E-document copy

ORDER

OF THE RECTOR OF VILNIUS UNIVERSITY ON THE AMENDMENT TO ORDER OF THE RECTOR OF VILNIUS UNIVERSITY NO. R-316 OF 25 MAY 2018 "ON THE APPROVAL OF THE DESCRIPTION OF THE PROCEDURE FOR THE PROCESSING OF PERSONAL DATA AT VILNIUS UNIVERSITY"

In accordance with Article 43(1)(19) of the Statute of Vilnius University and with the aim to implement Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation):

1. I hereby a m e n d the Description of the Procedure for the Processing of Personal Data at Vilnius University approved by Order of the Rector of Vilnius University No. R-316 of 25 May 2018 "On the Approval of the Description of the Procedure for the Processing of Personal Data at Vilnius University" (wording of Order of the Rector of Vilnius University No. R-391 of 25 September 2020), and recast it (attached).

2. I hereby a s s i g n the Data Protection Officer of Vilnius University to publish the Description of the Procedure for the Processing of Personal Data at Vilnius University approved in Item 1 of this Order on the website of Vilnius University.

APPROVED
by Order No. R-316 of 25 May 2018
of the Rector of Vilnius University (wording of
Order No. R-425 of 10 December 2021
of the Rector of Vilnius University)

DESCRIPTION OF THE PROCEDURE FOR THE PROCESSING OF PERSONAL DATA AT VILNIUS UNIVERSITY

CHAPTER I
GENERAL PROVISIONS

1. The Description of the Procedure for the Processing of Personal Data at Vilnius University (hereinafter the 'Description') establishes the requirements for the processing and protection of personal data, the scope and purposes of the personal data processing, the rights of data subjects and the procedure for exercising them, and the technical and organisational measures for data protection.

2. This Description has been prepared in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter the 'GDPR'), the Republic of Lithuania Law on Legal Protection of Personal Data (hereinafter the 'ADTAĮ'), the Labour Code of the Republic of Lithuania, and other legal acts.

3. All the University's employees, students, persons admitted for internship at the University, trainees, and persons performing functions or activities at the University on other grounds who process personal data held at the University or who have become acknowledged with such data in the course of their duties must comply with this Description.

4. The terms used in this Description shall be understood as they are defined in the GDPR, ADTAĮ, and other legal acts.

5. The personal data of the data subjects is processed by the data controller – Vilnius University, legal entity code 211950810, registered office address Universiteto g. 3, 01513 Vilnius.

6. The provisions of this Description may not extend or restrict the scope of application of the ADTAĮ and the GDPR and may not contradict the personal data processing requirements of the ADTAĮ and the GDPR as well as any other legal acts regulating the processing of personal data.

CHAPTER II
THE PURPOSES, LEGAL BASIS AND TIME LIMITS FOR THE PROCESSING OF PERSONAL DATA

7. Personal data shall be processed at the University in non-automated filing systems and/or by automated means for the following purposes:

7.1. For the purpose of administering the study process, on the basis of concluded agreements and legal obligations, the following data is processed: full name, full name of the representative (if the person is represented), personal identification number, date of birth, national ID number (optional), gender, address of residence, phone number, email address, nationality, marital status, emergency contacts (optional), length of employment, social status (belonging to a disadvantaged group), military service, education data (school code, name, type, year of graduation, country), data on the person's studies (cycle, form, faculty, programme, year, semester, group, type of studies, type of funding, amount and year of the State allowance for studies per

student, student identity card number, course units taken, form of assessment, date, assessments of the learning outcomes), other diploma data, identification numbers assigned to the studying person, bank account number, payments made and/or benefits received, amounts and dates thereof, as well as type, series, number, and date of validity (issue) of documents issued to the studying person, video and/or audio recordings of remote lectures and assessments.

7.2. For the purpose of administering the scientific process and publicising the results, on the basis of contractual relationships and legal obligation, to establish authorship of scientific production, for publishing scientific and other publications, assessing the results of the research (and artistic) activities of the staff and students, the following data is processed: data subject's (author's) full name, personal identification number, personal phone numbers, personal email address, address of residence, workplace, date of birth, institution (of work or studies), the unit of the institution (of work or studies), type of studies (for students), academic group (for students) of the data subject (author), date of commencement of studies (for students, residents, doctoral students), date of completion of studies (for students, residents, doctoral students), staff group (for staff), position, degree (for staff), date of commencement of employment, date of the end of employment and/or the date of defence, language in which the final thesis or research paper is written, the topic of the final thesis or research paper, the topic of the final thesis or research paper in English, the abstract of the final thesis or research paper in English and Lithuanian, the positions and identifying data of the participants in the defence process, the online access status of the final thesis or research paper, the time limit of the restriction, date of publication, the indication of performing coincidence verification of the final thesis or research paper, the result of the coincidence verification of the final thesis or research paper, data used to identify the person who carried out the coincidence verification, final thesis or research paper documents, video and/or audio recording of the meeting of the paper defence.

7.3. For the purpose of internal administration (structure management, information management of current and former staff, document management, management of available material and financial resources), the following data is processed on the basis of concluded contracts and legal obligations: full name, nationality, address of residence, personal identification number, date of birth, sex, photograph, signature, marital status, emergency contacts (optional), full names and personal identification numbers of family members and dependants, personal social security number, amounts of remuneration and social security contributions, details of voluntary insurance contracts, dates of insurance with public funds, details of participation in pension savings, current account number, phone number, email address, CV, job position, details of recruitment/reassignment, dismissal, length of service, position to which the person wishes to be appointed or transferred, tabular identification number of the employee, data on education and qualifications, pedagogical titles, identification code in the register of teachers, date of entry/change of data, data on leave, data on secondments, data on an individual work schedule, data on remuneration, allowances, compensation, benefits, information on working time, information on incentives and penalties, information on official misconduct or breach of work duties, data on the evaluation of the activities of the employee, details of declarations of public and private interests, passport and/or identity card number(s), date of issue, date of validity, issuing authority, registration date and number of documents, previous workplace and position, former surname, academic certificate numbers, vehicle license plate (if applying for a parking permit for the University's parking lots), and other personal data provided by the individual. Special categories of personal data related to health, criminal record (for specific positions), and other personal data provided by the individual and/or which the University is obliged to process by laws and other legal acts may also be processed. This data shall be processed in the information system throughout the duration of the employment relationship and 10 years after the end of the contractual relationship. Orders on personnel administration matters are kept for 50 years.

