# REGULATIONS OF THE INSTITUTIONAL E-MAIL SERVICE INTERNATIONAL MEDICAL UNIVERSITY OF ROME "UNICAMILLUS"

**First approval by the Organizing Committee of March 18, 2020**

**Review by the Organizing Committee of June 15, 2022**

UNICAMILLUS

## Index


| | |
|---|---|
| **Introduction, purpose and field of application** | **3** |
| **ARTICLE 1 - Regulatory framework and glossary** | **3** |
| **ARTICLE 2 - Email service Users – Personal mailboxes** | **6** |
| **ARTICLE 3 - Terms of access, conditions of use, limits and unauthorised uses** | **6** |
| **ARTICLE 4 - Mailbox availability** | **7** |
| **ARTICLE 5 - Impersonal mailboxes** | **8** |
| **ARTICLE 6 - Use of personal and impersonal mailboxes** | **8** |
| **ARTICLE 7 - Suspension and revocation of the service** | **9** |
| **ARTICLE 8 - Service deactivation** | **9** |
| **ARTICLE 9 - University's areas of responsibility** | **10** |
| **ARTICLE 10 - User's areas of responsibility** | **11** |
| **ARTICLE 11 - Email security** | **12** |
| **ARTICLE 12 - Mailing lists** | **12** |
| **ARTICLE 13 - Inspections and operational continuity** | **13** |
| **ARTICLE 14 - Certified Email (CEM)** | **14** |
| **ARTICLE 15 - Staff training and awareness** | **14** |
| **ARTICLE 16 - Fines and disciplinary measures** | **15** |
| **ARTICLE 17 - Final provisions** | **15** |

**Introduction, purpose and field of application**

Due to the constant technological evolution and the consequent processes of digitalisation, the *Saint Camillus International University of Health Sciences* (hereinafter referred to as "*UniCamillus*") requires the use of multiple IT tools, including the use of the email service, in order to perform its daily tasks and activities, as it is functional to didactics, research, administration and/or other related and instrumental tasks to the institutional purposes of the University.

The use of such tools must be disciplined by certain regulations as behaviour - even unconsciously not legitimate - may have serious consequences, both on a technical level (such as a block of functionality or loss of data) and on a legal level, with possible liability for those involved.

This service, for the provision of which UniCamillus may also use systems or infrastructures of third party operators (hereinafter referred to as "Providers"), includes, among other things, the creation and issue of email boxes and related additional services such as calendar, contacts, online storage space, etc.

In view of the above, UniCamillus University regulates and encodes the conditions and procedures for the correct use of the email service and the related possible controls, in its quality of data processing procedure Owner with the present Regulation. Said Regulation, together with the specific Information pursuant to art. 13 of Regulation (EU) 2016/679, attached to this document ***(Annex 1)***, are published on the University website as well as delivered in printed and/or digital form to all employees, lecturers, students, collaborators in various capacities and any further appropriately identified users, in order to guarantee specific knowledge about the relevant service in a clear, punctual and detailed manner

## ARTICLE 1 - Regulatory framework and glossary

EUROPEAN REGULATION

- Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC ("General Data Protection Regulation"), hereinafter also referred to as "GDPR".

ITALIAN REGULATION

- Legislative Decree No. 196 of June 30, 2003 ("Personal Data Protection Code") as amended by Legislative Decree No. 101/2018;
- Law No. 300 of May 20, 1970, Regulations on the protection of the freedom and dignity of workers, trade union freedom and trade union activity in the workplace and regulations on employment (so-called "Workers' Statute");
- Legislative Decree No. 231 of June 8, 2001, containing the 'Regulation on the administrative liability of legal persons, companies and associations, including those without legal personality, pursuant to Article 11 of Law No. 300 of September 29, 2000', published in the Official Gazette No. 140 of June 19, 2001, as amended and supplemented;

- Legislative Decree No. 150 of September 14, 2015 on the subject of employment services and active policies (so-called Jobs Act);
- Legislative Decree No. 195 of June 23, 2003 on the subject of services for the prevention and protection of workers;
- Article 15 of the Italian Constitution on the "Rights and duties of citizens";
- Civil Code - Article 2049: Indirect liability of the entrepreneur; - Article 2086: Management and hierarchy in the enterprise; - Article 2087: Protection of the physical integrity and moral personality of employees by the entrepreneur; - Article 2104: Diligence of the employee in respecting the instructions given by the entrepreneur;
- Criminal Code - Article 616: Violation of domicile and personal communications.

