LUNEX Whistleblower Protection Policy

Procedure for the protection of whistleblowers and for reporting breaches.

Valid from 17th January 2024

Date: 17.01.2024
14-0159-17.01.2024

Sign-off Page

Approved

Name	Signature	Date
Dr. Matthias Afting	*	17.01.2024
Prof. Dr. Andreas Mierau	*	17.01.2024
Ms. Mihaela Bozonca	*	17.01.2024

Signatures removed for privacy reasons.

Table of Contents

1. **STATEMENT**

LUNEX S.A., having its registered office at L-4671 Differdange, 50 Avenue du Parc des Sports, registered with the Trade and Companies Register under number B190186 (the **“Company**”), **intends to conduct its business with honesty, integrity and in accordance with its values and expected standards of behaviour.**

2. **ABOUT THIS PROCEDURE**

The Company's primary aim is to prevent wrongdoing at any level. However, if wrongdoing does occur, the aim is to remedy it and prevent it from happening again.

The Company considers compliance to be essential to the conduct of its business.

Everyone, regardless of their role in the Company's organisation, has the right to speak up if they witness any act or omission that is unlawful or goes against the object or purpose of directly applicable Luxembourg or European legal provisions (a “**Breach**”).

The purpose of this procedure (the “**Procedure**”) is to put in place a framework within which employees and third parties can report Breaches within the Company without fear of retaliation.

This Procedure does not impose an obligation to report Breaches within the Company. Instead, it offers an option to do so, accompanied by guarantees.

3. **SCOPE OF APPLICATION**

3.1 This Procedure applies in the context of professional relations inside and outside the Company's premises.

The Procedure applies to**:**

(a) employees of the Company (whether permanent, temporary, full-time or part-time) ("**Staff**");

(b) Company trainees;

(c) former employees of the Company and persons whose work-based relationship has not commenced yet in cases where information on Breaches has been acquired during the recruitment process or other pre-contractual negotiations;

(d) current and former employees of the Company's contractors, subcontractors and suppliers and persons involved in pre-contractual negotiations;

(e) volunteers;

(f) current and former self-employed workers in business contact with the Company;

(g) corporate governance members (shareholders and members of the Company's administrative, management or supervisory bodies, including non-executive members);

(h) facilitators, i.e. natural persons who assist a whistleblower during the reporting process in a professional context and whose assistance should be confidential;

(i) third parties who are connected with a whistleblower and who are at risk of retaliation in a professional context, such as colleagues or relatives of a whistleblower; and

(j) legal entities belonging to a whistleblower or for which they work, or with which they have a professional relationship.

(“**Relevant Person(s)**”).

3.2 Breach does not include work-related personal grievances, which are grievances relating to the current or former employment or engagement of a Relevant Person, which have implications for them personally and do not fall within the definition of Breach. Work-related personal grievances may be raised through **the channels defined under the LUNEX Grievance Policy**. Examples of work-related personal grievances include disputes between members of Staff and decisions relating to the employment or engagement of a member of Staff, such as transfer, promotion or disciplinary action.

3.3 This Procedure takes into account the Luxembourg law of 16 May 2023 implementing Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (the “**Law of 16 May 2023**”).

3.4 In the event of a conflict between the provisions of this Procedure, the Law of 16 May 2023 and any other relevant Luxembourg laws, the provisions of the Law of 16 May 2023 and any other relevant Luxembourg laws shall prevail.

4. INFORMATION RELATING TO THE REPORT

4.1 Whistleblowing is the communication of information about Breaches (the “**Report**”) by a Relevant Person (hereinafter the “**Whistleblower(s)**”).

4.2 A Report may concern, for example:

- criminal activities;
- a health or safety hazard;
- damage to the environment;
- failure to comply with a legal or regulatory obligation;
- bribery or corruption;
- unauthorised disclosure of confidential information;
- conduct that harms or is likely to harm the financial position of the Company, its affiliates, branches or subsidiaries directly or indirectly related to the Company or its successors;
- conflicts of interest or unlawful taking of an interest; or
- deliberate concealment of any of the above matters.

4.3 Whistleblowers may report Breaches relating to the conduct of Company employees and of third parties, such as investors, suppliers or external service providers, whether based in Luxembourg or elsewhere.

5. RESPONSIBILITY

5.1 The Company's obligations are as follows:

- make an internal reporting channel that complies with the Law of 16 May 2023 and any other relevant Luxembourg law available to Relevant Person(s); and

- protect Whistleblowers against any form of retaliation.

