DATA PROTECTION POLICY

INTRODUCTION

This Policy sets out the obligations of COGNICERT LIMITED regarding data protection and the rights of customers and business contacts ("data subjects") in respect of their personal data under Data Protection Act 2018 (Formally EU Regulation 2016/679 General Data Protection Regulation ("GDPR")). The Data Protection Act 2018 defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Purpose

This Policy sets the Cognicert's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

ROLES AND RESPONSIBILITIES

Data Protection Officer

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the Data Protection Act 2018 and other applicable data protection legislation.

- The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
- The name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;
- The purposes for which the Company collects, holds, and processes personal data;
- Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- Details of how long personal data will be retained by the Company; and
- Detailed descriptions of all technical and organizational measures taken by the Company to ensure the security of personal data.

Accountability and Record-Keeping

- The Company's Data Protection Officer is Precious A.
- E-Mail: reachout@cognicert.com

Compliance Department

- Ensure that access to the personal data of Certification holders, Trainers, Examiners, Examinees, Invigilators and Auditors will not be shared with or provided to unauthorized parties
- Additional documents and data provided by applicants are being stored appropriately and centralized to ensure the confidentiality, integrity, availability of the data

Partnership Development Department

Ensure that access to COGNICERT Authorized Partners and Agents' personal data:

- Is restricted to authorized personnel only
- Will not be shared with or provided to unauthorized parties

System Administrator

Ensure that access to the personal data of members registered on the COGNICERT Website:

- Is restricted to authorized personnel only
- Will not be shared with or provided to unauthorized parties

DATA MANAGEMENT PROCESS

Data Protection Impact Assessments

- Cognicert shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data.
- Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
  1. The type(s) of personal data that will be collected, held, and processed;
  2. The purpose(s) for which personal data is to be used;
  3. The Company's objectives;
  4. How personal data is to be used;
  5. The parties (internal and/or external) who are to be consulted;
  6. The necessity and proportionality of the data processing with respect to the
  7. purpose(s) for which it is being processed;
  8. Risks posed to data subjects;
  9. Risks posed both within and to the Company; and
  10. Proposed measures to minimize and handle identified risks.

Personal Data Collected, Held, and Processed

- As part of our operations, we gather and process information or data that can make individuals or organization identifiable, including, but not limited to, full name, phone number, email address, qualification, experience and country. The personal data of Certification holders, Trainers, Examiners, Examinees, Invigilators and Auditors will not be shared with or provided to unauthorized parties

Secure Processing

- The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorized or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organizational measures which shall be taken are provided later in this Policy.

General Data Management Guidelines

Cognicert shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Data Protection Act 2018 and under this Policy, and shall be provided with a copy of this Policy;
- Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;
- The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Data Protection Act 2018 and this Policy by contract;
- All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Data Protection Act 2018;
- Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

- Personal data of stakeholders shall be restricted only to employees who need it to complete their job in line with their job responsibilities.

- Informally sharing data is prohibited. When access to confidential information is needed, employees shall request it from their immediate superior.
- All COGNICERT employees shall undergo comprehensive training to help them understand their responsibilities when handling personal data.
- Data in the process by employees shall be kept secure and stored following the data storage guidelines presented in the chapter below.
- In particular, account credentials and passwords shall be kept in encrypted storage with restricted access.
- Personal data shall not be disclosed or communicated to unauthorized people, either within the company or externally.
- When unsure about any aspect of data protection, employees shall request assistance from their immediate superior or the Data Protection Officer.

Data Storage

Data stored on paper shall be kept in secure storage limited to authorized personnel only. The guideline also applies to electronically stored data printed out for specific reasons.

- Hard copy files shall be kept in a locked drawer or filing cabinet.
- Employees with access to hard-copy files shall ensure confidentiality and maintain a clean desk policy.
- When no longer needed, printed files shall be securely shredded and disposed of.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts.

- Data shall be protected with strong passwords that are changed regularly and never shared between employees.
- Data shall not be stored on removable media (like a CD or DVD). If necessary for job purposes, removable media shall be kept locked and secure.
- Data shall only be stored on designated servers at COGNICERT premises and shall only be uploaded onto approved cloud computing services.
- The minimum requirements for encryption are AES 128 Bit. This is for data in transport or at rest, whether stored in premises or the cloud.
- Servers containing personal data shall be sited in a secure location where access is restricted to authorized personnel only. The site must be monitored and access-controlled.
- Data shall be backed up daily. Backups shall be tested regularly, in line with the company's standard backup procedures.
- Data shall never be saved directly to laptops or other mobile devices (e.g., tablets or smartphones).
- All servers and computers containing data shall be protected by approved security software and a firewall.
- All data entering COGNICERT systems and website are stored as unique and measures to prevent privilege escalation are taken.
- All data entering into the database of the COGNICERT website are protected with certificates that ensure encrypted communication when receiving and sending information.