MEASURES OF THE PERSONAL DATA PROTECTION AUTHORITY

- Guidelines of the Data Protection Authority on Electronic Mail and the Internet (Resolution no. 13 of March 1, 2007, published in the Official Gazette no. 58 of March 10, 2007);
- Provision of the Data Protection Authority of November 27, 2008, and subsequent amendments relating to "Measures and arrangements prescribed for data processing procedures Owners of processing operations carried out by electronic tools in relation to the assignment of the functions of System Administrator"; Provision of the Data Protection Authority No. 547 of 2016;
- Provision of the Data Protection Authority no. 138 of 2017;
- Provision of the Data Protection Authority No. 139 of 2018;
- Provision of the Data Protection Authority No. 53 of 2018;
- Provision of the Data Protection Authority No. 216 of 2019;
- Provision of the Data Protection Authority No. 214 of 2020;
- Circular of the Digital Italian Agency - AGID No. 2 of April 18, 2017, in relation to "Minimum ICT security measures for public administrations. (Directive of the President of the Council of Ministers of August 1, 2015)".

GLOSSARY

In compliance with Regulation (EU) 2016/679, data can be classified as follows:

**Personal data**: any information relating to an identified or identifiable physical person; an identifiable person is one who can be identified, directly or indirectly, by particular reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more features of his/her physical, physiological, genetic, mental, economic, cultural or social identity. Personal data are: first name and surname, address, tax code, photo, IP address or any other audiovisual record. In fact, the person can be identified also through other information that is not directly identifying (e.g. by associating the recording of a person's voice with his/her image, or the circumstances in which the recording was made: place, time, situation).

**Special categories of data**: special categories of data: personal data, which require special precautions due to their sensitivity; these data can reveal racial or ethnic origin, political

opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data intended to uniquely identify a natural person, as well as data relating to a person's health or sexual orientation.

**Legal data**: personal data relating to criminal convictions and offences or to related security measures (such as personal data suitable for detecting measures issued by the legal authorities and contained in the criminal record, the register of administrative sanctions dependent on offences and the related pending charges, or the quality of defendant or suspect pursuant to Articles 60 and 61 of the Code of Criminal Procedure).

"***Data processing***" means "*any operation or set of operations concerning the collection, recording, organisation, storage, processing, modification, selection, extraction, comparison, use, interconnection, blocking, communication, dissemination, deletion and destruction of data*".

The "***electronic mail service***" is an institutional work tool owned by UniCamillus University, made available to employees for the mere performance of their work.

All internal and external users authorised to use the University email service are required to comply with this Regulation. The use of the email box is subject to the full and unreserved application, by the user, of this Regulation. The use of the relevant service constitutes implicit acceptance of the prescriptions codified herein by the User.

"***Internal Users***" are individuals, who can use UniCamillus IT tools within the "corporate domain", on the basis of contractual or conventional agreements authorised by the University.

"***External Users***" are physical individuals, public and private companies and suppliers, who access some components of the University IT System from outside the "corporate domain", on the basis of contractual or conventional relationships agreements authorised by the University.

With regard to privacy roles, internal Users may be identified by UniCamillus, as so-called "*Privacy Referents*", for specific tasks and functions or as "Authorised Personal Data Processors" (formerly Data Processors), pursuant to article 29 of Regulation (EU) 2016/679 and artice 2-quaterdecies of Legislative Decree 196/2003 as amended by Legislative Decree 101/2018, while Users external to the University may operate as data processors, in the hypothesis of collaboration of physical or legal persons, conventions, consultancies, internships, contracts, etc., pursuant to article 28 of GDPR or as Authorised Processors, in compliance with the above-mentioned regulations (henceforth they are all also referred to as "Staff", "Workers", "Users").

