Terms and Privacy Statement – Whistleblowing reports

This Whistleblowing and Grievance Platform (including the hotline) is provided by CellMark[1] ("**CellMark**", or "**we**") for filing concerns of current or suspected violations of applicable laws or CellMark´s integrity principles as set out in CellMark´s Code of Conduct, policies and directives (that can be found on CellNet), or in CellMark´s Code of Conduct for Business Partners (a "**Misconduct**").

The laws and regulations of certain countries (the "**Local Laws**") may require that a person making a report containing their personal data must be notified and provided with information concerning the information and personal data submitted by that person and must accept the terms and conditions for the use of this Whistleblowing and Grievance Platform. This document ("**Terms and Privacy Statement**") is intended to provide such information.

1. General

To proceed further and for CellMark to be able to receive and process your report or question via this Whistleblowing and Grievance Platform, you must confirm that you have read this Terms and Privacy Statement in its entirety, and expressly consent to the processing of your personal data. If you agree to this Terms and Privacy Statement, you will then be able to file a report or ask a question. Note that you may withdraw your consent at any time, without affecting the lawfulness of the processing before such withdrawal.

If you do not wish to accept the terms in this Terms and Privacy Statement and thereby consent to the processing of your personal data, we are unable to accept any information through this Whistleblowing and Grievance Platform.

In this case, we suggest you report the matter to your manager or another manager within your Division or, if you are an external stakeholder (business partners, customers, and other third parties involved with CellMark), you may report the incident to you CellMark contact or another person within CellMark.

If you are not comfortable reporting in this manner or if you believe that the concern or potential violation is serious[2] or relates to several managers within CellMark, you may also report your concerns directly to the VP of ESG & Compliance via:

- email: compliance@cellmark.com, or
- telephone: +46 70-673 66 14, or
- postmail: CELLMARK AB
  Attn: VP ESG & Compliance,
  Lilla Bommen 3C,

[1] "**CellMark**" refers to CellMark Investment AB and its subsidiaries, i.e., all persons and entities directly or indirectly controlled by CellMark Investment AB, where control may be by management authority, equity interest or otherwise.

[2] "**Serious misconduct**" covers misconduct that can potentially have a severe financial or reputational impact on CellMark. Note that certain areas are always deemed to potentially have a severe financial or reputational impact: anti-bribery and anti-corruption, anti-trust, sanctions and export control, discrimination and harassment, health and safety, human rights and data protection.

411 04 Göteborg, SWEDEN

For additional information and guidance, you can refer to the FAQ or, if you are a CellMark employee, you can refer to CellMark´s Whistleblowing Policy which can be found on CellNet (CellMark´s Intranet), and which is an integral part of this document.

Misconduct can be filed through this Whistleblowing and Grievance Platform by any individual having a work-based relationship with CellMark (a "**Reporter**"), regardless of the nature of their activities and whether they are paid:

- CellMark employees, regardless of function, position, or location, whether working full-time or part-time, under a permanent contract or on a temporary basis;
- consultants or agency personnel who work at one of CellMark´s premises or under the direction of CellMark (who, usually, have an email address provided by Cellmark);
- individuals working for CellMark´s business partners (customers, suppliers and service providers) or directly providing services to the Group;
- other individuals linked to CellMark´s business, such as job applicants or previous employees, or former consultants and agency personnel, or individuals working for a Tier-x supplier or a sub-contractor.

2. Use of this Whistleblowing and Grievance Platform

Use of this Whistleblowing and Grievance Platform is voluntary and is intended to supplement the other reporting options described in section 1 above. CellMark employees are first encouraged to discuss their concerns with or report violations or suspected violations to their manager, or any other manager within their Division.

In certain countries, CellMark may only accept reports through this Whistleblowing and Grievance Platform if they relate to certain areas. If your report pertains to a matter that, under applicable local laws, may not be accepted by CellMark through this Whistleblowing and Grievance Platform, you may use any of the other reporting options (see section 1 above) to submit your report.

The information you submit (including your identity and contact details) will be treated confidentially. It may only be shared with relevant individuals or organizations supporting the assessment of your report and, if applicable, with the internal investigation, or if required by applicable local laws. In these cases, the disclosure of information will be limited to the extent necessary and according to the applicable local laws.

Please be aware that the information you provide may result in decisions that affect others. Therefore, you are required to only provide information in good faith, i.e. provide information for which you have a reasonable ground to believe that it is true at the time of your report. You will not be subject to retaliation from CellMark for any report of suspected misconduct that is made in good faith, even if it later turns out to be incorrect or unsubstantiated.

On the other hand, knowingly providing false or misleading information or otherwise making a report in bad faith will not be tolerated and may expose you to disciplinary measures. Note that you may also face possible prosecution or civil claims by the

individual(s) subject of the bad faith report (if a report is made in bad faith, we may disclose your identity to the individual(s) you reported).

Certain Local Laws may allow anonymous reporting. However, as the default way of reporting, we encourage you to identify yourself for CellMark to easily follow up with questions we may have. Please note that subject to the above circumstances, we shall not disclose your identity.

