# Data Processing Agreement

Provisions on data protection and data security for commissioned data processing

concluded by and between

CONTROLLER GmbH
Address

– Controller –
(hereinafter referred to as “the Controller”)

and

Searchmetrics GmbH
Greifswalder Straße 212
10405 Berlin
Germany
email: data.protection@searchmetrics.com

– Processor –
(hereinafter referred to as “the Processor”)

(Both jointly hereinafter referred to as “Parties”)

# Preamble

In order to specify the rights and obligations arising from the contractual data processing relationship in accordance with the statutory obligation under Art. 28 of the GDPR, the contracting Parties conclude the following agreement.

Within the scope of the order, the subsidiary of the Processor, Searchmetrics Inc. a Delaware corporation, with an address at 1100 Park Place, Suite 150, San Mateo, CA 94103, may access the data of the client. Therefore, the Standard Contractual Clauses (Controller to Processor) according to Commission Decision C(2010)593 also apply, and are concluded by the Processor on behalf of Searchmetrics Inc. as data importer with the client as data exporter.

# 1 Subject matter, nature and purpose of processing

(1) Access to the Searchmetrics Software (Sofware as a Service)

(2) Furthermore, the subject matter of the processing arises from the main contract.

An additional processing of personal data of the Controller by the Processor is not intended.

(3) The processing of personal data takes place exclusively in the territory of the Federal Republic of Germany, in a Member State of the European Union or in another contracting state of the Agreement on the European Economic Area. Any transfer to a third country requires the prior documented instruction of the Controller (Art. 28 para. 3 lit. a GDPR) and may only take place if the special requirements of Art. 44 - 49 GDPR are fulfilled.

# 2 Type of personal data, categories of data subjects

(1) Type of data:

☒ Personal master data (name, company address)
☒ Communications data (telephone, e-mail)
☒ Contract data (contractual relationship, product or contractual interests)
☒ Customer history
☒ Contract billing information and payment information

(2) Categories of data subjects:

☒ Employees (who logs into Searchmetrics Software)

# 3 Duration of the commission

(1) The duration of this commission (“Term“) corresponds to the duration of the Main contract and follow up contract

(2) Irrespective of the provisions of the Main contract, the Controller may terminate this Agreement at any time without notice if the Processor has committed a serious breach of the provisions of this Agreement, if the Processor cannot or does not wish to carry out instructions from the Controller, or if the Processor refuses to provide information or to grant the Controller access within the context of inspections, contrary to the contract.

After termination, the Processor may no longer process any personal data of the Controller

# 4 Responsibility and authority to issue instructions

(1) The Controller is responsible for compliance with data protection regulations, in particular for the lawfulness of data transfer to the Processor and for the lawfulness of data processing (Art. 4 no. 7 GDPR). The Processor shall not use the data for any other purpose and in particular shall not be entitled to pass them on to third parties. Copies and duplicates will not be made without the Controller's knowledge. Exceptions shall apply only to the extent specified in paragraph 2 of this clause.

(2) The Processor processes personal data only on documented instruction from the Controller, unless otherwise required under Union law or the law of the Member State to which the Processor is subject. In the event of any contrary obligation, the Processor shall immediately inform the Controller of the corresponding legal requirements before processing.

(3) If the Processor is of the opinion that an instruction infringes data protection regulations, the Processor shall inform the Controller without delay in accordance with Article 28 para. 3 sentence 3 GDPR. The Processor shall be entitled to suspend the execution of the instruction until such instruction has been confirmed or changed.

# 5 Confidentiality

The Processor shall only employ persons for the execution of the work who have committed themselves to confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b GDPR and who have previously been acquainted with the data protection provisions relevant to them. The Processor and any person under the Processor’s control who has access to personal data may process such data exclusively in accordance with the instructions of the Controller, including the powers conferred in this Agreement, unless they are under a statutory obligation to process the data.

# 6 Data Security

(1) The Processor shall take appropriate technical and organisational measures for the appropriate protection of personal data, in accordance with Art. 28 para. 3 lit. c GDPR in conjunction with Art. 32 para. 1 GDPR, in order to guarantee the security of the processing by the Processor. For this purpose, the Processor shall

- ensure the confidentiality, integrity, availability and resilience of systems and services in connection with processing in the long term,
- ensure the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident; and
- maintain a procedure for the regular review, assessment and evaluation of the effectiveness of technical and organisational measures to ensure the safety of processing.

