GENERAL TERMS AND CONDITIONS FOR osapiens CLOUD SERVICES ("GTC")

1. DEFINITIONS

Capitalized terms used in this document are defined in the Glossary.

2. USAGE RIGHTS AND RESTRICTIONS

2.1 Grant of Rights.

osapiens grants to Customer a non-exclusive, non-transferable and world-wide right to use the Cloud Service (including its implementation and configuration), Cloud Materials and Documentation solely for Customer's and its Affiliates' internal business operations. Permitted uses and restrictions of the Cloud Service also apply to Cloud Materials and Documentation.

2.2 Authorized Users.

Customer may permit Authorized Users to use the Cloud Service. Usage is limited to the Usage Metrics and volumes stated in the Order Form. Access credentials for the Cloud Service may not be used by more than one individual, but may be transferred from one individual to another if the original user is no longer permitted to use the Cloud Service. Customer is responsible for breaches of the Agreement caused by Authorized Users.

2.3 Acceptable Use Policy.

With respect to the Cloud Service, Customer will not:

(a) except to the extent such rights cannot be validly waived by law disassemble, decompile, reverse-engineer, copy, translate or make derivative works,

(b) transmit any content or data that is unlawful or infringes any intellectual property rights, or (c) circumvent or endanger its operation or security.

2.4 Verification of Use.

Customer will monitor its own use of the Cloud Service and report any use in excess of the Usage Metrics and volume. osapiens may monitor use to verify compliance with Usage Metrics, volume and the Agreement.

2.5 Suspension of Cloud Service.

osapiens may suspend or limit use of the Cloud Service if continued use may result in material harm to the Cloud Service or its users. osapiens will promptly notify Customer of the suspension or limitation. osapiens will limit a suspension or limitation in time and scope as reasonably possible under the circumstances.

2.6 Third Party Web Services.

The Cloud Service may include integrations with web services made available by third parties (other than its Affiliates) that are accessed through the Cloud Service and subject to terms and conditions with those third parties. These third party web services are not part of the Cloud Service and the Agreement does not apply to them.

2.7 Mobile Access to Cloud Service.

Authorized Users may access certain Cloud Services through mobile applications obtained from third-party websites such as Android or Apple app store. The use of mobile applications may be governed by the terms and conditions presented upon download/access to the mobile application and not by the terms of the Agreement.

2.8 On-Premise Components.

The Cloud Service may include on-premise components that can be downloaded and installed (including updates) by Customer. The Software Service Availability SLA does not apply to these components

3. OSAPIENS RESPONSIBILITIES

3.1 Provisioning.

osapiens provides access to the Cloud Service as described in the Agreement.

3.2 Support.

osapiens provides support for the Cloud Service as referenced in the Order Form.

3.3 Security.

osapiens will implement and maintain appropriate technical and organizational measures to protect the personal data processed by osapiens as part of the Cloud Service as described in the Data Processing Agreement for osapiens Cloud Services incorporated into the Order Form in compliance with applicable data protection law.

3.4 Modifications.

(a) The Cloud Service and osapiens Policies may be modified by osapiens. osapiens will inform Customer of modifications by email, the support portal, release notes, Documentation or the Cloud Service. The information will be delivered by email if the modification is not solely an enhancement. Modifications may include optional new features for the Cloud Service, which Customer may use subject to the then-current Supplement and Documentation.

(b) If Customer establishes that a modification is not solely an enhancement and materially reduces the Cloud Service, Customer may terminate its subscriptions to the affected Cloud Service by providing written notice to osapiens within thirty days after receipt of osapiens' informational notice.

3.5 Analyses and Improvements of Cloud Service.

osapiens and osapiens Affiliates may use the Customer Data and information derived from Customer's use of the Cloud Service and Consulting Services to create analyses, as set forth below ("**Analyses**"), and, based on the Analyses, to further improve the Cloud Service, to derive correlations from the Customer Data and to use the subsequently improved Cloud Service at its own discretion. Analyses will anonymize and aggregate information, therefore, contain neither Customer Data nor Personal Data and will be treated as Cloud Materials. The Customer Data will not be shared with third parties and the Customer remains the owner of the Customer Data.

Analyses may be used for the following purposes:

(a) product improvement (in particular, product features and functionality, workflows and user interfaces) and development of new osapiens products and services,

(b) improving resource allocation and support,

(c) internal demand planning,

(d) training and developing machine learning algorithms,

(e) improving product performance,

(f) verification of security and data integrity

(g) identification of industry trends and developments, creation of indices and anonymous benchmarking.

(h) Finding patterns and correlations for artificial intelligence purposes

Unless otherwise agreed, personal data contained in Customer Data is only used to provide the Cloud Service and Consulting Services in accordance with this GTC.

4. CUSTOMER AND PERSONAL DATA

4.1 Customer Data.

Customer is responsible for the Customer Data and entering it into the Cloud Service. Customer grants to osapiens (including its Affiliates and subcontractors) a nonexclusive right to process Customer Data solely to provide and support the Cloud Service.

4.2 Personal Data.

Customer will collect and maintain all personal data contained in the Customer Data in compliance with applicable data privacy and protection laws.

4.3 Security.

Customer will maintain reasonable security standards for its Authorized Users' use of the Cloud Service. Customer will not conduct or authorize penetration tests of the Cloud Service without advance approval from osapiens.

4.4 Access to Customer Data.

(a) During the Subscription Term, Customer can access its Customer Data at any time.

(b) Before the Subscription Term expires, Customer may use osapiens' self-service export tools (as available) to perform a final export of Customer Data from the Cloud Service.

(c) At the end of the Agreement, osapiens will delete the Customer Data remaining on servers hosting the Cloud Service unless applicable law requires retention. Retained data is subject to the confidentiality provisions of the Agreement.

(d) In the event of third party legal proceedings relating to the Customer Data, osapiens will cooperate with Customer and comply with applicable law (both at Customer's expense) with respect to handling of the Customer Data.

5. FEES AND TAXES

5.1 Fees and Payment.

Customer will pay fees as stated in the Order Form. After prior written notice, osapiens may suspend Customer's use of the Cloud Service until payment is made. Customer cannot withhold, reduce or set-off fees owed nor reduce Usage Metrics during the Subscription Term. All Order Forms are non-cancellable and fees non-refundable.

