Data protection notice

PwC Luxembourg is the largest professional services firm in Luxembourg with a great appetite for technology and the use of the cloud environment. It strives to build trust in providing audit, tax and advisory services in ways that protect the information of its clients, people, and others with whom it does business through the design of its products and robust information security safeguards. PwC Luxembourg aspires to promote transparency through education initiatives, data protection principles and guidelines, and appropriate opportunities for choice, access, and correction with respect to personal information about data subjects.

This notice defines how PwC Luxembourg may process, in accordance with the applicable laws and for the purposes defined below, personal data collected from time to time (directly or indirectly, in a compulsory or voluntary manner, manually or otherwise) from data subjects themselves as well as from its clients, third parties (such as potential clients, subcontractors, providers or any stakeholders involved in an engagement with PwC Luxembourg) and/or from publicly available sources where applicable.

I. Definitions

- **Applicable Laws** means any laws, regulations and standards relating to the protection, privacy, confidentiality or security of personal data and applicable to PwC Luxembourg. The Applicable Laws include the "General Data Protection Regulation" (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);
- **Data subjects, personal data, processing, controller and processor** have the meanings given to them in the General Data Protection Regulation.
- **PwC Luxembourg** encompasses the Luxembourg member firms of the PwC network listed in Appendix 2.

II. Purposes of processing

PwC Luxembourg may process the personal data in accordance with the Applicable Laws and solely for the following purposes (together the "**Purpose(s)**"):

- To provide professional services including:
  - Audit and assurance;
  - Tax, Accounting and Reporting (Tax Consulting, Global Tax Compliance, Personal Tax, Accounting and Bookkeeping, etc.); and
  - Advisory (Consulting, Corporate Finance, Global Fund Distribution, Forensic, People & Organisation, Regulatory & Compliance, Technology, etc.).

- To maintain its administrative and client/supplier relationship management systems, including:
  - bid issuance and contract drafting;
  - clients/suppliers/alumni follow up and management;
  - invoicing and invoices payments;
  - advertising, communication and public relations;
  - event organisation;
  - quality reviews; and
  - client or user-experience improvement and personalisation of service delivery (such as via authentication, monitoring the performance and use of PwC applications where applicable).
- To apply acceptance and continuance procedures (including anti-money laundering, anti-bribery and counter-terrorist financing);
- To facilitate compliance with its legal, regulatory, professional and/or contractual obligations (including independence and archiving requirements);
- To maintain and protect its buildings, equipment, IT infrastructure and data (including access management and authentification, security and performance monitoring, etc.);
- To ensure its business continuity;
- To manage risks and litigations;
- To process data subjects' requests; and/or
- To manage its websites.

The Purposes above are based on at least one of the following legal bases:

- The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- The processing is necessary for compliance with a legal obligation to which PwC Luxembourg is subject;
- The processing is necessary for the purposes of the legitimate interests pursued by PwC Luxembourg or by a third party (such as protecting PwC Luxembourg asset, understanding its clients' needs and expectations or fulfilling its purpose or social interest); and/or
- The data subject has given consent to the processing for one or more specific purposes.

III. Categories of personal data processed

Depending on the purposes and the legal basis above, PwC Luxembourg may process the following categories of personal data:

- Identification data (e.g. name, photographs, audio and video recordings of individuals, …);
- Professional data (e.g. position, company, …);
- Administrative data (e.g. identity documents, birthdate, gender, language, …);
- Financial data (e.g. tax data, transactional data, ...);
- Numeric data (e.g. logs, IP address, …); and
- Relation data (e.g. relation history, attendance sheets, …);
- Environment data (e.g. marital status, characteristics, habits, social media information, …).

IV. Categories of data subjects

The personal data processed by PwC Luxembourg may concern the following data subjects, when applicable:

- Clients and potential clients;
- Clients and potential clients' future, former or current employees and trainees, beneficial owners and board members; and
- Clients and potential clients' suppliers, customers, agents, advisors and/or personnel who are employed by, deal with or are otherwise associated with a client or potential client or who are or may become involved in a transaction/contract with a client or potential client.

V. Categories of recipients and personal data transfers

To the extent permitted or required by the Applicable Laws, PwC Luxembourg may disclose the personal data to any recipients if they are concerned by the Purpose(s) and, when such recipients process the personal data on behalf of PwC Luxembourg, if they are bound by commitments substantially equivalent to those of PwC Luxembourg as expressed in this notice.

