roles
- ☑ Encryption of CD/DVD- ROM, external hard drives and/or Laptops (i.e. via operating system, TrueCrypt, Safe Guard Easy, WinZip, PGP)
- ☑ Measure to prevent unauthorised copying of data on data carriers suitable for external use (e.g. copy protection, blocking of USB ports, "Data Loss Prevention (DLP)-System")
- ☑ Segregation of duties
- ☑ Expert destruction of files and data carriers according to DIN 66399 (service provider is certified)
- ☑ Irreversible erasure of data carriers

d) Separation control || The following measures ensure that personal data collected for various purposes is processed separately.

- ☑ Backup of data records in physically separate databases
- ☑ Processing on separate systems
- ☑ Access authorisation according to functional competency
- ☑ Separate data processing through distinct access regulations
- ☑ Multi-client capability of IT systems
- ☑ Use of test data
- ☑ Separation of development and production environment

e) Pseudonymisation (Article 32 (1) lit. a GDPR; Article 25 (1) GDPR) || The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to respective technical and organisational measures.

No applicant data is processed at this location.

2. Integrity (Article 32 (1) b GDPR)

a) Transfer control || It is ensured that personal data cannot be read, copied, modified or removed during the transmission or storage on data carriers without authorisation and that it can be verified which person or which locations have received personal data. The following safeguarding measures have been implemented for this purpose:

- ☑ Encryption of storage medium of laptops
- ☑ Secured File Transfer (e.g. sftp)
- ☑ Secured data transport (e.g. SSL, ftps, TLS)
- ☑ Encryption of CD/DVD- ROM, external hard drives or USB sticks (e.g. TrueCrypt, Safe Guard Easy, PGP)
- ☑ Regulation regarding the handling of mobile storage media (e.g. laptop, USB stick, mobile phone)
- ☑ Protocolling of data transport (backup)
- ☑ Logging of read accesses within application
- ☑ Tunnelled remote data connections (VPN = Virtual Private Network)

b) Entry control || The following measures ensure that it can be verified who has processed personal data in data processing systems at which time.

- ☑ Access rights
- ☑ Functional responsibilities, organisationally specified competencies
- ☑ Multiple-eyes principle

3. Availability and resilience (Article 32 (1) b GDPR)

Availability control and resilience control || The following measures ensure that personal data is protected against accidental destruction or loss and is available to the Principal at all times.

- ☑ Security concept for software and IT applications
- ☑ Backup process
- ☑ Storage process for backups (fire-protected safe, separate fire compartment, etc.)
- ☑ Installation of security updates according to requirements
- ☑ Mirroring hard disks
- ☑ Establishment of an uninterruptible power supply (UPS)
- ☑ Climate-controlled server room
- ☑ Virus protection
- ☑ Firewall

- ☑ Emergency plan
- ☑ Successful emergency exercises
- ☑ Redundant locally separate data storage (off-site storage)

4. Procedure for regular verification, assessment and evaluation (Article 32 (1) d GDPR; Article 25 (1) GDPR)

a) Data protection management || The following measures are designed to ensure an established organisation compliant with the basic requirements of the Data Protection Act:

- ☑ Directives/instructions to ensure technical/organisational measures for data security
- ☑ Appointing a data protection controller
- ☑ Obligating employees to comply with data secrecy
- ☑ Adequate training of the employees in data protection matters
- ☑ Maintaining an overview of processing activities (Article 30 GDPR)
- ☑ External auditing of the information security (ISO certification 27001 and 9001)

b) Incident Response Management ||The following measures are designed to ensure that notification processes are triggered in the event of data protection violations:

- ☑ Notification process for data protection violations according to Article 4 No. 12 GDPR to supervisory authorities (Article 33 GDPR)
- ☑ Notification process for data protection violations according to Article 4 No. 12 GDPR to affected persons (Article 34 GDPR)

c) Data-protection-friendly settings (Article 25 (2) GDPR) ||

The default settings have to be considered in the standardised pre-settings of systems and apps as well as for the establishment of data processing actions. In this phase, functions and rights are specifically configured, the admissibility / inadmissibility of certain entries/entry options (e.g. free texts) are determined in terms of data minimisation and the availability of usage functions is decided (e.g. in terms of the extent of the processing). Also the type and the extent of the personal reference and/or anonymisation (e.g. at selection, export and analysis functions, which can be provided specified and pre-set or freely designable) or the availability of certain processing functions, recording etc. are determined.

