Danske Bank

Whistleblowing Policy

14 September 2022

1. Objective

Danske Bank Group (the "Group") is committed to conducting business with integrity, and to doing the right thing for our customers, our colleagues and society. The Group encourages the reporting of concerns about Breaches, or potential Breaches, of laws or regulations applicable to the Group, or of the Group's internal policies and standards (hereafter referred to as "Breaches").

The objective of the Whistleblowing Policy (this "Policy") is to set out the principles and standards for the management of Whistleblowers and Whistleblowing Reports. This Policy is compliant with the requirements of the European Union, European Data Protection Supervisor, and relevant Financial Supervisory Authorities.

Employees should share their concerns with their line manager, colleagues, Human Resources ("HR"), Compliance Officer and/or Risk Manager, and escalate those concerns, which may include potentially Problematic Cases in a timely manner. Situations may nevertheless arise wherein employees are reluctant or unable to share their concerns with these colleagues. The Whistleblowing Scheme supports the Group in these situations by providing a secure channel through which employees, and those outside the Bank (see Section 3.1), can report Breaches and other concerns through a confidential system that offers anonymity, and undertakes to defend Whistleblowers against unfair treatment.

Lack of adherence to this Policy may lead to disciplinary actions.

2. Definitions

The following definitions apply to the terms used throughout this Policy.

Breach(es)	instances of conduct that is wilful or negligent, or both, that results in violation of internal and/or external requirements. Internal requirements are here considered as all policies, instructions and business procedures in the Group. External requirements are the laws, regulations and generally accepted practices that apply to the Group's activities.
Consent	any freely given, informed, and unambiguous indication of the Whistleblower or Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.
Data Subject	any person whose Personal Data is being collected, held, or Processed in relation to a Whistleblowing Report.
Group	Danske Bank A/S and all subsidiaries.
Personal Data	any information relating to an identified or identifiable natural person.
Problematic Case	any extraordinary event or circumstance, or combination of events and circumstances, that may severely damage the Group or any of its components.

Processing	any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Reported Person	an individual against whom an allegation has been made.
Whistleblower	a person who has submitted a Whistleblowing Report or has claimed Whistleblower status with a view to making a report.
Whistleblowing	disclosure by a person, usually an employee in the Group but may also include persons external to the Group, of Breaches or actual or potential mismanagement, illegalities or other wrongdoings, to the department (Whistleblowing Operations) in charge of handling those disclosures.
Whistleblowing Operations	a specialist unit in Group Compliance handling Whistleblowing matters.
Whistleblowing Report	a concern submitted through the Whistleblowing Scheme about an actual or potential Breach.
Whistleblowing Scheme	the Group's internal channels to support easy and confidential reporting of concerns.
Whistleblowing Site	the Group's encrypted IT-based toolkit that can be accessed via the Group's internal intranet site, or external URL platform, allowing for electronic submission, storage and handling of Whistleblowing Reports.

3. Scope

This Policy lays out the principles for the Group's Whistleblowing Scheme.

3.1 Target group

This Policy applies to all of the Group including subsidiaries, once adopted by their respective management bodies (referred to as "In Scope Entities").

The management body of a subsidiary may approve this Policy with deviations to ensure this Policy is fit for purpose for the subsidiary. The policy administrator in the subsidiary should discuss the rationale behind the deviation and ensure that the administrator of the Group Policy is consulted on material deviations.

The administrator of this Policy must document and report material deviations from this Policy to the owner of this Policy.

This Policy applies to all of the following (referred to as "In Scope Persons"),")

- Employees,
- Persons belonging to management bodies, including non-executive members,
- Volunteers and unpaid trainees,
- Persons working under the supervision and direction of contractors, subcontractors and suppliers,
- Persons whose work-based relationship is yet to begin in cases where information concerning a Breach has been acquired during the recruitment process or other pre-contractual negotiation; and customers, shareholders and other stakeholders wanting to share a concern by submitting a Whistleblowing Report.

All In Scope Persons have access to the Whistleblowing Scheme.

A subsidiary may have an obligation under local law to establish its own Whistleblowing Scheme where Breaches can be reported and subsequently investigated by authorised employees in the subsidiary. In such cases, information

on how to report Breaches will be available for relevant In Scope Persons, for example via Danske Bank's intranet or the subsidiary's website. However, In Scope Persons may still report to the Group Whistleblowing Scheme via the reporting channels listed below in Principle 3 if they choose to.

4. Policy content

Principle 1: Breaches may be reported through the Whistleblowing Scheme

Subprinciple 1.1: What can be reported?

Any Breach of laws or regulations applicable to the Group, or of the Group's internal policies and standards, or any other issues of serious concern affecting the Group can be reported. Potential financial loss for, or reputational damage to, the Group are not prerequisites for use of the Whistleblowing Scheme.

In Scope Persons should share their concerns about Breaches, even if uncertain whether the concern in question is an actual or potential Breach.

