HACA PARTNERS

Audit & Governance

Certification Procedure

1. General

HACA Partners ("HACA PARTNERS") offers third party GDPR certification services ("Services") enabling prospective and existing Clients to demonstrate GDPR conformity to business partners, customers and end-users.

2. Certification Services

The GDPR certification services provided by HACA PARTNERS are carried out in accordance with the policies and procedures established by HACA PARTNERS based on the requirements of the accreditation standards.

HACA PARTNERS complies with the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) Version 3.0 4 June 2019.

This certification agreement does not reduce the responsibility of the applicant for compliance with Regulation 2016/679/EC and is without prejudice to the tasks and powers of the supervisory authorities which is competent as per Article 42(5).

3. General requirements

3.1. Non-discriminatory conditions

The service is provided on a non-discriminatory basis without pre-qualification of clients. Exceptions to this include but are not-limited to repeated or extended delays in payment or non-payment of fees, unreasonable or repeated delays in the supply of samples or certification information, any form of abuse or attempted bribery towards Company staff or its other clients, misuse of Certificates, logos and marks, failure to respond to requests for compliance, client participating in illegal activities, having a history of repeated non-compliances with certification requirements, or similar client-related issues.

HACA Partners confines its requirements, evaluation, review, decision and surveillance (if any) to those matters specifically related to the scope of certification.

3.2. Publicly available information

HACA Partners will maintain and make available upon request information about and reference to the CNPD website containing information regarding the certification mechanism, including evaluation procedures, rules and procedures for granting, for maintaining, for extending or reducing the scope of, for suspending, for withdrawing or for refusing the certification.

3.3. Rights and Duties of Clients

The Client agrees to comply with any conditions set by HACA PARTNERS for the entire certification process, the evaluation, the issue of a Certificate and recognises that HACA PARTNERS has clear and

explicit rights to revise the requirements of certification within the period of validity of the certificate.

The client will provide HACA PARTNERS with all information and access to its processing activities which are necessary to conduct the certification procedure pursuant to Article 42(6);

The Client will ensure full transparency to the CNPD and competent supervisory authority with respect to the certification procedure including contractually confidential matters related to data protection compliance pursuant to Articles 42(7) and 58(1)(c)

The Client consents to HACA PARTNERS using outsourced resources in the delivery of its obligations appertaining to this Contract.

The client will comply with applicable deadlines and procedures resulting from the certification programme or other regulations.

The Client shall ensure that its System complies with the current versions of the rules, regulations, and standard(s) against which it is certified. Current versions of the rules, regulations, and Standards can be obtained from the CNPD, or from HACA PARTNERS or from the Standards issuing authority.

The Client agrees to undergo regular surveillance and audit as determined by HACA PARTNERS and must provide HACA PARTNERS with reasonable cooperation and assistance, and allow HACA PARTNERS access to all premises, documentation, information, personnel and sub-contractors deemed necessary by HACA PARTNERS to verify the maintenance of the System.

The Client agrees that:
- CNPD and/or HACA PARTNERS have the right to undertake unannounced or short notice surveillance evaluations and/or audits with the participation of observers, if applicable.
- CNPD and/or HACA PARTNERS equally have the right to undertake unannounced or short notice audits for the investigation of complaints.
- CNPD and/or HACA PARTNERS have the right to implement higher surveillance frequencies based on a risk assessment of the Client's Certificate scope, System, and location.
- Additional surveillance visits, as deemed necessary by CNPD, will be charged at HACA PARTNERS's rates current at the time of supply of such services.
- surveillance might be carried out with the participation of observers (e.g. data protection supervisory authority representative).

The Client recognises that:
- Initial Certification will only be granted once all non-compliances are corrected.
- Ongoing certification is reliant on continued compliance with the Standards rules and regulations which may change from time to time, including the requirement to address any nonconformances to the satisfaction of HACA PARTNERS in the specified time periods.

The Client shall inform HACA PARTNERS promptly of any significant changes to its product(s), services, resources, management, System or any other circumstances, which may materially impact on the continued validity of its certification, for example but without limitation: change of site, additional sites, change of process, change of ownership, or change of scope. In such circumstances, the Client shall agree to the payment of any applicable additional fees and expenses deemed necessary for HACA PARTNERS to assess the impact and maintain confidence in the System.

In the case where the abovementioned circumstances or any other situations may involve the issuance of a new Certificate, the Client shall agree to return the original copy of the previous Certificate to HACA PARTNERS. However, the Client may retain a photocopy of the Certificate for record purposes.

The Client shall allow the CNPD access to any part of the audit or surveillance process for the purposes of witnessing HACA PARTNERS's audit team performing the audit of the System to determine conformity with the requirements of the Standard. This will include the right of access to confidential information. The Client will not have the right within this Contract to refuse such a request either by the CNPD or HACA PARTNERS.

The Client agrees that information relating to its certification and scope of certification can be made publicly available by HACA PARTNERS and the Accreditation Body(ies).

If the Client provides copies of the certification documents to others, the documents shall be reproduced in their entirety or as specified in the certification scheme.

The Client shall declare to HACA PARTNERS any activity that may create a conflict of interest in relation to its Certified System.

