Untis GmbH
Belvederegasse 11
A-2000 Stockerau

+43 2266 62241
office@untis.at
www.untis.at

Agreement

on the

Processing of Personal Data on Behalf of the Controller pursuant to Art. 28 GDPR (DPA)

Controller:

(hereinafter referred to as **Client**)

Processor:

Untis GmbH
Belvederegasse 11
AT-2000 Stockerau
(Austria)

(hereinafter referred to as **Processor**)

The parties are jointly also referred to as the **Parties**

§ 1 Subject Matter of the Agreement

(1) Processor provides services for Client on the basis of the Main Agreement concluded between the Parties or, where this is a free test or demo version for a limited period, on the basis of a specific agreement. In doing so, Processor processes personal data within the meaning of Article 4(1) GDPR for Client (hereinafter referred to as "Client Data") exclusively on behalf of and in accordance with Client's instructions. The framework and scope of the processing of personal data are determined by the Main Agreement.

(2) Client is responsible for assessing the lawfulness of the processing of personal data. Processor has no obligation to review Client's instructions for compliance with data protection law. However, if Processor considers that an instruction from Client infringes data protection law, it shall inform Client thereon. Processor shall be entitled to suspend implementation of the instruction concerned until the instruction is confirmed or amended. If, after being informed of an instruction which Processor considers unlawful, Client does not dispel Processor's concerns, Processor may refuse to implement the instruction insofar as it concerns Processor's sphere of responsibility.

(3) This Agreement refers to the following activities performed by Processor, the specific nature and scope of which are determined by the respective Main Agreements:

- Operation of the web services of the Untis Platform in accordance with the scope of services booked by Client, in order to make them available to customers via the Internet, including provision of the Mobile App, an application made available for mobile devices for accessing and using the web services, provided that it is activated by the user;
- Provision of support services for the applications of the Untis Platform in accordance with the scope of services booked by Client and for the Mobile App;
- Performance of maintenance activities for the applications of the Untis Platform in accordance with the scope of services booked by Client;
- Provision of individual integration solutions from third-party providers on the WebUntis platform.

(4) This Agreement specifies the obligations and rights of the Parties under data protection law in connection with Processor's handling of Client Data in performance of the Main Agreement.

§ 2 Duration of the Processing

(1) The term and termination of this Agreement shall be governed by the provisions on the term and termination of the Main Agreement. Termination of the Main Agreement shall automatically also result in termination of this Agreement.

(2) Separate termination of this Agreement is excluded.

§ 3 Subject Matter, Nature and Purpose of the Processing, Types of Personal Data, Categories of Data Subjects

(1) Processor processes Client Data exclusively on behalf of and in accordance with Client's documented instructions. Client remains the controller within the meaning of Article 4(7) GDPR.

(2) The processing of Client Data in the context of this Agreement shall be carried out in accordance with the specifications concerning the nature and purpose of the processing contained in **Annex 1**

to this Agreement. It relates to the types of Client Data specified in **Annex 1** and the categories of data subjects listed there.

(3) The processing of Client Data shall take place in the territory of the Republic of Austria, the Federal Republic of Germany, another Member State of the European Union or another contracting party of the Agreement on the European Economic Area. Any transfer to a third country may take place only if the specific requirements of Articles 44 et seq. GDPR are met. This shall also apply to Clients established outside the EU or the EEA.

§ 4 Rights and Obligations and Client's Authority to Issue Instructions

(1) Client shall be solely responsible for assessing the lawfulness of the processing and for safeguarding the rights of data subjects under Articles 12 to 22 GDPR.

(2) The processing of Client Data by Processor under this Agreement shall be carried out exclusively in accordance with Client's instructions pursuant to Article 28(3), second sentence, point (a) GDPR, unless Processor is required to carry out further processing under Union or Member State law to which it is subject. In such a case, Processor shall inform Client of those legal requirements, unless that law prohibits such information on important grounds of public interest.

(3) Within the scope of the description of processing agreed in this Agreement, Client reserves comprehensive authority to issue instructions concerning the nature and purposes of the processing of personal data, which it may specify by means of individual instructions.

(4) Individual instructions issued after conclusion of the Agreement must be in text form and shall be documented by both Client and Processor.