Employees should report through the Whistleblowing Scheme if they feel unable to raise their concerns to their line manager, to specialist departments such as HR or Compliance, or through other channels. They may feel unable to use these channels because of fear of reprisal or victimisation, because their concerns are particularly sensitive in nature, because they do not wish to be associated by colleagues with their concerns, or for other private or professional reasons. Although Whistleblowing Operations might ask about a Whistleblower's choice of using the Whistleblowing Scheme, the Whistleblower has no obligation to explain their preference for confidentiality and/or anonymity.

If the concern in question applies to the Compliance function, the Whistleblower should select options in the Whistleblowing Scheme that will ensure that Group Internal Audit will receive and manage the Whistleblowing Report.

Subprinciple 1.2: What should not be reported?

Employees should not report concerns about conventional employment issues such as their terms of employment, remuneration, or working environment through the Whistleblowing Scheme unless those concerns reflect Breaches of laws and regulations that the Whistleblower feels cannot be reported through regular channels. When Whistleblowing Operations receives a Whistleblowing Report of this kind about conventional employment issues, and the Whistleblowing Report does not describe sensitive issues that may require investigation and confidential management, Whistleblowing Operations will refer the reporter to the relevant function for further action, and close the Whistleblowing Report.

Customer complaints should usually be submitted to the customer complaints management function. However, as the Whistleblowing Scheme is open to external stakeholders, it is possible that customers will make use of it. In such circumstances, Whistleblowing Operations must judge whether the report is indeed a valid Whistleblowing Report or whether it should be referred to conventional customer complaint channels. Whistleblowing Operations will notify the reporter of such a decision.

A Whistleblowing Report should not contain sensitive Personal Data about a Data Subject. Sensitive Personal Data may comprise, but is not limited to, data about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and/or data concerning health unless the following exceptions apply:

1. The Whistleblower believes in good faith that it is relevant to the Whistleblowing Report

and/or

2. Consent was given by the Data Subject to include this information.

Whistleblowing Operations will not act upon, or forward, such personal information if they do not believe that it comprises one of these two exceptions.

Principle 2: Whistleblowers enjoy protection under the law

The Group undertakes to provide employment-related protection for Whistleblowers from retaliatory or unfair action where a Whistleblowing Report is filed in good faith with the Whistleblowing Scheme. When a Whistleblowing Report is filed with the Whistleblowing Scheme, the Group takes specific measures to safeguard Whistleblowers from unfair treatment, including employment-related consequences.

If any In Scope Person deliberately uses the Whistleblowing Scheme in bad faith, this may result in disciplinary action, and the Whistleblower will not be protected by the Whistleblowing Scheme.

In the event that the Whistleblower, or any affected party, feels that they have been subjected to retaliation or unfair treatment as a consequence of their engagement with the Whistleblowing Scheme, they should contact Whistleblowing Operations or HR Legal.

Retaliation includes, but is not limited to:

- Dismissal or termination
- Demotion, blocking of promotion, or re-assignment to a less desirable position
- Reduction of pay or overtime or Denial of benefits
- Inappropriate disciplinary action
- Inappropriate refusal to hire or rehire
- Threats, intimidation or harassment
- Actions that will damage an employee´s prospects such as denial of training or side-lining.
- Isolating, ostracising, mocking, or falsely accusing the employee of poor performance
- Blacklisting (intentionally interfering with an employee's ability to obtain future employment)
- Constructive dismissal (rendering an employee´s working conditions intolerable)

Principle 3: In Scope Persons must be able to file a Whistleblowing Report easily and confidentially

The following internal channels are available for submitting Whistleblowing Reports to the Whistleblowing Scheme:

- **The Whistleblowing Site.** A Whistleblower can submit a concern either through a written report or verbally (through voice-altering technology) via the Whistleblowing Site. Link: https://danskebank.whistleblowernetwork.net/.
- **Email.** By sending an email to Whistleblowing Operations in Group Compliance. If the Whistleblowing Report concerns Group Compliance, the email should be sent to Group Internal Audit.
- **Phone.** By calling Whistleblowing Operations/Group Internal Audit.
- **Regular email.** By mailing a letter to Whistleblowing Operations in Group Compliance. If the Whistleblowing Report concerns Group Compliance, the letter should be sent to Group Internal Audit.
- **Personal meeting.** Upon request, a physical meeting can be set up with Whistleblowing Operations, or if the Whistleblowing Report concerns Group Compliance, with Group Internal Audit.

These channels are separate from the day-to-day operational systems of the Group and guarantee anonymity for those who claim it. Only specified persons in Group Compliance and Group Internal Audit, who are responsible for managing the Whistleblowing Reports, have access to the original Whistleblowing Reports submitted through the Whistleblowing Scheme.

In addition to the internal channels listed above, some local Financial Supervisory Authorities/Data Protection Authorities also operate Whistleblowing Schemes (for example an independent, external reporting channel), which can be used to report Breaches. Nothing in this Policy prevents or restricts the use of external Whistleblowing Reporting channels.