7.4. For the purpose of servicing the readers and visitors of the Library, ensuring the security of the Library's property, the following data is processed on the basis of legal obligations, contracts, consent and/or legitimate interest: full name, address of residence, phone number, email

address, personal identification number of employees, students and other persons who visit the University Library. This data shall be processed in the information system throughout the duration of the provision of the services and for three years after the mutual obligations have been fully met.

7.5. For the purpose of administering the user account and identification, the following data is processed on the basis of the concluded contracts: data subject's full name, personal identification number, biometric data (upon separately informing and receiving consent of the data subject), personal phone numbers, scientific degree, student identity card number (for students), tabular identification number of the employee (for employees), electronic identity number (username), email address, institution (of work or studies), password reminder data, IP and MAC address of the computer, date and time of access to the system or website, cookies, sessions and other activity record information, which may also be used to investigate potential information, cyber, and personal data protection incidents. In the event of termination of contractual or other legal relationship with the data subject, the use of the account shall be suspended as soon as it becomes known, but no later than in 14 calendar days.

7.6. For the purpose of maintenance and monitoring of electronic communications traffic, on the basis of legal obligations, actions of users in information systems and networks are automatically entered in action logs. On the basis of the requirements of the Law on Electronic Communications, in order to ensure that data is available for the purpose of investigation, disclosure, and prosecution of serious and grave crimes as defined in the Criminal Code of the Republic of Lithuania, the data indicated in Annex 1 to this law is processed. This data, unless otherwise specified by law enforcement authorities, shall be processed for six months, except for the categories of data specified in the law, and shall be destroyed upon expiry of the period.

7.7. For the purpose of organising conferences and other events, the following data is processed on the basis of concluded contracts: data subject's full name, personal identification number, personal phone numbers, current account number (for natural persons-payers), personal email address, workplace, date of birth, institution (of work or studies), unit of the institution (of work or studies), job position, pedagogical and academic titles, scientific degree, email address, data from identification documents used for the identification of the conference participant, video and audio recordings of the conference, and the data of the services provided.

7.8. For the purpose of accommodation, the following data is processed on the basis of contracts and legal obligations: data subject's full name, personal identification number, phone numbers, other data for the purpose of financial settlements, email address, scientific degree, address of residence, data from identification documents for establishing identity, place of accommodation, dates of accommodation, license plate and model of the vehicle if a vehicle is to be parked, and data on the related accommodation services provided. This data shall be kept for five years after the provision of the services.

7.9. For the purpose of financial settlements, the following data is processed on the basis of concluded contracts: data subject's full name, personal identification number, phone numbers, current account number (for natural persons-beneficiaries), credit card number and validity period, email address, organisation or institution represented, job position, scientific degree, data from identification documents used to establish identity, and the data of the services provided. This data shall be kept for 10 years.

7.10. For the purpose of administering the selection of candidates, the following data is processed on the basis of consent of the candidates: data subject's full name, personal identification number, CV and the data contained therein, such as a photograph, personal phone numbers, email address, address of residence, current and former workplaces, date of birth, place of study (current or former), study institution (current or former), job position, scientific degree and other personal data voluntarily provided by the candidate. This data shall be processed throughout the duration of the selection process, but no longer than one year after the end of the selection process, and shall be destroyed at the end of the period if the subject has not been recruited and has not consented to the processing of data for the purpose of selection for other

positions. The data of selected candidates shall be processed throughout the employment period, in accordance with the procedures and within time limits laid down for the processing of data for internal administrative purposes.

7.11. For the purpose of investigating complaints, requests and applications from individuals and ensuring the quality of service to subjects, the following data is processed on the basis of legal obligations: data subject's full name, personal identification number, address of residence, phone number, email address, signature, date and number of the complaint, request or application (registration number in the University document management system), information contained in the complaint, request or application (including special personal data), the result of the investigation of the complaint, request or application, information received during the investigation of the complaint, request or application, and the date and number of the University's response to the complaints, requests or applications. This data shall be kept for the duration of the administration of the complaint or request and for one year after adopting the decision/response.

7.12. For the purpose of public order, parking and access control (to ensure the safety of employees, students and other persons visiting the University and the security of the University's property), the following data is processed on the basis of the University's legitimate interest: full name, signature, employee ID card number, time and date of arrival and departure from the building/auditorium/parking lot, vehicle license plate, security camera video recordings and photos. Video surveillance and access control at the University are carried out to ensure the safety of persons, property, and visitors as well as public order on the premises and in the territory of the University. Security cameras record the courtyards in the University's territory, entrances to the University's buildings, premises of shared use, aggregation points of network or engineering system equipment (server rooms, communication nodes, building management system control panels, etc.). Visual data shall be recorded and stored for no longer than 60 days, after which it shall be destroyed. Where visual data is used as evidence in civil, administrative or criminal proceedings or in other cases provided for by law, it may be kept for as long as necessary for those processing purposes and destroyed as soon as they are no longer needed.

7.13. For the purpose of communication with the community, the following data is processed on the basis of the contractual relationships and legitimate interest of the University: contact person's full name, academic and pedagogical titles, scientific degrees, phone number(s), date of birth, address of residence, email address(es), social network contacts (where provided), company represented, job position, address for correspondence, data on memberships in societies and groups of the University, choices of communication and consents. This data shall be processed throughout the contractual relationship.

7.14. To ensure the operation of the University's mobile apps, the following data is processed on the basis of user consent, contracts and legitimate interest of the University: user's account data (full name, unique identifier of the contact person), the language chosen by the user (LT, EN), consent to notifications and newsletter subscriptions, data of reminders of orders and related debts, consent to anonymous statistics on the use of the app. This data shall be processed in the information system throughout the usage of the app, but at least until full implementation of obligations of the parties. Once all obligations have been fulfilled and the mobile app is no longer used, the data shall be kept in the information system for three years.

7.15. For the purpose of marketing, on the basis of the data subject's consent and legitimate interest of the University, in order to inform community members and the public about the University's events, services and products (academic and other expert services of the University, tickets for paid University events, museums, botanical gardens, etc., goods of the University Press, advertising in social networks, etc.), the following contact data is collected and processed: email address, social network contacts (where provided), full name, phone number(s), address, video recordings for the purpose of marketing the event and publicising the results. Contact details shall be kept until consent is withdrawn.