3. What personal data and information is collected and processed?

The Whistleblowing and Grievance Platform may collect the following personal data and information that you may submit via the tool:

- The country in which you are located.
- Information about your identity (first and last name), your contact details, and your work relationship with CellMark.
- Information about your concern or the alleged violation(s):
  - Country where the incident occurred,
  - Identity of the person(s) engaged in the alleged violation and their company or organization
  - Detailed description of the alleged Misconduct, such as:
    - Description of the concern or violation
    - Where and when the incident occurred
    - How you became aware of the incident
    - Whether you have evidence or whether there is any witness (and, if so, information about their identity)
    - Whether you suspect or know that a supervisor or management is involved
    - Whether management been informed of the allegations
    - Whether anybody attempted to conceal the alleged violation (and, if so, information about their identity).

When filling your report via the Whistleblowing and Grievance Platform, please consider which personal data, both about yourself and about other individuals, is needed for your report to be properly understood and assessed by the recipient(s). We ask you not to include in your report any personal data that is not necessary (e.g. data that is not relevant to the reported situation, events, or behaviors).

4. How will the personal data and information you provide be processed and who may access personal data and information?

CellMark has entered into contractual commitments with NAVEX, to secure the information and the personal data you provide in accordance with applicable laws. NAVEX is committed to maintaining stringent privacy and security practices including those related to notice, choice, onward transfer, security, data integrity, access, and enforcement.

The personal data and information provided via the Whistleblowing and Grievance Platform will be stored in a database that is located on servers hosted and operated by a third-party service provider (see https://www.navex.com/en-us/service-hosting-providers/) and remains in the European Union. For more information on the third-party

service provider, see https://www.navex.com/en-us/service-hosting-providers/ethicspoint/#eu. For additional questions, please contact privacy@navex.com.

To process your report or question, conduct internal investigations, and if necessary, initiate disciplinary procedures and impose sanctions, the personal data and information you provide through the Whistleblowing and Grievance Platform or otherwise may be accessed and used by:

- any relevant CellMark personnel, on a need-to-know basis and subject to confidentiality; this includes, without limitation, CellMark Board members and CellMark management, individuals from ESG & Compliance, Human Resources, Finance, IT & Digital; and
- external advisors (e.g. legal advisors),

together the "**Authorized Persons**".
The personal data and information provided through the Whistleblowing and Grievance Platform may also be accessed by technical staff at NAVEX.

The Authorized Persons and the technical staff at NAVEX may be located in the European Union or elsewhere, and transfers of personal data to such persons are always secured by safeguards required by the local privacy laws. Any transfer of personal data from European citizens or residents to a person or organization located in a country outside of the European Union is based on either an adequacy decision or the standard contractual clauses issued by the European Commission.

The Authorized Persons may access and use the personal data and information provided through the Whistleblowing and Grievance Platform or otherwise, to conduct the assessment of your report or question, and if relevant perform an internal investigation. The Authorized Persons may also access and use any other information or personal data as needed to conduct the assessment or internal investigation, subject to compliance with applicable laws.

The personal data and information provided through the Whistleblowing and Grievance Platform or obtained otherwise may also be disclosed, if required or allowed by applicable law, to the police and/or other enforcement or regulatory authorities or courts. The relevant bodies that may receive and process personal data may be located in a country that may not provide the level of data protection available in the European Union.

The personal data processed collected and used in the context of a whistleblowing report or internal investigation will be handled according to applicable data protection legislation.

Subject to limitations under applicable laws, the personal data you provide will be kept as long as necessary to process your report or question, initiate proceedings, or complete the internal investigation, or if data must be preserved due to a legal requirement. The personal data may be stored for archiving purposes if allowed by applicable laws.

The personal data included in a whistleblowing report will be erased as required under applicable laws. The following retention periods are indicative and are subject to shorter or longer retention periods under applicable privacy laws:

- Immediately after the assessment of the report if the matter reported falls outside the scope of what can be reported.

- Within 2 months from the case closure date if the case is closed because the information reported is insufficient to assess the likelihood of the Misconduct and the whistleblower has not provided further information within 45 days of the initial report date.
- Within 6 months from the case closure date if the Misconduct reported was found to be unsubstantiated, unless there is a specific need to retain the relevant information for a longer period under applicable laws.
- If the Misconduct was found substantiated (in its entirety or partially), until the expiry of any applicable statutory limitation period for the Misconduct at stake and/or for the disciplinary measures taken, or any other applicable legal retention period

The information relating to internal investigations can be retained indefinitely if it has been anonymized, for example for statistics and/or data analysis purposes.

5. Rights of data subjects

Anyone having made a report through the Whistleblowing and Grievance Platform or obtained otherwise have the right to request access to and/or correction or deletion of their personal data, as well as any other rights (such as restriction, portability and objection) under applicable privacy laws.

If required by applicable laws, information about the processing of personal data during an internal investigation shall be provided to the relevant individuals at the moment of the investigation when such disclosure does not jeopardize the investigation itself and/or any subsequent investigations by competent authorities or any judicial proceedings. However, the identity of the reporter will not be revealed.

When informed about the processing of their personal data, the person(s) subject of a whistleblowing report or an internal investigation may exercise their rights under applicable laws (e.g., in certain countries: access to their personal data, request of correction or deletion of their personal data, or of restriction and objection to use their personal data).

In order to exercise the rights outlined in this section 5, anyone in scope can contact the VP of ESG & Compliance (contact information provided above, under Section 1 “General”).

If allowed under applicable laws, anyone whose personal data is processed in the context of a whistleblowing report or an internal investigation may complain to the relevant supervisory authority about the processing of their personal data in this context.