The state of the art, the costs of implementation and the nature, scope and purpose of processing, as well as the risk of varying likelihood and severity of the risk for the rights

and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account.

(2) The contracting Parties agree on the data security measures laid down in **Annex 1 "Technical and organisational measures"** to this Agreement.

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. The safety level may not fall below the specified measures. Significant changes must be documented and communicated to the Controller in writing.

# 7 Engagement of other processors (subcontractors)

(1) For the purposes of this provision, subcontractors shall be processors commissioned by the Processor whose services relate directly to the provision of the main service. This does not include ancillary services used by the Processor, for example, telecommunication services, postal/transport services, and cleaning. However, the Processor is obliged to take appropriate and legally compliant contractual agreements and control measures to guarantee data protection and data security of the Controller's data, even in the case of outsourced ancillary services.

(2) The outsourcing to subcontractors or the change of the existing subcontractor is permitted, as far as:

- the Processor notifies the Controller in advance with a reasonable period of time in writing or in text form of such outsourcing to subcontractors, and
- the Controller does not raise an objection against the planned outsourcing in writing or in text form until the date of handover of the data to the Processor.

(3) A contractual agreement is to be concluded with the subcontractor in accordance with Art. 28 para. 3 and 4 GDPR, which meets the requirements for confidentiality, data protection and data security of this Agreement. The Controller shall be entitled to inspect the Data Protection parts of Processor’s contracts with subcontractors and to demand that the Processor send a copy of these contracts.

(4) The transfer of the Controller's personal data to the subcontractor and the subcontractor's first action shall only be permitted if all the prerequisites for subcontracting are met. The subcontractors approved by the Controller at the time of conclusion of the contract are listed in **Annex 2** to this contract.

(5) If the subcontractor provides the agreed service outside the EU/EEA, the Processor shall ensure the admissibility with regard to data protection law by means of appropriate measures.

# 8 Support in protecting the rights of data subjects

(1) The Processor is obliged to support the Controller with appropriate technical and organisational measures to protect the rights of the data subjects as specified in Art. 12 to 22 GDPR (Art. 28 para. 3 sentence 2 lit. e GDPR). In particular, the Processor shall support the Controller in fulfilling the claims of data subjects for deletion of their personal data in accordance with Article 17 GDPR.

(2) If data subjects are able to exercise the right to data portability against the Controller, the Processor shall ensure that they can receive the data, which they have provided to the Controller, in a structured, commonly used and machine-readable format.

(3) The Processor may only correct, delete or restrict the processing of personal data in accordance with documented instructions from the Controller. The Processor may only provide information to third parties or the persons concerned after prior written consent by the Controller.

(4) If a data subject contacts the Processor directly in order to assert his rights in accordance with Articles 12 to 22 of the GDPR, the Processor will forward the request to the Controller without delay.

# 9 Support with documentation and reporting obligations

(1) If, according to Art. 37 GDPR, Section 38 BDSG-new, the Processor is legally obliged to appoint a data protection officer, the Processor shall inform the Controller of the data protection officer's contact details for the purpose of direct contact. A change of the data protection officer must be reported to the Controller immediately.

As data protection officer for the Processor, Mrs. Katharina Schluckebier,intersoftConsulting ,data.protection@searchmetrics.com has been appointed.

(2) If the Processor becomes aware of a violation of the protection of personal data, he shall immediately notify the Controller of this violation pursuant to Art. 28 para. 3 lit. f, Art. 33 para. 2 GDPR. The same applies if persons employed by the Processor violate this Agreement.

(3) After consultation with the Controller, the Processor shall immediately take the necessary measures to secure the data and to minimise any possible adverse consequences for the data subjects.

(4) The Processor shall support the Controller with all information at his disposal in fulfilling the information obligations in relation to the competent supervisory authority in accordance with Art. 33 GDPR and, if applicable, in relation to the data subjects affected by the violation of the protection of personal data in accordance with Art. 34 GDPR.