Besides the data subjects themselves, the categories of recipients are the following:

- Subcontractors, business partners and experts;
- Processors and Sub-processors such as IT suppliers (including systems administrators, cloud services providers, hosting providers, etc.);
- Other PwC entities;
- PwC Luxembourg's external counsels, agents or auditors;
- Entities or individuals that have a relationship with the data subjects (employers, relatives, counsels, business or potential business partners, etc.); and/or
- Eupervisory bodies or public authorities.

PwC Luxembourg shall not transfer any personal data outside the EEA except i) to countries that provide an adequate level of protection for personal data as determined by the European Commission; or ii) to recipients under a suitable agreement that contains the requirements of the Applicable Laws for such transfer. A copy of the applicable safeguards and potential additional measures may be requested to the PwC Luxembourg's Data Protection Officer.

VI. Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, PwC Luxembourg shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access including inter alia as appropriate:

- The pseudonymisation and encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity and availability of its processing systems;
- The ability to restore the availability and access to personal data in the event of an incident; or
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

More details on PwC Luxembourg's information security controls are set forth in Appendix 1.

VII. PwC Luxembourg acting as processor

When PwC Luxembourg processes personal data on behalf of one or more data controllers, without exercising any influence on the purposes and means of the processing or without professional expertise (within the meaning of the Guidelines 07/2020 on the concepts of controller and processor in the GDPR issued by the European Data Protection Board), it acts as a data processor. This section concerns any outsourcing of an internal process or function of a controller (payroll, internal audit, tax reporting...) to PwC Luxembourg as a service provider.

In this context, PwC Luxembourg agrees to process the personal data only on the lawful documented instructions from the controller set in the contractual documents applicable to the services and this notice and shall ensure that its employees authorised to access the personal data are under an appropriate obligation of confidentiality. For avoidance of any doubt, this notice is designed to meet the requirements of Article 28 of the General Data Protection Regulation.

PwC Luxembourg shall make available to the controller lawful information necessary to demonstrate compliance with the obligations laid down in this notice and will allow for and contribute to audits and inspections, to the extent legally permitted, subject to reasonable prior notice and confidentiality obligations. Audits/inspections shall be conducted during normal Luxembourg business hours and no more than once a year. PwC Luxembourg hereby informs the controller that audits/inspections could not breach the legal, regulatory and contractual obligations incumbent on PwC Luxembourg, such as professional secrecy. Hence, the controller, and its potential auditors, shall not be entitled to access (i) data or information related to other clients of PwC Luxembourg, (ii) any PwC Luxembourg proprietary data or (iii) any other confidential information held by PwC Luxembourg that is not relevant or strictly necessary for the purposes of the audit/inspection.

PwC Luxembourg shall assist the controller by undertaking appropriate technical and organisational measures depending on the nature of the processing, insofar as this is possible, that are necessary for the fulfilment of the controller's obligation to:

- respond to requests for exercising the data subject's rights, as defined in this notice;
- carry out data protection impact assessments and conduct prior consultations with a supervisory authority or other government authority where required by the Applicable Laws;
- notify a personal data breach to the competent supervisory authority and/or data subjects. For that purpose, PwC Luxembourg shall notify the controller without undue delay of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the personal data; and
- provide information that the controller reasonably requests to enable the controller to comply with its obligations under Applicable Laws where the requested information is in PwC Luxembourg's possession or under its control and the controller has no other reasonable means of obtaining the information.

Where PwC Luxembourg engages other processors to carry out specific processing activities on behalf of the controller (**Sub-processor(s)**), it shall impose on them substantially similar data protection obligations as set out herein by way of a contract or other legal act under European Union or Member State law. The controller hereby provides a general authorisation to PwC Luxembourg for the engagement the Sub-processors as defined in Section V above. Any intended changes concerning the addition or replacement of the Sub-processor(s) shall be communicated to the controller, thereby giving the controller the opportunity to object to such changes.

VIII. Clients' obligations

Depending on the Purposes, the provision of the personal data is a statutory and/or contractual requirement; failure to provide these personal data might make it impossible for PwC Luxembourg to perform the services.