(5) If Client issues individual instructions concerning the handling of Client Data which go beyond the scope of services agreed in the Main Agreement, the costs thereby incurred shall be borne by Client.

(6) Client shall inform Processor without undue delay and in full, if he detects errors or irregularities in connection with the processing of Client Data by Processor or in connection with his instructions.

(7) The persons authorised to issue instructions on behalf of Client are:

_____

(First name, last name, e-mail-address, telephone)

The recipient of instructions at Processor is:

The data protection officer of Untis GmbH, Belvederegasse 11, A-2000 Stockerau (Austria); datenschutz@untis.at

(8) In the event of a change or long-term unavailability of the contact persons, the successors or representatives shall be notified to the other Party without undue delay and, as a rule, in writing or by electronic communication.

§ 5 Obligations of Processor

(1) Processor shall ensure, that the processing of Client Data in the course of providing services under the Main Agreement is carried out within his area of responsibility, which includes the sub-processors under § 9 of this Agreement, in compliance with the provisions of this Agreement.

(2) Upon request, Processor shall provide Client with the necessary information, including certifications and audit and inspection results, serving to demonstrate compliance with the obligations set out in this Agreement.

(3) Processor shall require persons authorised to process Client Data, pursuant to Article 28(3)(b) GDPR, to commit themselves to confidentiality in writing, unless they are already subject to an appropriate statutory obligation of confidentiality.

(4) Processor shall appoint in writing a competent and reliable data protection officer who can perform his or her activities in accordance with Articles 37, 38 and 39 GDPR, provided and for as long as the statutory requirements for mandatory appointment are met. Processor shall make the current contact details of the data protection officer easily accessible on his website (Article 37(7) GDPR).

(5) Processor and, where applicable, his representative shall maintain records of all categories of processing activities carried out on behalf of Client, containing all information pursuant to Article 30(2) GDPR. This obligation shall not apply if the requirements of Article 30(5) GDPR are met.

(6) Without Client's prior consent, Processor shall not make any copies or duplicates of Client Data in the context of this Agreement. This shall not include copies which are necessary to ensure proper processing of personal data and proper provision of the services under the Main Agreement (including data backup), or copies required to comply with statutory retention obligations.

(7) Processor shall assist Client in fulfilling his obligations under Articles 12 to 22 and Articles 32 to 36 GDPR, to the extent reasonable and necessary and against reimbursement of the expenses and costs incurred by Processor as a result. Taking into account the nature of the processing and the information available to the Processor, the assistance shall be provided and, where possible, by means of appropriate technical and organisational measures, in particular in responding to requests to exercise the rights of data subjects specified in Articles 12 to 22 GDPR (§ 10).

§ 6 Technical and Organisational Measures

(1) Processor shall implement the technical and organisational measures required to provide an appropriate level of protection for Client Data pursuant to Article 32 GDPR, in particular the measures relating to physical access control, access control, data access control, transfer control, input control, order control, availability control and segregation control set out in **Annex 2**.

(2) As the technical and organisational measures are subject to technological progress and technological development, Processor shall be permitted to implement alternative and adequate measures, provided that the level of security of the measures specified in **Annex 2** is not reduced thereby. Processor shall document such changes. Material changes to the measures shall require Client's prior consent.

§ 7 Notifiable Infringements by Processor

(1) Processor shall inform Client without undue delay if he determines that he or an employee has infringed data protection law or provisions of this Agreement when processing Client Data, provided that there is a risk of a personal data breach within the meaning of Article 4(12) GDPR.

(2) If, as a result of an incident under subsection (1), Client is subject to statutory information obligations due to unlawful acquisition of knowledge of Client Data, in particular under Articles 33 and 34 GDPR, Processor shall, at Client's request, assist Client in fulfilling those information obligations to the extent reasonable and necessary and against reimbursement of the expenses and costs incurred by Processor as a result.

(3) Processor shall take all necessary measures without undue delay to secure the data and mitigate possible adverse consequences for data subjects, inform Client accordingly and request further instructions.

(4) Processor may issue notifications under Articles 33 or 34 GDPR on behalf of Client only following Client's prior instruction.

§ 8 Audit Rights of Client

(1) At his own expense, Client shall satisfy himself of Processor's technical and organisational measures under **Annex 2** before the processing of data begins and thereafter on a regular basis, and shall document the result. This shall be done by obtaining a self-assessment from Processor, which Processor may also satisfy by presenting a suitable certificate from an expert.