(5) The Processor shall support the Controller with all information at his disposal in the data protection impact assessment pursuant to Art. 35 GDPR and, if necessary, in a prior consultation with the competent supervisory authority pursuant to Art. 36 GDPR.

(6) The Processor shall inform the Controller without delay of any checks and measures taken by the supervisory authority insofar as they relate to this Agreement.

# 10 Termination of the commission

(1) At the choice of the Controller, the Processor deletes or returns all the personal data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(2) The Processor shall, without explicit request, prove to the Controller in text form with date indication that he has returned all data carriers and other documents to the

Controller or that he has destroyed or deleted them in accordance with data protection regulations and has therefore not retained any of the Controller's data.

(3) The Processor shall keep any and all documentation which serves as evidence of the orderly and lawful data processing for the Controller beyond the end of the contract. The Processor can return them to the Controller at the end of the contract for his discharge.

## 11 Control rights of the Controller

(1) The Controller is entitled to regularly check the technical and organisational measures as well as compliance with this Agreement and data protection regulations before and during the provision of services relating to processing. For this purpose, the Controller or an authorized auditor may inspect the data processing equipment and the data processing systems of the Processor.

(2) For this purpose, the Processor shall be obliged to grant the Controller, during normal business hours, access to the premises where the Controller's data are physically or electronically processed. The Controller coordinates the inspections with the Processor in such a way that the operating procedures of the Processor are affected as little as possible.

(3) The Processor shall provide the Controller with all necessary information to prove the technical and organisational measures as well as compliance with this Agreement and data protection regulations. This information especially includes current attestations, reports or report extracts from independent bodies (e. g. financial auditors, external experts, IT security or data protection auditors) and suitable certification (e. g. according to the Basic Protection of the BSI – German Federal Office for Information Security). The Processor provides immediately the Controller with specific information on a case-by-case basis.

## 12 Liability

(1) According to Art. 82 para. 1 and 4 GDPR, the Controller and the Processor are liable in their external relationship for the material and immaterial damage suffered by a person as a result of an infringement of the GDPR. If both the Controller and the Processor are responsible for such damage, the Parties are internally liable for this damage in proportion to their share of the responsibility. If, in such a case, a person claims damages from one party in whole or in part, the other party can demand indemnification or indemnity from the other party corresponding to its part of responsibility for the damage.

(2) The Processor is also liable to the Controller for compliance with data protection regulations by the subcontractors, which he uses to fulfil his tasks. The fault of subcontractors shall be attributed to the Processor as if it were his own fault.

(3) The Processor shall assist the Controller with all information at its disposal if the Controller is subject to administrative or criminal proceedings, to the liability of an affected person or a third party or to any other claim in connection with the processing of data with the Processor.

## 13 Final provisions

(1) Data carriers and data records provided to the Processor remain the property of the Controller.

(2) If individual or several clauses of this Agreement should be ineffective, the effectiveness of the remaining agreement is not affected. In the event that individual or several provisions of the contract are invalid, the Parties shall immediately replace the invalid provision with a provision which most closely resembles the invalid provision in terms of commercial interests and data protection.

(3) In the event of a contradiction between the Main Agreement and this Agreement, this Agreement shall take precedence in so far as the contradiction concerns the processing of personal data.

(4) All services provided by the Processor in connection with the fulfilment of his obligations under this Agreement shall be settled with the remuneration from the Main Agreement.

(5) The following Annexes form an integral part of this Agreement:

- Annex 1 „Technical and organisational measures“
- Annex 2 „Approved subcontractors“
- Annex 3 “Standard Contractual Clauses”

| | |
|---|---|
| Place, Date: | Place, Date: |
| Signature of the Controller | Signature of the Processor<br>(Searchmetrics GmbH) |

# Annex 1
# Technical and organisational measures

Clause 6 of the Commissioned Data Processing Agreement refers to this annex for the specification of the technical and organisational measures.