3.4. Services Fees

Services Fees are quoted (and amended from time to time) for services agreed to be supplied pursuant to the Contract ("Services Fees") on the assumption that the information supplied by the Client is accurate and complete.

Services Fees include the cost of audit services and the use of the HACA PARTNERS logo and, where agreed, the Accreditation Body(ies) logo.

Expenses and disbursements may be charged separately in accordance with the quoted terms.

Any service required or supplied additional to the agreed services will be charged at HACA PARTNERS's rates current at the time of supply of such services.

Services Fees may be reviewed and amended from time to time, normally but not exclusively on an annual basis.

Payment is due as per the stated terms on the invoice. Payment shall be made in full, without set off or deduction.

All fees and expenses quoted are exclusive of all taxes including but not limited to value added or sales tax, which will be charged at the current rate of the Country in which the services are supplied.

3.5. Impartiality

To mitigate or eliminate any appearance of any conflicts of interest HACA Partners requires all audit staff and potential clients to declare any potential or real conflicts of interest. This declaration of conflicts is ensured through HACA Charter of conduct, objectivity & independence (Appendix 6 : Charte de conduite en matière d'objectivité et d'indépendance), HACA Procedure for the acceptance and continuance of missions (Appendix 20), Appointment Letter signed by all internal or external professional involved in the Certification (Appendix 22) as well as the GDPR Certification Agreement (Appendix 2) signed with all clients. HACA Partners decisions are based on objective evidence of conformity (or non-conformity) and its decisions are not influenced by other interests including financial returns or by other parties.

HACA Partners shall not provide certification services to a client if HACA Partners is

- the designer, implementer, operator or maintainer of the certified process;
- providing consulting services that impact the processing activity(ies) to be certified;
- offering or providing management system consultancy or internal audit services;
- a processor and / or joint controller for the organization to be certified
- involved in external DPO activities for the organization to be certified

Within a period of 2 years, HACA Partners personnel shall not be used to review or make a certification decision for a processing activity for which they have provided consultancy.

Should HACA Partners be in breach of this impartiality obligation, any person could take independent action and inform the CNPD accordingly in the respect of article 13 Confidentiality.

If the top management of the certification body does not follow the input of this impartiality mechanism, the mechanism shall have the right to take independent action (e.g. informing the CNPD, stakeholders). In taking appropriate action, the confidentiality requirements relating to the client and certification body shall be respected.

4. Obligations of HACA PARTNERS

4.1. Management of competence for personnel involved in the certification process

HACA PARTNERS will provide an appropriately qualified, competent and impartial audit team or individual Auditor to conduct audits and assessments of the Client's System in accordance with CNPD rules and procedures and HACA PARTNERS's management system requirements. HACA PARTNERS will use external experts for the evaluation activities for specific areas where it lacks relevant competencies internally, specifically lawyers and IT experts. HACA PARTNERS will ensure those external partners comply with the requirements of the certification mechanism as well as with relevant laws and regulations. This compliance is ensured by the signing of a cooperation agreement (Appendix 21 : Accord de Cooperation).

The audit team will have GDPR expertise which will be maintained through appropriate training and will be educated on the certification process.

Those training will be provided through a combination of online and traditional classroom training or on-the-job training, to provide professionals with the opportunity to strengthen their technical and professional skills, including professional judgment and critical thinking.

All new members of the GDPR Evaluation Team will receive a GDPR training (essentials) and a specific training on the GDPR Certification Mechanism.

Skills acquired during the training sessions will be formally validated.

In addition to attending GDPR online and traditional classroom training, members of the GDPR Evaluation Team will meet on a regular basis (at least twice a year) for a lunch & learn session to discuss on-going certification and specific issues arising.

4.2. Conflict of interest, confidentiality and procedure observation

All members of HACA Partners as well as external experts are required to (i) declare any conflict of interest prior to an audit or as soon as they become aware of a threat to the impartiality of the audit, (ii) protect the Confidential Information that will be disclosed during the GDPR Certification mission, (iii) strictly observe this procedure (Appendix 22 - Appointment Letter).

4.3 Changes affecting certification

When a certain standard is revised or certain requirements are established by a governing body or authority (changes affecting certification include among others: amendments to data protection legislation, the adoption of delegated acts of the European Commission in accordance with 43(8) and 43(9), decisions of the European Data Protection Board and court decisions related to data protection), HACA PARTNERS will disseminate the information of the changes to certified clients via the distribution of letters and statements.

4.4. Impartiality

HACA PARTNERS is responsible for the impartiality of its conformity assessment activities and shall not allow commercial, financial, or other pressures to compromise impartiality. HACA PARTNERS will be impartial in carrying out its management system certification activities and will manage any conflict of interest that may arise through periodic evaluation and analysis.

5. Scope of certification

5.1. What can be certified

- The personal data processing of Controllers and Processors;
- A data protection governance program from a controller or processor linked with the personal data processing;
- Potentially services (several processing).

