Procedure for Personal Data Protection

1.0 Purpose

To describe a procedure for ensuring that all processing of personal data carried out by Certi-Trust has the appropriate safeguards and complies with the applicable legislation (specifically with the General Data Protection Regulation).

2.0 Scope

This procedure covers the personal data protection all personal data handled, managed, processed or stored by Certi-Trust.

3.0 Responsibility

3.1 CEO is responsible for the communication of this procedure throughout all the organisation and ensuring that all employees of Certi-Trust process personal data according to this procedure.

3.2 Compliance Manager is responsible to ensure that this procedure complies with all applicable legislation, to update it when necessary (new processing of personal data, new purpose,…), to give attendance to the rights of data subjects, to promote trainings about personal data protection to all employees processing personal data and will be the point of contact with all data subjects.

4.0 Description of Activity

4.1 Purpose of the processing

4.1.1 Personal data of employees are processed to enable Certi-Trust to execute the employment agreement and comply with legal obligations. Within this context, Certi-Trust process personal data of its employees for the main following purposes:

- Recruitment and selection of staff and intermediaries. The administration of wages, commissions and salaries. The application of social legislation.
- Evaluation and monitoring of staff. Training and career planning.
- Planning and monitoring of tasks, workload and benefits.
- Maintain security of Certi-Trust assets.
- Protect employees from harassment conducts coming from other employees (team members or managers).

4.1.2 Personal data of clients and suppliers are processed to enable Certi-Trust to execute Certi-Trust agreements and comply with legal obligations. Within this context, Certi-Trust process clients and suppliers' data for the main following purposes:

- Client administration: order management, conducting audits, billing of services. The monitoring of solvency. Marketing and advertising (always of Certi-Trust own services and as long as such services are related to another services provided by Certi-Trust that a client has already acquired). The registration of the client on the database. Manage the examination and certification process for professionals following the requirements of ISO 17024.
- Suppliers' administration: Management of suppliers (also auditors), payment of suppliers. The prospection of potential suppliers and their evaluation.

4.1.3 Personal data of visitors to Certi-Trust website is processed to offer a better experience by using cookies and to be able to process any inquiry, complaint or question posted on the site. All information on how personal data are collected *via* Certi-Trust website can be found at: www.certi-trust.com

4.2 **Categories of personal data**

4.2.1 In order to fulfil the above-mentioned purposes Certi-Trust processes the following categories of personal data:

- Personal Identification Data: Name, Surname, address, telephone number
- Financial identification data: Account number, credit card
- CV: History of working life (for employees and external auditors).
- Salary: Payments, bonus; expenses, meal vouchers, retained taxes, labour union payments, payment methods,…
- Appraisal (Evaluation) / Psychological Data : Personal evaluation on how the employee is / feels on his/her position and exposition of possible problems
- Absence: Reason for the absence, measures envisaged
- Agenda: Actual responsibilities, projects, timesheet, agenda
- Electronic Data: such as IP address, cookies
- Examination: Exam, percentage of success, contact data for references, certificate number, expiration date, examination center.

4.3 **Categories of recipients**

4.3.1 Personal data processed by Certi-Trust as a controller (from employees, visitors, clients or suppliers) will only be disclosed to third parties such as public organizations when there exists a legal obligation for Certi-Trust to disclose it, to suppliers when it is necessary in order to receive the service provided and under a contract specifying the lawfulness of the processing done by the supplier and to clients when necessary to carry out some service provided by Certi-Trust. In particular:

- Relevant public bodies (such as CNS, Administration des Contributions Directes, CSSF);
- Certi-Trust providers: IT providers, accounting company, insurance broker, leasing company, meal vouchers issuer;
- Certi-Trust clients (to the extent necessary for the provision of services to Certi-Trust clients);

4.4 **Retention period**

4.4.1 All retention period can be seen in the procedure for Control of records (QP02), in the Master List of records.

4.5 **Security measures**

4.5.1 In order to protect all personal data processed and mitigate the risks for the rights and freedom of the data subjects which may result in the processing of their personal data, Certi-Trust will apply security measures (classified in legal, organizational and technical measures) to ensure integrity, confidentiality and availability of personal data

and to ensure the rights of the data subjects.

