Continental Theological Seminary

GDPR Privacy Notice

In accordance with the approved 27 April 2016 European Union (EU) General Data Protection Regulation (GDPR), this *GDPR Privacy Notice* of Continental Theological Seminary (CTS) explains usage, storage and handling of CTS personal data. The GDPR is enforceable beginning 25 May 2018. The regulatory instance in Belgium is the Commission for the protection of privacy (CPP).

CTS is an accredited private university for higher education located at Kasteelstraat 48, 1600 Sint-Pieters-Leeuw, Belgium.

Purpose

Personal data is information about a living individual (the data subject), who is identifiable from that information or who could be identified from that information combined with other data which CTS either holds or is likely to obtain. This includes names, contact details, photographs, salary, attendance records, student marks, sickness absence, leave, dates of birth, marital status, personal email address, online identifiers, IP addresses etc. Furthermore, any expression of opinion or any intentions regarding a person are also considered to be personal data.

CTS personal data is collected in the following departments for the following purposes:

The Administration Office

- In the area of accounting, Administration collects full names and email addresses provided by all CTS personnel: students, faculty and staff into an electronic CDM+ accounting database, in which data are processed, stored and secured in the cloud. Name and email address data are required for all invoices, receipts and financial statements generated by the accounting area and sent via email to CTS personnel. Such data areprocessed only by accounting area staff who work with any invoicing or student payment. The accounting database automatically generates a unique ID number for each person; therefore, personal national ID is not captured.
- In a separate electronic CDM+ vendor database, data concerning suppliers are collected by accounting personnel, stored and secured in the cloud. The accounting area retains data including name, general address, phone, fax, email and website of suppliers. Such data are required to maintain contact with suppliers, to reference product or service information, as well as for booking supplier invoices and payments.
- In a separate social secretarial database SDWorx, the main accountant retains all essential personal data of all employed faculty and staff for salary payment. Data include an employee's national ID number and social security number. All hardcopy employment contracts and salary documentation are filed and locked in the office of the main accountant. Only the main accountant has sole access to these documents.
- In hardcopy files stored in the administration office, Administration retains any information and correspondence with all CTS faculty, staff and volunteers. The CTS

President and the CTS President Assistant have sole access to these documents.

- All hardcopy data distributed to CTS personnel and authorized participants at any leadership or other administrative meeting for purposes of handling and deciding any matter are collected and fully destroyed by Administration upon conclusion of the matter.

The Academic Office

- With the application of prospective students, Academic Office staff collects various personal data such as name, address, gender, phone number and email address, which is entered into a central academic cloud-based system, Semafox, where data is stored and secured. The registration process is completed by various forms. Semafox enables retrieval of all collected personal data and contact information for any registered student or former student. During and after studies, data are essential for various documentation. Grades and evaluations of each student are entered and retained in this central academic database. Requests for a transcript of a former student are based on private data collected by the Academic Office staff into the central academic database.
- Personal data such as name, graduation date, dates of study are requested through an online form for a transcript request. Name, address, date of birth and other information are requested through the online form for a attestation request.
- The Academic Office retains a personal hardcopy file with completed application, registration forms, references, grades, evaluations of all academic work, any communication and any important documentation concerning each student. The academic database automatically generates a unique ID number for each student; therefore, national ID number is not captured.
- All student exams and essays, including all evaluation and marking forms by grading professors, are retained for reference and locked. Only the Registrar, the Academic Dean, Dean of Graduate Studies and the President have sole access to these documents.
- All hardcopy data distributed to faculty and authorized participants at any academic meeting for the reason of handling and deciding any student matters are collected and fully destroyed by Academic Office personnel upon conclusion of the matter.

The Library

- To use library resources and borrow books, any student, faculty member, staff and guest must register in the library database system "Softlink" with their name, gender and an email address. The data are needed to issue notice of overdue books or any other issue in reference to the book.

The Information Technology Office/Research Center

- For the CTS enterprise network running Microsoft Windows Server 2012 R2, the Information Technology (IT) Office collects first and last names, email address provided by the user for contact purposes, user-defined passwords to access the network, student's degree program - BA/MTH/MLE etc., year of the student - first year/second year/third year, and "on campus" or "off campus" as well as a system-defined user account

ID. Secured by an Administrator account and password which only the IT Director knows, user data is solely accessible by the IT Director.
- The research center user accounts security will be through Amazon Web Services. They will capture first and last names and email addresses for contact purposes. Users will define their own passwords.