## 1 Confidentiality (Art. 32 para. 1 lit. b GDPR)

### Access control to premises and facilities (physical access control)

| **Access control to premises and facilities**<br>**Unauthorized access to premises and facilities must be prevented, whereas the term is to be understood spatially.** | **existent yes** |
|---|---|
| Authorisation cards | ☒ |
| Electronic access code card / access transponders | ☒ |
| Access authorization concept | ☒ |
| Video surveillance | ☒ |
| Alarm system | ☒ |
| Key management | ☒ |
| Visitor badges | ☒ |
| Escorting of visitors‘ access by our own employees | ☒ |
| Attendance records of visitor accesses | ☒ |
| Securing off-hours by site security service | ☒ |
| Scaled security areas and controlled access | ☒ |
| Special glazing | ☐ |
| Separately secured access to the data center | ☒ |
| Storage of servers in locked rooms | ☒ |
| Locked storage of data carriers or storage in locked rooms | ☒ |
| Storage of data backups (e.g. tapes, CDs) in access-protected safe | ☒ |
| Instruction for issuing keys | ☒ |
| Other: Klicken Sie hier, um Text einzugeben. | ☐ |

## Access Control to Systems (Hardware access control)

| **Access control to systems**<br>**The intrusion of unauthorised persons into the data processing systems or their unauthorized use must be prevented.** | **existent yes** |
|---|---|
| Encryption of networks | ☒ |
| ▪ Encryption algorithms used: | |
| Data processing equipment is under lock (e.g. closed cage for servers) | ☒ |
| Password protection of screens of workstations | ☒ |
| Functional and/or time-limited assignment of user authorizations | ☒ |
| Use of individual passwords | ☒ |
| Automatic locking of user accounts after multiple incorrect password entries | ☐ |
| Automatic password-protected screen locking after inactivity (screen saver) | ☐ |
| Password policy with minimum requirements for password complexity: | |
| ▪ Minimum of 8 characters / upper and lower case, special characters, numbers (of which at least 3 criteria) | ☒ |
| ▪ Prevention of trivial passwords (e.g. Dog1, Dog2, Dog3) | ☒ |
| ▪ Password history (no re-use of the last 5 passwords) | ☒ |
| ▪ Other: | ☐ |
| Hashing of stored passwords | ☒ |
| ▪ Hashes are added with a “Salt“ or “Pepper“ | ☒ |
| Procedure for the assignment of authorisations with the entry of employees | ☒ |
| Procedure for revocation of authorisations due to department change of employees | ☒ |
| Procedure for revocation of authorisations due to exit of employees | ☒ |
| Obligation to confidentiality / data secrecy | ☒ |
| Logging and regular evaluation of system usage | ☒ |
| Controlled destruction of data carriers | ☒ |
| Others: Klicken Sie hier, um Text einzugeben. | ☐ |

## Access control to data (software access control)

| **Access control to data**<br>**Unauthorised activities in data processing systems outside of assigned authorisations must be prevented.** | **existent**<br>**yes** |
|---|---|
| Definition of access authorization, authorization concept | ☒ |
| Procedure for the recovery of data from backups (who, when, on whose request) | ☒ |
| Regular review of authorisations | ☒ |
| Restriction of free and uncontrolled query options for databases | ☐ |
| Regular evaluation of logs (log files) | ☒ |
| Partial access to data stocks and functions (Read, Write, Execute) | ☒ |
| Logging of file access | ☒ |
| Logging of file deletion | ☒ |
| Use of appropriate security systems (software/hardware)? | |
| ▪ Virus scanner | ☒ |
| ▪ Firewalls | ☒ |
| ▪ SPAM-Filter | ☒ |
| ▪ Intrusion prevention (IPS) | ☐ |
| ▪ Intrusion detection (IDS) | ☒ |
| ▪ Software for Security Information and Event Management (SIEM) | ☒ |
| Encrypted storage of data | |
| ▪ Encryption algorithms used: | ☒ |
| ▫ e.g. AES, RSA: | ☒ |
| ▪ Hash function used: | ☒ |
| ▫ SHA2 (256, 384, 512 bit) | ☒ |
| ▫ SHA3 | ☒ |
| ▫ Hashes are added with a “Salt“ or “Pepper“ | ☒ |
| Others: Klicken Sie hier, um Text einzugeben. | ☐ |