Principle 4: Security measures are taken to ensure protection of the confidential data stored in the Whistleblowing Scheme

Whistleblowing Operations will have processes in place to ensure the confidentiality of data held within the Whistleblowing Scheme. These measures include the completion of an information security risk assessment.

Principle 5: Whistleblowers are provided with the opportunity to report anonymously

The Whistleblowing Scheme and all the channels mentioned in Principle 3 under the Whistleblowing Scheme are set up to support and ensure anonymous reporting is available.

In certain circumstances, Whistleblowing Operations may request personal details from a Whistleblower to facilitate investigation or remediation of the issues that the Whistleblower has raised. It is entirely for the Whistleblower to decide whether to offer such personal details.

In rare cases involving serious crimes, and where the Whistleblower has voluntarily disclosed their identity, the Group may be required to pass on identity information to authorities for investigation purposes or court proceedings.

Principle 6: Whistleblowing Reports will prompt appropriate action

When Whistleblowing Operations receives a Whistleblowing Report, they will analyse and assess the report, and ensure it is referred to the relevant stakeholder for further analysis, investigation and actions, as appropriate.

- If the Whistleblowing Report describes a Breach or circumstances, or makes allegations, that require confidential investigation, then Whistleblowing Operations will refer the report to HR Legal, Compliance Investigations or another team or department qualified to undertake appropriate investigation.
- If the Report is more overt in nature and content, and describes circumstances already known, or which do not require confidential investigation, then Whistleblowing Operations will refer the Report to the teams or departments best placed to analyze the report and act upon it as appropriate. Recipients must, nevertheless, recognize the sensitivity associated by default with a Whistleblowing Report. If appropriate, Whistleblowing Operations may refer directly to a subsidiary or a team or an individual within a subsidiary.
- Whistleblowing Operations analysis and research, assisted by other departments as appropriate, may confirm that the Whistleblowing Report is inaccurate, or that the issues it raises have already been addressed or remediated. In such circumstances, Whistleblowing Operations must judge whether the report merits wider dissemination.
- Whistleblowing Operations should seek clarification of Whistleblowing Reports from a Whistleblower as necessary, either to support Whistleblowing Operations' own analysis or to support the work of those to whom it has referred a report. In some cases, development of an investigation, or remediation, may require extensive engagement with a Whistleblower or Whistleblowers over a long period.
- A Whistleblowing case will endure as long as a Whistleblower wishes, in good faith, to continue their dialogue with Whistleblowing Operations. Whistleblowing Operations may also wish to extend contact with the Whistleblower to help inform investigation or remediation.
- Although it is not the responsibility of Whistleblowing Operations to investigate or remediate the issues raised by Whistleblowers (see Principle 1), it may sometimes be the case that Whistleblowing Operations assesses that the Whistleblower's circumstances, or other factors, render resolution of the Whistleblowing case particularly urgent. Whistleblowing Operations will raise these concerns with the Head of Compliance Investigations or the Head of HR Legal who will escalate the issue accordingly.
- The Head of Whistleblowing Operations will refer any Whistleblowing Report remaining open for more than six months (described as "pending" by the Whistleblowing Operations IT system) to the Head of Compliance Investigations, who will refer it in turn to the Head of Central Compliance. Group Internal Audit have the same obligation within their own system.

Principle 7: Whistleblowing Operations must produce management information and retain a high-level record of actions and remediation underway as a result of Whistleblowing Reports

Whistleblowing Operations will produce management information about the Whistleblowing Scheme and Whistleblowing cases. Whistleblowing Operations will service interim requirements for management information from subsidiaries on a case-by-case basis.

Principle 8: Group Compliance provides regular reports to the Executive Leadership Team, and the Conduct & Compliance Committee, and annual reports to the Board of Directors, also reporting to the Danish Financial Supervisory Authority and other regulators

Group Compliance must provide reporting to senior management bodies and regulators. Whistleblowing Operations will ensure that this reporting contains no personal details about Whistleblowers.

Whistleblowing Operations will also produce proportionate reporting to Group subsidiaries who use the Whistleblowing Scheme, annually or as required. This reporting will note the number of Whistleblowing engagements and reports relevant to the subsidiary in question and will also describe specific or wider trends and any significant changes to Whistleblowing Operations' configuration or process.

5. Escalation

The Group has an Escalation Policy stating the requirements for appropriate and timely internal reporting of potentially Problematic Cases across the Group.

When a Whistleblowing Report describes a Breach or potential Breach that may constitute a Problematic Case, the Breach must be escalated in accordance with the Escalation Policy.

Breaches or potential Breaches of this Policy should be escalated to an appropriate level for management and remediation.

6. Review

This Policy is reviewed and updated at least annually. Changes to this Policy must be endorsed by the Executive Leadership Team and the Conduct & Compliance Committee and approved by the Board of Directors.