5.2 Whistleblowers must act in good faith and, in particular, must have reasonable grounds for believing that the information reported about Breaches is true at the time of reporting and that the information falls within the scope of the Law of 16 May 2023. They must therefore report genuine information or reasonable concerns. Whistleblowers acting in bad faith are subject to the sanctions described in clauses 6.5(c) and 12 of this Procedure.

5.3 Whistleblowers may be held liable if they obtain or access the information reported in a way that constitutes a self-standing criminal offence.

6. PROCEDURE FOR INTERNAL REPORTS

6.1 General principles

(a) The Company encourages Relevant Persons to make a Report about a Breach through the Company's internal reporting channel (an "**Internal Report(s)**") and prior to reporting through external reporting channels. The objective is to enable the Company to take action to prevent harm to Relevant Persons or damage to the Company's performance or reputation.

(b) The Company**,** with the consultation of the staff delegation, has put in place this Procedure to enable Relevant Persons to make an Internal Report through the Company's internal reporting channel. Relevant Persons must follow the guidelines below to make a Report.

(c) Safeguards are put in place at each stage of the Procedure to prevent the disclosure of any information that could lead to the identification of a Whistleblower. The Company's internal reporting channel is designed, implemented and managed in a secure manner that ensures the confidentiality of the identity of the Whistleblower and any third party mentioned in a Report, and prevents unauthorised personnel from accessing it.

(d) In order to ensure optimal operation of this Procedure, particularly Internal Reports, the Company has decided to call on an external service provider, namely the law firm:

Arendt & Medernach S.A.
41A Avenue John F. Kennedy
L-1855 Luxembourg
(the "**Service Provider**")

(i) The role of the Service Provider is as follows:

- act as a third party within the meaning of Article 6(4) of the Law of 16 May 2023, to which the Company's internal reporting channel is outsourced and which is instructed for the purpose of managing Internal Reports. Within this framework, the Service Provider has appointed a team of three people to receive Reports (the "**Recipients of Internal Reports**");

- assist the Company in handling and monitoring Internal Reports; and

- assist the Company in carrying out an investigation, as described in clause 6.3 below (the "**Investigation**"), if the Company decides to implement such an Investigation. The Investigation will be carried out by a specialist investigation team.

(ii) Using the services of the Service Provider enables the Company to:

- establish and manage the receipt of Reports in a secure manner that guarantees the confidentiality of the identity of the Whistleblower and any third parties mentioned in the Report;

- prevent unauthorised persons from accessing the internal reporting channel;

- ensure that all Internal Reports are dealt with promptly in accordance with the applicable legal provisions;

- prevent potential conflicts of interest and/or internal pressure;

- offer a professional service, provided by experts in the field; and

- ensure that Reports are handled impartially, objectively and confidentially.

(iii) The Service Provider is subject to the same requirements as the Company under the Law of 16 May 2023. The reporting channel is designed, implemented and managed in a secure manner that guarantees the confidentiality of the identity of the Whistleblower and any third party mentioned in the Report, and prevents access by any unauthorised person.

(iv) The Recipients of Internal Reports will communicate with the Company, following receipt of an Internal Report and depending on the circumstances, in order to determine precisely what action should be taken in response to the Internal Report.

6.2 Internal reporting channel

The following procedure must be followed by Relevant Persons wishing to make an Internal Report, as outsourced to the Service Provider:

(a) The Whistleblower should send the Internal Report in writing to the Service Provider as soon as possible after the Breach occurs or the Whistleblower becomes aware of the Breach or potential Breach, using one of the methods below:

(i) **by e-mail**: **lunex.whistleblowing@arendt.com**;

(ii) **by post**: Arendt & Medernach S.A. c/o Whistleblowing Procedures, 41A Avenue John F. Kennedy, L-1855 Luxembourg.

The Report can be made in any of the following languages: French, German, Luxembourgish and English.

One of the Recipients of Internal Reports will record the details of the Internal Report anonymously in a confidential file for monitoring purposes.

(b) The Internal Report should be made in writing and should indicate:

(i) the nature of the Breach;

(ii) the identity of the person(s) concerned;

(iii) the date(s) and time(s) when the Breach was committed or observed;

(iv) the apparent duration of the Breach;

(v) the names of witnesses (if any) to the Breach; and

(vi) the measures already taken (if any) to prevent or stop the Breach.

(c) Where the Whistleblower makes an Internal Report anonymously, such Report may, depending on the circumstances, prevent contact being made with the Whistleblower and thus prevent information being obtained that is necessary and useful in order to carry out an investigation into the Breach that is the subject of the Internal Report. Similarly, anonymity may prevent full and/or appropriate investigations from being carried out.

