INTERNAL WHISTLE-BLOWING SYSTEM

As part of its approach to the prevention and management of risks in terms of ethics and compliance, an approach described in greater detail in its Code of Ethics & Compliance, and in accordance with applicable laws and regulations, Group SEGULA TECHNOLOGIES has put in place this internal whistle-blowing system (hereinafter referred to as the "System") intended to allow for the collection and processing of reports and the protection of persons who initiate or have facilitated them.

The System will take effect on _____.

Since use of the System is optional, Group SEGULA TECHNOLOGIES will apply no sanctions, nor adopt any unfavourable measures, against any person who decides not to submit a report.

The introduction and implementation of the System implies that personal data is processed by entities of Group SEGULA TECHNOLOGIES. The processing of data performed within the framework of the System complies in this respect with the obligations by the European Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free circulation of such data.

For the Purpose of this System, Group SEGULA TECHNOLOGIES refers, whether collectively or separately, to all entities which, directly or indirectly, control, are controlled by or are under common control with Segula Holding.

1 In which situations can I "blow the whistle"?

i. Beneficiaries of the System

This System is open:

- to employees of Group SEGULA TECHNOLOGIES ;
- to occasional external employees of Group SEGULA TECHNOLOGIES (e.g. consultants, temporary staff);
- to former staff of Group SEGULA TECHNOLOGIES, to candidates for employment within Group SEGULA TECHNOLOGIES, to managers, shareholders or partners of Group SEGULA TECHNOLOGIES;
- to the co-contractors and subcontractors of Group SEGULA TECHNOLOGIES, as well as to the directors and staff of the latter.

For the purpose of this document, the above persons may hereinafter be referred to as "You" or the "Whistle-blower".

ii. Scope

You may submit a report in accordance with the procedures described in point 2 below, if You become aware, personally or through a third party who reported it to You in the course of your professional activity:

- of a situation, behaviour or actions contrary to the Ethics & Compliance Code of Group SEGULA TECHNOLOGIES;
- of an offense as provided for under the applicable Criminal Code;
- of a violation, or the attempted concealment of a violation, of an international commitment, lawfully ratified or approved, of a unilateral act by an international organisation taken on the basis of such a commitment, of European Union law, of the law or of a regulation;
- of facts likely to occur and which, under these conditions, constitute or could constitute one of the above situations.

These reports must be submitted in good faith and with no direct financial interest.

Facts, information or documents covered by confidentiality obligations as they constitute national defence secrets, matters concerning medical confidentiality and lawyer-client confidentiality may not be reported using this System.

2 How to submit a whistle-blowing report

i. Reporting Channels

When You are confronted with any of the situations mentioned in point 1 above, You may submit a report as follows:

- Internal channel:

The report may be submitted:

- To the internal contact person whose contact details are provided below:

Contact details of the internal contact person
***Email*: ethics@segula.fr**

- To your direct or indirect line manager

  Reporting to your direct or indirect line manager will be received as follows:

  - Verbal reporting:
    - On a recorded telephone line: with the consent of the Whistle-blower, it may be recorded either on a durable and recoverable medium, or in a written detailed report.

- On a telephone line without recording or voicemail: drawing up a written report
- Video conference or face-to-face meeting: with the consent of the Wistle-blower, the conversation may be recorded, or a record of it drawn up.

The data collected may be verified, corrected or approved by the Whistle-blower by signing the report.

➢ Written reporting: by email or letter.

Whatever the form of the report, the Whistle-blower must submit any information likely to support the reported facts (regardless of the medium) via the reception channels provided for this purpose (as described above). Otherwise, the report will be closed with no further action taken.

- <u>External Channel:</u>

The report may be sent to competent authorities, depending on the subject matter (judicial authorities, competition authorities, financial markets control authority, anti-corruption agency, tax authorities…).

You are free to choose whether to submit your report via an internal or external channel. You can use an internal channel and an external channel simultaneously.

