WHISTLEBLOWER POLICY REGARDING

NETCOMPANY BANKING SERVICES A/S WHISTLEBLOWER ARRANGEMENT

September 2025

WHISTLEBLOWER POLICY

1 INTRODUCTION AND PURPOSE

1.1 This Whistleblower Policy describes the purpose of Netcompany Banking Services A/S (hereinafter referred to as " Netcompany Banking Services") having introduced a Whistleblower Arrangement (hereinafter referred to as the "**Arrangement**"), how it works, who can make use of the Arrangement, and what may be reported through the Arrangement.

1.2 The purpose of the Arrangement is to ensure that a Whistleblower, as defined in this Whistleblower Policy, can swiftly and confidentially, through a special, independent and autonomous channel, report violations or potential violations within the scope of the Danish Act on the Protection of Whistleblowers (hereinafter referred to as the "**Whistleblower Act**"), allowing an independent and autonomous whistleblower unit to assess which steps are required in this respect.

1.3 The Whistleblower Arrangement has been established pursuant to Section 9 of the Whistleblower Act.

2 WHO CAN USE THE ARRANGEMENT?

2.1 The Arrangement can be used by persons who report information on violations to which the person in question has gained access in connection with his or her work-related activities, and who belong to the following categories of persons (hereinafter referred to as "**Whistleblower**"):

(i) Employees

(ii) Self-employed persons

(iii) Shareholders and members of the executive board, board of directors, or similar governing body in an undertaking

(iv) Volunteers

(v) Paid or unpaid trainees

(vi) Persons working under the supervision and management of contracting parties, subcontractors, and suppliers

(vii) Persons who are reporting or publishing information to which they have gained access in a work-related relationship that has ceased since then

(viii) Persons in work-related relationships that have not yet commenced, who report information on violations to which they have gained access during the course of the recruitment process or other pre-contractual negotiations.

2.2 Persons listed under section 9.4 can also file reports under the Arrangement (e.g., an intermediary assisting the Whistleblower with the reporting process in a work-related context).

2.3 Persons not included in the categories of persons stated in sections 2.1 or 9.4 cannot file reports under the Arrangement but have to report through Netcompany Banking Services' ordinary communication channels. If the conditions are otherwise fulfilled in this respect, reports can be filed through the external whistleblower system of the Danish Data Protection Agency, as described in section 10.

3 WHAT MAY BE REPORTED THROUGH THE ARRANGEMENT?

3.1 The Arrangement covers reports regarding serious offences or other serious matters (see section 3.4 (i)) as well as reports regarding violations of EU law within the scope of application of the Whistleblower Directive (see section 3.4 (ii)).

3.2 "Violations" means acts or omissions that

(a) are illegal or constitute a serious offence or other serious matters comprised by section 3.4; or

(b) allow circumventions of the purpose of the rules under section 3.4.

3.3 Any information may be reported, including reasonable suspicion about actual or potential violations or serious matters comprised by section 3.4, which have occurred or most probably will occur at Netcompany Banking Services, as well as any attempts to cover up such violations.

3.4 The report must concern violations or potential violations within the scope of the Whistleblower Act, defined as acts or omissions which:

i) are serious offences or other serious matters, like for instance:

- Violation of any duty of confidentiality
- Abuse of financial means
- Theft
- Deceit
- Embezzlement
- Fraud
- Bribery
- Violation of industrial safety rules
- Any form of sexual harassment
- Severe harassment, e.g., bullying, violence, and harassment due to race, political or religious affiliation.

ii) are illegal pursuant to EU law within a number of specific areas, including for instance:

- Public procurement
- Money-laundering
- Product safety and compliance
- Transport safety
- Food and feed safety
- Animal health and welfare
- Protection of the environment
- Public health
- Consumer protection
- Protection of privacy and personal data
- Security of network and information systems.

In this connection, reference is made to this list containing information on the legislation that is covered by the Arrangement.