Data Retention

- The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
- When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
- For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

Data Usage

- All data collected by COGNICERT are strictly for COGNICERT-related services. They are used to provide complete responses or services. No other non-COGNICERT related service will be offered from the data collected.
- When working with personal data, employees shall ensure their computer screens are always locked when left unattended.
- Data shall be encrypted before being transferred electronically.
- Employees shall not save copies of personal data to their computers. Always access and update the central copy of any data.

Data Accuracy and Action

To exercise data protection, COGNICERT takes reasonable steps and is committed to:

- Restrict and monitor access to sensitive data
- Establish effective data collection procedures
- Provide employees with online privacy and security training
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse
- Include contract clauses or communicate statements on how we handle data
- Update the data continuously
- Ensure that marketing databases are checked against industry suppression files
- Install tracking logs to monitor employees' activities ensuring data is not being misused
- Install firewall and protection software that prevents employees from sharing and distributing data from COGNICERT devices externally by means of detecting large amounts of data being transferred via email or external drives
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization, etc.)

DATA SUBJECT RIGHTS

The Rights of Data Subjects

- The Data Protection Act 2018 sets out the following rights applicable to data subjects
- The right to be informed'
- The right of access,
- The right to rectification,

- The right to erasure (also known as the 'right to be forgotten'),
- The right to restrict processing,
- The right to data portability,
- The right to object; and
- Rights with respect to automated decision-making and profiling.

Subject Access Requests

All individuals and organizations who are subject of personal and other data held by COGNICERT are entitled to:

- Ask what information COGNICERT holds about them and why
- Ask how to gain access to it
- Be informed on how to keep it up to date
- Be informed on how the company meets its data protection obligations

Our clients can request such information directly through a subject access request made via email at reachout@cognicert.com. We will always verify the identity of anyone making a subject access request before handing over any information. Confirmation will be asked from the data subject using the email data subject used to register an account at COGNICERT. The first copy of the requested data will be provided free of charge. Further requested copies are charged GBP50 USD. We aim to respond to the request within 14 days.

Data Modification

Our clients can request data modification or correction via email at reachout@cognicert.com . COGNICERT will verify the identity of anyone making a request before modifying or correcting any information.

Data Erasure

Our clients can request data erasure via email at reachout@cognicert.com. The data subject will be provided with all necessary information before erasure. Before proceeding with the erasure, the data subject will receive a statement from our Data Protection Officer explaining the outcome of the data being deleted. Erasure of data can be requested at any time.

Children

Our website is not intended for children or persons younger than 16. COGNICERT does not knowingly collect personally identifiable information (PII) of persons under the age of 16. We strive to comply with the provisions of the European Union General Data Protection Regulation (EU GDPR). If you are a parent or custodian of a child or person under 16 years old and you believe that they have provided us with information about themselves, please contact us at reachout@cognicert.com.

Disclosing Data

In certain circumstances, when required, COGNICERT can disclose data to law enforcement agencies without the consent of the data subject. However, the data controller will ensure the request is lawful, seeking assistance from the board and from the company's legal advisors, where necessary.

Data Security - Transferring Personal Data and Communications

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- All emails containing personal data must be encrypted using Encryption software;
- All emails containing personal data must be marked "confidential";
- Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted using deletion software;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail Registered or 1st or 2nd Class Signed For post; and
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

Transferring Personal Data to a Country Outside the EEA

Cognicert may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Data Protection Act 2018); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
- The transfer is made with the informed consent of the relevant data subject(s);

- The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
- The transfer is necessary for important public interest reasons;
- The transfer is necessary for the conduct of legal claims;
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Breach Notification

- All personal data breaches must be reported immediately to the Cognicert's Data Protection Officer at reachout@cognicert.com
- If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- Data breach notifications shall include the following information:
  - The categories and approximate number of data subjects concerned;
  - The categories and approximate number of personal data records concerned;
  - The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
  - The likely consequences of the breach;
  - Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

This policy has been approved & authorized by:

Signed: Managing Director

Date: 30th June, 2022

Review of Policy: Yearly