As an essential condition for performing the services, PwC Luxembourg assumes that the clients (and any stakeholders involved in an engagement with PwC Luxembourg, for which the clients concerned stand surety), ensure that:

- the personal data they provide (or give access) to PwC Luxembourg are accurate, adequate, relevant and limited to what is necessary for the specific Purpose for which they are disclosed and are adequately backed-up in their systems;
- they comply with the Applicable Laws in connection with PwC Luxembourg's processing of the personal data (including the lawfulness of the data provision and, where applicable, collecting and managing the data subject's consent accordingly);
- the data subjects are informed of the conditions and modalities of PwC Luxembourg's processing of their personal data as described in this notice in the form required by the Applicable Laws; and
- they will immediately inform PwC Luxembourg if any of the conditions above ceases to be met.

IX. Retention period

The personal data shall be kept in a form which permits identification of the data subjects for no longer than is necessary for each Purpose for which they have been collected, without prejudice to automatic IT back-ups and PwC Luxembourg's legal and regulatory archiving obligations.

X. Data subjects' rights

To the extent permitted by the Applicable Laws, data subjects may have the right to:

- request access to, rectification or erasure of their personal data;
- restriction of processing of their personal data;
- object the processing of their personal data; and
- data portability.

Should the processing of the data subject's personal data be exclusively based on his/her consent, the data subject shall have the right to withdraw such consent at any time, without affecting the lawfulness of the processing based on consent before such withdrawal.

To exercise the rights listed above, the data subject shall send an email to PwC Luxembourg's Data Protection Officer demonstrating his/her identity and specifying the right that he/she wishes to exercise.

Data subjects shall in addition have the right to lodge a complaint with the competent supervisory authority, the lead supervisory authority competent for personal data processed by PwC Luxembourg being the *Commission nationale pour la protection des données* (CNPD).

XI. Governing law - Validity

This notice sets the exhaustiveness of PwC Luxembourg's commitments regarding personal data processing and supplement any other commitments otherwise agreed.

To comply with the Applicable Laws and to reflect adequately the way in which PwC Luxembourg processes the data, this notice shall be updated from time to time.

This notice sets and all matters arising from or connected with it are governed exclusively by the laws of Luxembourg with the exclusive place of jurisdiction being Luxembourg-City.

Appendix 1
Security areas covered and controls featured

PricewaterhouseCoopers, Société coopérative has been assessed and found to be in accordance with the management system requirements under ISO/IEC 27001:2022. The Information Security Management System covers all information systems and processes employed by PricewaterhouseCoopers to store and process clients' data in accordance with Version 3.0 of the Statement of Applicability, dated of September 2023.

All PricewaterhouseCoopers member firms are expected to comply with, or exceed, the requirements of the Information Security Policy (ISP) defined, maintained and audited by the PwC Network Information Security Center (NIS). The ISP is aligned with the control requirements of ISO/IEC 27002.

This appendix summarises PwC Luxembourg's commitments towards security control domains defined by the ISO/IEC 27002 international information security management standard. The security controls and initiatives are not limited to the examples mentioned in this document which aims at giving an overview of PwC Luxembourg's information security maturity. The areas outlined below correspond to the objectives and controls outlined in ISO/IEC 27002, with adjustments tailored to PwC Luxembourg's business and security environment.

a. **Security Policy:** describes the need to protect our information and technology assets, to ensure compliance with regulatory and contractual obligations and any additional PwC Luxembourg policies, standards and local security policies. Controls include, but are not limited to:

   - The formal ISP aligned with the control requirements of ISO/IEC 27002;
   - An annual review of the ISP conducted in accordance with the defined PwC Network Information Security governance process;
   - An ongoing process to develop and maintain further or more comprehensive information security policies, standards, and guidelines established and implemented at PwC Luxembourg including development, review, approval, and publication. These security policies, standards, and guidelines are reviewed periodically to ensure that the PwC Luxembourg's information technology resources are adequately maintained and protected.

b. **Organisation of Information Security.** The security management at PwC Luxembourg, encompassing the firm-wide security model framework; third party access to its resources and security requirements for outsourced service providers. Controls include, but are not limited to:

   - A dedicated team of information security professionals;
   - A dedicated information security committee with key members from management;
   - A formalised commitment from top management to information security and delivering the resources and budget needed to comply with the information security strategy; and
   - Whenever confidential data is to be outsourced to a specific third party vendor, a specific security evaluation being part of the assessment process.

c. **Asset Management.** Classification and security of information assets and systems, including data classification. Controls include, but are not limited to:

   - Definition of a data classification scheme, communicated to all members of staff;
   - An inventory of all information systems assets is kept up-to-date; and
   - Software restricting the transferring of files on removable media from the firm's PCs.