(d) Internal Reports will in principle be investigated as described in clause 6.3 below (the "**Investigation**") and will be dealt with promptly, impartially, fairly, confidentially and with due regard to the rights of the Whistleblower and the alleged perpetrator(s). All Internal Reports will be taken seriously and assessed on their merits. Where appropriate, the Company, after assessing the situation, may decide that a Report is manifestly unfair, unfounded or insignificant and does not require further follow-up or investigation, other than closure of the procedure.

6.3 Investigation

If, after an initial analysis of the Internal Report, the Company decides to conduct an Investigation, this will be carried out by a specialised team (the "**Investigators**"), in accordance with the following rules:

(a) If deemed necessary in the course of an Investigation, care will be taken to ensure that the Whistleblower is not placed in a position where they could be identified or subjected to retaliation. Any such action will be taken for the sole purpose of facilitating the Investigation and must not be perceived as prejudicing the outcome of the Investigation, materially altering the Whistleblower's employment contract or as retaliation.

(b) Investigations will always be conducted by impartial Investigators who have the necessary experience and knowledge to deal with such matters.

(c) Notes will be taken during the Investigation.

(d) If the Whistleblower is identified or identifiable, the Investigators will interview them, with their consent, and ask them to give full details of the alleged Breach(es).

(e) The alleged perpetrator(s) of the Breach will be invited to meet with the Investigators, will receive detailed information about the allegations made against them, without prejudice to the confidentiality of the identity of the Whistleblower, and will be given the opportunity to respond to the allegations.

(f) Where witnesses are identified by either party, the Investigators will use their best endeavours to pursue the Investigation with those witnesses, without disclosing any information about the identity of the parties involved, to the extent legally possible.

(g) Where an Investigation requires other members of Staff to be interviewed, the interviews will be conducted in the strictest confidence. The need for confidentiality will be stressed to all members of Staff involved in the Investigation process and it will be made clear that any breach of confidentiality may result in disciplinary action.

(h) It may be necessary for the Investigators to review correspondence (electronic mailbox or instant messaging system) from the alleged perpetrator and/or any other person following the interview of witnesses. Reviews will be conducted in such a way as to limit the relevant period during which electronic mailbox and/or instant messaging system were exchanged and received to the minimum necessary to verify the allegations made in any Report. The Investigators will screen correspondence by key words before reviewing only the accordingly selected correspondence.

(i) When the Investigation is complete, a record will be made of the Investigation, its outcome and any action taken, subject to compliance with the GDPR[1] and relevant Luxembourg laws[2] .

6.4 **Deadlines**

The Company recognises that time is of the essence for Internal Reports and will ensure that the following rules are adhered to in relation to Internal Reports and Investigations:

(a) One of the Recipients of Internal Reports will acknowledge receipt of the Internal Report within seven (7) days from the date of receipt of the Report (the "**Receipt**").

---

[1] 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).

[2] In particular, the law of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters, as applicable and subject to any future amendments.

(b) Within three (3) months following the sending of the Receipt or, if no Receipt was sent to the Whistleblower, within three (3) months following the expiry of the period of seven (7) days after the Report was made, the Whistleblower will receive feedback on the measures envisaged or taken to assess the accuracy of the allegations made in the Report and, where appropriate, to remedy the reported Breach, including internal investigation, prosecution, action to recover funds, or termination of the proceedings, and the grounds for this follow-up (the "**Feedback**").

(c) However, the obligation of confidentiality and/or the fact that the Internal Report was made anonymously may prevent the communication of Feedback to the Whistleblower. The Whistleblower must treat all information provided as part of the Feedback as confidential.

(d) While it is desirable to resolve all Internal Reports quickly, this will not always be possible if the Investigation is to be both thorough and fair.

(e) The Company's Administration Department is responsible for ensuring that the Investigation is properly monitored.

6.5 **Investigation outcome**

(a) After the Investigation is concluded, the Investigators and the Company will ensure, so far as is reasonably practicable, that the Whistleblower is informed of the overall findings of the Investigation and the action taken or to be taken in accordance with clause 6.4(b).

(b) If a Breach is found to have occurred, this may lead to the Company taking disciplinary measures, up to and including dismissal with or without notice.

(c) If it is found that a Report was not made in good faith and was supported in the same way (e.g. by witnesses), disciplinary measures up to and including dismissal may, if the Company deems it appropriate, be taken. The Company reserves the right to bring a civil liability action against the Whistleblower, who will also be liable to criminal sanctions, including fines ranging from EUR 1,500 to EUR 50,000 and a term of imprisonment of between eight (8) days and three (3) months, in accordance with Article 27(5) of the Law of 16 May 2023.

(d) If the Company fails to comply with its obligations under this Procedure and fails to investigate a Report or does not provide Feedback in accordance with clause 6.4(b), the Whistleblower may raise concerns with any external competent authority in accordance with clause 7 of this Procedure.

