

General Data Protection Regulation

Dear Customers,

Protection of personal data has always been a top priority for Crescentia and we welcome the new General Data Protection Regulation (GDPR) that came into effect on May 25th 2018. One GDPR requirement is that we must describe how we ensure GDPR compliance and commit to this in a data processor agreement with our customers.

Some of you already have individual data processor agreements with Crescentia and for those who do not, the following Data Processor Agreement will govern this important part of our relationship.

Best regards,

Bruce Decaster
President & CEO, Crescentia Global Talent Solutions

Heide Duckert
General Manager

Data Processing Agreement

BETWEEN:

Crescentia GTS UG (haftungsbeschränkt)
(Crescentia Global Talent Solutions)

Registry: HRB 284144

Leopoldstr. 31,
80802 München,
Deutschland
("Crescentia")

AND

Each individual Crescentia Customer that Crescentia processes data for and that has not otherwise entered into a valid data processor agreement (the "Customer").
Solutions

1. INTRODUCTION

1.1 This Data Processing Agreement ("DPA") specifies the Parties' data protection obligations which arise from Crescentia's processing of Personal Data on behalf of Customer under the order form, service agreement or other agreement between the Parties ("the Agreement"). All capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement.

1.2 The DPA is adopted as an appendix to the Agreement. In the event that any provision of this DPA is inconsistent with any term of the Agreement, the DPA will prevail. If and to the extent the Standard Contractual Clauses conflict with any provision of the Agreement or the DPA, the Standard Contractual Clauses shall prevail to the extent of such conflict.

1.3 If Applicable Data Protection Law is amended, replaced or repealed, the parties shall, where necessary, negotiate in good faith a solution to enable the processing of Personal Data to be conducted in compliance with Applicable Data Protection Law.

2. PURPOSE, SCOPE AND RESPONSIBILITIES

2.1 Crescentia shall only process personal data in accordance with the terms of this DPA.

2.2 The parties agree the Customer is the Data Controller of Customer Personal Data. Crescentia is the Data Processor of Customer Personal Data, except where Crescentia acts as a Data Controller processing Customer Personal Data in accordance with Section 2.9.

2.3 Crescentia shall process Customer Personal Data for the limited purpose of performing the obligations set out under the Agreement and only in accordance with the Customer's lawful instructions or otherwise necessary to comply with Applicable Data Protection Law. Data may, for that purpose, be processed by any of Crescentia's entities.

2.4 Customer shall ensure that its instructions to Crescentia comply with all laws and regulations applicable to Customer Personal Data, and that the processing of Customer Personal Data following Customer's instructions will not cause Crescentia to be in breach of Applicable Data Protection Law. Customer is solely responsible for the accuracy, quality and legality of Customer Personal Data provided to Crescentia in accordance with this DPA.

2.5 Personal Data processed by Crescentia shall include such actions as may be specified in the Agreement. Further data processing outside the scope set out in this Section 2 shall require mutual written agreement of the parties.

2.6 If Crescentia becomes aware that any instruction given by Customer breaches Applicable Data Protection Law, Crescentia shall immediately inform Customer of this, giving details of the breach or potential breach.

2.7 The term of this DPA shall continue until the later of the following: the termination of the Agreement or the date at which Crescentia ceases to process Personal Data for Customer.

2.8 In no event will the data processed by Crescentia include financial data or Sensitive Data.

2.9 The parties acknowledge and agree that Crescentia may process Customer Personal Data for its own legitimate business operations as independent Data Controller, provided the data processing is limited to one of the following purposes: i) billing and account management; ii) internal reporting; iii) fraud and cyber-attacks prevention pertaining to the provision of the Services; iv) optimization and maintenance of the Services; and v) compliance with legal and tax requirements.

2.10 The types and categories of Customer Personal Data processed by Crescentia, and the purpose of such processing is set out in **Exhibit 1**.

3. OBLIGATIONS OF CRESCENTIA AS DATA PROCESSOR

3.1 Crescentia warrants that it will:

i) comply with Applicable Data Protection Law relevant to Crescentia's obligations under the Agreement;

ii) implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of Applicable Data Protection Law and ensure the protection of the rights of the data subjects; and

iii) make available to Customer all information reasonably necessary to demonstrate compliance with the obligations in this DPA; and reasonably cooperate with any audits performed by Customer or its independent auditor, at Customer's own expense and no more than once a year, of facilities under the control of Crescentia, in accordance with Section 10.2 of the Agreement.

4. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

4.1 Crescentia will implement and maintain throughout the term of the DPA and will procure its Sub-processors to implement and maintain through the term of the DPA, the appropriate technical and organizational security measures to protect Personal Data against accidental or unlawful destruction, loss, damage or alteration and against unauthorized disclosure, abuse or other processing in violation of the requirements of Data Protection Law.

4.2 Crescentia will ensure that it and its Sub-processors will at all times comply with the minimum data security requirements set out in **Exhibit 2**, which may, from time to time, be updated, provided that such updates and modifications do not degrade or diminish the overall security of the Services.

4.3 Customer has evaluated the security measures implemented by Crescentia and agrees that they provide an appropriate level of protection for Customer Personal Data.

5. PERSONNEL

5.1 Crescentia shall ensure that any personnel required to access Customer Personal Data have committed themselves to the obligation of confidentiality set out in the Agreement or are under a statutory obligation of confidentiality.

5.2 Crescentia shall ensure that its personnel required to access Customer Personal Data are informed of the confidential nature of Customer Personal Data and the security procedures applicable to the processing of or access to Customer Personal Data.

5.3 Crescentia's personnel's confidentiality obligations will survive the termination of the personnel engagement and the term of this DPA.

6. ASSISTANCE TO THE CUSTOMER AS DATA CONTROLLER

6.1 Crescentia shall provide reasonable and timely assistance, by appropriate technical and organizational measures to Customer to enable them to respond to: (i) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable); and (ii) any other correspondence, enquiry or complaint received from a data subject, Regulator or other third party in connection with the processing of the Personal Data. In the event that any such request, correspondence, enquiry or complaint is made directly to Crescentia, Crescentia shall promptly inform Customer providing full details of the same, unless prohibited by the applicable law.

6.2 Crescentia shall reasonably assist Customer with its obligation to conduct any data protection impact assessment required by Applicable Data Protection Law.

7. SUB-PROCESSORS

7.1 Currently, Crescentia does not use any sub-processors. If Crescentia decides to use any sub-processors, Crescentia will make this known to Customer prior to their use to obtain approval. Customer hereby gives a general authorization for the engagement of additional Sub-processors for the purpose of performing its obligations under the Agreement, provided Crescentia shall:

- maintain an up-to-date list of its Sub-processors on at <https://www.crescentiasolutions.com/legal/> (or any future website used by Crescentia);
- provide at least 30 days prior notice (except to the extent a 30 days' notice is not possible due to an emergency concerning Service availability or security) to Customer of any change to its Sub-processors via Crescentia's usual e-mail notification process;
- execute a written agreement that obligates the Sub-processor to (i) protect Customer Personal Data to the same extent required of Crescentia by the Agreement; and (ii) comply with Applicable Data Protection Law.

7.2 If Customer objects to such new Sub-processor on reasonable grounds within 30 days of receiving notice, the parties shall negotiate in good faith to find an alternative solution. If such alternative solution cannot be found and Crescentia decides to proceed with such Sub-processor, Customer may terminate the Agreement with 30 days prior written notice. Neither of the Parties shall be considered in breach of contract in the event of such termination. Customer acknowledges that Crescentia provides a standardized service to all customers which does not allow using different Sub-processors for different customers and, therefore, that the inability to use a particular new or replacement Sub-processor for the Services to the Customer may result in delay in performing the Services, inability to perform the Services or increased fees. Crescentia will notify Customer in writing of any change to Services or fees that would result from Crescentia's inability to use a new or replacement Sub-processor to which Customer has reasonably objected. If Customer does not object to a new Sub-processor's engagement within 30 days, that new Sub-processor shall be deemed accepted.

7.3 Crescentia shall be liable for the acts or omissions of its Sub-processors to the same extent that Crescentia would be liable if performing the Services of each Sub-processor directly under the terms of this DPA.

8. TRANSFER OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANIZATIONS

8.1 Customer acknowledges and agrees that Crescentia may transfer and process Customer Personal Data to its authorized Sub-processors in third countries for the provision of the Services. Any transfer of Personal Data to third countries or international organizations by Crescentia shall always take place in compliance with EU Data Protection Law, UK Data Protection Law and this DPA.