7.16. For the purpose of the individualisation of studies and the adaptation of the environment to individual needs due to disability, on the basis of consent and the requirements of legal acts,

data proving the disability, capacity for work, health impairments and individual needs of students and unclassified students with disabilities is processed. Documents containing health data of students and unclassified students with disabilities shall be kept in the information system and the units for the duration of their studies and for five years after the implementation of their obligations under the study agreement or the termination thereof. After the expiry of the time limit, the data shall be destroyed under the established procedure.

7.17. For the purpose of implementing public procurement and on the basis of the requirements of legal acts, the data of service providers, their representatives, and other persons referred to in the public procurement documents (full name, job position, the number of the individual activity certificate or business licence, address of the place of business, phone number, email address, bank and current account data, income under the contract, data of the documents proving education and qualifications or copies thereof (certificates, licences, etc.), and any other data of an economic or social nature specific to the person provided by the person concerned are processed for the purpose of performance and administration of public procurement contracts. This data shall be kept for five years after the end of the procurement.

7.18. For the purpose of the administration of the University's art groups and on the basis of contracts and consent, full name, email, phone number, date of birth, study programme, year, faculty, photographs, audio and video recordings are collected and processed. The data shall be kept for the entire period of participation in the activities of the art group.

7.19. For the purpose of distance and hybrid delivery of theoretical lectures, the following personal data of staff, students and other persons who are captured in the video camera footage is processed on the basis of legitimate interest for the purpose of streaming and, where necessary, recording the lectures: video monitoring data with audio. The processing of personal data is carried out through the Microsoft Office 365 cloud service, having concluded a contract with the data processor Microsoft Ireland Operations Limited which provides software licensing, rental, and hosting services. If the content of the lecture is only streamed to the participants who attend the lecture remotely, the retention period does not apply as no video recording is made. If the lecture is not only streamed but also recorded upon the lecturer’s decision, the duration of the processing of recordings shall be determined by the lecturer concerned. Once the processing objectives have been fulfilled, the recordings shall be destroyed. The destroying of the video shall be carried out by the lecturer who made the recording, by marking the videos to be destroyed, whose permanent destruction shall be carried out by the data processor, Microsoft Ireland Operations Limited. In all cases, the video recordings shall be automatically destroyed 180 days after the termination of the lecturer's contract.

7.20. The University uses cookies to make the use of websites faster and more convenient. Cookies concerning the use of services and the website traffic statistics are collected. Cookies are used on the website with the consent of the individual which can be revoked at any time by the individual, by changing the settings of their web browser. A list of the cookies used and the duration of their storage are set out in the Privacy Policy of the University.

7.21. Personal data contained in documents stored in the University archive are processed in the public interest, including for scientific or historical research or statistical purposes.

8. When processing the data subjects' personal data on the basis of consent, such consent shall be prepared in the form set out in Annex 3 to the Description, adapted as necessary.

9. All personal data shall not be stored at the University for longer than required by the purposes of processing the personal data. The time limits for the storage of personal data and the actions to be taken after the expiry of this time limit shall be determined by the legal acts governing the processing of the personal data concerned. The specific retention periods of documents related to study and research processes and internal administration are set out in the Index of the Periods of Storage of the Operational Documents of Vilnius University, approved by Order of the Chancellor of Vilnius University No. R-481 of 9 August 2019 “On the Approval of the Index of the Periods of Storage of the Operational Documents of Vilnius University and on the Repeal of Order of the Rector of Vilnius University No. R-545 of 30 October 2013 “On the

Approval of the Index of Periods of Storage of Special Operational Documents of Vilnius University"", and in other legal acts of the University.

10. At the end of the retention period of a document containing personal data, a decision shall be taken on its destruction or on the extension of its retention period. Once a decision has been taken to destroy a document, it shall be destroyed in accordance with the procedure laid down by the Republic of Lithuania Law on Documents and Archives, except for those documents which are to be transferred to the archive and are kept in accordance with the procedure and time limits laid down by the law.

CHAPTER III
THE PRINCIPLES OF THE PROCESSING OF PERSONAL DATA AT THE UNIVERSITY

11. The University, as data controller, shall:

11.1. ensure the exercising of the data subject's rights and fulfil the obligations of the controller laid down in the general requirements for organisational and technical measures for the security of personal data and other legal acts regulating the processing of personal data;

11.2. appoint a data protection officer and other persons responsible for the processing of personal data at the University;

11.3. ensure that the data protection officer is authorised to respond to requests and complaints from data subjects and is involved in an appropriate and timely manner in all matters relating to personal data protection;

11.4. ensure the necessary resources for the data protection officer to carry out the tasks assigned to them;

11.5. enable the data protection officer to maintain their expertise in the area of personal data protection;

11.6. ensure that the data protection officer does not receive any instructions in relation to the performance of the tasks entrusted to them for the processing of personal data and not assign tasks and duties which may give rise to a conflict of interest;

11.7. approve the legal acts governing the protection and processing of personal data and familiarise the University staff with them;

11.8. establish a procedure for the provision of data to data subjects for a fee;

11.9. ensure staff training and qualification development in the area of legal protection of personal data.

12. The University staff, in the performance of their functions and processing of personal data, shall:

12.1. ensure compliance with these processing principles:

12.1.1. personal data shall be processed following the GDPR, the ADTAĮ, and other normative and University legal acts regulating data protection;

12.1.2. personal data shall be processed for specified and legitimate purposes and are not further processed for purposes incompatible with those established before the personal data was collected;

12.1.3. when processing personal data, it shall be complied with the principles of purposefulness and proportionality and it shall not be required from personal data subjects to provide redundant data;

12.1.4. personal data shall be processed accurately, fairly and lawfully;

12.1.5. personal data shall be accurate and, where necessary for the processing of personal data, constantly updated; inaccurate or incomplete data must be rectified, supplemented, destroyed, or their processing suspended;

12.1.6. personal data shall be consistent throughout, appropriate and limited to what is necessary for their collection and further processing;

12.1.7. personal data shall be processed in such a way that the data subjects can be identified

for no longer than is necessary for the purposes for which the data was collected and processed;