(e) The special protection afforded to the Whistleblower in accordance with the Law of 16 May 2023 will generally cease after the end of the Investigation and any measures taken by the Company.

7. EXTERNAL REPORTING AND PUBLIC DISCLOSURE

7.1 Whistleblowers are encouraged to report Breaches through the internal reporting channel in accordance with this Procedure to ensure that the Report is handled as quickly and efficiently as possible.

7.2 However, Whistleblowers may also report information about Breaches using the channels and procedures referred to in Articles 17 and 19 of the Law of 16 May 2023, after having reported via the internal reporting channel or by reporting directly via external reporting channels. In this case, the Whistleblower may report to one of the twenty-two (22) competent authorities listed below (the "**External Report"**):

1. *La Commission de Surveillance du Secteur Financier (*Financial Sector Supervisory Commission*).*

2. *Le Commissariat aux Assurances (*Insurance Supervisory Authority*).*

3. *L'Autorité de la concurrence (*Competition Authority*).*

4. *L'Administration de l'enregistrement, des domaines et de la TVA (*Registration Duties, Estates and VAT Authority*.*

5. *L'Inspection du Travail et des Mines (*Inspectorate of Labour and Mines*).*

6. *La Commission nationale pour la protection des données (*National Commission for Data Protection*).*

7. *Le Centre pour l'égalité de traitement (*The Centre for Equal Treatment*).*

8. *Le Médiateur dans le cadre de sa mission de contrôle externe des lieux où se trouvent des personnes privées de liberté (*The Ombudsman, as part of their responsibility for external supervision of places where people are deprived of their liberty*).*

9. *Ombudsman fir Kanner a Jugendlecher.*

10. *L'Institut luxembourgeois de régulation (*Luxembourg Regulatory Institute*).*

11. *L'Autorité luxembourgeoise indépendante de l'audiovisuel (*Luxembourg Independent Audio-visual Media Authority*.*

12. *L'Ordre des avocats du Barreau de Luxembourg et l'Ordre des avocats du Barreau de Diekirch (*Luxembourg and Diekirch Bar Associations*).*

13. *La Chambre des notaires (*Chamber of Notaries*).*

14. *Le Collège médical (*Medical Board*).*

15. *L'Administration de la nature et des forêts (*Nature and Forest Agency*).*

16. *L'Administration de la gestion de l'eau (*Water Management Authority*).*

17. *L'Administration de la navigation aérienne (*Air Navigation Authority*).*

18. *Le Service national du Médiateur de la consommation (*National Consumer Ombudsman Service*).*

19. *L'Ordre des architectes et des ingénieurs-conseils (Association of Architects and Consulting Engineers).*

20. *L'Ordre des experts-comptables (Association of Chartered Accountants).*

21. *L'Institut des réviseurs d'entreprises (*Institute of Auditors*).*

22. *L'Administration des contributions directes (*Direct Taxes Authority*)***].**

7.3 The *Office des Signalements* (Reporting Office) is the competent body in Luxembourg if a Relevant Person needs advice on how to report a Breach**.**

7.4 In very limited circumstances, Whistleblowers may make a public disclosure of a Breach ("Public Disclosure") if:

(a) after an Internal and an External Report or an External Report only, no appropriate action has been taken within three (3) months and seven (7) days; or

(b) the Whistleblower has reasonable grounds to believe that:

(i) the Breach may constitute an imminent or manifest danger to the public interest, such as an emergency situation or a risk of irreversible damage; or

(ii) in the case of an External Report, there is a risk of retaliation or there is a low prospect of the Breach being effectively addressed, due to the particular circumstances of the case, for example where evidence may be concealed or destroyed or where an authority may be in collusion with the perpetrator of the Breach or involved in the Breach.

Breaches disclosed publicly in breach of the Law of 16 May 2023, as summarised in this clause, will not give rise to any protection for Whistleblowers, who will incur civil liability for any damage suffered by the Company.

8. DOCUMENTATION AND DATA PROTECTION

8.1 All relevant documents, including written statements from Whistleblowers, perpetrators of Breaches and witnesses, minutes of meetings and any other relevant supporting documentation, will be retained by the Company in accordance with the Law of 16 May 2023 and for the maximum period provided by the relevant Luxembourg laws and the GDPR, and may be used in disciplinary actions, as appropriate.

8.2 Relevant Persons who make a Report should endeavour to disclose only information relating to the Breach and avoid disclosing customer information, personal data relating to third parties or other sensitive information which is not related to the Breach.