- Public Disclosure

Finally, the report may be made public in the following cases:

- At the end of a period of 6 months following a report by an external channel;
- In the event of a serious and imminent danger;
- When the use of the external channel may expose the person submitting the report to a risk of reprisal;
- When the use of the external channel would not effectively remedy the subject of the disclosure, due to the particular circumstances of the case, and in particular if evidence could be concealed or destroyed or if You have serious grounds to believe that the external authority could be in a conflict of interests, in collusion with the perpetrator of the acts or involved in these acts.
- In the event of an imminent or obvious threat to the public interest, and in particular where an emergency or a risk of irreversible harm exists, when the information has been obtained during the course of the Whistle-blower's professional activities.

ii. <u>Reporting Methods</u>

- Whether submitted via an internal or external channel, the report may be made in writing and verbally, and may be anonymous.

- A Whistle-blower wishing to remain anonymous must provide every possibility at his/her disposal to communicate and facilitate the analysis and verification of the facts giving rise to the report.

- A Whistle-blower wishing to make a verbal report may do so by telephone or any other voicemail system and, at his/her request, during a video conference or a face-to-face meeting, which will be organised no later than 20 working days from his/her request.

- As part of the report he/she submits, the Whistle-blower provides the facts, information or documents likely to substantiate the report, regardless of their form or medium, formulated objectively. Only the information needed to assess the merits of the report must be supplied. If this information is not included, Group SEGULA TECHNOLOGIES may decide not to process your report.

3 Methods of processing reports

i. Acknowledgement of receipt

Where possible, within a maximum period of seven (7) business days, an acknowledgement of receipt of your report will be issued.

However, no such acknowledgement of receipt may be issued when the report is anonymous.

This acknowledgement of receipt does not, however, indicate the admissibility of the report.

Additional information may be requested from the Whistle-blower to support and verify the legitimacy of the facts being reported.

Where applicable, the Whistle-blower will also be informed of the reasons for which the report does not comply with the required conditions and will not therefore be taken further.

Under these conditions, the report will be classified for no further action and closed out.

ii. Time required to process reports

- Within a reasonable period not exceeding 3 months from the acknowledgement of receipt of the report or from the date of the report in the absence of acknowledgement of receipt, the internal contact person and/or the internal teams of Group SEGULA TECHNOLOGIES shall provide you with information on the measures envisaged or taken to assess the accuracy of the reported facts and/or, where applicable, remedy the issue raised in the report as well as the reasons for these measures.

- Upon receipt, the report is processed by the internal contact person and/or by the internal teams of Group SEGULA TECHNOLOGIES specifically responsible for analysing and verifying reports.

- The report may give rise to investigations and interviews.

- The processing period may be extended to six months if the particular circumstances of the case, related in particular its nature or complexity, require further work, in which case the Company will justify these circumstances to the Whistle-blower before the expiry of the three-month period mentioned above.

iii. Closure of the report

When the facts or allegations are inaccurate, unfounded, manifestly minor or when the report has become irrelevant, the report will be closed.

When the facts are proven, solutions must be implemented to remedy the issue raised by the report.

The Whistle-blower will be informed in writing of the actions taken as a result of the report where possible.

4 Protective measures

i. Beneficiaries

The protective measures described below have been put in place for the benefit of the Whistle-blower but also the:

- Facilitators:
  Natural persons and non-profit legal entities (associations and trade unions) who have encouraged the report

- Legal entities related to the Whistle-blower:
  Legal entities controlled by a whistle-blower or for which they work or with which they are connected in a professional context

- Natural persons related to the Whistle-blower:
  Natural persons related to the Whistle-blower as part of their professional activities and who may be subject to reprisals

ii. Privacy & confidentiality

The internal contact person and the relevant internal teams needing to know about the report take all necessary precautions to protect the confidentiality of the data reported or retained as part of the internal whistle-blowing system, including data relating to the person submitting the report, the facts reported and the identities of the people concerned by the report.
In particular, access to the processing of data is via an individual login and password, updated regularly, and the identity of the person submitting the report is kept confidential in order to ensure it suffers no prejudice as a result of the procedure.

Group SEGULA TECHNOLOGIES is committed to keeping Whistle-blowers' identities strictly confidential. In particular, the identity of the Whistle-blower will not be made known to any of the persons possibly reported, even in the event that the said persons exercise their right of access.