5.2 Taxes.

Fees and other charges imposed under an Order Form will not include taxes, all of which will be for Customer's account. Customer is responsible for all taxes, other than osapiens' income and payroll taxes. Customer must provide to osapiens any direct pay permits or valid tax-exempt certificates prior to signing an Order Form. If osapiens is required to pay taxes (other than its income and payroll taxes), Customer will reimburse osapiens for those amounts and indemnify osapiens for any taxes and related costs paid or payable by osapiens attributable to those taxes.

6. TERM AND TERMINATION

6.1 Term.

The Subscription Term is as stated in the Order Form.

6.2 Termination.

A party may terminate the Agreement:

(a) upon thirty days written notice of the other party's material breach unless the breach is cured during that thirty day period

(b) as permitted under Sections 3.4(b), 7.3(b), 7.4(c), or 8.1 (with termination effective thirty days after receipt of notice in each of these cases), or

(c) subject to applicable law, immediately if the other party files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors, or otherwise materially breaches Sections 11 or 12.6.

6.3 Refund and Payments.

For termination by Customer or an 8.1 termination, Customer will be entitled to:

(a) a pro-rata refund in the amount of the unused portion of prepaid fees for the terminated subscription calculated as of the effective date of termination, and

(b) a release from the obligation to pay fees due for periods after the effective date of termination.

6.4 Effect of Expiration or Termination.

Upon the effective date of expiration or termination of the Agreement:

(a) Customer's right to use the Cloud Service and all osapiens Confidential Information will end,

(b) Confidential Information of the disclosing party will be returned or destroyed as required by the Agreement, and

(c) Termination or expiration of the Agreement does not affect other agreements between the parties.

6.5 Survival.

Sections 1, 5, 6.3, 6.4, 6.5, 8, 9, 10, 11, and 12 will survive the expiration or termination of the Agreement.

7. WARRANTIES

7.1 Compliance with Law.

Each party warrants its current and continuing compliance with all laws and regulations applicable to it in connection with:

(a) in the case of osapiens, the operation of osapiens' business as it relates to the Cloud Service, and (b) in the case of Customer, the Customer Data and Customer's use of the Cloud Service.

7.2 Good Industry Practices.

osapiens warrants that it will provide the Cloud Service:

(a) in substantial conformance with the Documentation; and

(b) with the degree of skill and care reasonably expected from a skilled and experienced global supplier of services substantially similar to the nature and complexity of the Cloud Service.

7.3 Remedy.

Customer's sole and exclusive remedies and osapiens' entire liability for breach of the warranty under Section 7.2 will be:

(a) the re-performance of the deficient Cloud Service, and

(b) if osapiens fails to re-perform, Customer may terminate its subscription for the affected Cloud Service. Any termination must occur within three months of osapiens' failure to re-perform.

7.4 Software Service Availability.

(a) osapiens warrants to maintain an average monthly Software Service Availability for the production system of the Cloud Service as defined in the applicable service level agreement or Supplement ("SLA").

(b) Customer's sole and exclusive remedy for osapiens' breach of the SLA is the issuance of a credit in the amount described in the SLA. Customer will follow

osapiens' posted credit claim procedure. When the validity of the service credit is confirmed by osapiens in writing (email permitted), Customer may apply the credit to a future invoice for the Cloud Service or request a refund for the amount of the credit if no future invoice is due.

(c) In the event osapiens fails t o meet the SLA (i) for four consecutive months, or (ii) for five or more months during any twelve months period, or (iii) at a Software Service Availability level of at least 95% for one calendar month, Customer may terminate its subscriptions for the affected Cloud Service by providing osapiens with written notice within thirty days after the failure.

7.5 Warranty Exclusions.

The warranties in Sections 7.2 and 7.4 will not apply if:

(a) the Cloud Service is not used in accordance with the Agreement or Documentation,

(b) any non-conformity is caused by Customer, or by any product or service not provided by osapiens, or

(c) the Cloud Service was provided for no fee.

7.6 Disclaimer.

Except as expressly provided in the Agreement, neither osapiens nor its subcontractors make any representation or warranties, express or implied, statutory or otherwise, regarding any matter, including the merchantability, suitability, originality, or fitness for a particular use or purpose, non-infringement or results to be derived from the use of or integration with any products or services provided under the Agreement, or that the operation of any products or services will be secure, uninterrupted or error free. Customer agrees that it is not relying on delivery of future functionality, public comments or advertising of osapiens or product roadmaps in obtaining subscriptions for any Cloud Service.

8. THIRD PARTY CLAIMS

8.1 Claims Brought Against Customer.

In the event a claim is made or likely to be made, osapiens may (i) procure for Customer the right to continue using the Cloud Service under the terms of the Agreement, or (ii) replace or modify the Cloud Service to be non-infringing without a material decrease in functionality. If these options are not reasonably available, osapiens or Customer may terminate Customer's subscription to the affected Cloud Service upon written notice to the other.

8.2 Claims Brought Against osapiens.

Customer will defend osapiens against claims brought against osapiens, its Affiliates and subcontractors by any third party related to Customer Data.

9. LIMITATION OF LIABILITY

9.1 Unlimited Liability.

Neither party will exclude or limit its liability for damages resulting from:

(a) the parties' obligations under Section 8.1 and 8.2,

(b) unauthorized use or disclosure of Confidential Information,

(c) either party's breach of its data protection and security obligations that result in an unauthorized use or disclosure of personal data,

(d) gross negligence or willful misconduct, or

(e) any failure by Customer to pay any fees due under the Agreement.

9.2 Liability Cap.

Subject to Sections 9.1 and 9.3, the maximum aggregate liability of either party (or its respective Affiliates or osapiens' subcontractors) to the other or any other person or entity for all events (or series of connected events) arising in any twelve month period will not exceed the annual subscription fees paid for the applicable Cloud Service directly causing the damage for that twelve month period. Any "twelve month period" commences on the Subscription Term start date or any of its yearly anniversaries.