12.2. ensure that personal data is processed in accordance with the organisational and technical data security measures specified in the documents of the information systems to be processed (regulations, data security regulations, rules for the secure processing of electronic information, user administration rules);

12.3. be responsible for the preparation, registration, and submission to the data protection officer of unit documents (orders, agreements, minutes, contracts, notices, etc.) necessary for the processing of personal data, following the procedure set out at the University and in the laws (in the exercising of the rights of data subjects);

12.4. ensure the destruction of electronic and/or paper documents containing personal data after the expiry of the retention periods laid down for personal data;

12.5. carry out a data protection impact assessment in consultation with the data protection officer in the cases provided for in the General Data Protection Regulation and in Order of the Director of the State Data Protection Inspectorate No. 1T-35 (1.12.E) of 14 March 2019 “The List of Data Processing Operations Subject to the Requirement to Carry Out a Data Protection Impact Assessment”;

12.6. consult the data protection officer when they start processing personal data for new purposes or change the scope of previous processing;

12.7. keep a record of the unit's personal data processing activities and ensure their accuracy;

12.8. ensure the implementation of appropriate organisational measures to protect personal data processed by the unit against accidental or unlawful destruction, alteration, disclosure, or any other unlawful processing.

CHAPTER IV
DATA PROTECTION OFFICER

13. The data protection officer shall be responsible for the data processing activities carried out at the University within the limits of their competency.

14. The data protection officer shall:

14.1. control how the University staff and other personal data processors of the University comply with the personal data processing obligations set out in this Description and process personal data;

14.2. publicly announces, in accordance with the procedure laid down, the data processing actions carried out by the University;

14.3. provide suggestions and conclusions to the University's management on the establishment of data protection and data processing measures, and supervise the implementation and use of these measures;

14.4. give direct instructions to staff to remedy infringements of the processing of personal data;

14.5. consult on carrying out data protection impact assessments;

14.6. help data subjects to exercise their rights;

14.7. advise personal data processors on the choice of organisational and technical measures to be applied in the processing of personal data and on other personal data protection issues;

14.8. coordinate the production of records of data processing activities;

14.9. when necessary, contact the State Data Protection Inspectorate for prior consultations;

14.10. in the event of a personal data incident, take all reasonable steps to recover the personal data lost and/or mitigate the damage to personal data caused by the incident;

14.11. notify the data subject and the State Data Protection Inspectorate of a personal data incident in the cases specified;

14.12. ensure secrecy and/or confidentiality in relation to the performance of their tasks in accordance with the requirements laid down in the Republic of Lithuania and the University's internal legal acts;

14.13. inform the State Data Protection Inspectorate in writing if they find that personal data is being processed in violation of the provisions of the legal acts on data protection or if there is a refusal to comply with a direct order to remedy the violation;

14.14. carry out the other tasks and duties assigned to them in legal acts.

CHAPTER V
PROCESSING OF PERSONAL DATA

15. Personal data at the University shall be processed by automated means or in filing systems using personal data processing tools installed at the University.

16. Personal data shall be collected at the University in accordance with the procedure and on the grounds established by legal acts, by obtaining them directly from the data subject or other persons, as well as through official requests submitted to the entities that process the necessary information and have the right to provide it (in the case of a one-off collection of personal data) or on the basis of contracts for the provision of personal data (in the case of a multiple collection of personal data).

17. In accordance with the cases and procedure established by legal acts, the University shall provide personal data processed by it to the managers and/or processors of state registers and state information systems, state and municipal institutions, establishments, organisations and other persons to whom the provision of personal data is obliged by laws or other legal acts or to whom the University, following the procedure set out in the legal acts, provide personal data in the exercise of its functions or in accordance with a personal data provision agreement.

18. Personal data shall be provided to data recipients located in the Member States of the European Union and other countries of the European Economic Area under the same conditions and procedures as to data recipients located in the Republic of Lithuania.

19. Personal data processed or intended to be processed following a transfer to a third country or an international organisation shall only be transferred if the data controller and data processor comply with the GDPR.

20. The University may authorise data processors, i.e. information technology and electronic communications service providers, advisors, auditors, consultants, security services, and other persons to process the data controlled by the University for the purposes and on the instructions of the University.

21. The University shall enter into a written personal data provision agreement with the data processor, which shall specify the purposes and means of the processing of personal data, an exhaustive list of the personal data to be processed, the personal data processing activities that the processor is required to perform and may perform on behalf of the controller, and the application of organisational and technical measures to ensure the security of personal data.

22. The written data provision agreements between the University and the data processor shall:

22.1. indicate the purpose for which the personal data is used, the legal basis for providing and receiving it;

22.2. establish that a personal data processor may act only on the instructions of the data controller;

22.3. indicate the legal acts which govern the processing of personal data;

22.4. establish the purposes and means of the processing of personal data;

22.5. provide an exhaustive list of personal data to be processed;

22.6. indicate which processing operations on personal data must and may be carried out by the data processor on behalf of the data controller;

22.7. indicate how and in what cases personal data is revised, corrected, when it is updated, how personal data that has changed is processed, etc.;

22.8. discuss the procedure for exercising the data subject's rights;

22.9. provide the period of retention of personal data and the actions to be taken after the

expiry of that period;

22.10. establish compliance with the confidentiality requirement;

22.11. discuss the application of organisational and technical measures for the security of personal data;

22.12. establish liability for non-compliance with the terms of the agreement.

CHAPTER VI
RIGHTS OF THE DATA SUBJECT

23. A data subject whose data is processed in the course of the University's activities shall have the following rights:

23.1. the right to know (be informed) about the processing of their personal data;

23.2. the right to access their personal data and information on its processing;

23.3. the right to request rectification of their personal data or, taking into account the purposes of the processing, to have incomplete personal data completed;

23.4. the right to erasure of their personal data (with the exception of storage);

23.5. the right to restrict the processing of their personal data;

23.6. the right to object to the processing of their personal data;

23.7. the right to data portability;

23.8. the right to lodge a complaint with the State Data Protection Inspectorate.

24. The data subject shall have the right to know from which sources and what personal data has been collected and for what purposes they are processed.