No applicant data is processed at this location.

d) Order control || With the following measures, it is ensured that personal data can only be processed in accordance with the instructions.

- ☑ Agreement regarding consignment processing with regulations pertaining to the rights and obligations of the Contractor and the Principal
- ☑ Process for the issuance of and/or compliance with instructions
- ☑ Appointment of contact persons and/or responsible employees
- ☑ Control/verification of the execution of assignments subject to instructions
- ☑ Training, induction of all employees of the Contractor with access authority
- ☑ Obligating employees to comply with data secrecy
- ☑ Formalised contract management
- ☑ Documented process regarding the selection of the service provider

Annexure 2 - Technical-organisational measures according to Article 32 GDPR

The measures described in this document refer to **the location Wendenstrasse 408 in Hamburg, where the data processing centre is operated on level 3.** The measures therefore relate to the service provider who provides the infrastructure as well as the computers operated in the computer centre, to which the service provider does not have access.

1. Confidentiality (Article 32 (1) b GDPR)

a) Access control || The following implemented measures prevent unauthorised persons from accessing the data processing systems

- ☑ Access control system, pass reader (magnet/chip card)
- ☑ Door securities (electric door opener, combination lock, etc.)
- ☑ Grills in front of windows/doors
- ☑ Key management / documentation of key distribution
- ☑ Alarm system
- ☑ Video monitoring
- ☑ Special protective precautions of the server room: early recognition of fires and water penetration
- ☑ Special protective measures for the storage of backups and/or other data carriers
- ☑ Irreversible destruction of data carriers
- ☑ Employee and authorisation IDs
- ☑ Barred areas
- ☑ Visitor regulation (for example, pick-up at the reception, documentation of visiting times, visitor's ID, escorting the visitor to the exit)

b) Access control || The following implemented measures prevent unauthorised persons from accessing the data processing system.

- ☑ Personal and individual user log-in upon registering in the system and/or the company network
- ☑ Authorisation process for access authorisations
- ☑ Limitation of authorised users
- ☑ BIOS passwords
- ☑ Password process (specification of password parameters with respect to complexity and updating interval)
- ☑ Electronic documentation of passwords and protection of these documents from unauthorised access
- ☑ Logging access
- ☑ Additional systems log for certain applications

- ☑ Automatic blocking of clients after certain laps of time without user activity (also password-protected screen saver or automatic pausing)
- ☑ Firewall

c) Access control || The following implemented measures ensure, that unauthorised persons do not have access to personal data.

- ☑ Management and documentation of distinct authorisations
- ☑ Analysis / recording of data processing tasks
- ☑ Authorisation process for the authorities
- ☑ Approval routines
- ☑ Profiles/roles
- ☑ Segregation of Duties, see operational concept
- ☑ Expert destruction of files and data carriers according to DIN 66399

d) Separation control || The following measures ensure that personal data collected for various purposes is processed separately.

- ☑ Backup of data records in logically separate databases (principle: one service per server, one database per customer)
- ☑ Access authorisation according to functional competency
- ☑ Separate data processing through distinct access regulations
- ☑ Multi-client capability of IT systems
- ☑ Use of test data
- ☑ Separation of development and production environment

e) Pseudonymisation (Article 32 (1) lit. a GDPR; Article 25 (1) GDPR) || The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to respective technical and organisational measures.