9.3 Exclusion of Damages. Subject to Section 9.1:

(a) neither party (nor its respective Affiliates or osapiens' subcontractors) will be liable to the other party for any consequential, or indirect damages, loss of good will or business profits, work stoppage or punitive damages, and

(b) osapiens will not be liable for any damages caused by any Cloud Service provided for no fee.

9.4 Risk Allocation.

The Agreement allocates the risks between osapiens and Customer. The fees for the Cloud Service and Consulting Services reflect this allocation of risk and limitations of liability.

10. INTELLECTUAL PROPERTY RIGHTS

10.1 osapiens Ownership.

osapiens, their Affiliates or licensors own all intellectual property rights in and related to the Cloud Service, Cloud Materials, Documentation, Consulting Services, design contributions, related knowledge or processes, and any derivative works of them. All rights not expressly granted to Customer are reserved to osapiens, and its licensors.

10.2 Customer Ownership.

Customer retains all rights in and related to the Customer Data. osapiens may use Customer-provided trademarks solely to provide and support the Cloud Service.

10.3 Non-Assertion of Rights.

Customer covenants, on behalf of itself and its successors and assigns, not to assert against osapiens, their Affiliates or licensors, any rights, or any claims of any rights, in any Cloud Service, Cloud Materials, Documentation, or Consulting Services.

11. CONFIDENTIALITY

11.1 Use of Confidential Information.

(a) The receiving party will protect all Confidential Information of the disclosing party as strictly confidential to the same extent it protects its own Confidential Information, and not less than a reasonable standard of care. Receiving party will not disclose any Confidential Information of the disclosing party to any person other than its personnel, representatives or Authorized Users whose access is necessary to enable it to exercise its rights or perform its obligations under the Agreement and who are under obligations of confidentiality substantially similar to those in Section 11. Customer will not disclose the Agreement or the pricing to any third party.

(b) Confidential Information of either party disclosed prior to execution of the Agreement will be subject to Section 11.

(c) In the event of legal proceedings relating to the Confidential Information, the receiving party will cooperate with the disclosing party and comply with applicable

law (all at disclosing party's expense) with respect to handling of the Confidential Information.

11.2 Exceptions.

The restrictions on use or disclosure of Confidential Information will not apply to any Confidential Information that:

(a) is independently developed by the receiving party without reference to the disclosing party's Confidential Information,

(b) is generally available to the public without breach of the Agreement by the receiving party,

(c) at the time of disclosure, was known to the receiving party free of confidentiality restrictions, or

(d) the disclosing party agrees in writing is free of confidentiality restrictions.

11.3 Publicity.

Osapiens may use Customer's name and logo in customer listings, its own web page or quarterly calls with its investors. Also, if mutually agreed by the parties, osapiens might include customer as part of marketing efforts (including reference calls and stories, press testimonials, site visits, osapiens' event participation). Customer agrees that osapiens may share high level information on Customer with its Affiliates for marketing and training purposes.

12. MISCELLANEOUS

12.1 Severability.

If any provision of the Agreement is held to be invalid or unenforceable, the invalidity or unenforceability will not affect the other provisions of the Agreement.

12.2 No Waiver.

A waiver of any breach of the Agreement is not deemed a waiver of any other breach.

12.3 Electronic Signature.

Signatures in any electronic form (including email or dedicated signature solutions) are deemed original signatures.

12.4 Regulatory Matters.

osapiens Confidential Information is subject to export control laws of various countries, including the laws of the United States and Germany. Customer will not submit osapiens Confidential Information to any government agency for licensing consideration or other regulatory approval, and will not export osapiens Confidential Information to countries, persons or entities if prohibited by export laws.

12.5 Notices.

All notices will be in writing and given when delivered to the address set forth in an Order Form. Notices by osapiens relating to the operation or support of the Cloud Service and those under Sections 3.4 and 5.1 may be in the form of an electronic notice to Customer's authorized representative or administrator identified in the Order Form.

12.6 Assignment.

Without osapiens' prior written consent, Customer may not assign or transfer the Agreement (or any of its rights or obligations) to any party. osapiens may assign the Agreement to any of its Affiliates.

12.7 Subcontracting.

osapiens may subcontract parts of the Cloud Service or Consulting Services to third parties. osapiens is responsible for breaches of the Agreement caused by its subcontractors.

12.8 Relationship of the Parties.

The parties are independent contractors, and no partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties is created by the Agreement.

12.9 Force Majeure.

Any delay in performance (other than for the payment of amounts due) caused by conditions beyond the reasonable control of the performing party is not a breach of the Agreement. The time for performance will be extended for a period equal to the duration of the conditions preventing performance.

12.10 Governing Law.

This Agreement and any claims relating to its subject matter is subject exclusively to the law of the Federal Republic of Germany, excluding the provisions of the UN Convention on Contracts for the International Sale of Goods (CISG) and international private law.
The exclusive place of jurisdiction for all disputes arising from or in connection with this contract or its validity is Mannheim

12.11 Entire Agreement.

The Agreement constitutes the complete and exclusive statement of the agreement between osapiens and Customer in connection with the parties' business relationship related to the subject matter of the Agreement. All previous representations, discussions, and writings (including any confidentiality agreements) are merged in and superseded by the Agreement and the parties disclaim any reliance on them. The Agreement may be modified solely in writing signed by both parties, except as permitted under Section 3.4. An Agreement will prevail over terms and conditions of any Customer-issued purchase order, which will have no force and effect, even if osapiens accepts or does not otherwise reject the purchase order.

Glossary

1.1 "Affiliate" of a party means any legal entity in which a party directly or indirectly, holds more than fifty percent (50%) of the entity's shares or voting rights. Any legal entity will be considered an Affiliate as long as that interest is maintained.

1.2 "Agreement" means an Order Form and documents incorporated into an Order Form.

1.3 "Authorized User" means any individual to whom Customer grants access authorization to use the Cloud Service that is an employee, agent, contractor or representative of

(a) Customer,

(b) Customer's Affiliates, and/or

(c) Customer's and Customer's Affiliates' Business Partners.

1.4 "Business Partner" means a legal entity that requires use of a Cloud Service in connection with Customer's and its Affiliates' internal business operations. These may include customers, distributors, service providers and/or suppliers of Customer.