## Separation Control

| **Separation control**<br>**Data collected for different purposes must also be processed separately.** | **existent**<br>**yes** |
|---|---|
| Separation of customer data (multi-client capability of systems) | ☒ |
| File separation in databases | ☒ |
| Logical data separation (e.g. based on customer or client IDs) | ☒ |
| Processing of the data of different customers by different employees of the contractor | ☐ |
| Backups of the client data on separate data carriers (without data of other customers) | ☐ |
| Authorization concept that takes into account a separate processing of data of different customers | ☐ |
| Separation of functions | ☒ |
| Separation of development, test and production system | ☒ |
| Others: please insert | ☐ |
| | |

## Pseudonymisation

| **(Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)**<br>**The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without further information, provided that such additional information is kept separately and subject to appropriate technical and organisational measures** | **existent**<br>**yes** |
|---|---|
| Measures: | ☐ |
| | |

# 2 Integrity (Art. 32 para. 1 lit. b GDPR)

## Control of transmission

| **Control of transmission**<br>**Aspects of the transfer (transmission) of personal data are to be regulated: electronic transfer, data transport as well as their control.** | **existent yes** |
|---|---|
| What is the mode of transmission of data between Controller and third parties? | |
| ▪ Citrix connection (128 bit encrypted) | ☐ |
| ▪ VPN connection (IP-Sec) | ☒ |
| ▪ Email with encrypted ZIP file attached | ☐ |
| ▪ Data exchange via https connection | ☒ |
| ▪ Other mode of transmission: | ☐ |
| ▫ Encryption algorithm used: | ☒ |
| ▫ Hash function used: | ☒ |
| - Hashes are added with a “Salt“ or “Pepper“ | ☒ |
| Secured entrance for supply and delivery | ☒ |
| Documented management of data carriers, inventory control | ☒ |
| Definition of the areas in which data carriers are stored | ☒ |
| Encryption of data carriers with confidential data | ☒ |
| Encryption of laptop hard disks | ☒ |
| Encryption of mobile data carrier | ☒ |
| Controlled destruction of data: | ☒ |
| Data carrier disposal – Secure deletion of data carriers: | |
| ▪ Physical destruction (e.g. shredder with particle cut - 1000 mm² max.) | ☐ |
| ▪ Others: e.g. overwriting of tapes and hard drives | ☒ |
| Paper disposal: Secure destruction of paper documents: | |
| ▪ Closed metal containers (German so-called “Datenschutztonnen”), disposal by service provider | ☒ |
| ▪ Shredder according to DIN 66399 | ☒ |

| | |
|---|---|
| ▫ Security level: | ☐ |
| Regulations on duplications | ☐ |
| Backup copies of data carriers that will have to be transferred | ☒ |
| Documentation of the bodies to which transmissions are planned and the means of transmission | ☒ |
| Packaging and shipping instructions, encrypted email dispatch | ☒ |
| Control of completeness and correctness | ☒ |
| Others: Klicken Sie hier, um Text einzugeben. | ☐ |

## Entry control

| **Entry control**<br>**Traceability and documentation of data administration and maintenance must be guaranteed.** | **existent**<br>**yes** |
|---|---|
| Labelling of collected data | ☒ |
| Definition of user authorisations (profiles) | ☒ |
| Differentiated user authorisations: | ☒ |
| Read, modify, delete | ☒ |
| Partial access to data or functions | ☒ |
| Field access in databases | ☐ |
| Organisational definition of input responsibilities | ☒ |
| Logging of entries / deletions | ☒ |
| Log analysis system | ☒ |
| Obligation to confidentiality / data secrecy | ☒ |
| Log concept going beyond OS standard | ☒ |
| Dedicated log server | ☒ |
| Control of access authorisations to log servers (log admin) | ☒ |
| Regulations on retention periods for auditing/verification purposes | ☒ |
| Others: Klicken Sie hier, um Text einzugeben. | ☐ |