(2) Processor undertakes, upon Client's written request, to provide all necessary information concerning his obligations under this Agreement and, in particular, to demonstrate implementation of the technical and organisational measures in **Annex 2**. Evidence of measures which do not concern only the specific contract may be provided by adherence to approved codes of conduct pursuant to Article 40 or certifications pursuant to Article 42 GDPR; current attestations, reports or extracts from reports of independent bodies (e.g. auditors, internal audits, data protection officer, IT security department, data protection auditors, quality auditors); or a suitable certification by an IT security or data protection audit (e.g. under BSI Basic Protection (BSI-Grundschutz)).

(3) Client or a person appointed by him shall have the right to conduct the aforementioned audits during normal business hours. Such audits shall be announced in good time, generally at least two weeks in advance, and shall interfere with Processor's business operations as little as possible.

(4) If Client appoints a third party to conduct the audit, Client shall require the third party in writing to comply with the same obligations as Client under this Agreement. In addition, it shall require the third party to observe secrecy and confidentiality, unless the third party is subject to a professional obligation of confidentiality. At Processor's request, Client shall provide Processor with the agreements documenting those obligations. Client may not appoint a competitor of Processor to conduct the audit.

§ 9 Sub-processing

(1) Client expressly consents to the engagement of those sub-processors listed in **Annex 3**, subject to a contractual agreement in accordance with Article 28(1) to (4) GDPR. Processor is permitted to engage additional sub-processors (other processors).

(2) Processor shall inform Client without undue delay of any intended change concerning the addition or replacement of other sub-processors. Client may object to such changes for good cause, which he must demonstrate to Processor. The objection must be made in writing within one week of receipt of Processor's corresponding notification.

(3) No notification is required for the engagement of sub-processors where the sub-processor provides merely an ancillary service in support of providing the services under the Main Agreement, e.g. telecommunications services, postal/transport services, maintenance and user services or disposal of data carriers, or other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data-processing systems, even if access to Client Data cannot be ruled out. Processor shall also select these sub-processors with due care and conclude agreements to the extent necessary to ensure an appropriate level of protection for Client Data.

(4) Where a sub-processor is engaged, Processor shall impose on that sub-processor, by means of a contract or other legal act under Union or Member State law, the same data protection obligations as those set out in this Agreement. That contract shall be designed so that Client can, if necessary, conduct appropriate audits and inspections at the sub-processor, including on-site audits, or have them conducted by third parties appointed by the former.

(5) Where sub-processors in a third country are to be engaged, Processor shall ensure that an adequate level of data protection is guaranteed at the sub-processor (e.g. by concluding an agreement based on EU standard data protection clauses).

(6) Upon request, Processor shall demonstrate to Client that the aforementioned agreements with his sub-processors have been concluded.

§ 10 Rights of Data Subjects

(1) The rights of data subjects affected by the processing of personal data shall be exercised in respect of and against Client.

(2) If a data subject contacts Processor directly to exercise his or her rights under Articles 12 to 22 GDPR in relation to the data concerning him or her, Processor shall refer the data subject to Client.

(3) In all other respects, § 5(7) of this Agreement shall apply.

§ 11 Liability

(1) Client and Processor shall be jointly and severally liable for compensation for damage suffered by a person as a result of unlawful or inaccurate processing of personal data in the context of this Agreement.

(2) As between Client and Processor, Client alone shall be responsible for compensation for damage suffered by a data subject as a result of processing of Client Data in the context of this Agreement which is unlawful or inaccurate under applicable data protection law.

(3) Client undertakes to indemnify Processor internally against all third-party claims for as long as and insofar as Client does not demonstrate that Processor failed to comply with the obligations under the GDPR specifically imposed on Processor or acted in disregard of or contrary to a lawful instruction of Client.

(4) If a data protection authority or a court imposes a fine on Processor on account of processing by Processor which was based on an instruction of Client, Client shall reimburse Processor for the corresponding amount in full within 30 days of written notification.

(5) Client shall reimburse Processor for all costs arising from the infringement for which Client is responsible pursuant to subsections (3) and (4), including the costs of legal enforcement.