5.2. Limitations

- This certification mechanism does not certify the security technical measures implemented for the processing in scope; only governance criteria around data protection security principles are included in the scheme (risk analysis, risk treatment, audit of design and

implementation);

- This scheme is only applicable only to controllers and processors established in Luxembourg, under the supervision of the CNPD - the scheme can't be used yet to certify international transfers;
- The scheme shall not be used for
    - certifying personal data processing specifically targeting minors under 16 years old;
    - certifying processing activities in the context of a joint controllership;
    - certifying processing activities in the context of article 10 GDPR - Processing of personal data relating to criminal convictions and offences or related security measures -, except those that are clearly defined and regulated by Luxembourgish or European Laws and for which the CNPD is the competent supervisory authority
    - entities that have not officially designated a DPO (article 37 GDPR). It should be noted that entities are free to officially designate a DPO regardless of whether they are required by the GDPR to do so or not.

6. Application

When applying for a GDPR audit, a client must provide HACA PARTNERS with detailed information about:

- General information of the client, including its name and the address(es), significant aspects of its process and operations, and any relevant legal obligations;
- The scope and the object of the certification including interfaces and transfers to other systems and organizations protocols and other assurances;
- The list of processors used including a description of tasks, and the relevant controller/processor contract(s) / contractual templates.

On receiving a completed Application Form/Request for Quotation, HACA PARTNERS will review the information provided (a) to confirm the information received is sufficient to conduct the GDPR certification, (b) to resolve any difference in understanding, (c) to validate the scope of certification which implies an analysis to determine which services, business units, functional areas, and applications are material to the client's internal control over data protection, (d) to confirm the availability of competence and resources to conduct the certification.

HACA PARTNERS then prepares a quotation detailing audit cost which will be forwarded to the Client together with the GDPR Certification Agreement. The client agrees to accept these specific and general terms and conditions by signing and returning the quotation document and GDPR Certification Agreement.

On receipt of the signed acceptance of the quote, HACA PARTNERS will issue an invoice to the Client who in turn will make payment to HACA PARTNERS. The audit will then be planned and carried out in accordance with HACA PARTNERS accredited management system processes.

If it is discovered after the engagement has been accepted, that one or more preconditions (as set out by this certification mechanism as well as the International Standard on Assurance Engagements ISAE 3000) for an assurance engagement is not present, the Auditor will discuss the matter with the appropriate party(ies), and will determine (a) whether the matter can be resolved to the Auditor's satisfaction, (b) whether it is appropriate to continue with the engagement; (c) how to address the matter on the assurance report and escalate the issue to the CNPD.

If it is discovered after the engagement has been accepted, that the mission should have been declined, HACA PARTNERS will discuss the matter with the appropriate party(ies) and take the necessary actions.

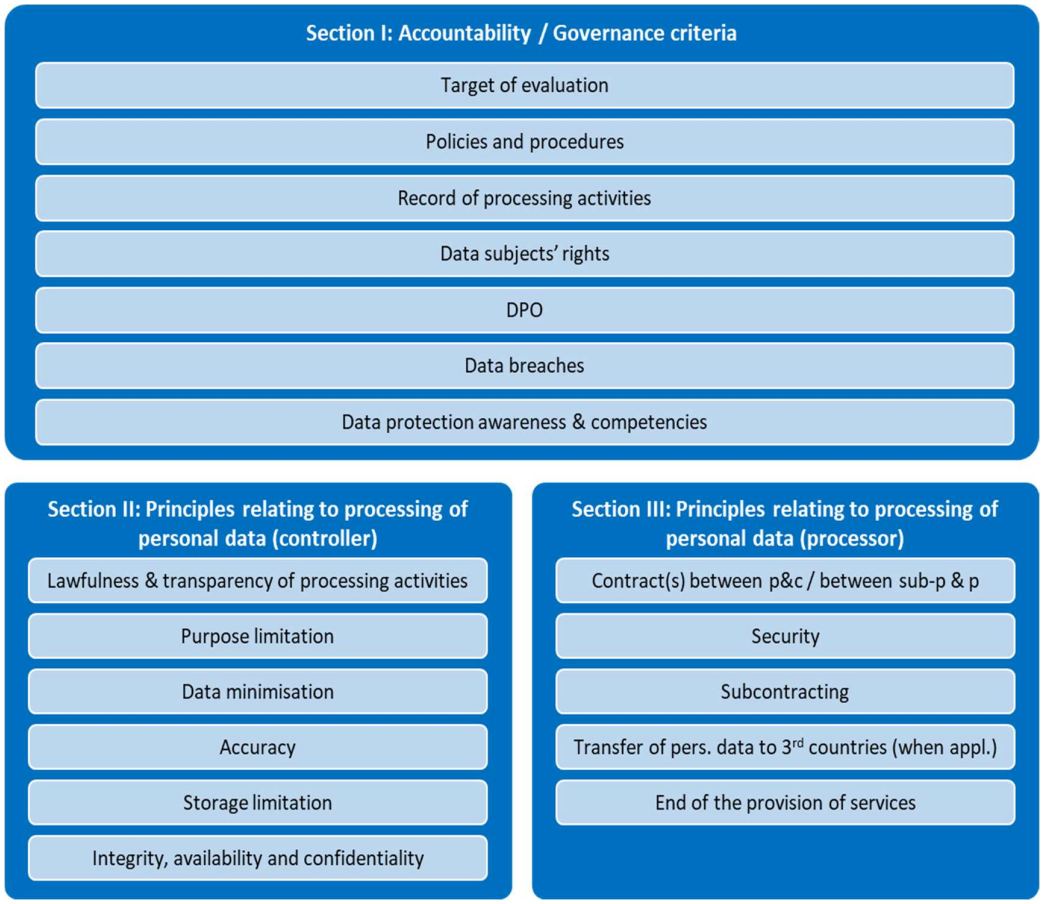
Changes to the scope following acceptance of the quotation could result in amendment to the fees.