8.3 Where the Whistleblower requests a meeting with Authorised Recipients (as defined in clause 9.1 below), the Company will, with the consent of the Whistleblower, ensure that a full and accurate record of the meeting is kept in a durable and retrievable form. The Whistleblower has the right to check, correct and approve the record of the meeting by signing it.

8.4 Personal data that is clearly not relevant to the processing of a specific Report will not be collected or, if collected accidentally, will be deleted as soon as possible.

8.5 Any processing of personal data under the Procedure will be carried out in accordance with the Data Protection Laws (as set out in Annexe 1) and any data protection provisions set out in the data protection policy relating to the protection of whistleblowers attached to the Procedure as Annexe 1 or provided by the Service Provider along with the Receipt (the "**Policy**"). This Policy supplements, to the extent necessary, the Company's information notice applicable to the processing of the personal data of the Company's employees.

8.6 In relation to legal advice provided to the Company by the Service Provider, the Service Provider acts as data controller. In this respect, Relevant Persons acknowledge that they have read the Service Provider's information notice attached to the Procedure as Annexe 2 or provided by the Service Provider along with the Receipt.

9. CONFIDENTIALITY

9.1 The information provided by the Whistleblower will be treated as confidential to the extent possible and in accordance with the Company's legal obligations and its obligation to conduct a thorough review of the Report. It will be received by the Internal Report Recipients and, where appropriate, shared with the Investigators conducting the Investigation (the Internal Report Recipients and the Investigators are together referred to as the "**Authorised Recipients**") (unless disclosure is prohibited or required by law or by a regulatory authority).

9.2 The identity of the Whistleblower will not be disclosed to anyone other than the Authorised Recipient(s) without the explicit consent of the Whistleblower. This provision also applies to any other information from which the identity of the Whistleblower may be directly or indirectly deduced.

9.3 By way of derogation, the identity of the Whistleblower and any other information mentioned in the Report may be disclosed only if this is a necessary and proportionate obligation imposed by Luxembourg law or European Union law in the context of investigations carried out by national authorities or in the context of legal proceedings, in particular with a view to safeguarding the rights of defence of the person concerned.

9.4 Disclosures made pursuant to clause 9.3 above shall be subject to appropriate safeguards. In particular, the Whistleblower will be notified before their identity is disclosed, unless such notification is likely to compromise the investigations or legal proceedings concerned.

9.5 When notifying the Whistleblower, the Company will send them a written explanation of the reasons for the disclosure of the confidential data concerned.

10. TRAINING

Specific training may be organised for personnel managers to raise their awareness of whistleblowing.

11. PROTECTION OF WHISTLEBLOWERS AND MEASURES AGAINST RETALIATION

11.1 The Company will not tolerate any act of retaliation against a Whistleblower, including threats of retaliation and attempts of retaliation, because of a Report they have made in accordance with this Procedure and the Law of 16 May 2023, their objection to a Breach or their testimony in connection with a Breach. Any act of retaliation will be punished by nullifying the act in question.

11.2 To benefit from this protection, the Whistleblower must:

(a) have reasonable grounds to believe that the information reported about the Breach was true at the time of reporting and that this information falls within the scope of the Law of 16 May 2023, and

(b) have made either an Internal Report in accordance with this Procedure, or an External Report or a Public Disclosure in accordance with clause 7 and the Law of 16 May 2023.

11.3 A Whistleblower who makes a Report anonymously may only benefit from the protection offered by the Law of 16 May 2023 and this Procedure if (i) they are subsequently identified and suffer retaliation as a result of the Report, and (ii) they fulfil the conditions set out in clause 11.23.

11.4 A Whistleblower who reports a European Union Breach to the competent EU institutions, bodies, offices or agencies may benefit from protection under the same conditions as persons who make an External Report.

11.5 Retaliation may include, but is not limited to:

- suspension of an employment contract, lay-off, dismissal, failure to renew or early termination of a fixed-term employment contract or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of workplace, reduction in salary, change in working hours;
- withholding of training;
- imposition or administering of any disciplinary measure, reprimand or other penalty, including financial penalties;
- failure to convert a temporary employment contract into a permanent contract, where the employee had legitimate expectations that they would be offered a permanent job;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- negative performance assessment or employment reference;
- harm, including to the person's reputation, particularly on social media networks, or financial losses, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide formal or informal agreement, which may entail that the person will not find employment in the future in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;

- psychiatric or medical referrals.

12. DISCIPLINARY MEASURES AND SANCTIONS

12.1 The Company may take disciplinary measures in accordance with this Procedure and the Law of 16 May 2023 against, in particular, the perpetrators of Breaches, their accomplices, bad faith Whistleblowers and Whistleblowers who obtain or access information in a criminal manner. Depending on the results of the Investigation (if one takes place) and the circumstances, disciplinary measures may be imposed in accordance with the Luxembourg law and may include but are not limited to:

- negative impact on promotional opportunities;
- exclusion from performance-related bonuses/salary increases;
- formal warning;
- demotion;
- dismissal (with or without notice);
- termination of business relationship; or
- revocation of authority (*ad nutum* revocation).