25. The data subject shall have the right to demand the personal data concerning them to be erased by the University without delay, provided that one of the following grounds applies:

25.1. the personal data is no longer necessary for the purposes for which it was collected or otherwise processed;

25.2. the data subject withdraws the consent on which the data processing is based pursuant to Article 6(1)(a) or 9(2)(a) of the GDPR and there is no other legal basis for the processing;

25.3. the data subject objects to data processing pursuant to Article 21(1) of the GDPR and there are no overriding legitimate grounds for data processing, or the data subject objects to data processing pursuant to Article 21(2);

25.4. the personal data has been processed unlawfully;

25.5. the personal data must be erased in accordance with a legal obligation imposed by the law of the European Union or a Member State that is applicable to the data controller;

25.6. the personal data was collected in the context of the offer of information society services referred to in Article 8(1) of the GDPR.

26. If the data subject, having familiarised themselves with their personal data processed by the University in the provided response, finds their personal data to be incorrect, incomplete or inaccurate, they shall ask the University to correct it. The data protection officer shall suspend the processing of such personal data, with the exception of storage, and, after checking the personal data, shall take measures to rectify the incorrect, incomplete, inaccurate personal data, and shall provide the data subject with a reply informing them of the action taken.

27. If the data subject, having familiarised themselves with their personal data processed by the University in the provided response, finds their personal data to be processed unlawfully or unfairly and contacts the University, the data protection officer shall check the accuracy, lawfulness and fairness of the processing of the personal data and shall take measures to immediately destroy the unlawfully and unfairly collected personal data or to suspend the processing of such personal data, with the exception of storage, and shall inform the data subject of the actions taken.

28. If the data subject, having familiarised themselves with their personal data processed by the University in the provided response, finds further processing of their personal data to be inappropriate, withdraws their prior consent to the processing of the data, and asks the University

to forget them, the data protection officer shall take measures to destroy the personal data processed on the basis of the consent, with the exception of storage, and shall either inform the data subject of the steps taken or inform them of the reasons why the data cannot be destroyed.

29. Where the University has made publicly available personal data concerning a data subject but is obliged to erase the personal data at the request of the data subject, the data protection officer shall, taking into account the technology used by the University and the cost of implementation, take reasonable steps, including technical measures, to ensure that such personal data and/or copies or duplicates thereof are destroyed as soon as possible.

30. The requirements to forget and erase personal data shall not apply in the event of failure to verify the identity of the requesting subject or to substantiate the reasons for the request as well as in the cases provided for in Article 17(3) of the GDPR, including when:

30.1. legal obligations are imposed on the University which require it to process data in order to perform a task in the public interest;

30.2. for archiving purposes in the public interest, for scientific or historical research purposes, or for statistical purposes in accordance with the GDPR and other requirements set out in the law;

30.3. in other cases provided for in the GDPR and other legal acts.

31. The University, having suspended the processing of personal data at the request of the data subject, shall store the personal data for which processing has been suspended until they are rectified or destroyed (at the request of the data subject or after the expiry of the data retention period).

32. The University shall ensure that the rights of the data subject are properly exercised and that all information is provided to the data subject in a clear, intelligible, and acceptable form. The purposes of personal data processing, the rights of data subjects and the procedures for their exercising set out in this Description shall be set out in a simplified form in the Privacy Policy of the University which shall be published on the University's internet and intranet sites.

33. The University may exclude data subjects from exercising these rights in cases where, as provided for by the laws, it is necessary to ensure the prevention, investigation and detection of crimes, breaches of official or professional ethics, as well as the protection of the rights and freedoms of the data subject or other persons, or in other cases provided for by the laws or legal acts.

CHAPTER VII
EXERCISING OF DATA SUBJECTS' RIGHTS

34. In order to exercise their personal data protection rights under the General Data Protection Regulation, the data subject shall have the right to contact the University orally or in writing by submitting an appeal, complaint or request (hereinafter the ‘request’) in person, by post, or by electronic means.

35. When contacting the University in writing in regards to exercising the data subject's rights, it is recommended to submit a request in the form set out in Annex 1 to the Description.

36. University staff shall submit their requests in the University document management system or via the means of information systems where data query functionality is implemented. Other subjects shall contact the University's data protection officer or the unit processing data at the publicly listed contacts.

37. The request must be legible, signed, contain the full name, address and other contact details of the data subject in order to keep contact in the preferred form of communication, and must indicate which of the data subject's rights, and to what extent, are to be exercised.

38. When submitting the request at the unit, if there is any doubt as to the identity of the subject, the identity document of the person submitting the request shall be checked.

39. A data subject may only exercise their (or another lawfully represented subject's) rights after having given the University the opportunity to verify their (and the represented subject's)

identity.

40. When verifying the identity document of the data subject at the point of contact or remotely, the relevant identity document shall be shown in one of the following ways:

40.1. both sides of identity documents that are in card format are shown;

40.2. when showing a person's passport, the page of the document containing the natural person's photo and the passport cover are shown;

40.3. the date of validity of the presented document is checked.

41. When presenting an identity document, the subject must allow the employee checking the document to properly inspect the presented document. The employee shall have the right to refuse to register a request if the subject refuses to present the document properly, if the document is damaged or illegible.

42. In the case of electronic submission of an identity document, the photographs of the documents (parts thereof) listed above shall be authenticated by means of at least an advanced electronic signature complying with the requirements of Article 26 of Regulation (EU) No. 910/2014.

43. The advanced electronic signature used to authenticate documents and photographs must be valid for at least one month after the request is submitted.

44. When authenticating with an advanced electronic signature, the person processing the request must verify the validity and authenticity of the signature.

45. The photographs transmitted must be of such quality that the information in the identity documents submitted can be easily read and the features of the person depicted in the photograph can be clearly seen.

46. In the case of a one-off collection of personal data, if the request of the data subject or of a legal person is made via the National Information System of Electronic Parcel Delivery Using the Postal Network, the identity of the person making the request shall be deemed to be satisfactory established.

47. If there are doubts as to the identity of the data subject, the University employee shall ask for additional information necessary to verify the identity of the data subject.

48. The data subject may exercise their rights themselves or through a representative authorised in the manner provided for in the Civil Code of the Republic of Lithuania.

49. If a representative of a person submits a request on behalf of the represented data subject, they must indicate in their request their full name, address of residence, contact details, as well as the full name, address of residence of the represented person, the information on which of the data subject's rights referred to in the Description and to what extent the data subject wishes to exercise, and must attach a document confirming the representation or a copy thereof, certified in accordance with the procedure laid down by the legal acts. The request submitted by a representative must satisfy the same requirements as set out for the request of the individual represented.