7. Evaluation

7.1. Evaluation Criteria

The certification criteria are those defined by the CNPD in the GDPR-CERTIFIED ASSURANCE REPORT BASED PROCESSING ACTIVITIES CERTIFICATION CRITERIA, hereafter GDPR-CARPA certification.

The criteria are organized in 3 sections.



- Section I: Accountability / Governance criteria

This section contains the criteria relevant to how an entity manages personal data protection concerns from a governance point of view to ensure its management can assume accountability. Those criteria apply to both entities acting as controllers and processors.

- Section II: Principles relating to processing of personal data (controller)

This section contains the criteria relevant to how an entity manages personal data protection requirements for a given processing activity in scope, where it acts as controller. This section is composed of sub-sections, which respectively relate to the principles of processing of personal data as defined under GDPR, and complemented by additional relevant elements, namely:

- Subsection II-a: Lawfulness, fairness and transparency
- Subsection II-b: Purpose limitation
- Subsection II-c: Data minimization
- Subsection II-d: Accuracy
- Subsection II-e: Storage limitation
- Subsection II-f: Integrity and confidentiality - Security
- Subsection II-g: Privacy by design and by default

- Section III: Principles relating to processing of personal data (processor)

This section contains the criteria relevant to how an entity manages personal data protection requirements for a given data processing activity in scope, where it acts as data processor.

7.2. Evaluation Process

7.2.1. Planning the evaluation

HACA PARTNERS will respect the requirements set out in the International Standard on Assurance Engagements ISAE 3000 (Assurance Engagements Other than Audits or Reviews of Historical Financial Information) issued by the International Auditing and Assurance Standards Board (IAASB) as well as the International Standard on Quality Control 1 (Quality Control for Firms that Perform Audits and Reviews of Financial Statement, and Other Assurance and Related Services Engagements).

HACA PARTNERS will have a plan for the evaluation activities to allow for the necessary arrangements to be managed.

The Auditor shall plan the engagement so that it will be performed in an effective manner, including setting the scope, timing and direction of the engagement, and determining the nature, timing and extent of planned procedures that are required to be carried out in order to achieve the objective of the Auditor.

HACA PARTNERS involves at least one individual with legal or regulatory competencies and one individual with IT technical competencies in the attestation engagement.

7.2.2. Conducting the evaluation

The first stage of the evaluation requires the Auditor to conduct an on-site readiness review of the Client's management system to assess the documentation and if the implementation of the management system is at a level sufficient to progress to the Stage two evaluation. When satisfied with the compliance of the documentation and system readiness the Auditor will agree a date with the Client for the Stage 2 audit. The Stage 2 audit will then be conducted in accordance with HACA PARTNERS management system processes. The purpose of the Stage 2 audit is to evaluate the implementation, including effectiveness, of the client's management system. The audit will be carried out against agreed evaluation criteria.

The Auditor will ensure all necessary information and/or documentation is made available by the Client for performing the evaluation tasks.

If one or more of the requested written representations are not provided or the Auditor concludes that there is sufficient doubt about the competence, integrity, ethical values, or diligence of those providing the written representations, or that the written representations are otherwise not reliable, the Auditor will (a) discuss the matter with the appropriate party(ies), (b) evaluate the effect that this

may have on the reliability of representations (oral or written) and evidence in general (c) determine how to address the matter on the report and escalate the issue to the CNPD.

The Auditor will evaluate the sufficiency and appropriateness of the evidence obtained in the context of the engagement, will form a conclusion about whether the information is free of material misstatement and, if necessary, attempt to obtain further evidence. The Auditor will consider all relevant evidence, regardless of whether it appears to corroborate or to contradict the measurement or evaluation of the underlying subject matter against the applicable criteria.

If the Auditor is unable to obtain sufficient appropriate evidence, a scope limitation exists and the Auditor will express a qualified conclusion, disclaim a conclusion, or withdraw from the engagement, where withdrawal is possible under applicable law or regulation, as appropriate.

7.2.2. Results of the evaluation

At the end of the evaluation, HACA PARTNERS will inform the client of all nonconformities through a non-conformity report listing all nonconformities, if any.

The results of the evaluation activities will be documented and will be made available to the CNPD upon request.

The Auditor will prepare an engagement documentation that provides a basis for the assurance report that is sufficient and appropriate to enable an experienced Auditor, having no previous connection with the engagement, to understand

a) The nature, timing and extent of the procedures performed to comply with relevant ISAEs and applicable legal and regulatory requirements;
b) The results of the procedures performed, and the evidence obtained; and
c) Significant matters arising during the engagement, the conclusions reached thereon, and significant professional judgments made in reaching those conclusions.

The Auditor will assemble the engagement documentation in an engagement file before the date of the assurance report.