d. Human Resources Security. Areas affecting personnel security such as employee vetting, terms and conditions of employment, confidentiality agreements, and user awareness training. Controls include, but are not limited to:

- A Security Awareness Programme which keeps the employees aware of their role and responsibilities in relation with information security. This Security Awareness Programme includes training of all new employees, multiple awareness communications during the year and specific awareness programmes tailored to certain roles at PwC Luxembourg;
- Definition of information security responsibilities in job descriptions; and
- Background checks of employees which include education, professional licences and prior employment. Change of employment status (new hires, move/change of position, leaving, etc.) are directly notified to the relevant IT personnel in order to update or revoke access rights and return any PwC Luxembourg' assets.

e. Physical and Environmental Security. Building access control, clean desk policy and laptop security with the overall aim of ensuring that our business premises and the information and technology assets residing within them are adequately protected. Controls include, but are not limited to:

- Access to the premises controlled through personal access cards. All PwC Luxembourg employees must carry such a badge, displaying their ID photograph, at all times;
- Data centers are equipped with specific access control, fire detection and fire suppression mechanisms, cooling systems and backup power capabilities;
- Each PwC Luxembourg employee having their own storage space, lockable with a personal security code;
- Each PwC Luxembourg employee having a security cable being required to attach his/her laptop at any time to prevent theft; and
- Documents printing made secure by the employees' individual badge being required.

f. Communications and Operations Management. Secure operation and management of information processing centers. Controls include, but are not limited to:

- Clear separation of test and production environments;
- We have a secondary data center distant from the primary data center. This secondary data center offers the following capabilities:
  – real-time replication of data with our main data centre;
  – backup Internet line; and
  – server redundancy (online or on standby mode, depending on the availability requirements).
- Backup of all servers are performed daily on disks and tapes. A set of the backup tapes are encrypted and stored in a distant site;
- Our Internet architecture in based on a "3-tiers" model and is protected by network firewalls, application firewalls and Intrusion Detection/Prevention systems (network-based and host-based). Redundancy is in place at each layer;
- Each PC (including laptop) and Server is equipped by an anti-virus managed centrally and updated at least daily (emergency update possible in real-time). In addition, each PC is equipped with Desktop Firewall and HIPS (Host Intrusion Prevention Systems);
- Hard disks (including laptop) are fully encrypted;
- For confidential file exchange, we maintain a secure file transfer platform, which enables authentication for file access and encryption during file transfer over the Internet.

g. **Access Control.** To ensure that correct and appropriate access is assigned to our information and technology assets based upon a data classification scheme and assigned roles and responsibilities. Controls include, but are not limited to:

- Role-based access control is applied throughout PwC Luxembourg and roles are defined according to the employees' functions. Changes of access rights are subject to specific approval workflows, adapted to the nature of the information to be accessed;
- PwC Luxembourg employees do not have privileged access on their computer (no administrator rights);
- All privileged accesses are performed through a PUM (Privileged User Management) system and are logged and monitored in PwC's SIEM (Security Information and Event Management);
- To access privilege accounts, dynamic MFA (Multi Factor Authentication) is required;
- Remote access is only possible from corporate devices (device authentication by certificate) and through an encrypted channel (VPN);
- Access to internal application from mobile devices managed through a secure Mobile Device Management system;
- Wireless connections to our internal network are only authorised from corporate computers (device authentication by certificate).

h. **Information Systems Acquisition, Development and Maintenance.** Development and ongoing maintenance of information systems to ensure adequate security controls are included during the conceptual design phase. Controls include, but are not limited to:

- Any change on production goes through a validation process supervised by our Change Advisory Board;
- For every IT project, a mandatory information security risk assessment has to be performed. These risk assessments lead to security action recommendations and are reviewed and validated by the project manager, the CIO, the information owner, the chief security officer, the project sponsor, as well as a risk management responsible when appropriate;
- Each new application has to undergo a security penetration test before going into production, unless specified otherwise in the information security risk assessment. The penetration tests for web applications accessible from the Internet and hosting confidential information are done by an independent third-party and performed again every year;
- Vulnerability scans are performed on our servers on a monthly basis;
- Installation of software is only possible after proper authorisation. Use of new software is subject to a security evaluation before being allowed;
- SAAS (Software As A Services) solutions undergo security analysis, the providers of those solutions are also assessed through a third party risk management process.

i. **Information Security Incident Management.** Controls to communicate information security events and weaknesses associated with information systems in a manner allowing timely corrective actions to be taken. Controls include, but are not limited to:

- Tools to detect potential incidents in log files and automatic notifications are in place;
- Periodical reviews of the log files of Security Devices are performed to detect potential incidents;
- Periodical reporting of information Security Incidents is in place and includes escalation to Risk Management representatives of each Business line;
- Specific procedures in place for internal/external communication of incidents.

j. **Business Continuity Management.** Business continuity and disaster recovery planning based upon service level agreements and recovery time objectives with the overall aim of ensuring minimal impact to our business in the event of a disaster. Controls include, but are not limited to:

- Redundancy measures are in place for all our systems and applications, according to the business requirements;
- Periodical tests are conducted to ensure of the efficiency of our redundancy measures;
- We have a secondary - distant - data center where our data and systems are replicated;

- Our business continuity and disaster recovery plans are reviewed and updated periodically and after each important change.

k. Compliance. Outlines controls that measure and monitor compliance of PwC Luxembourg and its systems with PricewaterhouseCoopers' policies and other relevant security standards. Controls include, but are not limited to:

- Our policies, procedures, processes and systems relative to information security are regularly audited by the NIS;
- Our team of dedicated lawyers and legal experts are included in the review of contracts signed with third parties as well as appropriate policies and procedures.

Disclaimer

PricewaterhouseCoopers refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate legal entity. For more information about PwC please visit www.pwc.com/structure. The intent of this document is only to provide a high level overview of the IT Security measures implemented to help protect information as well as PwC Luxembourg's IT infrastructure and applications.

1 PwC Luxembourg

PricewaterhouseCoopers

A Luxembourg cooperative company *(Société coopérative)*
Registered Office: 2, rue Gerhard Mercator, L-2182 Luxembourg
Tel / Internet site: +352 494848 1 / www.pwc.lu

Authorised audit firm (*Cabinet de révision agréé*) and chartered accountant *(Expert-comptable*, with government authorisation No. 10028256)
R.C.S. Luxembourg B65477 - TVA LU25482518

PricewaterhouseCoopers Assurance

A Luxembourg cooperative company (Société coopérative)
Registered Office: 2, rue Gerhard Mercator, L-2182 Luxembourg
Tel / Internet site: +352 494848 1 / www.pwc.lu

Authorised audit firm (Cabinet de révision agréé) and chartered accountant (Expert-comptable, with government authorisation No. 10181659)
R.C.S. Luxembourg B294273 - TVA LU36559370

PricewaterhouseCoopers Tax and Advisory

A Luxembourg cooperative company (Société coopérative)
Registered Office: 2, rue Gerhard Mercator, L-2182 Luxembourg
Tel / Internet site: +352 494848 1 / www.pwc.lu

Chartered accountant (Expert-comptable, with government authorisation No. 00123855)
R.C.S. Luxembourg B60245 - TVA LU36628247

PwC Regulated Solutions

A Luxembourg private limited liability company (Société à responsabilité limitée)
Registered Office: 2, rue Gerhard Mercator, L-2182 Luxembourg
Tel / Internet site: +352 494848 1 / www.pwc.lu/en/pwc-regulated-solutions.html

Specialised PFS (PSF spécialisé, with government authorisation No. 08/17)
Professional of the Insurance Sector (Professionnel du secteur des Assurances)
R.C.S. Luxembourg B47205 - TVA LU15947475

PricewaterhouseCoopers Training Administration Service Centre S.à r.l.

A Luxembourg private limited liability company (Société à responsabilité limitée)
Registered Office: 2, rue Gerhard Mercator, L-2182 Luxembourg
Tel / Internet site: +352 494848 1 / www.pwc.lu

Continuing vocational training organisation (Organisme de formation professionnelle continue, with government authorisation No. 00137787)
R.C.S. Luxembourg B118509

PricewaterhouseCoopers Academy S.à r.l.

A Luxembourg private limited liability company (Société à responsabilité limitée)
Registered Office: 2, rue Gerhard Mercator, L-2182 Luxembourg
Tel / Internet site: +352 494848 4040 / www.pwcacademy.lu

Continuing vocational training organisation (Organisme de formation professionnelle continue, with government authorisation No. 00123773)

2 Data Protection Officer

PwC Luxembourg has appointed a Data Protection Officer who can be contacted at the following address: lu-data-protection-office@pwc.lu.

The following address is available to facilitate the exercise of data subject rights under Articles 15 to 22 of the General Data Protection Regulation: www.pwc.lu/dataprotection-contact.