(6) Unlimited liability: Processor shall have unlimited liability for intent and gross negligence, for breach of a contractual guarantee and in accordance with the Product Liability Act (Produkthaftungsgesetz). Processor shall be liable for slight negligence in the event of damage arising from injury to life, body or health of persons. In all other respects, the following limited liability shall apply: in the event of slight negligence, Processor shall be liable only in the event of breach of a material contractual obligation of the Main Agreement, the fulfilment of which is essential for the proper performance of the Main Agreement and on compliance with which Client may regularly rely (cardinal obligation). Liability for slight negligence shall be limited in amount to the foreseeable damage at the time of conclusion of the Main Agreement, the occurrence of which must typically be expected.

§ 12 Return and Erasure of Client Data Provided

(1) After completion of the contractual services, in particular upon expiry of the agreed free test or demo version, cancellation or other termination of the Main Agreement, Processor shall, at Client's choice, return or erase all Client Data and destroy existing copies, unless Union or Member State law requires storage of the data.

(2) Processor shall document the erasure or destruction of Client Data and provide evidence thereof to Client upon request.

(3) Documentation serving to demonstrate proper processing on behalf of Client and proper processing or to comply with statutory retention periods shall be retained by Processor beyond the term of the Agreement in accordance with the applicable retention periods.

§ 13 Miscellaneous

(1) Unless this Agreement contains special provisions, the provisions of the Main Agreement shall apply. In the event of a conflict between this Agreement and provisions of other contracts, in particular the Main Agreement, the provisions of this Agreement shall prevail.

(2) Client and Processor and, where applicable, their representatives shall cooperate with the supervisory authority upon request in the performance of its tasks.

(3) Only the German version of this Agreement shall be deemed authentic. This English version only serves informational purposes.

Annexes:

Annex 1 Nature and Purpose of the Processing, Types of Data and Categories of Data Subjects
Annex 2 Technical and Organisational Measures
Annex 3 Permitted Sub-processors

Annex 1 – Nature and Purpose of the Processing, Types of Data and Categories of Data Subjects

Processor provides the services agreed in this Annex to Client exclusively in accordance with Client's instructions and on the basis of the Agreement on the Processing on Behalf of the Controller between the Parties.

Processor processes the following personal data on behalf of Client for the stated purposes:

Types	Nature and purpose of the processing	Categories of data subjects
The following basic processing operations are carried out: • Short name • Surname • Text • Title • First name • Personnel number • E-Mail address • Telephone number • Date of birth • Date of joining • Date of leaving • Mobile telephone • Gender • Timetable / event schedule	The data are stored. In the context of hosting and operation, access to these data cannot be ruled out. Instruction-based adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, or alignment of these data may take place.	Teachers / lecturers
For Web App (SaaS), the following also applies: • Active • ID • External ID • Teacher/lecturer status • Target hours/week • Teacher/lecturer (relevant for billing) • Other activities [%] • Room • Assigned departments • Photo • Assigned teaching qualifications • Class form teacher / semester head • Foreground colour • Background colour • Fax number • Street • Postcode • City • Technical log data	As above	Teachers / lecturers

• Absences (including reasons) • Allocations (hours) • Curriculum content • Homework • Examinations		
For Web App (SaaS), the following also applies: • Photo • Surname • First name • Short name • ID • External ID • National ID • Date of birth • Gender • Date of joining • Date of leaving • Class/semester • Text • Medical certificate required • Compulsory schooling • Adult • Catalogue number • Foreground colour • Background colour • E-mail address • Mobile telephone • Telephone number • Fax number • Street • Active • Postcode • City • Technical log data • Timetable	As above	Pupils / students
When using Digital Class Register, the following also applies: • Absences • Class register entries • Grades • Exemptions • Class duties • Curriculum content • Homework • Examinations	As above	Pupils / students
For Web App (SaaS), the following also applies: • Username • ID • External username • Person role	As above	Users (parents / legal guardians, teachers / lecturers, pupils / students)