The signed ISAE 3000 type 2 assurance report is the result of the evaluation phase.

The assurance report will state the period of time to which the measurement or evaluation of the underlying subject matter relates and the scope limitation, meaning the areas which are not in scope of the engagement. This scope limitation will be specific, detailed at process level and clearly understandable by a third person.

Audit methodology will include interviews, observation of activities, electronic and hard copy document and record review. Conclusions will be based on the evidence obtained during the audit. The Auditor(s) will use sampling techniques to obtain the evidence and no guarantee can be given that a different conclusion may have been reached previously or if a different sample had been taken.

7.2.3. Review

On completion of the evaluation, the Auditor will submit the report with a recommendation for either granting or refusing registration for review to at least one qualified person. This person reviews all information and results related to the evaluation. The review will be carried out by person(s) who have not been involved in the evaluation process, according to the requirements set

out in the International Standard on Quality Control 1 (Quality Control for Firms that Perform Audits and Reviews of Financial Statement, and Other Assurance and Related Services Engagements).

7.2.4. Certification Decision

Following the review of the report, a committee within HACA PARTNERS consisting of the *Réviseur agréé* not involved in the evaluation process will make the certification decision and authorise the issue of the certificate. The certification decision will be based on the documentation of all certification activities including the engagement quality review and will be duly documented.

Any non-conformities raised during an audit must be corrected and closed prior to a certification decision being made. The Client agrees to meet the extra visit or documentation review costs involved in closing out the non-conformities.

HACA PARTNERS will notify the client of a decision not to grant certification and will identify the reasons for the decision.

8. Management System Requirements

8.1. Review & Control

HACA PARTNERS will review its management system on a yearly basis in order to ensure its continuing suitability, adequacy and effectiveness, including the stated policies and objectives related to the fulfilment of this certification mechanism.

This review will include inspection of at least one completed engagement for each engagement partner and require that those performing the engagement or the engagement quality control review are not involved in inspecting the engagements in accordance with Manuel Assurance Qualité – 8. Revue de contrôle qualité d'une mission.

This review shall be conducted at least once a year and an agenda for such a Management Review meeting has been established listing the inputs and outputs (action plan) from the Management Review (Appendix 24 - Management Review Agenda).

8.2. Internal Audit

HACA PARTNERS has established an Internal Audit Strategic Plan (Appendix 27 – Internal Audit Strategic Plan) to verify that it fulfils the requirements of this certification mechanism and that the management system is effectively implemented and maintained. This Internal Audit Strategic Plan takes into consideration the importance of the processes and areas to be audited, as well as the results of previous audits.

These Internal audits will be performed at least once every 12 months, or completed within a 12-month time frame for segmented (or rolling) internal audits. A documented decision-making process will be followed to change (reduce or restore) the frequency of internal audits or the time frame in which internal audits shall be completed. Such changes will be based on the relative stability and ongoing effectiveness of the management system. Records of decisions to change the frequency of internal audits, or the time frame in which they will be completed, including the rationale for the change, will be maintained.

HACA PARTNERS ensures that:

a) internal audits are conducted by personnel knowledgeable in certification, auditing and the requirements of this certification mechanism;
b) auditors do not audit their own work;
c) personnel responsible for the area audited are informed of the outcome of the audit;
d) any actions resulting from internal audits are taken in a timely and appropriate manner;
e) any opportunities for improvement are identified.

8.3. Corrective actions

Following complaints, as a result of the internal audit or as a result of a regulatory update, HACA PARTNERS will identify and manage nonconformities in its operations. For each nonconformity, HACA PARTNERS will evaluate the effect of deficiencies and determine whether they are either:
a) Instances that do not necessarily indicate that its system of quality control is insufficient to provide it with reasonable assurance that it complies with professional standards and applicable legal and regulatory requirements, and that the reports as well as certificates issued by the certification body or engagement partners are appropriate in the circumstances; or
b) Systemic, repetitive or other significant deficiencies that require prompt corrective action.

HACA PARTNERS will issue a "Corrective Actions Report" for the identification and management of nonconformities in its operations. This Report will be covering the following:
a) identification of nonconformities (e.g. from complaints and internal audits);
b) determination of the causes of nonconformity;
c) correction of nonconformities;
d) evaluation of the need for actions to ensure that nonconformities do not recur;
e) determination and implementation of the actions needed in a timely manner;
f) record of the results of actions taken;
g) review of the effectiveness of corrective actions.

HACA PARTNERS will take actions to eliminate the causes of nonconformities in order to prevent recurrence. Those corrective actions could include one or more of the following:
a) Taking appropriate remedial action in relation to an individual engagement or member of personnel;
b) The communication of the findings to those responsible for training and professional development;
c) Changes to the quality control policies and procedures; and
d) Disciplinary action against those who fail to comply with the policies and procedures of the certification body, especially those who do so repeatedly.

For cases where the results of the monitoring procedures indicate that a report may be inappropriate or that procedures were omitted during the performance of the engagement, HACA PARTNERS will determine what further action is appropriate to comply with relevant professional standards and applicable legal and regulatory requirements and consider whether to obtain legal advice.

8.4. Preventive actions

HACA PARTNERS will take preventive actions to eliminate the causes of potential nonconformities.