Identification is generated when the data set of an applicant is created, which is used in the further progression of the processing.

2. Integrity (Article 32 (1) b GDPR)

a) Transfer control || It is ensured that personal data cannot be read, copied, modified or removed during the transmission or storage on data carriers without authorisation and that it can be verified which person or which locations have received personal data. The following safeguarding measures have been implemented for this purpose:

- ☑ Encryption of storage media of laptops
- ☑ Secured data transport (e.g. SSL, ftps, TLS)
- ☑ Regulation regarding the handling of mobile storage media (e.g. laptop, USB stick, mobile phone)
- ☑ Protocolling of data transport (backup)
- ☑ Logging of read accesses within application

b) Entry control || The following measures ensure that it can be verified who has processed personal data in data processing systems at which time.

- ☑ Access rights
- ☑ Logging by the system
- ☑ Functional responsibilities, organisationally specified competencies

3. Availability and resilience (Article 32 (1) b GDPR)

Availability control and resilience control || The following measures ensure that personal data is protected against accidental destruction or loss and is available to the Principal at all times.

- ☑ Security concept for software and IT applications
- ☑ Backup process
- ☑ Storage process for backups (fire-protected safe, separate fire compartment, etc.)
- ☑ Installation of security updates according to requirements
- ☑ Mirroring hard disks
- ☑ Establishment of an uninterruptible power supply (UPS)
- ☑ Fire / extinguishing water protection of server room
- ☑ Climate-controlled server room
- ☑ Virus protection
- ☑ Firewall
- ☑ Emergency plan
- ☑ Successful emergency exercises

☑ Redundant locally separate data storage (off-site storage)

4. Procedure for regular verification, assessment and evaluation (Article 32 (1) d GDPR; Article 25 (1) GDPR)

a) Data protection management || The following measures are designed to ensure an established organisation compliant with the basic requirements of the Data Protection Act:

☑ Directives/instructions to ensure technical/organisational measures for data security

☑ Appointing a data protection controller

☑ Obligating employees to comply with data and bank secrecy

☑ Adequate training of the employees in data protection matters

☑ Maintaining an overview of processing activities (Article 30 GDPR)

☑ External auditing of the information security (ISO certification 27001 and 9001)

b) Incident Response Management ||The following measures are designed to ensure that notification processes are triggered in the event of data protection violations:

☑ Notification process for data protection violations according to Article 4 No. 12 GDPR to supervisory authorities (Article 33 GDPR)

☑ Notification process for data protection violations according to Article 4 No. 12 GDPR to affected persons (Article 34 GDPR)

c) Data protection-friendly pre-settings (Article 25 (2) GDPR) || The default settings have to be considered in the standardised pre-settings of systems and apps as well as for the establishment of data processing actions. In this phase, functions and rights are specifically configured, the admissibility / inadmissibility of certain entries/entry options (e.g. free texts) are determined in terms of data minimisation and the availability of usage functions is decided (e.g. in terms of the extent of the processing). Also the type and the extent of the personal reference and/or anonymisation (e.g. at selection, export and analysis functions, which can be provided specified and pre-set or freely designable) or the availability of certain processing functions, recording etc. are determined.

☑ Only those data of the applicant required for the application shall be recorded.

☑ Only those data required for the service will be transferred when exporting the data to subcontractors.

d) Order control || With the following measures, it is ensured that personal data can only be processed in accordance with the instructions.

- ☑ Agreement regarding consignment processing with regulations pertaining to the rights and obligations of the Contractor and the Principal
- ☑ Process for the issuance of and/or compliance with instructions
- ☑ Appointment of contact persons and/or responsible employees
- ☑ Control/verification of the execution of assignments subject to instructions
- ☑ Training, induction of all employees of the Contractor with access authority
- ☑ Obligating employees to comply with data secrecy
- ☑ Formalised contract management
- ☑ Documented process regarding the selection of the service provider