• Person • User group • User access active • User access blocked • Language • E-mail address • Last login • Password • Google Authenticator key • Office 365 identity		
For Web App (DaaS) the following also applies: • Description • Statistical identifier • Status • Departments • Main school • Personnel no. 2 (Austria) • PM-SAP number (Austria) • Secured lessons (Austria) • Time preferences • Foreground colour • Background colour • Class teacher	As above	Teachers / lecturers
When using Lesson Planning and Value Calculation, the following also applies: • Teaching qualifications • Target hours/week • Actual/target values • Allocations (hours) • Teaching values • Value corrections • Hourly rate	As above	Teachers / lecturers
When using Course Planning and/or Student Timetables, the following also applies: • Short name • Surname • Text • Description • Statistical identifier • First name • Student number • Student's class • Date of birth • Optimisation identifier • Gender (male, female, x (inter)) • E-mail address • Examinations	As above	Pupils / students

When using Substitution Planning, the following also applies: • Absences • Reasons for absence • Standbys • Cover arrangements • Cancelled lessons • Supervision • Cover counters • Value correction • Events • Reservations • Examinations	As above	Teachers / lecturers
When using Department Timetables, the following also applies: • Department	As above	Teachers / lecturers
When using Untis MultiUser, the following also applies: • External name • Username • User rights	As above	Teachers / lecturers, school management, school office
When using Break Supervision, the following also applies: • Break supervision • Maximum minutes • Substitute break supervision (in combination with the Substitution Planning module)	As above	Teachers / lecturers
WebApp (DaaS) users: • User name • First name • Last name • E-mail address	As above	Teachers / lecturers, school management, school office

Annex 2 – Technical and Organisational Measures pursuant to Art. 32 GDPR

Untis has a continuously valid ISO 27001 certification.

The following is an excerpt describing the technical and organisational measures taken by Processor to implement and comply with the requirements of Article 32 GDPR.

Confidentiality

Physical Access Control

The servers for operating the web applications of the Untis Platform are hosted in Vienna by the hosting provider next layer Telekommunikationsdienstleistungs- und Beratungs GmbH. The hosting provider ensures physical access control at its hosting centres by means of an access-control and monitoring system, a video surveillance system and security staff. A multi-stage system is in place for identifying persons authorised to enter (ID card, fingerprint verification).

Physical access to the servers is ensured by a locked server cabinet in the access-controlled building. The allocation of keys is precisely regulated and restricted to the persons who need them.

Access Control

Only selected employees named to the respective hosting centre and hosting provider have access to the servers on which the web applications of the Untis Platform and/or their extension modules are operated. These servers are therefore maintained and serviced exclusively by employees of UNTIS GMBH or its partners.

The server systems can be reached via the Internet exclusively through VPN access. Access passwords are subject to password management corresponding to the current state of the art and are continuously adapted to the current state of the art.

Data Access Control

The applications of the Untis platform and its extension modules have password-protected user access. The authorisation system enables access and responsibility restrictions. A firewall protects the servers against unauthorised access. The hosting providers have no authorisation to access the servers of UNTIS GMBH and its partners. The Untis platform data of the individual clients are stored in separate databases. Mixing of data stocks and mutual access by different clients are prevented by the specific allocation of defined data areas to defined clients.

Processing Control

All relevant data are protected against unauthorised access during processing by appropriate logs and security measures (e.g. encryption).

Integrity

Transfer Control

By using appropriate encryption controls and appropriate transmission protocols, alteration of data during transport or during storage and processing is excluded. To ensure transfer control, all personal data are subjected to HTTPS encryption, in accordance with the state of the art, during transmission in the cases specified.

Input Control

Alteration of personal data is restricted by appropriate access restrictions or can be traced by suitable measures. Every login to the system is logged and all data required for traceability are recorded. Unsuccessful login attempts are also recorded. All changes to the transaction data are automatically logged by the Untis Platform. This includes both the substantive change and the person who carried out the change.

Order Control

No processors within the meaning of Article 28 GDPR are engaged without a corresponding instruction from Client, e.g. clear contractual arrangements, formalised order management, strict selection of the processor (ISO certification, e.g. ISO 27001), prior verification obligation and subsequent checks.