Preventive actions taken will be appropriate to the probable impact of the potential problems.

HACA PARTNERS will issue a "Preventive Actions Report" to eliminate the causes of potential nonconformities. This Report will be covering the following:

a) identification of potential nonconformities and their causes;
b) evaluation of the need for action to prevent the occurrence of nonconformities;
c) determination and implementation of the action needed;
d) record of the results of actions taken;
e) review of the effectiveness of the preventive actions taken.

9. Certification Marks

9.1. Certificate

Following the decision to grant certification, HACA PARTNERS will provide the client a formal certificate created according to the GDPR-CARPA template provided by the CNPD with the unique certification ID provided by the CNPD. This certificate will state (a) the name and address of the client, (b) the name and address of HACA PARTNERS, (c) the date the certification is granted, (d) the scope of the certification, (e) the period of validity, (f) the data protection mark or seal, (g) a unique certification ID, as well as any revision ID, if applicable (indicated by "R" followed by the revision date), (h) the signature of a Partner of HACA PARTNERS. The Partner will be among the approved independent auditor within HACA PARTNERS.

When a certificate is renewed after its initial validity period, a new certification ID provided by the supervisory authority will be issued.

Certificates will not be issued unless certification requirements have been fulfilled, the decision to grant or extend the scope of certification has been made, the certification agreement has been signed and payment in full has been received. The certificate is valid for three years, providing the client maintains the management system to the required standard.

HACA PARTNERS will create the certificate according to the GDPR-CARPA template provided by the CNPD.

9.2. Rules for Certification Marks

9.2.1 HACA PARTNERS will award a licence to the Client to use the certification mark(s) and logo(s) for the duration of the Certificate when used in accordance with the applicable Terms of Use set by the CNPD.

9.2.2. The use and display of certification logos and/or marks indicating a processing activity is certified shall be done in compliance with the requirements of HACA PARTNERS or as specified by the certification mechanism.

9.2.3. When providing copies of the certification documents, the client shall reproduce those documents in their entirety.

9.2.4. HACA PARTNERS will audit the use and display of certification logos and/or marks indicating a processing activity is certified.

9.2.5. The certificates, seals and marks shall be used in a clear and transparent manner preventing any confusion or misleading communication about the scope of the certified processing activities. Incorrect references to the certification mechanism, or misleading use of certificates, seals or marks, or any other mechanism for indicating a processing activity is certified, found in documentation or other publicity, will be dealt with by suitable action:

- Taking any action to stop the misleading / wrong communication and thus removing the visibility of the data protection certificate, mark and seal;
- Informing the public about the misuse;
- Immediately informing the Data Protection Supervisory Authority about the misuse;
- Suspension of the authorization to use the data protection certificate, mark and seal for the process in question.

The type of corrective action to be taken will be influenced by the nature of the misuse and its subsequent consequences.

9.2.6. The notification to the misuser will be confirmed in writing with a copy sent to the CNPD. This notification contains:

- the reason(s) for corrective action,
- the action(s) to be taken by the misuser to resolve the issue, and
- a request for a statement from the misuser formalizing his engagement to perform the action(s) to be taken to ensure that the data protection certificate, mark or seal is not applied to any ineligible processes.

9.2.7. When the data protection certificate, mark and seal has not been used in compliance with the contract, legal proceedings might result in a court of law deciding what the corrective action will be.

9.2.8. The client keeps a record of all complaints made known to it relating to compliance with certification requirements and makes these records available to the certification body when requested, and (i) takes appropriate action with respect to such complaints and any deficiencies found in processing activities that affect compliance with the requirements for certification; and (ii) documents the actions taken.

9.3. Directory of certified processing activities

HACA PARTNERS will maintain available a directory of certified processing activities indicating for each certificate granted (a) the certification ID, (b) the identity of the client, (c) the scope of the certification, (d) the period of validity, (e) any changes on the certification granted.

HACA PARTNERS will provide to the public upon request an executive summary of the evaluation report containing at minimum:

a) the scope of the certification and a meaningful description of the object of certification;
b) the respective certification criteria (including version or functional status); and
c) the result(s).

The aim of this executive summary is to help with transparency around what has been certified and how it was assessed.

Pursuant to Article 43(5) GDPR, HACA PARTNERS will inform the CNPD of the reasons for granting or revoking the requested certification.

9.4. Suspension, Reduction or Withdrawal of Certification

HACA PARTNERS is entitled to continue certification upon specific conditions, suspend, reduce the scope, withdraw the Client's certification on a 7 days' written notice (or with immediate effect in the case of urgent need) and reserves the right to make public the fact that such action has been taken when, in the reasonable opinion of HACA PARTNERS: i) the Client's management system has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the management systems, ii) the Client does not allow Surveillance or Recertification audits to be conducted at the required frequencies, iii) the Client has voluntarily requested suspension of its certification, iv) the Client fails to take corrective actions for nonconformity(ies) raised within the specified timeframe, v) the Client has incorrectly made references to its certification status or misleading use of certificate, marks, or audit reports, vi) the Client infringed the requirements of the certification contract. vii) The Client has been involved in serious incident related to occupational health and safety, for example serious accident or serious breach of regulation.