8.2 Any transfer of Customer Personal Data made from EEA, Switzerland or United Kingdom to a Restricted Country will be subject to the Standard Contractual Clauses (together with the UK Addendum, where UK Data Protection Law applies) and any other supplementary measures required to enable the lawful transfer of Customer Personal Data. The Parties agree to promptly undertake to amend this DPA if necessary to incorporate an updated data transfer mechanism to maintain compliance with EU Data Protection Law and UK GDPR.

8.3 If any Customer Personal Data originates from any country (other than an EEA country) with one or more laws imposing data transfer restrictions or prohibitions and Customer has informed Crescentia of such data transfer restrictions or prohibitions, Customer and Crescentia shall ensure an appropriate transfer mechanism (satisfying the country's data transfer requirements) is in place, as reasonably requested by Customer and mutually agreed upon by both Parties, before transferring or accessing Customer's Data outside of such country. For the avoidance of doubt, this transfer restriction does not apply to Customer's or its Affiliates' Authorized Users who have access to the Services and Customer Data, and Crescentia shall not be held responsible for actions of Customer or its Affiliates' Authorized Users. Neither Customer nor its Authorized Users shall be entitled to use the Services in any country with data localization laws that would require Customer's environment to be hosted in said country.

9. OBLIGATIONS OF THE CUSTOMER

9.1 Customer and Crescentia will be separately responsible for conforming with Applicable Data Protection Law, as applicable to each.

9.2 Customer will inform Crescentia in writing without undue delay following Customer's discovery of a failure to comply with Applicable Data Protection Law with respect to processing of Personal Data in accordance with this DPA.

9.3 Customer shall be responsible for providing accurate and relevant contact details at the time of entering into the Agreement and thereafter to assist with Crescentia's notification obligations.

9.4 Customer represents and warrants it has provided and will continue to provide all notices and has obtained and will continue to obtain all consents and rights required under Applicable Data Protection Law for Crescentia to process Customer Personal Data for the purposes of this Agreement.

10. NOTIFICATION OF DATA BREACH

10.1 Crescentia shall without undue delay, and no later than 48 hours, notify Customer in writing of any identified Data Breach.

10.2 The notification referred to in section 10.1. will, to the extent possible:

a) describe the nature of the Data Breach including the categories and approximate number of data subjects concerned and the categories and approximate amount of Personal Data impacted,

b) provide Crescentia contact details where more information can be obtained,

c) describe the likely consequences of the Data Breach, and

d) describe the measures taken or proposed to be taken by Crescentia to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

11. ADDITIONAL ASSIGNMENTS

11.1 In respect of tasks assigned to Crescentia, that are not an obligation under this DPA and go beyond Crescentia's statutory obligations, Crescentia shall be entitled to charge Customer for the additional resources, time and material necessary to fulfill the required task(s), unless such services are already included in the Services provided under the Agreement.

11.2 Crescentia will notify Customer in advance of such additional charges and, to the extent possible, provide Customer with a quote of the expected costs.

11.3 If Customer does not agree to the costs, Crescentia is not required to perform the additional assignment.

12. DELETION AND RETURN OF PERSONAL DATA

12.1 Following the expiration or earlier termination of the Agreement, Crescentia will retain Customer Data in a limited function account, securely isolated and protected from any further processing, for 90 days. Once the 90-day retention period ends, Crescentia shall disable Customer's account and delete all Customer Personal Data associated with it, or irreversibly anonymize them in such a manner that the data subject is not identifiable, unless Crescentia is permitted or required by applicable law, or authorized under this DPA, to retain such data. At all times during the term of the Agreement, Customer will have the ability to access, extract and delete Customer Personal Data stored in its tenant.

12.2 Upon Customer's request, Crescentia shall certify in writing the destruction or complete anonymization of Customer Personal Data.

13. LAW ENFORCEMENT REQUESTS

13.1 If a court, law enforcement authority or intelligence agency contacts Crescentia with a demand for Customer Personal Data, Crescentia will first assess if it is a legitimate order. If compelled to disclose or provide access to any Customer Personal Data to law enforcement, Crescentia will promptly notify Customer and provide a copy of the request, unless legally prohibited from doing so.