Employees are required to access their assigned email box at least on a daily basis and to use this tool for any interpersonal communication within the scope of work purposes. In order to safeguard the integrity and confidentiality of email messages and contents, it is forbidden in any case to disclose the news, data and any other information learned when receiving or sending e-mails to unauthorised persons, in compliance with the duty of secrecy to which Users are bound and in accordance with the duties of loyalty and fairness.

**ARTICLE 2 - Email service Users – Personal mailboxes**

By means of non-exhaustive examples, the following categories of users are provided with an electronic mailbox (so-called personal mailbox):

1. students enrolled in any course of study (degree courses, post-graduate degrees, PhDs, specialisation schools): in this case, the email address is made up of 2 letters (first letter of the first name and first letter of the surname), the student's immatriculation number and the *@students.unicamillus.org* domain;
2. university staff in active service, on fixed-term or permanent contracts, for the duration of the employment relationship: in this case, the format of the email address is *nome.cognome@unicamillus.org*, except in cases of homonymy;
3. assignees, contract workers and collaborators: in this case, the format of the email address is *nome.cognome@unicamillus.org*, except in cases of homonymy. For lecturers on contract or in retirement, the request for activation or possible temporary preservation of the email address must be validated by the Rector and made by the applicant through a special procedure;
4. subjects other than the above, who are provided with an email address with the *@unicamillus.org* domain, following an assessment of opportunity.

Finally, UniCamillus University reserves the right to individually examine the assignment of e-mail boxes for further cases, which are not included in the above-mentioned categories.

**ARTICLE 3 - Terms of access, conditions of use, limits and unauthorised uses**

Access to the mailbox is normally granted exclusively to the assignee, through credentials (username and password) uniquely associated to the mailbox itself and exclusively managed by the assignee under his/her own responsibility.

The password must be kept secret, adopting appropriate measures for its safekeeping; the User commits to actively ensuring that its confidentiality is safeguarded and to report any situation that may invalidate it. The User shall be responsible for the activity performed through his/her account.

The User is obliged not to disclose his/her authentication credentials (UserID and password) to anyone, including colleagues, system administrators and superiors, taking the utmost care in their safekeeping and preserving their secrecy even when typing them in. Should the User become aware that someone may have seen the typing or otherwise have knowledge of the password, he/she shall immediately change it.

Should the User be asked to pass on the password in any form whatsoever (by telephone, e-mail, etc.), he/she must refuse and immediately inform the Head of the University Information Systems Service of the event.

It is forbidden to use the “auto-fill” or “remember password” options, which may be present in browsers or other applications, when configuring email boxes.

It is forbidden to communicate, exchange or share passwords between several users (even if they belong to the same work team) or to disclose personal passwords to third parties (even if they are

colleagues or system administrators); any behaviour, which does not comply with this requirement, may result in disciplinary sanctions.

The minimum requirements for password strength are:

- upper and/or lower case characters;

- use of symbols, numbers, punctuation and letters;

- passwords must be numerically at least 8 characters long;

- passwords must not be based on personal information, family references or in any case data relating directly to the password holder.

It is forbidden to use work-related passwords (e.g. for accessing a PC, mail or various applications) for registration on other websites.

The Staff is obliged to change the password to access IT tools at least every 90 days. Only in exceptional cases may the password be reset by the staff of the University IT Service.

Passwords must be kept with diligence to prevent third parties from gaining knowledge of them, and any loss, theft or disclosure must be promptly reported to the staff of the University IT Service.

Under no circumstances must unencrypted passwords be recorded on either paper or computer media.

It is strictly forbidden to send messages by simple email with file attachments (or in the body of the text) containing special categories of data or data relating to criminal convictions or offences. Such documents may be transmitted either by using the more secure PEC (certified email), or by adopting appropriate protection to prevent them from being read by unauthorised persons; it will then be possible to forward the documents by simple email, but by placing them in a ZIP file protected by a password. The access key must then be sent by a different communication channel (e.g. by SMS) or by telephone.