50. Where letters are submitted by a legal person, it must be verified that the signatory has been authorised by the institution. If the representative of a legal person acts in accordance with articles of association, the information is checked against public sources if the suspicion arises, and if the information is not confirmed, it is checked if they are registered in the Register of Legal Entities. The data protection officer shall carry out checks in the Register of Legal Entities at the initiative of the head of the responsible unit.

51. All requests from data subjects regarding the processing of personal data and the responses thereto shall be registered in the University document management system.

52. In the event of inaccuracies in the data subject's request, the University may ask the data subject to revise them, and if the data subject refuses to do so, the request shall not be processed. The data protection officer shall inform the applicant in writing of the grounds for refusing the request.

53. Requests from persons shall be responded to in the State language and in the manner in which the request was made, unless the person expresses their wish to receive the response in

another manner.

54. Where appropriate, a request may be responded to in a language other than the State language when the request is made by a foreign public authority, other foreign entity, or international organisation in accordance with international legal acts.

55. The coordination of preparing the response to the request, consultations to the relevant units, and provision of the response to the data subject shall be carried out by a core unit of the University, the data protection officer, or another person authorised by the Rector of the University.

56. The response to the request shall be clear and reasoned, indicating all the circumstances relevant to the examination of the request and the specific provisions of the legal acts relied upon in assessing the content of the request.

57. Received requests shall be answered in 30 (thirty) calendar days from the date of the data subject's enquiry. Upon the decision of the data protection officer, in the cases provided for in the GDPR and other legal acts, depending on the complexity of the request and the number of other requests, the response may be postponed for two more months by informing the data subject thereof.

58. Actions in response to requests from the data subject to exercise the data subject's rights may be provided free of charge, except in cases requiring unreasonable organisational and technical measures. In such cases, the data protection officer shall have the right to decide not to grant such a request or not to grant it in full, or to provide the data in accordance with the University's service rates and payment procedures.

59. In examining the requests, the University staff must be guided by the principles of respect for human rights, justice, fairness, and reasonableness.

60. It is forbidden to refuse the examination of requests due to an absence of the employee performing this function. In the case of leave, secondments, and other absences of the above-mentioned employee, the examination of requests and complaints must be delegated to other employees.

61. The employee who examines the request shall withdraw themselves from the examination of the request or may be withdrawn by a decision of the Rector or their authorised person if the data subject submits a request related to the activities of the employee of the University who processes the personal data, or if the following circumstances arise:

61.1. the employee is a close relative (as defined in the Civil Code of the Republic of Lithuania), a brother- or sister-in-law, or a cohabitant who has registered the partnership following the procedure set out in the laws of the person who is the subject of the complaint;

61.2. there is a subordination relationship between the employee and the person submitting the request;

61.3. the impartiality of the employee is reasonably doubted on any other grounds which might give rise to a conflict between public and private interests.

62. The data subject, either by themselves or via their representative, shall have the right to appeal against the actions or inaction of the University in the exercise of the data subject's rights to the State Data Protection Inspectorate or to the Vilnius Regional Administrative Court.

CHAPTER VIII
ORGANISATIONAL AND TECHNICAL MEASURES TO PROTECT PERSONAL DATA

63. The University, in protecting personal data, shall implement and ensure appropriate organisational and technical measures to protect personal data against accidental or unlawful destruction, alteration, disclosure, or any other unauthorised processing.

64. The security of personal data processed in the University's information systems shall be ensured in accordance with the requirements of the University's information systems' regulations and the documents implementing the security policy: data security regulations, rules for secure processing of electronic information, the management plan for the continuity of activities, and the

user administration rules.

65. Personal data (documents containing personal data or copies thereof) shall be kept in designated premises, local area networks, and computer hard drives. Personal data (documents containing personal data or copies thereof) must not be kept in a visible place accessible to all, where unauthorised persons could access it without hindrance.

66. The University staff shall comply with the provisions of the Description and contribute to the implementation of the organisational and technical measures put in place at the University. Staff processing personal data must:

66.1. familiarise themselves with this Description and undertake to process personal data in compliance with the General Data Protection Regulation, the Republic of Lithuania Law on Legal Protection of Personal Data, and other requirements set out in the legal acts related to personal data protection;

66.2. in the University document management system or in another way that provides evidence of familiarisation, sign the Commitment to Keep Personal Data Secret (Annex 2 to the Description);

66.3. comply with the provisions of this Description and the Commitment to Keep Personal Data Secret;

66.4. respect confidentiality requirements and not disclose to third parties any information relating to personal data which has come to their knowledge in the performance of their functions, unless such information is public pursuant to the provisions of applicable laws or legal acts. This obligation shall also apply after the end of the employment or other contractual relationship;

66.5. immediately notify the data protection officer and/or the head of a structural unit of the University of any personal data breaches;

66.6. immediately report electronic information security incidents in accordance with the time limits and procedures set out in the University's Description of the Response and Investigation Procedure for Electronic Information Security Incidents;

66.7. change their password immediately if there is a threat of hacking into a computer with protected personal data, or if suspected that the password has become known to third parties, etc.;

66.8. avoid making redundant copies of documents containing personal data, keep these documents out of public view and store them properly;

66.9. ensure that documents containing personal data are kept in accordance with the legal requirements;

66.10. notify the head of a structural unit of the and/or the data protection officer of the University if they assess and determine that the organisational and technical measures for personal data protection are not reliable.

67. The heads of the structural units of the University shall ensure protection against unauthorised physical access to personal data by the following measures: locked premises, a functioning access control system (physical or electronic), restricted access to specific premises, or other risk-appropriate measures.

68. Personal data security breaches at the University shall be investigated in accordance with the procedure set out in the University's Description of the Response and Investigation Procedure for Electronic Information Security Incidents.

69. In the implementation of the privacy by design and privacy by default principles, it must be ensured that the processing of personal data and the associated risks are continuously assessed.

70. Before the introduction of new measures of collecting and processing personal data, such as the implementation of an information system or its updates, the acquisition of software or the introduction of other measures of processing personal data, the data protection officer shall be consulted as to the appropriateness of the intended measures of processing, taking into account the stated purpose of the processing of personal data and the volume of data required as well as the organisational and technical data security measures essential in the specific case. In all cases, account must be taken of the state of the art of the technical capabilities, the cost of implementation and the nature, scope, context, and purposes of the processing, as well as the risks

posed by the data processing to the rights and freedoms of data subjects.