4.5.2 Such mechanisms include procedures to give attendance to all rights of the data subjects, procedures to comply with the fundamental principles of personal data protection (such as data minimisation, purpose limitation, lawfulness, transparency, storage limitation, ...), safe deletion procedure, logical and physical access controls, passwords policies, data breach notification, DPIA,... which are detailed in the documents “Information security policy” and DPIA:Methodology”.

4.6 **Data Breach Notification**

4.6.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

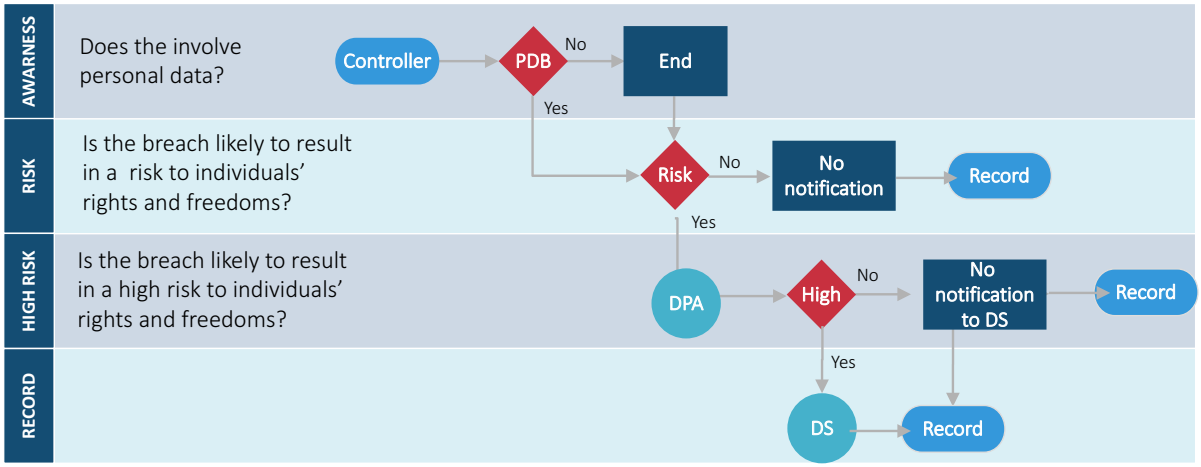
4.6.2 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

4.6.3 When a personal data breach has occurred, Certi-Trust will establish the likelihood and severity of the resulting risk to data subjects’ rights and freedoms. If it’s likely that there will be a risk then Certi-Trust will notify the CNPD. This notification to the CNPD will be done at the latest 72h after Certi-Trust becomes aware of the data breach.

4.6.4 If the data breach is likely to result in a high risk to data subjects’ rights and freedoms, Certi-Trust will notify all data subjects were feasible. Otherwise, Certi-Trust will do a public communication.

4.6.5 The communication will include at least:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if the organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.



Rights of the data subjects

4.7 **Lawfulness of processing**

4.7.1 The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever Certi-Trust process personal data:

- Consent: the individual has given clear consent for Certi-Trust to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract Certi-Trust have with the individual, or because they have asked Certi-Trust to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for Certi-Trust to comply with the law (not including contractual obligations).
- Legitimate interests: the processing is necessary for Certi-Trust legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

4.7.2 All processing of personal data done by Certi-Trust (as a controller) is well defined and all purposes set in accordance with the GDPR. (point 3.0 of this Procedure for personal data protection)

4.8 **Right of access**

4.8.1 According to Article 15 of the GDPR individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Under the GDPR, individuals will

have the right to obtain from Certi-Trust:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information (included in this privacy policy).

4.8.2 Certi-Trust must verify the identity of the person making the request, using 'reasonable means' before giving attendance to it.

4.8.3 If the request is made electronically, Certi-Trust should provide the information in a commonly used electronic format.

4.8.4 Once Certi-Trust has verified the identity of the individual making the request, will provide an answer within a time period of a month.

4.8.5 Certi-Trust can refuse to comply with a request for access if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

4.8.6 If Certi-Trust considers that a request is manifestly unfounded or excessive it can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

4.8.7 In either case Certi-Trust will justify its decision. Certi-Trust will base the reasonable fee on the administrative costs of complying with the request.

4.9 **Right of rectification**

4.9.1 Under Article 16 of the GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

4.9.2 Certi-Trust must verify the identity of the person making the request, using 'reasonable means' before giving attendance to it.

4.9.3 If the request is made electronically, Certi-Trust should provide the information in a commonly used electronic format.