**ARTICLE 4 - Mailbox availability**

The personal mailbox is granted to assignees as long as their user status is active, according to article 2, except in cases of suspension of service as provided for in article 7.

Without prejudice to the provisions of article 8 of the present Regulation, the following rules also apply according to certain statuses, which determine the relationship between the User and UniCamillus University:

- end of the employment or study relationship. The mailbox shall be deactivated immediately. However UniCamillus may consider the possibility of granting an extension period in which the user may read and receive mail messages upon express and motivated request, after which time the mailbox shall be deactivated;

- in the case of emeriti or retired lecturers, who continue to carry out research and/or lecturing activities under contracts stipulated with the University, please refer to article 2 point 3 of the present Regulation.

- secondment/waiting/suspension. UniCamillus reserves the right to assess individual cases in order to establish which email box functions can be kept active and for how long and which, instead, can be revoked.

**ARTICLE 5 - Impersonal mailboxes**

In addition to the provisions of Article 2, UniCamillus University makes available email addresses for the University Offices, shared by the operators assigned to them, i.e. to academic positions, organisational positions and structures, work groups (so-called impersonal mailboxes), in order to make the non-private nature of institutional correspondence clear; in this case, the format of the email address is *denominazione@unicamillus.org*.

The University promotes the use of impersonal mailboxes among the categories of users, also with a view to improving the functioning of the University organisation, in compliance with the principles of confidentiality.

Impersonal mailboxes are issued at the request of the position holder or the head/coordinator of the work unit. The applicant assumes the role of pro-tempore "main assignee" of the mailbox and is responsible for its correct use in a very analogous way to the use of a personal mailbox, in accordance with the present Regulation.

The main assignee grants access to the mailbox to all the employees, the individual assignees are responsible for the use of the mail service, in accordance with the present Regulation.

In the event of a new owner/manager taking over the organisational position, the assignment may be transferred to the successor, who assumes the role of new pro-tempore main assignee.

The impersonal mailbox remains active until a request for deactivation is made by the pro-tempore main assignee, without prejudice to the cases of suspension of the service, as provided for in Article 7.

Where University Offices and components require, for particular needs (events, projects, programmes, initiatives), a service email address on the *@unicamillus.org* domain, they may submit a specific motivated request through their Responsible on a special "activation form" addressed to: *privacy@unicamillus.org*.

**ARTICLE 6 - Use of personal and impersonal mailboxes**

For all internal communications (exchange of emails with other UniCamillus Staff members provided with personal mailboxes) only personal mailboxes should be used (*nome.cognome@unicamillus.org*).

For all external communication, with lecturers (even if they have personal mailboxes) and with students, impersonal mailboxes should normally be used (*denominazione@unicamillus.org*).

The contents of all emails, both personal and impersonal, must be signed at the bottom with the sender's name and surname in any case, also in order to identify him/her within the same work unit.

**ARTICLE 7 - Suspension and revocation of the service**

LUniCamillus University may suspend the use of the mailbox in the following cases:

1. non-compliance of the present Regulation by the user;
2. situations referred to in articles 4 and 13;
3. lack of use of the mailbox by the user for a period of more than six months;
4. emerging University's reasons of interest or new assessment of the University's original interest.

**ARTICLE 8 - Service deactivation**

Upon end of the relationship with UniCamillus University for any reason whatsoever (e.g. retirement, dismissal, transfer to another employer, end of course of study, etc.), the User's institutional email account (owned by the University) shall be deactivated and automatic systems shall be adopted to inform third parties and provide them with alternative addresses. The deactivation of the account will be followed by the deletion of the institutional email address and the final deactivation of receiving incoming messages. Emails will be retained only for the purposes of protecting rights in court, within the limits set out in Article 160-bis, Paragraph 1 of Legislative Decree 196/2003 as amended by Legislative Decree 101/2018.