3.5 The Arrangement may only be used for reporting violations or potential violations in relation to the issues described in section 3.4 that have occurred or most probably will occur in Netcompany Banking Services' organisation, committed for instance by employees, executive board, or members of the board of directors of Netcompany Banking Services. In connection with reports on incidents committed by Netcompany Banking Services, please note that such incidents may be reported

although the incident cannot be attributed to an individual person but may be due to a basic systemic failure at Netcompany Banking Services.

3.6 Offences that are not comprised by the Arrangement must be reported through ordinary communication channels. If the conditions are otherwise fulfilled in this respect, reports can be filed through the external whistleblower system of the Danish Data Protection Agency, as described in section 10.

4 CONTENTS OF THE REPORT

4.1 To facilitate further investigation of the reported issue, and to be able to identify the offence, it is important that the Whistleblower describes the offence in the best possible way. It is thus not possible to make any further investigations of a report if the report is not specified or if it only contains very general allegations without any further clarification.

4.2 Therefore, it is important that the Whistleblower - to the utmost extent - provides the following information:

- a description of the matter;
- the person(s) involved;
- whether others are aware of the suspicion about the matter;
- whether the executive board knows about the matter;
- whether documents exist that support the matter;
- whether and where further information may be found about the matter;
- for how long the matter has gone on; and
- whether the Whistleblower knows about any attempts to hide the offence.

4.3 Manifestly unfounded reports will not be investigated further.

5 HOW CAN A REPORT BE SUBMITTED AND WHO IS TO RECEIVE THE REPORT?

5.1 Netcompany Banking Services has appointed a whistleblower unit that

(a) will receive the reports and be in contact with the Whistleblower;
(b) will follow-up on the reports; and
(c) give feedback to the Whistleblower.

5.2 The whistleblower unit in charge of the tasks mentioned in section 5.1 consists partly of two lawyers from Plesner Law Firm (hereinafter "**Plesner**"), and partly of an impartial group of persons at Netcompany Banking Services.

5.3 Written reports are submitted through Plesner's Whistleblower Portal which can be found on Netcompany's website.

5.4 Written reports are received by two lawyers at Plesner Law Firm. Plesner will make a legal capacity assessment of the persons of the whistleblower unit who are able to process the report, after which the report will be forwarded to the relevant persons (hereinafter referred to as "**Case Managers**") at Netcompany Banking Services. Before forwarding the report, Plesner will assess whether the report falls within the scope of application of the Arrangement.

5.5 It is only possible to submit written reports under the Arrangement.

5.6 The whistleblower unit will treat all written reports as confidential.

5.7 The Case Managers appointed to receive and follow up on the reports are subject to a duty of confidentiality regarding the information contained in the reports.

6 ANONYMITY

6.1 Netcompany Banking Services encourages the Whistleblower to state his or her name when submitting a report so that the Case Managers are able to ask clarifying questions and subsequently provide feedback on the further course of the investigation. However, anonymous communication between Plesner and a Whistleblower who chooses to be anonymous is possible (see sections 6.4 and 6.5).

6.2 If the Whistleblower chooses to submit an anonymous report, it is recommended - to ensure full anonymity - that the Whistleblower uses a private PC or, for instance, a PC located at a public library.

6.3 Plesner will make a communication module available, allowing the Whistleblower to communicate with Plesner for the purpose of providing additional information about the reported matter, which Plesner will then pass on to the Case Managers.

6.4 If the Whistleblower chooses to submit an anonymous report, it is possible for the Whistleblower to communicate with Plesner through the communication module. The Whistleblower can provide additional information to Plesner through the communication module and remain anonymous. In connection with the reporting, a one-off code is generated which, in order to safeguard the anonymity, cannot be re-created. Therefore, it is **important** that the Whistleblower keeps the code and remembers to log on the communication module to communicate with the whistleblower unit.

6.5 The communication module can be accessed through the above-mentioned link under the Arrangement (see section 5.3) to log on the communication module. If the Whistleblower chooses to be anonymous, it is important that the Whistleblower regularly enters the communication module to check whether Plesner has asked any questions. If the Whistleblower is anonymous, Plesner is not able to come into contact with the Whistleblower in any other ways, for instance to inform the Whistleblower that additional questions etc. have been submitted.