Availability and Resilience

Availability Control

The availability and stability of the systems are ensured by technical and organisational measures:

- Backup strategy (online/offline; on-site/off-site)
- Emergency planning
- Uninterruptible power supply (UPS, diesel generator)
- Firewall systems according to the current state of the art
- Distributed Denial of Service (DDoS) protection (vUntis and WebUntis)
- Standard processes when employees change or leave
- Storage of access credentials in a bank safe
- Regular restore tests

Mirrored hard disks in the respective server, database replication to a second server and daily backup protect the data against accidental destruction or loss. UNTIS GMBH and its partners process personal data exclusively within the scope of the service in question and in accordance with Client's instructions. They do not use the data made available for processing for any other purposes. To protect the data against accidental destruction or loss, replications and backups of the data are created at regular intervals. In this context, Client is assured that daily backups shall be made going back one month and monthly backups (on the first day of each month) shall be made going back six months. No other copies or duplicates shall be made without Client's knowledge. Client is also assured that the personal data of Client disclosed in the context of the service, or personal data of pupils, students and teaching staff entered by Client in WebUntis or its extension modules, shall be kept confidential.
Client itself also has the possibility at any time to create a backup of his data.

Recoverability

Rapid recoverability is achieved through appropriate segmentation of the data, meaning that, in the event of an error, only the affected data statuses need to be restored.

Data Erasure

Upon termination of the cooperation, data can be specifically erased immediately by means of a simple command. Erasure from the backups shall then also take place in due time through a regulated process. During the cooperation, erasure shall take place in accordance with Client's specifications.

Measure for Testing, Assessing and Evaluating the Effectiveness of the Technical and Organisational Measures

An appropriate data protection management system, including regular employee training, has been established.
An established incident response management system is in place. Regular audits are conducted to establish an adequate level of security.
All default settings are implemented in a data-protection-friendly manner.

Annex 3 – Permitted Sub-processors

Sub-processor name	Address / country	Service
next layer Telekommunikationsdienstleistungs- und Beratungs GmbH	Mariahilfer Gürtel 37/7 1150 Vienna Austria	Operation of the server infrastructure of the Untis Platform
Sleekplan GmbH	Georgenstrasse 66 80799 Munich Germany	Sending news and receiving feedback contributions. No transfer of data to a third country takes place.
SFDC Ireland Limited	Salesforce Tower 60 R801 North Dock Ireland	Operation of the "Salesforce" ticketing system for processing customer enquiries. No transfer of data to a third country takes place.
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Ireland	The Mobile App uses services provided by Firebase (a Google product): • Firebase Cloud Messaging, for sending push notifications; • Firebase Crashlytics, for evaluating automatically generated error messages (e.g. in the event of crashes); • Firebase Remote Config, for configuration adjustments in the app without having to publish a new version in the store.
Prof. Mag. Michael Kurzthaler	Helenen-Weg 8b 9900 Lienz Austria	Support and other services for the Untis Platform in the federal states of Carinthia and Tyrol
Franz Stefan Schreiner	Grymgasse 16 3100 St. Pölten Austria	Support and other services for the Untis Platform in the federal states of Lower Austria and Upper Austria
Educ Oy Tuomas Heinonen	Mäntytie 7 86300 Oulainen Finland	Support and other services for the Untis Platform in Finland
Dialog Computer Systeme GmbH	Helmholtzstr. 2-9 10587 Berlin Germany	Support and other services for the Untis Platform in the federal state of Berlin and Saxony
PEDAV das Softwarehaus für Schulen GmbH & Co. KG	Schönebecker Straße 1 45359 Essen Germany	Support and other services for the Untis Platform in the federal state of North Rhine-Westphalia and Hessen
TechTalk GmbH	Leonard-Bernstein-Straße 10 1220 Vienna Austria	Second-level support and other services for the Untis Connector for Moodle and the Untis Connector for Teams
LUMASERV GmbH	Universitätsstraße 3 56070 Koblenz Germany	Second-level support and other services for course selection and emergency assistance

When the following optional integrations from third-party providers are activated by Client via the WebUntis (integration) platform, the operator of that integration ("Integration Partner") shall, for the purpose of operating those integrations, additionally become a sub-processor of Untis GmbH, the engagement of which is approved by Client from the outset:

Name of Sub-processor	Address / Country	Service
Untis Development GmbH	Zum Schwimmbad 44 65232 Taunusstein Germany	Operation, maintenance and support for the WebUntis School-Year Calendar and WebUntis Grades Integrations
eAsistent	Cerkvena ulica 11 4290 Tržic Slovenia	Operation, maintenance and support for the "eAssistent" Messenger integration
Sdui GmbH	Universitätsstrasse 3 56070 Koblenz Germany	Operation, maintenance and support for the "Sdui" Messenger integration