In particular, the mailbox shall be deactivated:

- for permanent and fixed-term staff, both lecturers and technical-administrative staff, upon end of employment with the University;
- for students at the end of their studies;
- for PhDs, at the end of the PhD cycle, subject to the possibility of extension;
- for other users, on the expiry date indicated in the "activation form", subject to the possibility of early conclusion due to achievement of the intended purposes.

For justified reasons connected with the University's institutional activity, it is possible to request an extension of the expiry date by means of a reasoned communication to be sent to *privacy@unicamillus.org*, for possible approval by the Rector.

Before the deactivation of the email box, the user will receive an email containing a specific notice.

Email addresses requested for special purposes will be deactivated automatically, unless an extension request is made on the scheduled expiry date.

**ARTICLE 9 - University's areas of responsibility**

UniCamillus University commits to using the user's identification data for the mere purpose of providing and managing the service. This data will be protected in accordance with the current legislation on the processing of personal data.

UniCamillus is not responsible for the suspension of the institutional email service due to, for example:

a) ordinary or extraordinary maintenance;

b) malfunctions and unforeseen and unpredictable events;

c) interventions for security reasons.

In any case, UniCamillus is not responsible in relation to the deletion, damage, failure to send/receive or failure to store email messages or other content, resulting from failures and/or malfunctions of the management equipment and, in general, from the provision of the email service itself or any additional services provided by the Provider.

UniCamillus will not store messages, that exceed any space limits made available for each of them, either incoming or outgoing for individual mailboxes. The University does not make mail backups, so it is up to the User to make a local copy of the messages and their backup.

In the messages sent through corporate (service and/or named) emails, the following Disclaimer will be enclosed, in Italian and English language:

"*Ai sensi dell'art. 13 del Regolamento 2016/679/UE, La informiamo che la presente e-mail proviene dall'Università Saint Camillus International University of Health and Medical Sciences (Unicamillus) e s'intende inviata per scopi lavorativi. Per tale ragione non è possibile garantire che, rispondendo alla stessa, il contenuto venga visualizzato esclusivamente dal soggetto cui è indirizzata la risposta. Si precisa che le informazioni contenute in questo messaggio sono confidenziali, riservate e a uso esclusivo del destinatario. Qualora lo stesso Le fosse pervenuto per errore, La preghiamo di eliminarlo immediatamente dandocene cortese comunicazione. Grazie.*".

"*Pursuant to Article 13 of Regulation (EU) 2016/679, we inform you that this email comes from Saint Camillus International University of Health and Medical Sciences (UniCamillus) and is intended to be sent for business purposes. For this reason, it is not possible to guarantee that, by replying to it, the content will be viewed exclusively by the person to whom the reply is addressed. It is specified that the information contained in this message is confidential and for the exclusive use of the recipient. If it was received by mistake, please delete it immediately by giving us, kindly, notice. Thank you.*".

**ARTICLE 10 - User's areas of responsibility**

The mailbox is the tool dedicated to institutional communications of the University. Therefore, users commit to using it for such purposes.

Users agree not to use the services subject to the present Regulation for illegal purposes, which do not comply with the same or that may cause damage or harm to UniCamillus or third parties in any case.

Users agree to use mailboxes only for activities related to their relationship with the University. Any further use involving commitments for the University outside this context will be considered illegal, unless expressly authorised.

Should users need to use the service for personal reasons of particular and proven seriousness and urgency, they may make a request to their direct supervisor. In the aforementioned hypotheses, UniCamillus may authorise the private use of the service, even only from certain workstations or specific boxes and, in any case, outside of working hours or during breaks.

Users assume all criminal and civil liability and any charges arising from improper use of the service.

In particular, users may not use email to send, even via links or attachments in any format (text, images, video, audio, executable code, etc.), messages containing or referring to:

- non-institutional, obvious or subliminal advertising;
- advertising and/or requests for funding in favour of other entities or external structures;
- private commercial communications;
- so-called "Chains letters";
- incitement to violence and criminal behaviour;
- material and content of a pathological nature (such as torture, etc.);
- pornographic or similar material, in particular in violation of Law No. 269 of 1998 on: "Rules against the sexual exploitation of minors under 18 years of age" and subsequent amendments and additions;
- material that is discriminatory or damaging in relation to race, sex, religion, etc.;
- material violating privacy legislation;
- content or material violating the property rights of third parties;
- defamatory or patently offensive content;
- any content that does not comply with the provisions of the University Ethical Code and the current legislation.