13.2 Crescentia shall only cooperate with the issued request or order if legally obliged to do so and, where possible, Crescentia shall judicially object to the request or order or the prohibition to inform Customer about this or to follow the instructions of Customer. Crescentia shall not provide more Customer Personal Data than is strictly necessary for complying with the request or order.

14. JURISDICTION SPECIFIC TERMS

14.1 To the extent Crescentia processes Personal Data originating from and protected by Applicable Data Protection Law in one of the jurisdictions listed in **Exhibit 3** (Jurisdiction Specific Terms) of this DPA, the terms specified in **Exhibit 3** with respect to the applicable jurisdiction(s) apply in addition to the terms of this DPA.

15. LIABILITY

15.1 Each party's liability for one or more breaches of this DPA shall be subject to the limitations and exclusions of liability set out in the Agreement.

16. LEGAL VENUE AND APPLICABLE LAW

16.1 This DPA shall be governed by Danish Law.

16.2 Any claim or dispute arising from or in connection with this DPA must be settled by the Copenhagen City Court as first instance.

17. DEFINITIONS

The terms “**Data Controller**”, “**Data Processor**”, “**data subject**”, “**processing**” and “**process**” shall have the meaning given in Applicable Data Protection Law.

“**Applicable Data Protection Law**” means any applicable law which applies to each party in any territory in which they process Personal Data and which relates to the protection of individuals with regards to the processing of Personal Data and privacy rights, and may include EU Data Protection Laws, UK Data Protection Laws, Canada's Personal Information Protection and Electronic Documents Act (“**PIPEDA**”), the California Consumer Privacy Act, as amended by the California Privacy Right Act of 2020 and its implementing regulation (“**CCPA**”); the Privacy Act 1988 (Cth) of Australia, as amended (“**Australian Privacy Law**”), the Virginia’s Consumer Data Protection Act (“**VCDPA**”); the Colorado Privacy Act (“**CPA**”); the Connecticut’s Act Concerning Data Privacy and Online Monitoring (“**CTDPA**”), and the Utah Consumer Privacy Act (“**UCPA**”).

“**Customer Personal Data**” means the Personal Data that is generated by or provided to Crescentia by, or on behalf of, Customer through use of the Services.

“**Data Breach**” means a breach of security which results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data processed by Crescentia.

“**EU Data Protection Laws**” means all data protection laws and regulation applicable to the European Economic Area (“**EEA**”) and Switzerland, including the General Data Protection Regulation 2016/679 (“**GDPR**”) and supplementing data protection law of the European Union Member States, the ePrivacy Directive 2002/58/EC (the “**Directive**”), together with any European Union Member national law implementing the Directive and the Swiss Federal Data Protection Act (“**Swiss DPA**”).

“**Personal Data**” means any information defined under Applicable Data Protection Law as “personal data”, “personal information”, “personally identifiable information” or any other similar term relating to an identified or identifiable natural person.

“**Regulator**” means any local, national or multinational agency, department, official, public or statutory person or any regulatory or supervisory authority for administering, providing guidance on, supervising and enforcing Applicable Data Protection Law.

“**Restricted Country**” mean a country, territory or jurisdiction which (i) when GDPR applies, is not covered by an adequacy determination by European Commission, as described under the GDPR, (ii) when Swiss DPA applies, is not included on the list of adequate jurisdictions published by the Swiss Regulator or (iii) when UK Data Protection Law applies, is not recognized as providing an adequate level of protection for Personal Data pursuant to Section 17A of the UK GDPR.

“**Sensitive data**” means any (i) special categories of Personal Data defined under EU Data Protection Law and UK Data Protection Law, (ii) data relating to criminal convictions and offences defined under EU Data Protection Law and UK Data Protection Law or (iii) within the definition of “sensitive personal information” under the CCPA.

“**Standard Contractual Clauses**” means: (i) where the GDPR applies, the contractual clauses annexed to the European Commission’s Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries (“**EU SCCs**”) and (ii) where the Swiss DPA applies, the standard data protection clauses issued, approved or otherwise recognized by the Swiss Regulator (“**Swiss SCCs**”), each as amended, supplemented or replaced from time to time.

“**Sub-processor**” mean any Crescentia Affiliate and any sub-contractor engaged by Crescentia in the processing of Customer Personal Data under the terms of the Agreement and this DPA.

“UK Addendum” mean the UK Addendum issued by the United Kingdom Regulator under section 119A(1) of the Data Protection Act 2018, being an addendum to the Standard Contractual Clauses.