CHAPTER IX
NOTIFICATION OF A PERSONAL DATA SECURITY BREACH

71. A University employee who becomes aware of a possible personal data security breach must immediately inform their immediate superior and/or the data protection officer.

72. The head of the University unit must notify the data protection officer of any potential personal data security breach and discuss the extent and consequences of the potential breach with them.

73. The data protection officer shall ensure that the State Data Protection Inspectorate is notified of a personal data security breach without undue delay and, where possible, no later than in 72 hours after becoming aware of it, unless the personal data security breach is unlikely to endanger the rights and freedoms of natural persons. If the State Data Protection Inspectorate is not notified in 72 hours, the notification shall state the reasons for the delay.

74. The notification to the State Data Protection Inspectorate shall be submitted in accordance with the procedure and conditions set out in the Description of the Procedure for Submitting the Notification on a Personal Data Security Breach to the State Data Protection Inspectorate approved by Order of the Director of the State Data Protection Inspectorate No. 1T-72(1.12.E) of 27 July 2018 "On the Approval of the Description of the Procedure for Submitting the Notification on a Personal Data Security Breach to the State Data Protection Inspectorate".

75. Where a personal data security breach is likely to result in a serious risk to the rights and freedoms of natural persons, the data protection officer must ensure that the data subject is notified of the personal data security breach without undue delay.

76. It is not necessary to notify the data subject of a personal data security breach if the University:

76.1. has implemented appropriate technical and organisational security measures and they have been applied to the personal data affected by the personal data security breach;

76.2. immediately after a personal data security breach, has taken measures to ensure that the rights and freedoms of data subjects are not seriously jeopardised;

76.3. would be required to put a disproportionate effort. In such a case, instead of notifying the data subject of the personal data security breach, the breach shall be announced publicly or otherwise effectively communicated.

77. The data protection officer shall record all personal data breaches and collect information on the causes, impact, and consequences of such breaches, the measures taken, the reasons for the decisions to notify/not notify the State Data Protection Inspectorate and/or the data subject, the reasons for the delay in notification, and any other information.

CHAPTER X
RECORDS OF THE DATA PROCESSING ACTIVITIES

78. For each purpose of processing personal data, the University shall keep records of the data processing activities.

79. Records of the data processing activities shall be kept in electronic form.

80. Records of the data processing activities shall be regularly checked and updated.

81. Records of the data processing activities shall be maintained and the responsibility for its content and accuracy shall lie with the unit implementing the specific purpose of data processing at the University.

CHAPTER XI
FINAL PROVISIONS

82. The Description shall be reviewed periodically and updated as necessary.

83. University staff shall be liable for personal data breach in accordance with the procedure set out in the legal acts.

84. Where necessary, an audit of the organisational and technical security measures for the processing of personal data may be carried out at the units.

85. The Description is published on the University's website.

86. The legal acts implementing this Description shall be approved by an order of the Rector of the University or their authorised person.

_____

Annex 1
to the Description of the Procedure for the Processing of Personal Data at Vilnius University

(Recommended form of a Request to Exercise the Data Subject's Right(s))

_____
(Full name, personal identification number of the data subject)

_____ _____
(Address and/or other contact details (phone number or email address (voluntarily provided by the person submitting the request)))

_____
(Representative and grounds for representation if the request is made by a representative of the data subject)

To Vilnius University
Universiteto g. 3
01131 Vilnius

REQUEST
TO EXERCISE THE DATA SUBJECT'S RIGHT(S)

_____
(Date)

_____
(Place)

1. I hereby request to exercise the data subject's right(s) (indicate).
(Cross the appropriate box):

□ The right to receive information about data processing
□ The right of access to data
□ The right to request rectification of the data
□ The right to erasure of the personal data (‘the right to be forgotten’)
□ The right to restrict the processing of data
□ The right to data portability
□ The right to object to the processing of data
□ The right to request that a decision based solely on automated processing, including profiling, is not applied

2. Specify your request and provide as much information as possible to enable the proper exercise of your right(s) *(e.g. if you wish to receive a copy of your personal data, indicate the specific data a copy whereof you wish to receive; if you wish to have your data rectified, indicate the specific inaccuracy of the data; if you object to the processing of your personal data, indicate the grounds for your objection, including the specific data processing you object to):*

_____
_____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____
_____

ATTACHED[1]:

1. _____.
2. _____.
3. _____.
4. _____.

I would like to receive an answer by (tick one):

- □ post;
- □ contacting the Vilnius University unit at_____;
- □ email (only if the request is signed with a qualified electronic signature).

_____ _____

(Signature) (Full name)

The employee who verified the identity:

_____ _____ _____

(Position) (Signature) (Full name)

[1] If the request is sent by post, it shall be accompanied by a copy of a personal identity document certified by a notary or following another procedure set out in the legal acts.
If a request is made to rectify inaccurate data, copies of the documents proving the accurate data shall be provided; if they are sent by post, they must be certified by a notary or following another procedure set out in the legal acts.
If the data subject's personal data, such as full name, have changed, the request shall be accompanied by a copy of the documents confirming the change; if they are sent by post, they must be certified by a notary or following another procedure set out in the legal acts.

Annex 2
to the Description of the Procedure for the Processing of Personal Data at Vilnius University

(Form of the commitment to keep the personal data secret)

COMMITMENT TO KEEP THE PERSONAL DATA SECRET

_____
(date)

_____
(place of signing)

I, _____,
(full name)

_____,
(job position)

hereby confirm that I am familiar with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), the Republic of Lithuania Law on Legal Protection of Personal Data, the Description of the Procedure for the Processing of Personal Data at Vilnius University, and other legal acts regulating personal data protection, and promise:

1. To keep personal data secret throughout the duration of the contractual or other relationship with the University and after the termination of that relationship if that personal data is not intended for public disclosure.
2. To process personal data only for legitimate and specified purposes.
3. To process accurate personal data and, where necessary, update, rectify or supplement inaccurate and/or incomplete data and/or to stop processing such personal data.
4. To process personal data only to the extent necessary for its processing and for the performance of its function.
5. To implement the provisions of legal acts regulating personal data protection that establish how to protect personal data against unlawful processing or disclosure.
6. Not to disclose, transfer or make available by any means the information processed by me to any person who is not authorised to use it, either inside or outside Vilnius University.
7. To report to my immediate superior and the data protection officer any suspicious situation that could jeopardise the security of personal data.
8. To ensure the exercising of the data subject's rights in accordance with the law.
9. To comply with other legal acts governing the processing and protection of personal data.