The above list is to be understood as an example and not exhaustive.

Furthermore, Users may not use the service to undermine or interfere with the proper functioning of the email system and the use of the service by other users. Under no circumstances may users use email to disseminate malicious computer code such as viruses and similar.

Users may not attempt to access mailboxes for which they are not authorised, by hacking, password forgery or other illegal or fraudulent means. If a threat is detected, the service will be suspended.

Users commit to actively safeguarding the confidentiality of their passwords and to reporting any situation that may invalidate them. In particular, users must carefully avoid clicking on links and/or opening attachments whose origin, security and function are uncertain.

Users commit to implementing all suitable and necessary measures at their email access point in order to avoid, or at least minimise, the dissemination of computer viruses and similar.

Users are aware that knowledge by third parties of their access codes (username and password) would allow them to access their mailbox and use all its functions; to this end, they agree to:

- change their initially assigned password with one of their own choice every 90 days;
- not disclose their access codes to third parties.

Users are responsible to the University and to third parties for the use of their access codes.

UniCamillus reserves the right to report any violations of the present conditions of use to the competent bodies, for the appropriate inspections and measures..

**ARTICLE 11 - Email security**

UniCamillus University may use appropriate tools and procedures to verify, quarantine or delete messages, which could compromise the proper functioning of the email service. This is without prejudice to the University's right to carry out inspections in the cases provided for in Article 13.

**ARTICLE 12 - Mailing lists**

Without prejudice to the provisions of Article 9, the use of mailing lists by the University is provided for and authorised for institutional purposes only.

Mailing lists are used by the University to send messages to the users referred to in Article 2.

Each user will be included in one or more mailing lists (e.g. the list of students of a given Degree Course, of all lecturers, of all the technical-administrative University Staff, etc.).

**ARTICLE 13 - Inspections and operational continuity**

The mailbox may be subject to inspection by UniCamillus University, being an institutional and not a private tool, with the help of specially authorised internal or external technical staff, in the following cases:

1. anomalies;
2. suspected illegal activities;
3. request by legal authorities.

In the event of necessity and urgency and/or in the presence of any anomalies, UniCamillus University therefore reserves the right to carry out inspections on the methods and purposes of the use of email, especially in order to verify the functionality and security of the IT system, in full compliance with current legislation, the freedom and dignity of workers as well as the principle of necessity, relevance and non-excessiveness. Except in cases of unforeseeable urgency, inspections shall be carried out gradually: in the first stage, they shall be carried out on an occasional and/or sample basis, by group, office and University organisational unit inspections, in order to identify the area to be called upon to comply with the rules, and only afterwards, when the anomaly is repeated and if necessary, shall inspections also be carried out on an individual basis and on the entire data traffic area of the University email. UniCamillus commits not to carrying out prolonged and/or indiscriminate inspections and to guaranteeing their traceability.

In the event of serious and proven reasons, which may detect the occurrence of offences or illegal conduct, UniCamillus may carry out so-called *"defensive inspections"* on institutional University accounts, for the purposes of defence, protection of the assets and safety of the work and University structure, aimed at ascertaining the well-founded suspicion of possible illegal conduct by the worker.

The inspections will also be carried out by UniCamillus upon notification by the Legal Authority as part of investigations conducted for the suppression, detection and prevention of crimes.

UniCamillus University commits not to processing any data that may be extracted from the institutional email account, except for their storage in order to protect rights in legal proceedings for the time strictly necessary for this purpose.

In the event of any access to the email account granted to the User, the data of third parties will be protected and the identity of the User's interlocutors will not be revealed.

In the event of planned absence and in order to guarantee its own operational continuity, UniCamillus University requires the User to enter - via the appropriate function of the email client - the following notice to the senders of email messages: "*I will be absent from_____to_____. For emergencies, please contact the Office _____ at the email address _____or contact Mr ____or at the email address _____*".

