PRIVACY NOTICE OF THE UNIVERSITY OF LUXEMBOURG (Whistleblowing)

Introduction

In accordance with transparency obligations of the EU Regulation 2016/679 General Data Protection Regulation (hereafter the "GDPR"), this Privacy Notice (hereafter "the Notice") explains how the University of Luxembourg and KPMG process your Personal Data in relation to submissions of Whistleblowing reports.

1. Who are we

The University of Luxembourg (hereinafter "University") is a public higher education and research establishment, operating under the supervision of the Ministry for higher education.

MAISON DU SAVOIR
2, avenue de l'Université
L- 4365 ESCH-BELVAL
Phone number: Tel.: (+352) 46 66 44 1
Internet address: https://www.uni.lu/en/

The University has appointed a Data Protection Officer (DPO) reachable during working hours. Further information is provided on the webpage of the University dedicated to data protection and an email address is available: dpo@uni.lu. The DPO can also be contacted by mail at the postal address of the University by indicating to the attention of the Data Protection Office.

2. Why does the University process your personal data and on which legal basis?

In the frame of compliance with the obligations in the Luxembourg Act of 16 May 2023, which transposes the EU Directive (EU) 2019/1937 on the Protection of Persons who report breaches of Union law ('Whistleblower Directive') [1], the University will process personal data of any person allowed to report a breach of national or directly applicable European law. More specifically, this personal data processing is necessary for submission and management of Whistleblowing reports as defined in the Whistleblowing policy of the University.

The Whistleblowing policy allows the following categories of data subjects to report a breach of national or directly applicable European law:

- University staff, including civil servants
- The members of the Board of Governors
- Students
- Volunteers and paid or unpaid interns
- Contractors, sub-contractors and suppliers.

The personal data processing of University staff, including civil servants, members of the Board of Governors, Volunteers and paid or unpaid interns, contractors, sub-contractors and suppliers is necessary for compliance with a legal obligation to which the University as controller is submitted as the University must comply with the Luxembourg Act of 16 May 2023 (art.6.1 c) GDPR).

[1] Loi du 16 mai 2023 portant transposition de la directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union.

The personal data processing of University students is based on the legitimate interest of the University. The University considers the whistleblowing procedure as an important objective of general public interest as raised by the Whistleblowing European Directive. The whistleblowing procedure will constitute a significant contribution to effective detection, investigation and prosecution of breaches of the law and of enhancing transparency and accountability. Therefore, the University wishes to ensure that its activities are carried out in a lawful manner thus allowing students to report potential violations of the law. (Art.6.1 f) GDPR).

The reports are submitted in an encrypted format on a secure external platform run by the provider EQS who has no access to unencrypted data held on the platform.

3. Which standard personal data do we collect and further process?

As part of submitting a Whistleblowing report, Whistleblowers will be required to submit their Identification data (name, surname) and professional identifier (University employee or student number for these categories of Whistleblowers) and an email address. This data will be processed, to allow for an investigation into the report and protection in the event of retaliation.

Depending on the information submitted in the Whistleblowing report, further categories of personal data relating to the Whistleblower, those accused in the report and/or witnesses listed below may be processed to allow for further investigation, such as:

- Name, last name of those accused and/or witnesses
- Contact details: telephone number, email address
- Professional data: grade, position, student or employee number
- Pictures and sounds: videos, photographs, recordings.

4. Which sensitive personal data do we collect and based on which derogation under Article 9 GDPR?

Depending on the information submitted in the Whistleblowing report, the categories of sensitive data that may be processed to allow for further investigation is listed below,

- Health data
- Data revealing information about origin
- Data conveying information about personal beliefs /opinion
- Sexual orientation

The special categories of personal data processing of University staff, including civil servants, members of the Board of Governors, volunteers, paid or unpaid interns, contractors, sub-contractors and suppliers, and University students, is based on processing being necessary for the establishment, exercise or defence of legal claims (art.9.2 f) GDPR).

5. Who are the recipients of your personal data?

Personal data collected as part of your Whistleblowing report will be communicated:

5.1. Internal recipients

a) the Rector, the Secretariat of the Board of Governors, the University's Legal Counsel and other members of the University management relevant to the Whistleblowing report received, to decide on how to pursue the report.
b) Members of an internal University investigation team, should the University decide to establish one to pursue the report.