1.5 "Cloud Service" means any distinct, subscription-based, hosted, supported and operated ondemand solution provided by osapiens under an Order Form.

1.6 "Cloud Materials" mean any materials provided or developed by osapiens (independently or with Customer's cooperation) in the course of performance under the Agreement, including in the delivery of any support or Consulting Services to Customer. Cloud Materials do not include the Customer Data, Customer Confidential Information or the Cloud Service.

1.7 "Confidential Information" means

(a) with respect to Customer: (i) the Customer Data, (ii) Customer marketing and business requirements, (iii) Customer implementation plans, and/or (iv) Customer financial information, and

(b) with respect to osapiens: (i) the Cloud Service, Documentation, Cloud Materials and analyses under Section 3.5, and (ii) information regarding osapiens research and development, product offerings, pricing and availability.

(c) Confidential Information of either osapiens or Customer also includes information which the disclosing party protects against unrestricted disclosure to others that (i) the disclosing party or its representatives designates as confidential at the time of disclosure, or (ii) should reasonably be understood to be confidential given the nature of the information and the circumstances surrounding its disclosure.

1.8 **"Consulting Services"** means professional services, such as implementation, configuration, custom development and training, performed by osapiens' employees or subcontractors as described in any Order Form and which are governed by the Supplement for Consulting Services or similar agreement.

1.9 **"Customer Data"** means any content, materials, data and information that Authorized Users enter into the production system of a Cloud Service or that Customer derives from its use of and stores in the Cloud Service (e.g. Customer-specific reports). Customer Data and its derivatives will not include osapiens' Confidential Information.

1.10 **"Documentation"** means osapiens' then-current technical and functional documentation as well as any roles and responsibilities descriptions, if applicable, for the Cloud Service which is made available to Customer with the Cloud Service.

1.11 **"Order Form"** means the ordering document for a Cloud Service that references the GTC.

1.12 **"osapiens Policies"** means the operational guidelines and policies applied by osapiens to provide and support the Cloud Service as incorporated in an Order Form.

1.13 **"Subscription Term"** means the term of a Cloud Service subscription identified in the applicable Order Form, including all renewals.

1.14 **"Supplement"** means the supplemental terms and conditions that apply to the Cloud Service and that are incorporated in an Order Form.

1.15 **"Usage Metric"** means the standard of measurement for determining the permitted use and calculating the fees due for a Cloud Service as set forth in an Order Form.

SLA and SUPPORT POLICY FOR osapiens CLOUD SERVICES

This SLA and Support Policy for osapiens Cloud Services is part of an Agreement for certain osapiens Cloud Services ("Agreement") between osapiens and Customer.

DEFINITIONS

1.1. **"Credit"** means 2% of Quarterly Subscription Fees for each 1% below the System Availability SLA, not to exceed 100% of Monthly Subscription Fees.

1.2. "**Downtime**" means the Total Minutes in the Month during which the production version of the Cloud Service is not available, except for Excluded Downtimes.

1.3. "**Excluded Downtime**" means the Total Minutes in the Month attributable to a Maintenance Window; or any Major Upgrade Window for which the Customer has been notified at least 48 hours in advance or unavailability due to **Force Majeur events**

1.4. "**Force Majeur events"** factors outside of osapiens' reasonable control which could not have been avoided even if reasonable care had been exercised.

1.5. "**Maintenance Window**" means the weekly maintenance windows for the Cloud Service identified https://support.osapiens.com osapiens may update the Maintenance Window from time to time in accordance with the Agreement.

1.6. **"Major Upgrade Window"** means the extended upgrade maintenance windows for the Cloud Service identified in https://support.osapiens.com osapiens may update the Major Upgrade Window from time to time in accordance with the Agreement.

1.7. "**Month**" means a calendar month.

1.8. "Quarter" means each calendar period of 3 consecutive Months starting on 1 January, 1 April, 1 July and 1 October

1.9. "**Monthly Subscription Fees**" means the monthly (or 1/12 of the annual fee) subscription fees paid for the applicable Cloud Service which did not meet the System Availability SLA.

1.10. **"System Availability Percentage"** is calculated and defined as follows:

$$\left(\frac{\text{Total Minutes in the Quarter - Excluded Downtime - Downtime}}{\text{Total Minutes in the Quarter - Excluded Downtime}}\right) * 100$$

1.11. "**System Availability SLA"** means an average 99.5% (Standard) or 99.8% (Extended) System Availability Percentage during each Quarter for the production version of the Cloud Service.

1.12. "**Total Minutes in the Quarter**" are measured 24 hours at 7 days a week during a Quarter.

1.13. "**UTC**" means Coordinated Universal Time standard being the start time for the applicable Maintenance Window and Major Upgrade Window.

SYSTEM AVAILABILITY SLA AND CREDITS

2.1. Credit

If osapiens fails to meet the System Availability SLA for a particular Quarter, Customer may claim a Credit, which Customer may apply to a future invoice relating to the Cloud Service that did not meet the System Availability SLA (subject to Sections 2.1.1 and 2.1.2 below).

2.1.1. Claims for a Credit must be made in good faith and through a documented submission of a support case within thirty (30) business days after the end of the relevant Quarter in which osapiens did not meet the System Availability SLA for the Cloud Service.

2.1.2. Customers who have not subscribed to the Cloud Service directly from osapiens must claim the Credit from their applicable osapiens partner.

2.2. System Availability Report

osapiens will provide Customer with a monthly report containing the list of downtimes related to the System Availability Percentage for the Cloud Service either by email following a request to Customer's assigned osapiens account manager; through the Cloud Service; or through an online portal made available to Customer, if and when such online portal becomes available.

CHANGES TO WINDOWS

3.1. If Customer wishes to be notified of changes to Maintenance Windows and Major Upgrade Windows, it must subscribe to receive notifications at support.osapiens.com.

SUPPORT Policy SERVICES

osapiens offers the following support levels; osapiens Standard Support and osapiens Extended Support. osapiens Standard Support is included in the subscription fees for osapiens Cloud Services stated in the Order Form.