Student Life Office

- Student Life agreement is handed out and requested to be signed with the writing out of the name and date at registration. At the same time the student needs to fill in a campus service and maintenance form with their name, off/on campus status, work experience/training, preferences, a ministry form with the first and last name, email, phone number, study level, language, church involvement, means of transportation and a music information form with the name and various information about music and instrument experiences.
- For the Personal Tutorial Program each student must complete a student profile form providing their first and last name, address, study level, age, date and place of birth, family situation, languages, academic background, ministry, interests and hobbies. This information is for use by the tutor with the student, the Personal Tutorial Program officer and the registrar.

Legal Basis

- All personal data are received by consent. In completing required forms, students, faculty and staff agree to use of their data within CTS.
- To be conforming with the new EU General Data Protection Regulation, every person that provides data allows, by their signature on a privacy notice, the use of their requested, private data. Along with the privacy notice, personnel are requested to sign the consent clause on page 8.
- All private data is connected with the public task and official authority for the work of CTS and is carried out in all core functions.
- For special categories and sensitive personal information, a special justification must be submitted.
- Any data concerning student, faculty and staff that is neither legally required to be retained nor remains in use by the institution will, if in hardcopy, be directly and completely destroyed and, if in electronic format, be deleted from any database of the institution.

Third Parties

- Any student, faculty and staff data is strictly used within the organization of CTS and by authorized persons.
- CTS is required to share certain and specific personal data to third parties such as

institutions, official organs, etc.Applicable third parties are listed as follows:

Third Party	Kind of data	Reason for disclosure
Ministry of Education/NVAO	Data for statistics; for accreditation - various student data, marks, performances	State requirements; essential for program accreditation, information and control
Academic Examiners	Student exams and essays with marks and evaluation of instructors	In accordance with the academic evaluation procedure
Financial auditors	Data from the accounting office over financial matters with all files of student and vendor databases.	Legally required financial audit procedure as well as in accordance with the institutional Bylaws
Social Secretarial SDWorx	Personal data of employed faculty and staff	Legal requirement for the salary/tax processing
Employment Safety Enterprise Mensura& Insurance	Personal data of employed faculty and staff	Legal requirement for workers' health and safety
Local Commune	Personal data for registration with the commune	Legal requirement to register
Health Insurance/Partena	Personal data for those registering with the national health insurance	Legal requirement of health insurance
Institutional Headquarters of Assemblies of God World Missions	No detail personal data, but general data, accounting results and statistics	In accordance with the organizational & institutional Bylaws
CDM+ accounting support	Access to software data	Technical support

Overseas transfers

- Overseas transfers are limited to data transfers to United States (US) online services and the institutional headquarters of AGWM. In the US online services data are only stored, but not used by these services themselves.
- Storage of all academic data on the cloud system of Semafox.com in the US
- Storage of all accounting data on the cloud system of cdmplus.com in the US and UK
- Website server of ctsem.edu at blogs.com in the US
- Basic data in an annual financial report sent to AGWM headquarters in the US via email to the assigned person.

- Concerning the US transfer an "EU-US Privacy Shield" exists: The EU-US Privacy Shield decision was adopted on 12 July 2016 and the Privacy Shield framework became operational on 1 August 2016. This framework protects fundamental rights of anyone in the EU whose personal data is transferred to the United States for commercial purposes. The framework also brings legal clarity for businesses relying on transatlantic data transfers. The new arrangement includes:
  - strong data protection obligations on companies receiving personal data from the EU
  - safeguards on US government access to data
  - effective protection and redress for individuals
  - an annual joint review by EU and US to monitor the correct application of the arrangement.

  The first annual review took place in September 2017 and, on that basis, the Commission published on 18 October 2017 a report on the functioning of the Privacy Shield.