HACA PARTNERS will inform the CNPD in writing without undue delay about measures taken in case of substantiated nonconformities with certification requirements.

In the event of HACA PARTNERS's withdrawal from accreditation or inability to continue to supply GDPR certification HACA PARTNERS will notify the Client within thirty (30) days of such withdrawal.

Upon the suspension, withdrawal or termination of certification, the Client shall immediately cease to use the granted GDPR Certificate and to make any claims or advertising that that contains any reference to the GDPR Certificate or imply that they comply with the requirements for certification.

The Client shall advise all relevant existing customers of the suspension or withdrawal in writing within seven (7) working days (or other period as determined by HACA PARTNERS) of the withdrawal or suspension taking effect, and maintain records of that advice.
The Client shall, as requested by HACA PARTNERS, either destroy all electronic and hardcopy Certificates relating to the certification and at its own expense remove all claims, service mark(s), trademark(s), other names or logos and copyright works from products, documents, advertising and marketing materials with immediate effect or return all such certification to HACA PARTNERS. The Client shall also cooperate with HACA PARTNERS and the CNPD to confirm that these obligations have been met and shall, if requested, confirm in writing the destruction or return of all such references or certificates by one of its directors.

If certification is terminated (by request of the client), suspended or withdrawn, HACA PARTNERS will make all necessary modifications to formal certification documents, public information, authorizations for use of marks, etc., in order to ensure it provides no indication that the processing activity continues to be certified.

If a scope of certification is reduced, HACA PARTNERS will make all necessary modifications to formal certification documents, public information, authorizations for use of marks, etc., in order to ensure the reduced scope of certification is clearly communicated to the client and clearly specified in certification documentation and public information.

If a certification is suspended, HACA PARTNERS will communicate to the client the actions needed to end suspension and restore certification for the processing activity(ies).

Where it considers it appropriate, HACA PARTNERS may inform the Client of its intention to suspend or withdraw certification and to allow the Client a reasonable opportunity to take corrective actions, within such timescales as HACA PARTNERS may reasonably specify, before the suspension or withdrawal takes effect.

If certification is reinstated after suspension, HACA PARTNERS will make all necessary modifications to formal certification documents, public information, authorizations for use of marks, etc., in order to ensure all appropriate indications exist that the processing activity continues to be certified.

If a decision to reduce the scope of certification is made as a condition of reinstatement, HACA PARTNERS will make all necessary modifications to formal certification documents, public information, authorizations for use of marks, etc., in order to ensure the reduced scope of certification is clearly communicated to the client and clearly specified in certification documentation and public information.

9.5. Termination of certification

Upon termination of certification, the client discontinues its use of all advertising matter that contains any reference thereto and takes action as required by the certification mechanism and takes any other required measure.

9.6. Certification Renewal

When a certificate is renewed after its initial validity period, the CNPD will issue a new certification ID. The CNPD keeps a record with information regarding all certificates granted and their historical evolution.

9.7. Certification process

The management system certification services provided by HACA PARTNERS are carried out in accordance with the policies and procedures established by HACA PARTNERS based on the requirements of the GDPR accreditation standards.

HACA PARTNERS will establish, document, and maintain policies and objectives for fulfilment of this certification mechanism and will ensure the policies and objectives are acknowledged and implemented at all levels of its organization. In order to ensure this acknowledgement and commitment, an Agreement form to respect HACA GDPR Certification Procedure (Appendix 22 - Appointment Letter) is signed by all the persons involved in the Certification, be it as auditor (evaluation), reviewer or certifier.

Upon request, HACA PARTNERS will provide evidence of its commitment to the development and implementation of the management system and its effectiveness in achieving consistent fulfilment of this certification mechanism. This commitment takes, inter alia, the form of an engagement to maintain a high level of GDPR training amongst the GDPR team.

All documentation, processes, systems, records, etc. related to the fulfilment of the requirements of this certification mechanism will be included, referenced, or linked to documentation of the management system.

All professionals involved in certification activities have access to the parts of the management system documentation and related information that are applicable to their responsibilities.

The generic certification process is as follows:

Applicant files Application Form and submit to HACA PARTNERS. Applicability (Target of Evaluation) is reviewed.

Based on the information, Quotation For Certification Services (QCS) will be prepared. The quotation provides an estimate for the total cost for certification.

Upon acceptance of the quotation, the applicant is required to sign the GDPR Certification Agreement and Engagement Letter. An audit team leader responsible for the client file will be appointed.

Stage 1 audit is carried out to determine the adequacy of the client's management system documentation and readiness to proceed to the Stage 2 audit. After the findings from the Stage 1 audit have been resolved, the client is to notify the Audit Team Leader on the readiness to proceed to the Stage 2 audit.

The purpose of the Stage 2 audit is to evaluate the implementation, including effectiveness, of the client's management system.

Upon satisfactory completion of the Stage 2 audit and verification of any nonconformity(ies) raised, the Audit Team Leader will prepare an Assurance Report (ISAE 3000 Attestation Report & Classification of non-conformities) based on GDPR CARPA certification criteria.

A qualified HACA PARTNERS Partner reviews the Assurance Report and approves the recommendation for certification.