Osapiens Extended Support is offered for an additional fee, or as an add-on to osapiens Standard Support for certain osapiens Cloud Services. osapiens Extended Support is not available, and is not provided, for any third-party cloud services purchased through osapiens

SYSTEM AVAILABILITY

osapiens promises the Customer an average availability of the Cloud Service that is listed in the Agreement. The average System Availability is measured during each calendar quarter.

	Standard Support	**Extended Support**
System Availability SLA	99.5 %	99.8 %

SUPPORT SERVICE AVAILABILITY

Initial response times are measured during the support hours only.

	Standard Support	**Extended Support**
Support Hours	Monday – Friday, 8:00 am – 6:00 pm (DE/Berlin time zone)	Monday – Sunday, 24 hours "24x7"

Primary support language is English.

For private cloud instances we expect ssh access to the server and a access to the Webapplication (via Internet or OpenVPN). If these prerequisites are not given this will influence the response time mentioned in the SLA.

SUBMITTING SUPPORT REQUESTS

Customer's designated contact person will submit support requests according to osapiens ticketing guidelines. The support request should assign a Severity Level as set forth in the next section and adequately describe and document the reported error so it can be reproduced.

Support Requests are to be submitted through the customer's own user in the osapiens Support portal, to ensure correct SLA's can be applied.

osapiens may re-characterize the Severity Level with a valid business reason or if the customer does not respond within the agreed response times.

SEVERITY LEVEL

osapiens responds to submitted support requests (also referred to as "case", "incident", or "issue") as described in the table below The Severity Level means a perceived error in the osapiens Cloud Service is reportedly having the impact as shown in the table below.

Initial response time begins when the Customer submits a support request in proper form in the osapiens Support Portal. Support requests received outside of the agreed support hours are measured at the beginning of the next support hours window. Initial response time ends with the acknowledgement and/or resolution of the support request or begin of technical analysis and interaction with the Customer. Osapiens' response time commitment is as follows

Response times are subject to real time (customer-) system access.

Priority	Definition	Response Level
P1	**Very High:** An incident should be categorized with the priority "very high" if the problem has very serious consequences for normal business processes or IT processes related to core business processes. Urgent work cannot be performed. This is generally caused by the following circumstances: - A productive service is completely down. - The imminent system Go-Live or upgrade of a production system cannot be completed. - The customer's core business processes are seriously affected. A workaround is not available for each circumstance. The incident requires immediate processing because the malfunction may cause serious issues.	**Initial Response:** Within two hours of case submission for standard support, or within one hour for extended support. **Ongoing Communication:** Unless otherwise communicated by osapiens Support, once every hour. **Resolution Target:** osapiens to provide for issues either a (i) resolution, or (ii) workaround or (iii) action plan within eight hours for standard support or within four hours for Extended support customers

P2	**High:** An incident should be categorized with the priority "high" if normal business processes are seriously affected. Necessary tasks cannot be performed. This is caused by incorrect or inoperable functions in the Cloud Service that are required immediately. The incident is to be processed as quickly as possible because a continuing malfunction can seriously disrupt the entire productive business flow.	**Initial Response:** Within eight hours of case submission for Standard support or within four hours of case submission for Extended support customers. **Ongoing Communication:** Unless otherwise communicated by osapiens, once every six hours. **Resolution Target:** osapiens to provide for issues either a (i) resolution, or (ii) workaround or (iii) action plan within three business days for Extended support customers only
P3	**Medium:** An incident should be categorized with the priority "medium" if normal business processes are affected. The problem is caused by incorrect or inoperable functions in the Cloud Service.	**Initial Response:** Within two business days of case submission for osapiens Standard Support customers or next business day for Extended Support customers. **Ongoing Communication:** Unless otherwise communicated by osapiens Support, once every three business days for Non-Defect Issues and ten business days for product defect issues.
P4	**Low:** An incident should be categorized with the priority "low" if the problem has little or no effect on normal business processes. The problem is caused by incorrect or inoperable functions in the Cloud Service that are not required daily, or are rarely used.	**Initial Response:** Within five business days of case submission for Standard Support customers or within three business days of case submission for osapiens Extended Support customers. **Ongoing Communication:** Unless otherwise communicated by osapiens Support, once every week.

The following types of incidents are excluded from customer response levels as described above: (i) incidents regarding a release, version and/or functionalities of osapiens Cloud Services developed specifically for customer (including those developed by osapiens and/or by osapiens subsidiaries, or individual content services); (ii) the root cause behind the incident is not a malfunction, but missing functionality ("development request") or the incident is ascribed to a consulting request ("how-to")**;** (iii) the customer does not respond to osapiens support questions within the initial response times set forth above

EXCLUDED DOWNTIME

The following events are excluded from the SLA/System Availability calculation

- Scheduled Downtime and Force Majeure Events.

- Software service downtime in the case that the root cause of the downtime is outside of the responsibility of osapiens as set forth in next section. Specifically, but not limited to On-Premise operation models. For example (non-exhaustive):
    - The solution is operated on-premise within the Customers own data-center. The Cloud Service is unavailable due to a hard-disk error and no redundancy has been set up.
    - The solution is operated on-premise by the Customer within a cloud platform virtual environment (eg. AWS or Azure). The Cloud Service is unavailable due to network

connectivity issues between the cloud platform and the Customer's network.

- Downtimes due to interruptions caused by the Customer

- Downtimes due to software errors within the Customer's IT landscape or with Customer's applications if osapiens is not the responsible party for the erroneous component.

- Downtimes caused by network (including Internet) errors or network component issues if the malfunctioning network section is not within the responsibility of osapiens.
    - For Public Cloud Platform operation, the internet hubs of osapiens's data center are the handover points of the responsibility, for both – backend connections as well as mobile client connections.
    - For other operation models this is defined on a case by case basis, depending on the individual technical setup.