5.2. External recipients

a) KPMG Tax and Advisory S.à r.l. (hereinafter "KPMG") as processor
For submission of Whistleblowing reports the University has appointed KPMG to collect and process on its behalf personal data you submit for reporting acts or omissions that are illegal ('Whistleblowing reports') for the purpose of complying with the Luxembourg Act on Whistleblowing. The University and KPMG have concluded a data processing agreement in accordance with art.28 GDPR in order to ensure the processor will offer appropriate safeguards for the protection of personal data processed.

b) EQS as provider of the platform. The University and EQS have concluded a data processing agreement in accordance with art.28 GDPR in order to ensure the processor will offer appropriate safeguards, including data encryption, for the protection of personal data processed. EQS only act as a data processors in terms of saving encrypted data on their servers, and have no access to unencrypted personal data held on the platform.

c) Members of an external investigation team, should the University decide to establish one to pursue the report.

d) External legal authorities such as the judiciary or police, should a legal investigation be established to pursue the report.

6. Does the University transfer your personal data outside of the European Union?

Your Personal Data is processed within the European Union for the different purposes listed in section 2.

7. How long does the University store your personal data?

The retention period will depend on the decision on how to pursue to the report.

Reports that are judged by the University, after KPMG's assessment, to be manifestly out of scope will be anonymised as soon as possible thereafter, and the anonymised report will be kept on the EQS platform for the retention period of its most serious allegation, in case of repeat allegations.

Reports that are judged by the University, after KPMG's assessment, to be in scope and where investigation is conducted will be anonymised as soon as possible after investigation is concluded. The anonymised report will be kept on the EQS platform for the retention period of its most serious allegation, in case of repeat allegations.

Reports that are judged by the University, after KPMG's assessment, to be in scope and where investigation is not conducted, for example due to lack of evidence, will be anonymised once a decision is taken not to conduct an investigation, and no later than one year after submission of the report. The anonymised report will be kept on the EQS platform for the retention period of its most serious allegation, in case of repeat allegations.

For all of the three situations above, anonymisation will take place at least 3 months and one day after a decision not to conduct an investigation or an investigation has been concluded, to comply with the legal period for claimants to lodge a legal case against the University. In case of legal claim against the University or a third-party involved, the personal data may be kept longer, meaning during the legal prescriptions related to the claim.

8. What are your rights with regard to the processing of your personal data?

According to the GDPR, you benefit notably from the following rights: right to be informed, right to access to your personal data, right to rectification, right to erasure, right to restrict the scope of the processing, right to object, right to data portability, right to lodge a complaint.

- Right to be informed: you have the right to know how your personal data is collected and used.
- Right to access you have the right to obtain a copy of the personal data we hold about you and to check whether it is lawfully processed.
- Right to rectification: you have the right to request the University to rectify any inaccurate personal data we hold about you.
- Right to erasure: you have the right to obtain from us the erasure of personal data concerning you without undue delay where one of the specific grounds applies and the processing is not necessary according to Art. 17 paragraph 3 GDPR.
- Right to restrict the processing: you have the right to restrict the processing of your personal data under certain circumstances.
- Right to object: you have the right to object on grounds relating to your situation, based on points (e) or (f) of Article 6 (1) GDPR.
- Right to data portability: in the instances where the processing is based on your consent and is carried out by automated means.
- Right to withdraw consent: in the instances where you have consented to the processing, you can withdraw your consent at any time by contacting the relevant department.

The University provides further information on its website page to the exercise of rights section.

In practice, you can exercise your rights by contacting the DPO, the contact details are dpo@uni.lu.

Any request shall be processed by the University of Luxembourg without undue delay, and where feasible no later than one (1) month after its receipt, at least in order to inform you about the status of your request. This period may be extended for two (2) additional months for complex cases or due to a high volume of requests.

9. How can you lodge a complaint?

If you consider that the Processing of Personal Data relating to you infringes the GDPR, you will have the right – without prejudice to any other administrative or judicial remedy – to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement.

In Luxembourg, the competent authority is the Commission Nationale pour la Protection des Données (CNPD).

Contact of the CNPD:

Commission Nationale pour la Protection des Données
1, avenue du Rock'n'Roll

Service des réclamations
L-4361 Esch-sur-Alzette

Tel. : (+352) 26 10 60 -1
Fax : (+352) 26 10 60 -29
You can also use their contact form, at: https://cnpd.public.lu/fr/support/contact.html