12.2 The Company also reserves the right to impose any other sanction it deems appropriate in the circumstances, and/or to initiate (i) legal proceedings with a view to obtaining, *inter alia*, compensation for any loss suffered, and (ii) criminal proceedings against bad faith Whistleblowers as described in clause 6.5(c) and/or Whistleblowers who have obtained or accessed information in a manner which constitutes a self-standing criminal offence.

12.3 Any measures taken to put an end to a Breach will not be to the detriment of the Whistleblower.

12.4 The competent authorities and the *Office des Signalements* may, among other things, impose fines on individuals and legal persons who:

(a) obstruct or attempt to obstruct a Report;

(b) refuse to provide the competent authorities with the information they request and consider necessary, or provide incomplete or false information;

(c) infringe the confidentiality conferred on Whistleblowers;

(d) refuse to remedy an identified Breach.

The fines range from EUR 1,500 to EUR 250,000. These amounts may be doubled in the event of a repeat offence within five (5) years.

12.5 Fines ranging from EUR 1,250 to EUR 25,000 may be imposed on Staff who retaliate against Whistleblowers or who initiate vexatious proceedings against them.

13. LEGAL ACTIONS

13.1 A Whistleblower who is a victim of retaliation may exercise any right available to them under the relevant Luxembourg laws, and in particular their rights under the Law of 16 May 2023.

13.2 The Company reserves the right to refer allegations of Breach to the competent law enforcement authorities and/or public authorities (including the Public Prosecutor's Office). If an investigation leads to criminal proceedings, it may be necessary for the Whistleblower to provide evidence or to be questioned by the public authorities. This does not affect the Company's right to investigate and, if appropriate, punish allegations of Breach and vice versa.

13.3 The rules set out in this Procedure and the provisions of the Law of 16 May 2023:

(a) do not prevent Relevant Persons from exercising their legal rights at any time;

(b) do not affect the rules relating to the exercise by employees of their right to consult their representatives or trade unions, and entitling them to protection against any unjustified prejudicial measure arising from such consultation, nor do they affect the autonomy of social partners (partenaires sociaux) or their rights to conclude collective agreements;

(c) do not prevent a Relevant Person, from making an External Report or a Public Disclosure, in accordance with the applicable legal provisions.

14. REVIEW OF THE PROCEDURE

This Procedure will be reviewed regularly, and any changes will be notified to Relevant Persons.

The Company will use its best endeavours to maintain and ensure the continuous improvement of this Procedure, including, but not limited to, review of applicable procedures to prevent and combat Breaches. This internal audit will be conducted on a regular basis.

The Company reserves the right to modify this Procedure at any time after involving the staff delegation, if applicable.

15. ANY QUESTIONS?

Any questions relating to this Procedure should be addressed to the Administration Department via hr@lunex.lu

ANNEXE 1 - DATA PROTECTION POLICY RELATING TO THE PROTECTION OF WHISTLEBLOWERS

All capitalised terms used but not defined in this Annexe have the same meaning ascribed to them in the Procedure.

The purpose of this whistleblower data protection policy (the "**Policy"**) is to provide Relevant Persons and any other person with information on how their personal data may be processed by the Company in the context of the Procedure.

In this regard, the Company, acting as data controller, collects, stores and processes, by electronic or other means, personal data provided by Relevant Persons, and any other person (the "**Data Subject(s)**"), in accordance with the provisions of the GDPR and any applicable national data protection law (including, but not limited to, the Luxembourg law of 1 August 2018 organising the National Commission for Data Protection and the general data protection framework, as it may be amended or replaced) (collectively, the "**Data Protection Laws**") and the provisions of this Policy.

Contents

1. WHAT PERSONAL DATA DOES THE COMPANY COLLECT AND FOR WHAT PURPOSES?

As part of the Procedure, the Company may process the following personal data for the following purposes:

1.1 Purpose no. 1: processing and examining Reports

CATEGORIES OF PERSONAL DATA	LEGAL BASES
The Company may process the following categories of personal data relating to the Data Subjects: • **Identification details**: name, age, gender, professional title, address; • **Contact details**: e-mail address, telephone number; • **Information on disciplinary matters and grievances**;	The Company uses the following legal bases to process personal data: • **Compliance with a legal obligation** to which the Company is subject; • The processing is necessary for the purposes of **carrying out the obligations and exercising the rights specific to the controller or the Data**