Responsibility Matrix

	Cloud Service Public	**Cloud Service Private**	**On-Premise**
SLA Options	Standard or Extended	Standard or Extended	Standard or Extended
Technical System Monitoring	osapiens	osapiens	Customer**
System Scaling	osapiens	osapiens	Customer**
Disaster Failover	osapiens	osapiens	Customer**
Application Updates	osapiens	osapiens	Customer**
Operating System and Third-Party Software Updates	osapiens	osapiens	Customer**
Hardware Maintenance	osapiens	osapiens	Customer**
Network	osapiens*	osapiens*	Customer**

* Starting from osapiens Service Load Balancer and beyond. Not covering network/connectivity from systems and devices to the osapiens Service Load Balancer (eg. internet connectivity).

** Customer itself or a Third-Party service provider which has been mandated by the customer. Responsibility is with osapiens in case osapiens itself has been mandated by the customer for the specific area of responsibility.

Customer Responsibilities

11..1 Customer Contact. In order to receive support, Customer will designate at least two and up to five qualified English speaking contact persons (each a "Customer Contact", "Designated Support Contact", "Authorized Support Contact", "Key User" or "Application Administrator" – system administrator roles within specific Cloud Services) who are authorized to contact or access osapiens Support. The Customer Contact is responsible for managing all business-related tasks of the Cloud Service related to Customer's business, such as:

(i) Support end users and manage their incidents. This includes searching for known solutions in available documentation and liaising with osapiens support in the event of new problems;
(ii) Manage background jobs and the distribution of business tasks across users (if available);
(iii) Manage and monitor connections to Customer's third-party systems (if available);
(iv) (iv) Support the adoption of the Cloud Service.

11.2 Contact Details. Customer will provide contact details (in particular, e-mail address and telephone number) through which the Customer Contact or the authorized representative of the Customer Contact can be contacted at any time. Customer will update its Customer Contacts for a Cloud Service through the osapiens Support Portal at https://support.osapiens.com Only authorized Customer Contacts may contact osapiens' support organization.

11.3 Cooperation. To receive support services, Customer will reasonably cooperate with osapiens to resolve support incidents, and will have adequate technical expertise and knowledge of its configuration of the Cloud Service to provide relevant information to enable osapiens to reproduce, troubleshoot and resolve the experienced error such as e.g. reference ID, issue examples, screenshots.

11.4 Collaboration Upon the Customer's request, osapiens will adequately support the Customer in incident analysis, even if an incident occurs in connection with other services of the Customer or other Third Parties. osapiens will provide its defect analysis and cooperate adequately with the Customer and commissioned Third Parties for analysing and eliminating incidents where reasonably possible. If osapiens is not responsible for the incident, the Customer will compensate such efforts caused by this clause on a time and material basis with a mutually agreed hourly rate.

PERSONAL DATA PROCESSING AGREEMENT FOR osapiens CLOUD SERVICES

1. BACKGROUND

1.1 Purpose and Application. This document ("**DPA**") is incorporated into the Agreement and forms part of a written (including in electronic form) contract between osapiens and Customer. This DPA applies to Personal Data processed by osapiens and its Subprocessors in connection with its provision of the Cloud Service. This DPA does not apply to non-production environments of the Cloud Service if such environments are made available by osapiens, and Customer shall not store Personal Data in such environments.

1.3 GDPR. osapiens and Customer agree that it is each party's responsibility to review and adopt requirements imposed on Controllers and Processors by the General Data Protection Regulation 2016/679 ("**GDPR**"), in particular with regards to Articles 28 and 32 to 36 of the GDPR, if and to the extent applicable to Personal Data of Customer/Controllers that is processed under the DPA.

1.4 Governance. osapiens acts as a Processor and Customer and those entities that it permits to use the Cloud Service act as Controllers under the DPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use osapiens as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the Cloud Service. Where osapiens informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the Cloud Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

2. osapiens OBLIGATIONS

2.1 Instructions from Customer. osapiens will process Personal Data only in accordance with documented instructions from Customer. The Agreement (including this DPA) constitutes such documented initial instructions and each use of the Cloud Service then constitutes further instructions. osapiens will use reasonable efforts to follow any other Customer instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Cloud Service. If any of the before-mentioned exceptions apply, or osapiens otherwise cannot comply

with an instruction or is of the opinion that an instruction infringes Data Protection Law, osapiens will immediately notify Customer (email permitted).

3.2 Processing on Legal Requirement. osapiens may also process Personal Data where required to do so by applicable law. In such a case, osapiens shall inform Customer of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

3.3 Personnel. To process Personal Data, osapiens and its Subprocessors shall only grant access to authorized personnel who have committed themselves to confidentiality. osapiens and its Subprocessors will regularly train personnel having access to Personal Data in applicable data security and data privacy measures.

3.4 Cooperation. At Customer's request, osapiens will reasonably cooperate with Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding osapiens' processing of Personal Data or any Personal Data Breach. osapiens shall notify the Customer as soon as reasonably practical about any request it has received from a Data Subject in relation to the Personal Data processing, without itself responding to such request without Customer's further instructions, if applicable. osapiens shall provide functionality that supports Customer's ability to correct or remove Personal Data from the Cloud Service or restrict its

processing in line with Data Protection Law. Where such functionality is not provided, osapiens will correct or remove any Personal Data, or restrict its processing, in accordance with the Customer's instruction and Data Protection Law.

3.5 Personal Data Breach Notification. osapiens will notify Customer without undue delay after becoming aware of any Personal Data Breach and provide reasonable information in its possession to assist Customer to meet Customer's obligations to report a Personal Data Breach as required under Data Protection Law. osapiens may provide such information in phases as it becomes available. Such notification shall not be interpreted or construed as an admission of fault or liability by osapiens.

3.6 Data Protection Impact Assessment. If, pursuant to Data Protection Law, Customer (or its Controllers) are required to perform a data protection impact assessment or prior consultation with a regulator, at Customer's request, osapiens will provide such documents as are generally available for the Cloud Service (for example, this DPA, the Agreement, audit reports or certifications). Any additional assistance shall be mutually agreed between the Parties.

4. DATA EXPORT AND DELETION

4.1 Export and Retrieval by Customer. During the Subscription Term and subject to the Agreement, Customer can access its Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format. Export and retrieval may be subject to technical limitations, in which case osapiens and Customer will find a reasonable method to allow Customer access to Personal Data.