# 3 Availability and Resilience (Art. 32 para. 1 lit. b GDPR)

### Availability control

| **Availability control**<br>**The data must be protected against accidental destruction or loss.** | **existent**<br>**yes** |
|---|---|
| Data protection and backup concept | ☒ |
| Carrying out data protection and backup concept. | ☒ |
| Restriction of access to server rooms to authorised personnel | ☒ |
| Fire alarm systems in server rooms | ☒ |
| Smoke detectors in server rooms | ☒ |
| Waterless firefighting systems in server rooms | ☒ |
| Air-conditioned server rooms | ☒ |
| Lightning / overvoltage protection | ☒ |
| Water sensors in server rooms | ☒ |
| Server rooms in separate fire compartments | ☒ |
| Keep backup systems in separate rooms and fire compartment | ☒ |
| Ensure technical readability of backup storage media for the future | ☒ |
| Storage of archive storage media under necessary storage conditions (air conditioning, protection requirements, etc.) | ☒ |
| $CO^2$ fire extinguishers in the immediate vicinity of the server rooms | ☒ |
| Agreement regarding transfer of the (data) backups | ☒ |
| Emergency plan (e.g. water, fire, explosion, threat of attacks, crash, earthquake) | ☒ |
| Observation of the influence of adjacent buildings | ☒ |
| Vulnerability analysis (terrain protection, building protection, intrusion into computers, computer networks) | ☒ |
| Storage of data in data storage cabinets, safes | ☒ |
| UPS system (uninterruptible power supply) | ☒ |
| Power generator | ☒ |
| Other: Klicken Sie hier, um Text einzugeben. | ☐ |

## Resistance and reliability control

| **Resistance and reliability control**<br>**Systems must be able to cope with risk-related changes and must be tolerant and able to compensate disruptions.** | **existent**<br>**yes** |
|---|---|
| Alternative data centers available (Hot- or Cold-Stand-by?): Hot | ☒ |
| Redundant power supply | ☒ |
| Redundant UPS system | ☒ |
| Redundant power generators | ☒ |
| Redundant air conditioning | ☒ |
| Redundant fire fighting | ☒ |
| Other redundant systems / procedures: | ☐ |
| Hard disk mirroring | ☒ |
| Computer Emergency Response Team (CERT) | ☐ |
| Loadbalancer | ☒ |
| Data storage on RAID systems (RAID 1 and higher) | ☒ |
| Delimitation of critical components | ☒ |
| Performance of penetration tests | ☒ |
| System hardening (deactivation of non-required components) | ☒ |
| Immediate and regular activation of available software and firmware updates | |
| ▪ Identification of the different devices that make up the network and identification of their hardware version as well as their current software and firmware versions. | ☒ |
| ▪ Communication channel with manufacturers to stay up-to-date on any new updates and patches released for the devices owned. | ☒ |
| ▪ Definition of time periods in which the updates shall be implemented (e.g. periods of lower operations, maintenance times, etc.) | ☒ |
| ▪ Use of redundant systems to maintain operations while main devices are being updated. | ☒ |
| ▪ Progressive deployment of updates / patches to detect any issues early without affecting multiple devices. | ☒ |
| ▪ Specify a testing period to verify the correct implementation of the update and ensure that operations continue to run smoothly with the new updates. | ☒ |

| | |
|---|---|
| Security is included as a main consideration during the design phase of the systems. | |
| ▪ Definition of security measures to protect and validate communication between system components. | ☒ |
| ▪ Limitation of authorizations on a need-to-know basis. | ☒ |
| ▪ External contractors (service providers) and maintenance personnel must have a specific access, which must only be active during the intervention and remain disabled the rest of the time. | ☒ |
| Periodic security training and awareness campaign within the organisation | |
| ▪ Awareness campaigns to inform users of the security concepts of specific systems and traditional IT systems | ☒ |
| ▪ Specific security training to teach how to apply security measures and behaviours on the daily processes with the least impact possible. | ☐ |
| Take out cyber-insurance | |
| ▪ Identification of the devices, assets, and network systems within the organisation's infrastructure. | ☒ |
| ▪ Carrying out a risk analysis considering all these systems, devices and assets identified to determine the threats they are exposed to, their likelihood and impact. | ☒ |
| Others: Klicken Sie hier, um Text einzugeben. | ☐ |

