Danske Bank

Whistleblowing Policy

3 November 2020

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 sharing concerns of any potential breaches of laws or regulations applicable to the Group, as well as the Group's internal policies and standards (hereafter referred to as "Breaches") in the Group.

The objective of the Whistleblowing Policy ("the Policy") is to set out the principles and standards for the management of Whistleblowing Reports. The Policy also serves to identify Whistleblowing related roles and responsibilities. The Policy is designed to ensure compliance with the overall requirements of the European Union, European Data Protection Supervisor, and relevant Financial Supervisory Authorities.

Employees are always encouraged to share their concerns with their Line Manager, colleagues, Human Resources ("HR"), Compliance Officer and/or Risk Manager and escalate potentially problematic cases in a timely manner. Situations may nevertheless arise where employees do not feel comfortable, or feel it is not appropriate to share their concerns with the above-mentioned contacts. The Whistleblowing Scheme supports the Group in these situations by providing a secure channel to report Breaches, and by enabling additional measures to safeguard Whistleblowers from unfair treatment. The Whistleblowing Scheme does also apply to individuals outside the Group (See Section 3.1).

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

2. Definitions

In addition to terms that are defined in the text of the Policy, the following defined terms are used:

"Abuse of law": acts or omissions falling within the scope of applicable laws which do not appear to be unlawful in formal terms but defeat the object or the purpose pursued by the applicable laws.

"Breaches": potential (which implies suspicious) or actual activity which violates or abuses laws or regulations applicable to the Group, as well as the Group's internal policies and standards. These activities can include criminal offenses, fraud and harassment.

"**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 incl. all subsidiaries.

"Identifiable Natural Person": any person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

"Personal Data": any information relating to an identified or identifiable natural person ("Data Subject").

"Process": a series of actions in order to achieve a result.

"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 submitted a Whistleblowing Report.

"Whistleblowing Report": a concern submitted about an actual or potential Breach by using the Whistleblowing Scheme.

"Whistleblowing Operations": a specialised and trained unit in Group Compliance handling Whistleblowing matters.

"Whistleblowing Scheme": the Group's reporting scheme to support easy and confidential reporting of Breaches.

"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 concerns. A person using the Whistleblowing Site can choose to direct the Whistleblowing Report to Group Compliance or to Group Internal Audit if the Whistleblowing Report concerns Group Compliance.

"Witness": a person who may have knowledge of a Breach.

3. Scope

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

3.1. Target Group

The Policy applies to all units in the Group and all subsidiaries once adopted by their respective management bodies (referred to as "In Scope Entities").

The management body of a subsidiary may approve the Policy with deviations in case the Policy conflicts with local regulatory requirements or the business model of the subsidiary. The subsidiary should justify the rationale behind the deviation and ensure that the administrator of the Policy is consulted on any deviations on the Policy.

The administrator of this Policy must document and report any deviations from the Policy to the Executive Leadership Team of Danske Bank. The Executive Leadership Team shall report all deviations from Group Policies to the Board of Directors of Danske Bank.

The Policy applies to persons who acquired information on Breaches in a work-related context with an In Scope Entity (referred to as "In Scope Persons"), including:

- Employees;
- Persons belonging to the management body, including non-executive members;
- Volunteers and unpaid trainees;
- Persons working under the supervision and direction of contractors, subcontractors and suppliers to the Target Group;
- 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 use the Whistleblowing Scheme.

4. Policy Content

Principle 1: **Breaches must be reported through the Whistleblowing Scheme**

Subprinciple 1.1: What can be reported?

Any Breach of laws or regulations applicable to the Group, as well as the Group's internal policies and standards.

The potential or actual Breach may be in the organisation in which the Whistleblower works or has worked, or in another organisation with which he or she is or was in contact through his or her work with the Group.

It is not a requirement for using the Whistleblowing Scheme that a reported Breach would potentially cause financial losses for the Group, impact the Group's reputation, or the like.

In Scope Persons are always encouraged to share their concerns of Breaches, even if uncertain whether the concern in question is an actual or potential Breach, provided they have reasonable grounds to believe that the information reported was true at the time of reporting.

Any employee of the Group, including former employees; any contractors or consultants employed by the Group; any Process; and any department may potentially be the subject of a Whistleblowing Report.

Subprinciple 1.2: What cannot be reported?

Concerns or issues about personal matters or personal grievances such as dissatisfaction with salary, or other employment terms, violations of working environment standards (e.g. the Group's smoking or alcohol guidelines), are out of scope of the Whistleblowing Scheme and should not be reported through this channel (but should be reported through other channels such as the Line Manager or HR). Customer complaints must be submitted to the customer complaint services.

Where a Whistleblowing Report about such concerns and issues is received, the concern will be referred to the relevant function for further action and the Whistleblowing Report will be closed. The Whistleblower will be informed about the referral.

Sensitive information on a Data Subject, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data concerning health or sex life not relevant for the Whistleblowing Report should be avoided. However, this information should be documented if any of the following exceptions apply:

1. It is relevant to the Whistleblowing Report; and/or

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

Principle 2: Whistleblowers must enjoy protection under the law.

The Group guarantees 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 and employment related consequences.