Group SEGULA TECHNOLOGIES will only disclose the identity of the Whistle-blower with his/her prior consent. The identity of the person in question will only be revealed insofar as this is strictly necessary and only on the condition that the facts that are the subject of the report are definitively established.

Notwithstanding the foregoing, the identity of the person who issued a report and that of the person implicated may always be disclosed to the judicial authorities pursuant to the legal obligations incumbent on Group SEGULA TECHNOLOGIES.

iii. Protection for the person submitting a report

- Protection against so-called gagging or bullying procedures:
  The use of the internal whistle-blowing system in good faith, even if the facts subsequently prove to be inaccurate or do not give rise to any follow-up action, will not result in the Whistle-blower being exposed to any disciplinary sanction or any discriminatory measures, whether direct or indirect (such as suspension, lay-off, dismissal, refusal to promote, change of place of work, disadvantageous treatment, etc.).

- Civil Immunity
  You are entitled to civil immunity for any damages caused as a result of reporting or public disclosure if You had reasonable grounds to believe that the reporting or public disclosure of such information was necessary to safeguard the interests in question.

- Criminal immunity

However, the misuse of the System and/or its use with malicious intent may expose You to possible disciplinary action or prosecution.

5 Data Management

i. Data processing

Only the following data categories can be processed as part of the System:

- The identity, job title and contact details of the Whistle-blower;
- The identity, job title and contact details of the people reported;
- The identity, job title and contact details of people involved in compiling and/or processing the report;
- The facts reported;
- The information gathered for verification of the facts reported;
- Report summarising the verification operations;
- Action taken following the report.

ii. Data retention period

All data relating to a report and considered not falling within the scope of the System will be destroyed or archived immediately after anonymisation.
If the report is not followed by a disciplinary or judicial procedure, the data relating to this report is destroyed or archived, after anonymisation, within two months from the completion of the procedure.

If disciplinary or judicial proceedings are initiated against the person reported or the author of an abusive report, the data relating to the report is retained until the end of the judicial proceedings.

The data is stored in accordance with the general archive retention policy applied within the Group SEGULA TECHNOLOGIES, for a period not exceeding the limit for litigation proceedings.

iii. Data transfers

For the processing of reports, certain personal data may be transferred outside the European Economic Area. Group SEGULA TECHNOLOGIES is committed to ensuring a suitable level of protection for data transferred within this context, in particular through the signing of Standard Contractual Clauses approved by the European Commission (which can be accessed by sending an email to informatiqueetlibertes@segula.fr) or signing up to *Privacy Shield* (human resources data included) for recipients of data located in the United States.

iv. Rights with regard to personal data

The Whistle-blower and the persons concerned by the report are assured of the confidentiality of the information collected and its integrity.

Any person reported will be informed once data relating to them is recorded, whether electronically or otherwise, in order to allow them to oppose the processing of such data. When protective measures are required, in particular to prevent the destruction of evidence relating to the report, the person concerned will be informed only after the adoption of these measures.

In accordance with the applicable legislation regarding the protection of personal data, the people identified within the context of the System have a number of rights regarding the collection and processing of their personal data, namely:

- The right to be informed of how their personal data is processed. Such information must be concise, transparent and understandable;

- The right of access: You and the persons concerned by the report have the right to obtain (i) confirmation that your personal data is being processed and (ii) access to such data (together with a copy thereof);

- The right to rectification: You and the persons concerned by the report have the right to obtain the rectification of inaccurate personal data. You and the persons concerned by the report also have the right to have any incomplete personal data updated.

- The right to erasure: in certain cases, You and the persons concerned by the report have the right to have your personal data erased. However, this is not an absolute right, and Group SEGULA TECHNOLOGIES may have legal or legitimate reasons to retain the said data.

- The right to the limitation of processing: in certain cases, You and the persons concerned by the report have the right to restrict the processing of your personal data.

- The right to lodge a complaint with a supervisory authority: You and the persons concerned by the report have the right to contact the data protection authority (CNIL in France) in order to lodge a complaint concerning Group SEGULA TECHNOLOGIES' practices relating to the protection of personal data.

To exercise these rights, the people identified within the context of the whistle-blowing system may send a request to the Personal Data Controller of Group SEGULA TECHNOLOGIES at the following address: informatiqueetlibertes@segula.fr