By signing this commitment, I confirm that I understand that non-compliance with this commitment will be subject to legal liability.

_____	_____	_____
(title of position)	(signature)	(full name)

_____

Annex 3
to the Description of the Procedure for the Processing of Personal Data at Vilnius University

(Model form of consent to the processing of personal data)

CONSENT TO THE PROCESSING OF PERSONAL DATA

__(day) _____ (month) 20__ (year)

_____
(place)

I,_____,
(full name, date of birth)

as an employee/student of Vilnius University (delete as appropriate),

hereby agree/disagree (delete as appropriate) that:

1. The public institution Vilnius University (hereinafter the 'University') would receive and process the following personal data about me[2]:

_____

2. The personal data listed above would be processed for the following purposes[3]:

_____

3. The following processing operations would be carried out on the personal data listed[4]:

_____

4. The personal data would be obtained
   - ☐ from[5]: me directly,
   - ☐ public registers and information systems,
   - ☐ information systems controlled and managed by the
   - ☐ University, other sources[6] _____
5. Personal data would be transferred[7] _____
6. Time limit for processing with consent[8] – _____
7. Data controller – public institution Vilnius University, Universiteto g. 3, LT-01513 Vilnius;
8. Contacts of the data protection officer – email dap@vu.lt, address Universiteto g. 3, LT-01513 Vilnius.
9. Legal basis for the processing – this consent shall be the legal basis for the processing of your personal data indicated in this consent.

_____

2 This Item shall contain a list of the personal data necessary to achieve the specific purpose(s) of the processing on the basis of this consent as set out in the VU Records of the Data Processing Activities, e.g. full name, date of birth, qualification, length of employment, etc.

3 This Item shall contain the specific purposes for which VU will use personal data on the basis of this consent.

4 This Item shall set out specific actions that will be made in relation to the processing of the data indicated in Item 1 of the consent for the purposes indicated in Item 2, e.g. data evaluation and analysis.

5 Data sources shall be indicated, e.g. the data subject themselves, public registers or information systems, natural or legal persons.

6 Other possible sources shall be indicated.

7 This Item shall indicate data recipients to whom data would be transferred on the basis of this consent.

8 The estimated duration of the processing in years shall be indicated.

10. I am informed that this consent and the personal data contained therein will be kept for three years from the date of withdrawal or expiry of the consent or from the date of the University's decision to stop processing personal data for the purposes set out in the consent.

11. I am informed that, following the procedure set out in the laws, I have all the rights set out in this consent, the Description of the Procedure for the Processing of Personal Data at Vilnius University, and other rights provided for in the General Data Protection Regulation and the Republic of Lithuania Law on Legal Protection of Personal Data, including but not limited to the right to:

11.1. contact Vilnius University with a request for information about the personal data processed by the University and the purposes for which they are processed;

11.2. request rectification of incorrect, incomplete or inaccurate personal data and/or suspend the processing of such personal data where, after consulting the personal data, it is established that the data are incorrect, incomplete or inaccurate;

11.3. restrict the processing of the personal data collected until the lawfulness of the processing is verified;

11.4. request the erasure of the personal data provided in this consent (‘to be forgotten’);

11.5. object to the processing of personal data for direct marketing purposes, including profiling;

11.6. withdraw consent without affecting the use of personal data performed prior to the withdrawal of consent.

12. I am informed that the Description of the Procedure for Personal Data Processing at Vilnius University which sets out the requirements for the processing and protection of personal data, the rights of personal data subjects and the procedure for their implementation at Vilnius University are published and made publicly available at https://www.vu.lt/en/privacy-policy.

_____	_____	_____
(Place and date of consent)	(signature)	(full name)

_____

DETAILED METADATA	
Author(s) of the document	Vilnius University | Universiteto g. 3, LT-01513 Vilnius, Lithuania, registration code 211950810
Title (heading) of the document	ON THE AMENDMENT TO ORDER OF THE RECTOR OF VILNIUS UNIVERSITY NO. R-316 OF 25 MAY 2018 “ON THE APPROVAL OF THE DESCRIPTION OF THE PROCEDURE FOR THE PROCESSING OF PERSONAL DATA AT VILNIUS UNIVERSITY”
Document registration date and number	No. R-425 of 10 December 2021
Document receipt date and document receipt registration number	-
Document specification ID	ADOC-V1.0
Purpose of the signature	Signing
Full name and job position of the person who created the signature	Rimvydas Petrauskas, Rector, Central Administration
Certificate issued	RIMVYDAS,PETRAUSKAS LT
Date and time of the signature	10 December 2021 09:53:25 (GMT+02:00)
Signature format	XAdES-T
Timestamp embedded in the signature	10 December 2021 09:53:38 (GMT+02:00)
Information on the certification service provider	EID-SK 2016, AS Sertifitseerimiskeskus EE
Date of validity of the certificate	6 February 2020 08:50:07 – 4 February 2025 23:59:59
Information on the methods used to ensure the integrity of metadata	The integrity of ‘Registration’ metadata was ensured through a certificate ‘Document Management System Avilys, Vilnius University, registration code 211950810 LT’, issued by ‘RCSC IssuingCA, State Enterprise Centre of Registers, registration code 124110246 LT’; the certificate is valid from 27/12/2018 14:18:54 to 26/12/2021 14:18:54
Number of the main document’s annexes	-
Number of accompanying documents	-
Originator(s) of the accompanying document	-
Accompanying document’s title (heading)	-
Accompanying document’s registration date and number	-
Software used to generate the e-document	Document Management System Avilys, version 3.5.54
Information on the validity check of the e-document and electronic signature(s) (date of the check)	Complies with the specification requirements. All the electronic signatures are valid (10 December 2021 09:54:15)
Search link	-
Additional metadata	The copy was generated on 10 December 2021 09:54:15 by the Document Management System Avilys