• **Other information contained in the Report**: statements by the Whistleblower, the alleged perpetrator of the Breach, witnesses etc; • **Sensitive data**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, data concerning a person's sex life or sexual orientation included in the Report or mentioned by the Whistleblower, the alleged perpetrator or witnesses; • **Personal data relating to criminal convictions and offences**.	**Subject in the field of employment law insofar as** such processing is authorised by European Union law, by the law of a Member State or by a collective agreement entered into under the law of a Member State which provides appropriate safeguards for the fundamental rights and interests of the Data Subject;

1.2 **Purpose 2: risk management and establishing, exercising or defending legal claims**

CATEGORIES OF PERSONAL DATA	LEGAL BASES
The Company may process the following categories of personal data relating to Data Subjects: • **Identification details**: name, age, gender, professional title, address; • **Contact details**: e-mail address, telephone number; • **Information on disciplinary matters and grievances;** • **Other information contained in the Report**: statements by the Whistleblower, the alleged perpetrator of the Breach, witnesses etc; • **Sensitive data**: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health, data concerning a person's sex life or sexual orientation included in the Report or mentioned by the Whistleblower, the alleged perpetrator or witnesses; • **Personal data relating to criminal convictions and offences.**	The Company uses the following legal bases to process personal data: • **The legitimate interests pursued by the Company** or by third parties, unless the interests or the fundamental rights and freedoms of the Data Subject require protection of personal data; • Processing is necessary for the **establishment, exercise or defence of legal claims.**

The Company may collect personal data from the following sources:

(a) Whistleblowers.

(b) The alleged perpetrator(s) of the Breach.

(c) The witness(es).

(d) The Company's legal counsel/Arendt & Medernach S.A.

(e) The service company involved in the investigation/Arendt Regulatory & Consulting S.A.

(f) The Company's files and, where applicable, the electronic mailbox or instant messaging system of the alleged perpetrator of the Breach or of other persons in accordance with the provisions of paragraph 6 of this Annexe.

Data Subjects may, at their discretion, refuse to communicate personal data to the Company. In this case, the Company may not be able to properly process and investigate the Report.

2. WITH WHOM WILL PERSONAL DATA BE SHARED?

The Company may communicate the aforementioned personal data to the following entities ("**Recipients**"):

- The Whistleblower/alleged perpetrator of the Breach (as the case may be).
- The Company's legal counsel/Arendt & Medernach S.A.
- The service company involved in the investigation/Arendt Regulatory & Consulting S.A.
- External consultants/investigators.
- The police.
- The Public Prosecutor's Office.
- *L'Administration de l'enregistrement, des domaines et de la TVA (*Registration Duties, Estates and VAT Authority).
- *L'Inspection du Travail et des Mines (*Inspectorate of Labour and Mines).
- *La Commission nationale pour la protection des données (*National Data Protection Commission).
- *Le Centre pour l'égalité de traitement (*The Centre for Equal Treatment).
- *Le Médiateur dans le cadre de sa mission de contrôle externe des lieux où se trouvent des personnes privées de liberté (*The Ombudsman, as part of their responsibility for external supervision of places where people are deprived of their liberty).
- *Ombudsman fir Kanner a Jugendlecher*.

- *Le Service national du Médiateur de la consommation* (National Consumer Ombudsman Service).
- *L'Institut des réviseurs d'entreprises* (Institute of Auditors).
- *L'Administration des contributions directes* (Direct Taxes Authority).
- *L'Office des signalements.*

The Recipients may, under their own responsibility, disclose personal data to their agents and/or delegates (the "**Sub-Recipients**"), who will process the personal data for the sole purpose of assisting the Recipients in providing their services to the Company and/or assisting the Recipients in fulfilling their own legal obligations.

The Recipients and Sub-Recipients may, as the case may be, process personal data as processors (where they process personal data on behalf of and on the instructions of the Company and/or the Recipients) or as separate data controllers (where they process personal data for their own purposes, namely the performance of their own legal obligations).

3. WHERE CAN PERSONAL DATA BE TRANSFERRED?

Personal data processed as part of the Procedure will not be transferred outside the European Economic Area.

4. HOW LONG WILL PERSONAL DATA BE KEPT?

The GDPR requires personal data to be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which it is processed.

The Company will retain personal data for the duration of the Investigation and for as long as any possible legal action relating to or based on the Report is not time-barred.

In certain circumstances, personal data may be rendered anonymous so that it can no longer be associated with the Data Subjects, in which case it no longer constitutes personal data and may be kept for an unlimited period. When the Company no longer needs the personal data for the purposes for which it was collected, it will destroy it securely in accordance with the applicable laws and regulations and its internal policy in this regard.