4.9.4 Once Certi-Trust has verified the identity of the individual making the request, will provide an answer within a time period of a month.

4.9.5 Certi-Trust can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

4.9.6 If Certi-Trust considers that a request is manifestly unfounded or excessive it can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

4.9.7 In either case Certi-Trust will justify its decision.

4.9.8 Certi-Trust will base the reasonable fee on the administrative costs of complying with the request.

4.10 **Right of erasure ("to be forgotten")**

4.10.1 Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

4.10.2 Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which Certi-Trust originally collected or processed it for;
- Certi-Trust is relying on consent as its lawful basis for processing the data, and the data subject withdraws their consent;
- Certi-Trust is relying on legitimate interests as its basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- Certi-Trust is processing the personal data for direct marketing purposes and the individual objects to that processing;
- Certi-Trust has processed the personal data unlawfully;
- Certi-Trust has to do it to comply with a legal obligation; or
- Certi-Trust has processed the personal data to offer information society services to a child.

4.10.3 Once Certi-Trust has verified the identity of the individual making the request, will provide an answer within a time period of a month.

4.10.4 Certi-Trust can refuse to comply with a request for erasure if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

4.10.5 If Certi-Trust considers that a request is manifestly unfounded or excessive it can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

4.10.6 In either case Certi-Trust will justify its decision.

4.10.7 Certi-Trust will base the reasonable fee on the administrative costs of complying with the request.

4.11 **Right to restrict processing**

4.11.1 Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

4.11.2 Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information Certi-Trust holds or how Certi-Trust has processed their data.

4.11.3 In brief, the right to restrict processing implies that when applied, Certi-Trust will only keep the personal data (store it) without doing any further processing until the right to

restrict processing is completed.

4.11.4 Individuals have the right to request Certi-Trust restrict the processing of their personal data in the following circumstances:

- the individual contests the accuracy of their personal data and Certi-Trust is verifying the accuracy of the data;
- the data has been unlawfully processed and the individual opposes erasure and requests restriction instead;
- Certi-Trust no longer needs the personal data but the individual needs Certi-Trust to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to Certi-Trust processing their data under Article 21(1), and Certi-Trust is considering whether its legitimate grounds override those of the individual.

4.11.5 Once Certi-Trust has verified the identity of the individual making the request, will provide an answer within a time period of a month.

4.11.6 Certi-Trust can refuse to comply with a request for rectification if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

4.11.7 If Certi-Trust considers that a request is manifestly unfounded or excessive it can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

4.11.8 In either case Certi-Trust will justify its decision.

4.11.9 Certi-Trust will base the reasonable fee on the administrative costs of complying with the request.

4.12 **Right to data portability**

4.12.1 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

4.12.2 The right to data portability only applies to personal data an individual has provided to a controller (Certi-Trust); where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means.

4.12.3 The information must be provided free of charge. Certi-Trust will respond without undue delay, and within one month.

4.12.4 This time period could be extended by two months where the request is complex or Certi-Trust receives a high number of requests. In such cases, Certi-Trust will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

4.13 **Right to object**

4.13.1 Individuals have the right to object to processing based on legitimate interests or the

performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics.

4.14 **Complaints handling**

4.14.1 Certi-Trust will do its best to comply with the GDPR, not only as a legal obligation, but also because we do truly believe in Privacy as a fundamental principle that everyone should follow.

4.14.2 However, in case there is an infringement of the regulation (GDPR) or anyone thinks that personal data is not being processed according to expectations, anybody have the right to lodge a complaint to the Data Protection Authority of its country.

4.15 **Consent**

4.15.1 Whenever the legal basis of the processing is based on the consent provided by the data subject, Certi-Trust will make sure that the consent request is prominent, concise, separate from other terms and conditions, and easy to understand.

4.15.2 Certi-Trust will ask individuals to actively opt in.

4.15.3 Certi-Trust will keep records to evidence consent – who consented, when, how, and what they were told.

4.15.4 Individuals have the right to withdraw its consent at any time. To do so they can request the withdrawal of the consent at:

- e-mail: info.services@certi-trust.com
- phone number: +352 (0)20 30 10 44
- Address: 12, Avenue de la Porte Neuve, L-2227 Luxembourg

5.0 **References**

5.1 QP02 Procedure for Control of records

6.0 Enclosures None

7.0 Forms / Exhibits

None