Security

- CTS network electronic data is secured through Microsoft Windows Server 2012 R2 and backed up onsite as well as offsite. The network server hardware is secured behind three physical locks within the CTS facility - server cabinet, server closet, and research center door. IT does not monitor user data retained on the network that is created, maintained, or accessed by the users. CTS IT personnel do not know or track user passwords. User accounts definitions are only accessible by the IT Director, secured by an Administrator account and password which only the IT Director knows.
- All desktops and laptops of CTS are password-protected and well-secured from outside. By signed policy, any person working with a CTS-owned desktop must lock or close their account when leaving their working place. Personnel who work from home or outside the institution must keep data secure and constantly lock their laptop or desktop when leaving it or not working on it. Laptop or desktop with data from CTS may not be used by a third person not belonging to CTS or being authorized to use it.
- CTS uses Google Suite for Education where the only information IT captures for users is name - first name and last name. Users define their own passwords. Various data of departments, faculty, staff and students are stored on their cloud-based Google drives, saved by their own passwords. Emails are encrypted by Google.
- All personal electronic data from the academic office is stored in the cloud of Semafox.com and protected by a password. Only authorized personnel have access to the system.
- All personal electronic data of the business office is stored in the cloud of cdmplus.com and protected by a password. Only authorized personnel have access to the system.
- All personal electronic data of the library is stored in the cloud of Softlink Europe Ltd and protected by a password. Only authorized personnel have access to the system.
- The IT department monitors the Wifi network to exclude the use of illegal websites. We are not working with Website Cookies or Google Analytics.
- All student paper files in the academic office are stored in a secured location and locked. Only limited authorized personnel have access to the files.

- All faculty, staff, supplier files and legal accounting paper documents are stored in a secured location and locked. Only limited authorized personnel have access to the documentation.
- There is an ongoing process of scanning and storing data on electronic data storage, abiding with paper storage requirements in all institutional departments.

Retention

- Network accounts containing personal data that have not been used for seven years and longer are deleted.
- Accounting documents such as invoices, payment receipts, and ledgers are retained as required through the legal time of ten years and then destroyed.
- Since the institution needs to give accountability for all the work and achievements for all students that went through any of our study programs at any time in the history, we need to keep all files and information infinite. The same is for personal electronic data in the accounting program. Persons that are not active in the institution are put on non-active and thus not seen at the daily use of data. However they are stored on the database.
- The personal data of the library will be deleted when a student finishes studies or any other person has not used the library for a certain time.
- Any other data not referring to the academic or accounting data, can be deleted on a person's request.
- If a person does not want to be photographed or recorded for the website or Facebook account during any open event in the institution, please contact and inform the Data Protection Officer.

Sources of data

Where personal data has not been obtained directly from the data subject, details should be provided.

Your rights

You have the right to request to see a copy of the information we hold about you and to request corrections or deletions of the information that is no longer required.

If you provide consent for us to use your personal data in the ways outlined above, you have the right to subsequently withdraw your consent.

In some circumstances you may have the right to object to the processing of your personal data, to request it is erased where it is no longer required for the stated purposes, or that inaccurate information about you is corrected. For more information about your rights see the *Data*

Protection Policy.

To exercise these rights please use the contact details below:

Contact details

If you have any questions relating to this form or the way we are planning to use your information please contact:

Sascha Wyrwal, Vice President Operation

Continental Theological Seminary

Kasteelstraat, 48

1600 Sint-Pieters-Leeuw

Belgium

Email: accountant@ctsem.edu

Phone: +32.2.334.85.35

Fax: +32.2.334.85.59

Website: www.ctsem.edu

The Data Protection Officer of CTS is Sascha Wyrwal, Vice President of Operation. If you have any questions relating to data protection, these can be addressed to: accountant@ctsem.edu in the first instance.

Consent clause

☐ I consent to Continental Theological Seminary processing my personal data for the purposes detailed in the *CTS GDPR Privacy Notice*.

☐ I consent to Continental Theological Seminary using photographs and/or video/audio recordings including images of me both internally and externally to promote the University. These images could be used in print and digital media formats including print publications, websites, e-marketing, posters, banners, advertising, film, social media, teaching and research purposes.

I understand that images on websites can be viewed throughout the world and not just in Belgium and that some overseas countries may not provide the same level of protection to the rights of individuals as EU/Belgium legislation provides.

I understand that some images or recordings may be kept permanently once they are published and be kept as an archive of CTS life.

I have read and understand the conditions and consent to my images being used as described.

I have read and understand how my personal data will be used.

Printed Name:……..

Signed: .....

Date: .....

Appendix 1 – Template for notice of Photography/Filming

Photography/ Filming in Progress

Please note that filming/photography is taking place [at this event/in this area] for promotional and archival purposes. The photographs and recordings made are likely to appear on our website.

If you would prefer not to be photographed please let the photographer know.

For further information contact:
[Name and contact details of event organizer/ representative at the event]