“UK Data Protection Law” means all data protection laws and regulation applicable to the United Kingdom, including the United Kingdom's Data Protection Act 2018 and the GDPR as incorporated into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (“UK GDPR”), each as amended, supplemented or replaced from time to time.

18. SIGNATURES

Signed for and on behalf of Crescentia

Date: April 27, 2023

Name: Heide Duckert

Title: General Manager



EXHIBIT 1: INFORMATION ABOUT THE PROCESSING

- 1. The purpose of the data processor’s processing of Personal Data on behalf of the data controller is:**

Crescentia is a recruiting and executive search company, assigned by Customer to provide recruitment services. The content of this DPA reflects the limited amount of Personal Data Crescentia handles for Customer.

- 2. The data processor’s processing of Personal Data on behalf of the data controller shall mainly pertain to (the nature of the processing):**

The provision of the Recruitment Services by Crescentia to Customer.

- 3. The processing includes the following types of Personal Data about data subjects:**

Name, business/personal e-mail address, business/personal phone number, job title, LinkedIn or Facebook profiles, home address; as well as documents, images and other content or data in electronic form stored or transmitted by End Users for the purposes of Recruitment Services.

- 4. The processing includes the following type of Sensitive data about data subjects:**

None.

- 5. Processing includes the following categories of data subject:**

Customer's employees.

Or as determined by Customer through their use of Crescentia's Services.

6. **The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:**

Personal data is stored with Crescentia until Customer requests that the data is erased or returned, pursuant to Section 12.1 of this DPA.

EXHIBIT 2: DESCRIPTION OF MINIMUM DATA SECURITY

Crescentia has implemented and will maintain appropriate administrative, technical and physical safeguards to protect Personal Data as further described on <https://www.crescentiasolutions.com/legal/> and additionally set forth below. Security Contact. Requests regarding information security can be directed to the Crescentia at info@crescentiasolutions.com.

Technical and organizational measures baseline

1. **Physical Access Controls:** Crescentia shall take reasonable measures to prevent physical access, such as secured buildings, to prevent unauthorized persons from gaining access to Personal Data.
2. **System Access Controls:** Crescentia shall take reasonable measures to prevent Personal Data from being used without authorization. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.
3. **Data Access Controls:** Crescentia shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorization in the course of processing. Crescentia shall take reasonable measures to implement an access policy under which access to its system environment, to Personal Data and other data by authorized personnel only.
4. **Transmission Controls:** Crescentia shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.
5. **Input Controls:** Crescentia shall take reasonable measures to provide that it is possible to check and establish whether and by whom Personal Data has been entered into data processing systems, modified or removed. Crescentia shall take reasonable measures to ensure that (i) the personal data source is under the control of data exporter; and (ii) Personal Data integrated into Crescentia's systems is managed by secured file transfer from the Crescentia and data subject.

EXHIBIT 3: JURISDICTION SPECIFIC TERMS

California (CCPA):

1.1. The definition of “data subject” includes “Consumer” as defined under CCPA. Any data subject rights, as set forth in Section 6 of this DPA, apply to Consumer rights.

1.2. The definition of “Data Controller” includes “Business” as defined under CCPA. The definition of “Data Processor” includes “Service Provider” as defined under CCPA.

1.3. Crescentia will process, retain, use, and disclose Personal Data only as necessary to provide the Services under the Agreement. Crescentia agrees not to (a) sell or share (as defined by the CCPA) Customer’s Personal Data; (b) retain, use, or disclose Customer’s Personal Data for any commercial purpose (as defined by the CCPA) other than providing the Services; (c) retain, use, or disclose Customer’s Personal Data outside of the scope of the Agreement.

1.4. Crescentia may deidentify (as defined by the CCPA) Customer Personal Data as part of performing the Services in the Agreement, in accordance with limitation on Services Providers under the CCPA. Crescentia shall not re-identify any Customer deidentified Data.

1.5. Crescentia certifies that its Sub-processors, as set forth in Section 7 of this DPA, are Service Providers under CCPA, with whom Crescentia has entered into a written contract that includes terms substantially similar to this DPA.

1.6. If Crescentia becomes aware that it cannot longer meet any of its obligations under the CCPA, Crescentia shall immediately notify Customer.