A person delegated by UniCamillus (e.g. the Head of the organisational unit to which he/she belongs or the superior) shall be entitled to view the email messages of the absent worker in the presence of at least one other person identified by the latter as a witness and subject to

deactivation of the access password by the system administrators, in the event of urgent work necessity and in order not to compromise or slow down the production processes and institutional activities of the University, in the event of sudden or prolonged absence of an employee, if it is necessary to know the content of email messages sent to the University address or in the event of maintenance or urgency reasons. The aforementioned person, designated by UniCamillus, shall draw up a report of this activity and inform the User, where possible in advance, otherwise at the first useful opportunity. The User shall be required to enter a new password to access his/her mailbox at the first useful opportunity.

## ARTICLE 14 - Certified Email (CEM)

The Certified Email (so-called CEM) is a communication system similar to standard email to which security and transmission certification features are applied. These features add legal value to transmitted messages. The legal value is ensured by the sender and the receiver's CEM mail operators, who certify:

1. date and time of sending of the message by the sender;
2. date and time of delivery of the message to the receiver;
3. integrity of the message (and any attachments) in transmission from the sender to the receiver.

Mail operators also ensure that the sender and the receiver are notified of any problems occurring during transmission.

CEM transfers the concept of "Registered mail with return receipt" to digital. The use of email as opposed to traditional mail guarantees real-time delivery. Legal value: unlike traditional email, CEM is given full legal value and receipts can be used as proof of sending, receipt and even the content of the transmitted message. The communication has legal value only if sent and received by CEM.

The CEM extension pec.unicamillus.org only accepts documents from CEM boxes in order to guarantee users by countering spamming and incorrect use.

## ARTICLE 15 - Staff training and awareness

UniCamillus University organises and implements, with its own DPO and with experts in the relevant sector, specific training and updating courses on personal data protection and security measures, in order to increase workers' skills and awareness and also improve the management of institutional information on an ongoing basis and at all the various stages of the users' working life (from the moment they enter the service on the occasion of changes in duties or the introduction of significant new tools relevant to the processing of personal data, and then also with subsequent periodic reminders). Training and full awareness of the Staff in safely carrying out work activities is among the first security measures on the subject of confidentiality and personal data protection, communications and information.

Said continuous training is intended to be additional to the instructions already given by UniCamillus, the data processing procedure Owner, pursuant to Article 29 of Regulation (EU) 2016/679 and Article 2-quaterdecies of Legislative Decree 196/2003 as amended by Legislative Decree 101/2018. The Data Protection Officer (rpd@unicamillus.org) is the point of contact for all employees and Users (internal and external) for activities concerning and implying personal data processing, and is available for any doubts or reports. Please note that the provided training courses are not optional and that failure to attend and unjustified absence may lead to the adoption of disciplinary measures.

## ARTICLE 16 - Fines and disciplinary measures

Failure to comply with or violation of the rules contained in the present Regulation shall be punishable by disciplinary measures under the current legislation, as well as, in the most serious cases, by civil and criminal prosecution. However, a temporary ban may be applied immediately on the use o fIT tools as a precautionary measure. The disciplinary sanctions provided for by the applicable National Collective Labour Agreement (NCLA) will be applied depending on the seriousness of the committed violation.

However, the employee will be asked to justify the reason for the incorrect use of the institutional email before any disciplinary decision is taken.

Finally, it should be noted that, the present Regulation is delivered to all Users in paper or digital form also for disciplinary purposes, and upon activation of the UniCamillus University email service account, in addition to being always available and downloadable on the institutional website, together with the specific Privacy Notice pursuant to Article 13 of Regulation (EU) 2016/670.

## ARTICLE 17 - Final provisions

For anything not expressly governed by the present Regulation, please refer to Regulation (EU) 2016/679 and the amended Privacy Code, the provision in terms of Internet and email issued by the Data Protection Authority, correct Resolution no. 13 of March 1, 2007, as well as the other relevant applicable legislation.