An Impartiality Committee makes the decision to grant the Certificate based on the Assurance Report. The certification decision is communicated to the CNPD and is recorded in a Public Register.

The Certificate will be issued upon payment of all fees due and the signing of the Certification Agreement. The certificate is valid for 3 years from the date of approval.

All certified organizations might be subject to a surveillance audit at anytime. Renewal of certification is subject to a satisfactory Recertification audit carry out before the expiry of the certificate.

9.8. Records

HACA PARTNERS will keep all documentation confidential, complete, comprehensible, up-to-date and fit to audit.

Records will be established for certification, personnel involved in the certification, nonconformities and corrective actions.

Records will be kept according to HACA PARTNERS Manuel Assurance Qualité (art. 9. Documentation de la mission). However, the period of retention of GDPR records will be of five years starting from the date of the Auditor's report.

10. Information Requests, Appeals and Complaints

10.1 Clients wishing to complain or appeal about the decisions of HACA PARTNERS shall do so by contacting HACA PARTNERS or sending a mail directly to Saïd Hadji (shadji@hacapartners.lu).

10.2. HACA PARTNERS has developed a GDPR Certification Complaint Process that is provided to all clients upon request. This GDPR Certification Complaint Process specifies inter alia :

a) who can file complaints or objections;
b) who processes them on behalf of the certification body;
c) which verifications take place in this context; and
d) the possibilities for consultation of interested parties.

10.3 Upon receipt of an information request, complaint or appeal, HACA PARTNERS will confirm whether the information request, complaint or appeal relates to certification activities for which it is responsible and, if so, will address it.

10.4. HACA PARTNERS will acknowledge the receipt of the information request, complaint or appeal and will provide the Client with progress reports.

10.5. HACA PARTNERS will take subsequent action needed to resolve the complaint or appeal, and will provide the Client with the result and decision of the complaint or appeal.

11. Materiality (Basis of Opinion)

11.1 HACA PARTNERS conducts its audit activity through a sampling process to determine if the System meets the Standard(s).

11.2 Any statement of conformity issued by HACA PARTNERS in the form of reports, Certificates or other communications is based on these sampling processes. HACA PARTNERS does not warrant, represent or undertake that these statements mean that all activities are in compliance with the relevant Standard(s) at the time of the audit or that subsequent to the audit activity those activities audited will continue to be in conformity with the relevant Standard.

11.3 The Client undertakes to make all customers and end users aware of the foregoing provisions of this Clause. HACA PARTNERS accepts no liability to the Client in the event that any loss or claim is suffered by the Client as a result of any finding that the System does not comply with the Standards.

12. Services Fees

12.1. Services Fees are quoted (and amended from time to time) for services agreed to be supplied pursuant to the Contract ("Services Fees") on the assumption that the information supplied by the Client is accurate and complete.

12.2 Services Fees include the cost of audit services and the use of the HACA PARTNERS logo and, where agreed, the Accreditation Body(ies) logo.

12.3 Expenses and disbursements may be charged separately in accordance with the quoted terms.

12.4 Any service required or supplied in addition to the agreed services will be charged at HACA PARTNERS's rates current at the time of supply of such services.

12.5 Services Fees may be reviewed and amended from time to time, normally but not exclusively on an annual basis.

12.6 Payment is due as per the stated terms on the invoice. Payment shall be made in full, without set off or deduction.

12.7 All fees and expenses quoted are exclusive of all taxes including but not limited to value added or sales tax, which will be charged at the current rate of the Country in which the services are supplied.

13. Confidentiality

13.1 Except as may be required by law or required by the CNPD, HACA PARTNERS and the Client will treat as strictly confidential and will not disclose to any third party without prior written consent of the other, any information which comes into their possession, the possession of their employees, agents or others by virtue of the Contract, provided that this Clause shall not extend to information which was rightfully in the possession of such party prior to the commencement of the negotiations leading to the Contract or which was already public knowledge or becomes so at a future date (otherwise than as a result of a breach of this Clause) or which is required to be disclosed by law. The foregoing obligations as to confidentiality shall survive any termination of the Contract.

13.2 HACA PARTNERS will be responsible, through legally enforceable commitments, for the management of all information obtained or created during the performance of certification activities.

13.3 Except for information that the Client makes publicly available, or when agreed between HACA PARTNERS and the Client (e.g. for the purpose of responding to complaints), all other information is considered proprietary information and shall be regarded as confidential. HACA PARTNERS shall inform the Client, in advance, of the information it intends to place in the public domain.

13.4 When HACA PARTNERS is required by law or authorized by contractual arrangements to release confidential information, the Client or person concerned shall, unless prohibited by law, be notified of the information provided.

13.5 Information about the Client obtained from sources other than the client (e.g. from the complainant or from regulators) shall be treated as confidential.

14. Administrative language

The administrative languages of HACA PARTNERS are French and English.

15. Appendices

Appendix 2 : GDPR Certification Agreement

Appendix 6 : Charte d'Indépendance et d'objectivité

Appendix 20 : Questionnaire for the acceptance and continuance of missions

Appendix 21 : Accord de coopération

Appendix 22 : Appointment Letter

Appendix 24 : Management Review Agenda

Appendix 27 : Internal Audit Strategic Plan