# 4 Procedures for a regular testing, assessing and evaluating (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

### Control procedures

| **Control procedures**<br>**A procedure is to be implemented for regularly testing, assessing and evaluating the effectiveness of the data security measures.** | **existent**<br>**yes** |
|---|---|
| Records of processing activities are reviewed and at least updated annually (where applicable). | ☒ |
| Notification of new/changed data processing procedures to the Data Protection Officer. | ☒ |
| Notification of new/changed data processing procedures to the IT Security Officer. | ☒ |
| Processes for reporting new/changed procedures are documented. | ☒ |
| Privacy-friendly settings are selected. | ☒ |

| | |
|---|---|
| Security measures are subject to regular internal audits | ☒ |
| In the event of a negative outcome of the above-mentioned review, the security measures are adjusted, renewed and implemented in line with the risks involved. | ☒ |
| There is a process to prepare for security breaches (attacks) and system failures as well as to identify, contain, eliminate and recover them (incident response process). | ☒ |
| Others: Klicken Sie hier, um Text einzugeben. | ☐ |

## Control of instructions

| **Control of instructions**<br>**It must be ensured that commissioned data processing by service providers (subcontractors) is only processed in accordance with the instructions of the Processor.** | **existent**<br>**yes** |
|---|---|
| Contracts according to the requirements of Sec. 11 BDSG / Art. 28 GDPR | ☒ |
| Centralized registration of commissioned service providers (contract management) | ☒ |
| Regular monitoring of the technical and organisational measures taken by the service providers (during contract period) | ☒ |
| On-site inspection at the services providers' premises and facilities | ☐ |
| Auditing of the contractor's data security concept | ☐ |
| Inspection of existing IT security certificates of contractors | ☒ |
| Others: Klicken Sie hier, um Text einzugeben. | ☐ |

# Annex 2
# Approved subcontractors

The Controller agrees to the commissioning of the following subcontractors, but only under the condition of a contractual agreement in accordance with Sections 11, 9 BDSG / Art. 28 para. 2-4 GDPR:

| Company (subcontractor), address | Processing site | Type of service |
|---|---|---|
| Amazon Web Services Inc. | 410 Terry Avenue North, Seattle WA 98109 United States | Hosting data servers in Ireland |
| Hetzner | Industriestr. 25 91710 Gunzenhausen Germany | Datacenter Provider data servers in Germany |
| Telekom Deutschland GmbH | Landgrabenweg 151 53227 Bonn Germany | Microsoft Datacenter Provider, data servers in Ireland |
| Searchmetrics Inc. | 1100 Park Place – Suite 150 San Mateo, CA 94403 United States | Product and Service Support, data servers in Europe |
| Strikedeck Inc. | 830 Stewart Dr, Sunnyvale, CA 94085, Sunnyvale, CA 94085 United States | Data bank for product service, data servers in Ireland |
| Marketo Inc. | Mariners Island BLVD, Suite 500 San Mateo, CA 94404 United States | Client Relationship Database Data servers in London |
| Oracle Netsuite | Oracle America, Inc. 500 Oracle Parkway Redwood Shores, California USA | Datacenter, data servers in Ireland and the Netherlands |
| Celigo Inc | Celigo, Inc., 1820 Gateway Drive #260 San Mateo, CA USA | Datacenter, data server in Germany |
| Salesforce.com Deutschland GmbH | Kurfürstendamm 194 10707 Berlin Germany | Datacenter, Data server in Germany |
| Auth0 Inc. | 10800 NE 8th St #700, Bellevue, WA<br><br>USA | Datacenter,<br><br>Data server in Germany |

# Annex 3:

**Commission Decision C(2010)593 „Standard Contractual Clauses (processors)“**

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
**Unit C.3: Data protection**

---

**Commission Decision C(2010)593**
**Standard Contractual Clauses (processors)**

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

- *Clause 1*

- ***Definitions***

For the purposes of the Clauses:

(a) *'personal data'*, *'special categories of data'*, *'process/processing'*, *'controller'*, *'processor'*, *'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

- *Clause 2*

- ***Details of the transfer***

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

- *Clause 3*

- ***Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal

obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

- *Clause 4*

- ***Obligations of the data exporter***

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

- *Clause 5*

- ***Obligations of the data importer***[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

---

2 Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

- *Clause 6*

- ***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The

liability of the subprocessor shall be limited to its own processing operations under the Clauses.

- *Clause 7*

- ***Mediation and jurisdiction***

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

- *Clause 8*

- ***Cooperation with supervisory authorities***

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

- *Clause 9*

- ***Governing Law***

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely: Germany

- *Clause 10*

- ***Variation of the contract***

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

- *Clause 11*

- ***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely: Germany

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

- *Clause 12*

- ***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.