If a whistleblowing concern is reported deliberately 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 affected party feels that they have been subjected to unfair treatment as a consequence of reporting, immediate contact should be made with Whistleblowing Operations or Human Resources.

Principle 3: The Group has established easy and confidential access to the Whistleblowing Scheme, enabling In Scope Persons to file a Whistleblowing Report in an available preferred language.

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

- **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.

- **Regular mail.** By mailing a letter to the Whistleblowing Operations Team 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 the specialists in the Whistleblowing Operations team, or if the Whistleblowing Report concerns Group Compliance, with Group Internal Audit.

The internal channels are independent, allow for anonymity, and are external from the day-to-day operational systems of the Group. Only persons in Group Compliance and Group Internal Audit who are responsible for managing the Whistleblowing Reports have access to Whistleblowing Reports submitted through the Whistleblowing Scheme.

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

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

The security measures include the completion of an information security risk assessment of the Whistleblowing Scheme, which serves to identify potential threats to the Whistleblowing handling process, and confirms that such threats are identified, assessed, and the results are reviewed to determine if additional security measures should be taken to protect the confidential information stored in the Whistleblower Site.

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. The Group's legal obligation towards a Whistleblower, to protect his or her identity, does not cease to exist when (i) the Whistleblower chooses to disclose his or her identity to the public, and/or when (ii) the investigation of the Whistleblowing Report is concluded. In rare cases involving serious crimes – and where the identity of the Whistleblower is known - the Group may pass on identity information to authorities to be used for case management purposes.

Principle 6: Where the Whistleblowing Report concerns an individual, the rights of that individual must be protected

The Group will ensure the Reported Persons fully enjoy the right to an effective remedy and to a fair investigation as well as the presumption of innocence and the rights of defence. This includes the right to be heard and the right to access their file, with the exemption of cases where this may compromise the safeguarding of the Whistleblower and/or the integrity of the investigation.

➢

Principle 7: All investigations must be carried out on a case-by-case basis.

The basis for a final determination of an investigation is made based on the type of information provided and the individual facts and circumstances of the matter.

➢

Principle 8: All investigations within the Whistleblowing Scheme must be conducted and finalised as soon as possible but no longer than six months after the date of reporting the Breach.

If the Whistleblowing Report is still open after six months, an approval must be granted from the Head of Surveillance & Investigations. Thereafter, the key conclusions from the investigation and the outcome of the investigation must be summarised in a "Completion Report."

Principle 9: Where a Whistleblowing Report is submitted to the Whistleblowing Scheme, Group Compliance must assess the need for establishing an Ad Hoc Steering Group that is responsible for providing support and advice to the Investigation Team.

The Ad Hoc Steering Group has the mandate to determine whether an investigation has been sufficiently conducted, and whether the investigation can be completed. The Ad Hoc Steering Group is empowered to challenge the Investigation Team and can request further investigations. Furthermore, the Ad Hoc Steering Group can determine if actions should be taken by the Investigation Team or by relevant management. It should continue to remain in existence for as long as the Ad Hoc Steering Group assesses this to be needed.

If an Ad Hoc Steering Group is established it should, as a minimum, be comprised of:

- Two participants from Group Compliance, or two participants from Group Internal Audit if the Whistleblowing Report concerns Group Compliance;
- One member from HR Legal; and
- One member from the Executive Leadership Team or the designated deputy.

Where a Whistleblowing Report concerns one or more members of the Group's Board of Directors, the Group's Chief Audit Executive or a member of the Group's Executive Leadership Team, an Ad Hoc Steering Group must be established. In these circumstances, the Ad Hoc Steering Group must include the Chairman of the Group Conduct and Compliance Committee and one other member of the Group Conduct and Compliance Committee. In the event the Whistleblowing Report concerns the Chairman of the Conduct & Compliance Committee then another member of the Conduct & Compliance Committee should replace the Chairman of the Conduct & Compliance Committee on the Ad Hoc Steering Committee.

The mandatory members of the Ad Hoc Steering Group can decide to include internal or external participants as member(s) of, or as advisor(s) to, the Ad Hoc Steering Group.

If, in the course of an investigation, circumstances change or evidence emerges that would require that the members of the Ad Hoc Steering Group be changed, a new Ad Hoc Steering Group will be established.

Principle 10: Group Compliance provides reports to the Executive Leadership Team, the Conduct & Compliance Committee, the Board of Directors, and relevant Financial Supervisory Authorities on the number of Whistleblowing Reports received and a high-level trend analysis of the types of concerns raised in the Whistleblowing Reports.

Group Compliance must keep case data complete and current in the appropriate system of record to provide required parties and other parties with the necessary metrics, reporting, and analytics, which are used to support appropriate corrective actions and a consolidated Group-wide view of Whistleblowing Reports. All reporting information including any information retained for statistical purposes shall be made anonymous, including the removal of any information that may result in indirect identification.

5. Escalation

The Group has an Escalation Policy stating the requirements for appropriate and timely internal reporting of potentially problematic cases across Danske Bank Group.

The requirements in the Escalation Policy must always be considered when the Group receives a Whistleblowing Report, no matter which channels the Whistleblowing Report is submitted through.