4.2 Deletion. Before the Subscription Term expires, Customer may use osapiens' self-service export tools (as available) to perform a final export of Personal Data from the Cloud Service (which shall constitute a "return" of Personal Data). At the end of the Subscription Term, Customer hereby instructs osapiens to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period in line with Data Protection Law (not to exceed six months) unless applicable law requires retention.

5. Audit rights

5.1 Audit Rights. Subject to this section 5, osapiens shall make available to the Customer on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer in relation to the Processing of the Customer Personal Data by osapiens.

5.2 Limitation. Information and audit rights of the Customer only arise under section 5.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

5.2 Scope of Audit. Customer shall provide at least sixty days advance notice of any audit unless mandatory Data Protection Law or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to osapiens.

5.3 Cost of Audits. Customer shall bear the costs of any audit unless such audit reveals a material breach by osapiens of this DPA, then osapiens shall bear its own expenses of an audit. If an audit determines that osapiens has breached its obligations under the DPA, osapiens will promptly remedy the breach at its own cost.

6. SUBPROCESSORS

6.1 Permitted Use. osapiens is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

(a) osapiens shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. osapiens shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement.

(b) osapiens will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

7. INTERNATIONAL PROCESSING

7.1 Conditions for International Processing. osapiens shall be entitled to process Personal Data, including by using Subprocessors, in accordance with this DPA outside the country in which the Customer is located as permitted under Data Protection Law.

7.2 Standard Contractual Clauses. Where (i) Personal Data of an EEA or Swiss based Controller is processed in a country outside the EEA, Switzerland and any country, organization or territory acknowledged by the European Union as safe country with an adequate level of data protection under Art. 45 GDPR, or where (ii) Personal Data of another Controller is processed internationally and such international processing requires an adequacy means under the laws of the country of the Controller and the required adequacy means can be met by entering into Standard Contractual Clauses, then:

(a) osapiens and Customer enter into the Standard Contractual Clauses.

(b) Customer enters into the Standard Contractual Clauses with each relevant Subprocessor as follows, either (i) Customer joins the Standard Contractual Clauses entered into by osapiens and the Subprocessor as an independent owner of rights and obligations ("Accession Model") or, (ii) the Subprocessor (represented by osapiens) enters into the Standard Contractual Clauses with Customer ("Power of Attorney Model"). The Power of Attorney Model shall apply if and when osapiens has expressly confirmed that a Subprocessor is eligible for it through the Subprocessor list provided under Section 6.1(c), or a notice to Customer; and/or

(c) Other Controllers whose use of the Cloud Services has been authorized by Customer under the Agreement may also enter into Standard Contractual Clauses with osapiens and/or the relevant Subprocessors in the same manner as Customer in accordance with Sections 7.2 (a) and (b) above. In such case, Customer will enter into the Standard Contractual Clauses on behalf of the other Controllers.

7.3 Relation of the Standard Contractual Clauses to the Agreement. Nothing in the Agreement shall be construed to prevail over any conflicting clause of the Standard Contractual Clauses. For the avoidance of doubt, where this DPA further specifies audit and subprocessor rules in sections 5 and 6, such specifications also apply in relation to the Standard Contractual Clauses.

7.4 Governing Law of the Standard Contractual Clauses. The Standard Contractual Clauses shall be governed by the law of the country in which the relevant Controller is incorporated.

8. DOCUMENTATION; RECORDS OF PROCESSING

Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an

electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

9. EU ACCESS

9.1 Optional Service. EU Access is an optional service that may be offered by osapiens. osapiens shall provide the Cloud Service eligible for EU Access in accordance with this Section 9. Where EU Access is not expressly specified and agreed in the Order Form, this Section 9 shall not apply.

9.2 EU Access. osapiens will use only European Subprocessors to provide support requiring access to Personal Data in the Cloud Service and osapiens shall not export Personal Data outside of the EEA or Switzerland unless expressly authorized by Customer in writing (e-mail permitted) on a case by case basis; or as excluded under Section 9.4.

9.3 Data Center Location. Upon the effective date of the Agreement, the Data Centers used to host Personal Data in the Cloud Service are located in the EEA or Switzerland. osapiens will not migrate the Customer instance to a Data Center outside the EEA or Switzerland without Customer's prior written consent (email permitted). If osapiens plans to migrate the Customer instance to a Data Center within the EEA or to Switzerland, osapiens will notify Customer in writing (email permitted) no later than thirty days before the planned migration.

9.4 Exclusions. The following Personal Data is not subject to 9.2 and 9.3:

(a) Contact details of the sender of a support ticket; and

(b) Any other Personal Data submitted by Customer when filing a support ticket. Customer may choose not to transmit Personal Data when filing a support ticket.

10. DEFINITIONS

Capitalized terms not defined herein will have the meanings given to them in the Agreement.

10.1 "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to osapiens be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

10.2 "Data Center" means the location where the production instance of the Cloud Service is hosted for the Customer

10.3 "Data Protection Law" means the applicable legislation protecting the fundamental rights and freedoms of persons and their right to privacy with regard to the processing of Personal Data under the Agreement (and includes, as far as it concerns the relationship between the parties regarding the processing of Personal Data by osapiens on behalf of Customer, the GDPR as a minimum standard, irrespective of whether the Personal Data is subject to GDPR or not).

10.4 "Data Subject" means an identified or identifiable natural person as defined by Data Protection Law.

10.5 "EEA" means the European Economic Area, namely the European Union Member States along with Iceland, Liechtenstein and Norway.

10.6 "European Subprocessor" means a Subprocessor that is physically processing Personal Data in the EEA or Switzerland.

10.7 "Personal Data" means any information relating to a Data Subject which is protected under Data Protection Law. For the purposes of the DPA, it includes only personal data which is (i) entered by Customer or its Authorized Users into or derived from their use of the Cloud Service, or (ii) supplied to or accessed by osapiens or its Subprocessors in order to provide support under the Agreement. Personal Data is a sub-set of Customer Data (as defined under the Agreement).

10.8 "Personal Data Breach" means a confirmed (1) accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or unauthorized third-party access to Personal Data or (2) similar incident involving Personal Data, in each case for which a Controller is required under Data Protection Law to provide notice to competent data protection authorities or Data Subjects.