5. THE RIGHTS OF DATA SUBJECTS

In accordance with the conditions and limitations laid down in the Data Protection Laws, Data Subjects acknowledge their rights to:

- access their personal data;
- correct their personal data if it is inaccurate or incomplete;
- object to the processing of their personal data;
- restrict the use of their personal data;
- require the deletion of their personal data;

- request the portability of their personal data.

Data Subjects also have the right to withdraw their consent at any time, without this affecting the lawfulness of the processing based on consent prior to its withdrawal.

Data Subjects and any other person whose personal data is processed under the Procedure may exercise the above rights by writing to the Company at the following address: **[postal and/or e-mail address to be included]**, Luxembourg.

Data Subjects and any other person whose personal data is processed under the Procedure also acknowledge the existence of their right to lodge a complaint with the *Commission nationale pour la protection des données* (the "**CNPD**") at the following address: 15, Boulevard du Jazz, L-4370 Belvaux, Grand Duchy of Luxembourg; or with any competent data protection supervisory authority in their Member State of residence.

6. IT POLICY

The Company may access the professional electronic mailbox and, where applicable, the instant messaging system made available to Staff as part of their work, where evidence that makes the alleged Breach likely emerges from the Investigation through witness accounts and insofar as this is necessary to conduct the Investigation as required by the Law of 16 May 2023, and for its legitimate interests as listed above.

This review may cover the entire period during which the alleged Breach took place and, as far as possible, will use key words to select the correspondence to be reviewed. The review will at all times be carried out in strict compliance with applicable privacy protection laws and regulations.

7. CHANGES TO THIS POLICY

The Company reserves the right to update this Policy at any time and will make an updated copy directly available to the Data Subjects. Data Subjects will be notified of any material updates to the Policy.

ANNEXE 2 - INFORMATION NOTICE FROM ARENDT & MEDERNACH S.A.

In accordance with the legal provisions applicable in the Grand Duchy of Luxembourg regarding the protection of personal data and Regulation (EU) No. 2016/679 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 ("**Data Protection Laws**"), you acknowledge that Arendt & Medernach S.A., acting as data controller, collects, stores and processes, electronically or by any other means, your personal data provided in connection with your request for services and in order to comply with our legal obligations.

If you are a natural person, the data processed includes your name, address, date and place of birth, nationality, profession, contact details, preferred language of communication, bank details and any other personal data contained in your files. If you are a legal entity, the same categories of data may be processed in respect of (i) contact persons within your organisation and (ii) economic beneficiaries of your organisation ("**Personal Data**").

Personal Data is processed in order to process your requests, manage your files, maintain our commercial relationship, and comply with any applicable legal obligations, in particular with regard to combatting money laundering and the financing of terrorism.

You also have the right to:

(i) access your Personal Data;

(ii) request rectification of your Personal Data if it is inaccurate or incomplete;

(iii) restrict the use of your Personal Data;

(iv) object to the processing of your Personal Data;

(v) request the deletion of your Personal Data; and

(vi) exercise your right to the portability of your Personal Data under certain conditions defined in the Laws relating to the protection of personal data.

You also have the right to object to the processing of your Personal Data for marketing purposes.

The above rights may be exercised by sending an e-mail to dpo@arendt.com or by writing to our Data Protection Officer:

Arendt & Medernach
For the attention of: Nathalie Bloch, Data Protection Officer
41A Avenue John F. Kennedy
L-1855 Luxembourg
Grand Duchy of Luxembourg

You also have the right to lodge a complaint with the *Commission nationale pour la protection des données (CNPD)* at the following address: 15, Boulevard du Jazz, L-4370 Belvaux, Luxembourg; or with any competent data protection supervisory authority of your EU Member State of residence.

Personal Data may be transferred to other entities or individuals located inside or outside the European Union (in particular, our related entities (including Arendt Regulatory & Consulting S.A.), independent experts, notaries, bailiffs or foreign lawyers). Personal Data will under no circumstances be transferred to third parties located in a country outside the European Union which does not guarantee an adequate level of protection unless you have given your prior written consent to such transfer, or unless we have taken specific measures (such as appropriate contractual clauses) to ensure that data protection obligations have been met. To the extent permitted by law, Arendt & Medernach S.A. and/or Arendt Regulatory & Consulting S.A. may also disclose Personal Data to judicial authorities and/or administrative authorities within and outside the European Union. In any event, any transfer of Personal Data will only be carried out in compliance with the strict obligations of professional secrecy applicable in Luxembourg.

Finally, and subject to the legal statute of limitations, Arendt & Medernach S.A. will not retain your Personal Data for longer than is necessary for the purposes for which it is to be processed.