10.9 "Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, be it directly as processor of a controller or indirectly as subprocessor of a processor which processes personal data on behalf of the controller.

10.10 "Standard Contractual Clauses" or sometimes also referred to the "EU Model Clauses" means the (Standard Contractual Clauses (processors)) or any subsequent version thereof published by the European Commission (which will automatically apply).

10.11 "Subprocessor" means osapiens Affiliates, and third parties engaged by osapiens, osapiens' Affiliates in connection with the Cloud Service and which process Personal Data in accordance with this DPA.

Appendix 1 to the DPA

Standard Contractual Clauses (Processors)[1]

For the purposes of Article 26(2) of Directive 95/46/EC (or, after 25 May 2018, Article 44 et seq. of Regulation 2016/79) for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

[...]

(in the Clauses hereinafter referred to as the '**data exporter'**)

and

[...]

(in the Clauses hereinafter referred to as the **'data importer'**)

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 Annex 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;

(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 sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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;

[1] Pursuant to Commission Decision of 5 February 2010 (2010/87/EU)

(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 Annex 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 sub-processor 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 Annex 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 sub-processor 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 Annex 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing 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 sub-processing, 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 Annex 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;

(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 sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex 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 sub-processing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any sub-processor 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 sub-processor 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 sub-processor 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor 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 sub-processor, 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 sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, 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.

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

Sub-processing

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 sub-processor as are imposed on the data importer under the Clauses [(3)]. Where the sub-processor fails to fulfill its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing 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.

4. The data exporter shall keep a list of sub-processing 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 sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall 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 sub-processor 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.

(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.

(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.

(3) This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

ANNEX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Data exporter

The data exporter is as defined in these Model Clauses as the **data exporting organisation**.

Data importer

osapiens and its Subprocessors provide the Cloud Service that includes the following support: osapiens support the Cloud Service data centers remotely from osapiens facilities where osapiens employs personnel. Support includes:

- *Monitoring the Cloud Service*
- *Backup & restoration of Customer Data stored in the Cloud Service*
- *Release and development of fixes and upgrades to the Cloud Service*
- *Monitoring, troubleshooting and administering the underlying Cloud Service infrastructure and database*
- *Security monitoring, network-based intrusion detection support, penetration testing*

osapiens provide support when a Customer submits a support ticket because the Cloud Service is not available or not working as expected for some or all Authorized Users. osapiens answers phones and performs basic troubleshooting, and handles support tickets in a tracking system that is separate from the production instance of the Cloud Service.

Data subjects

The personal data transferred concern the following categories of data subjects:

Unless provided otherwise by the Data Exporter, transferred Personal Data relates to the following categories of Data Subjects: employees, contractors, business partners or other individuals having Personal Data stored in the Cloud Service.

Categories of data

The personal data transferred concern the following categories of data:

Personal Details including: name and surname; business email and telephone details; information that Customer personnel submit via the Cloud Services, location data, device data including Internet protocol (IP) address used to connect their computer to the Internet, their login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify): *NA*

Processing operations

The transferred Personal Data is subject to the following basic processing activities:

- *use of Personal Data to set up, operate, monitor and provide the Cloud Service (including Operational and Technical Support)*
- *provision of Consulting Services;*
- *communication to Authorized Users*
- *storage of Personal Data in dedicated Data Centers (multi-tenant architecture)*
- *upload any fixes or upgrades to the Cloud Service*
- *back up of Personal Data*
- *computer processing of Personal Data, including data transmission, data retrieval, data access*
- *network access to allow Personal Data transfer*

- *execution of instructions of Customer in accordance with the Agreement.*

ANNEX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The Data Importer shall adhere to the following **technical security measures** as further reflected in its information security policies:

Security Requirements

1 osapiens shall at all times ensure that its IT systems are fit for the purpose of securing Client Data in accordance with Good Industry Practice and this Agreement and are regularly maintained and, if necessary, upgraded to ensure this.

2 osapiens shall at all times comply with ISO/IEC27001 or otherwise comply with Good Industry Practice relating to data protection, and implementation and maintenance of back-up systems.

3 Where osapiens, as part of the Cloud Service, provides Customer with access to any IT system or stores any Customer Data on its own systems or any systems of any Affiliate, Sub-Processor or contractor, osapiens shall, undertake annual application and/or infrastructure level penetration testing using a UK-based independent CREST certified contractor and provide Customer with details of the results of such tests. If penetration testing is run on request of Customer, Customer will bear the cost. Remedial actions identified by such penetration testing shall be undertaken by osapiens at the osapiens' cost.

4 osapiens shall (at no cost to the Customer):

4.1 restore, recompile or recreate (in a timely manner and in accordance with good industry practice) all Customer Data which is lost, deleted or corrupted by osapiens or any of the osapiens personnel as a result of a Data Protection Breach;

4.2 on Customers' request at any time give to the osapiens a copy of all or part of Customer Data then in the Agency's possession, custody or control, which is in electronic form, in such format as Customer ay require;

4.3 ensure that if any Customer Data is disposed of, such disposal takes places in a secure manner such that the Customer Data is not recoverable;

4.4 preserve so far as possible the security of Customer Data and prevent any loss, disclosure, theft, manipulation or interception of Customer Data;

4.5 take all precautions in accordance with good industry practice to prevent the installation of any virus or other unauthorized computer program into its computer systems or those of Customer and otherwise prevent corruption of Customer Data and, if a virus or such other programs is introduced into any of Customer's systems do as a result of the osapiens' act or omission, osapiens shall immediately notify Customer and provide all necessary assistance to Customer to minimise the effects.

4.6 ensure that if any Customer Data is placed on a portable electronic device (including laptops, memory sticks and back-up tapes) or transmitted electronically, it is securely encrypted;

4.7 procure that osapiens personnel shall inform Customer immediately should they be aware of, or reasonably suspect, any unauthorised or accidental disclosure, loss or damage of Customer Data; and

4.8 ensure that regular back-up copies of Customer Data are made in accordance with good industry practice (in any event no longer than every 30 days) and kept in a secure physical location separate to the primary copy of the Customer Data.