7 INFORMATION TO THE WHISTLEBLOWER

7.1 The Whistleblower will receive:

- an acknowledgement of receipt of the report within three (3) days of that receipt; and
- feedback soonest possible and in principle within three (3) months from the acknowledgement of receipt of the report.

7.2 "Feedback" means a notification about the measures taken by Netcompany Banking Services to assess the correctness of the allegations made in the report and, where relevant, to counter the reported offence. The feedback provided by the whistleblower unit must, at any time, observe the rules under data protection law, which may entail limitations in relation to the contents of the feedback to the Whistleblower.

7.3 Depending on the circumstances, an extension of the timeframe for the feedback may be required, where necessary due to the specific circumstances of the case, in particular the nature and complexity of the report, which may require a lengthy investigation. If this is the case, the Whistleblower must be notified in this respect.

8 INFORMATION TO AND PROTECTION OF THE PERSON CONCERNED

8.1 After a preliminary investigation has taken place and all relevant evidence has been secured, the person concerned, i.e., the person reported under the Arrangement, will for instance be informed about:

- the identity of the Case Manager(s) responsible for the investigation of the report; and
- the issues of the report.

8.2 Pursuant to the Whistleblower Act, the person concerned is entitled to protection of his or her identity during the case management and has a right to effective defence.

8.3 Under certain circumstances, the person concerned will also have the right of access to information about the Whistleblower's identity where necessary for the person concerned to exercise his or her right to an effective defence (see section 9.6).

8.4 Otherwise, Netcompany Banking Services observes the rights of the person concerned under the General Data Protection Regulation. Reference is made to Netcompany Banking Services' Privacy Policy for the Arrangement, which can be found on Netcompany's website, containing further information on the processing of personal data and the rights of the data subject.

9 PROTECTION OF THE WHISTLEBLOWER

9.1 Pursuant to the Whistleblower Act, the Whistleblower is protected against retaliation when submitting a report to the Arrangement. Such protection only applies if the following conditions are fulfilled:

- The person submitting the report meets the conditions to be considered a whistleblower (see section 2).
- The Whistleblower had reasonable grounds to believe that the reported information was correct at the time of reporting and that the reported information falls under the scope of application of the Whistleblower Act (see section 3.4).

9.2 "Retaliation" means unfavourable treatment or unfavourable consequences as a reaction to a report. This may be suspension, dismissal, demotion, or equivalent measures.

9.3 If the Whistleblower submits a report in bad faith and is fully aware of the fact that the reported information is not correct, the Whistleblower is not protected against retaliation. Depending on the circumstances, the Whistleblower can be sanctioned with a fine if he or she has deliberately submitted false reports. If the Whistleblower is employed by Netcompany Banking Services**,** it may also have employment-related consequences, entailing inter alia the summary dismissal of the Whistleblower.

9.4 In addition to the group of persons mentioned in section 2.1, the protection described in this section 9 also applies to the following persons or entities:

1) Intermediaries, i.e. a natural person assisting the Whistleblower with the reporting process in a work-related context.
2) Third parties who are connected to the Whistleblower and who risk being subject to retaliation in a work-related context (e.g., a colleague).
3) Undertakings and authorities which the Whistleblower owns or works for or is otherwise connected with in a work-related context (e.g., an undertaking owned by the Whistleblower).

9.5 Information about the identity of the Whistleblower or any other information that directly or indirectly may reveal the Whistleblower's identity will only be disclosed to other persons than the whistleblower unit after having obtained prior explicit consent from the Whistleblower.

9.6 However, information on the Whistleblower's identity may be disclosed without consent to other public authorities where this is necessary for the prevention of offences (e.g., a criminal act that has not yet been committed), or with a view to safeguarding the rights of defence of the persons concerned. The right of defence of the person concerned will, inter alia, be relevant in connection with the right of information of the person concerned in criminal proceedings.

9.7 If the identity of the Whistleblower is disclosed without consent, the Whistleblower will be informed accordingly and be provided with the grounds for the disclosure, unless such information would jeopardize the related investigations or judicial proceedings. Concerning the disclosure of the Whistleblower's identity, reference is also made to section 8.3.

9.8 The identity of the Whistleblower may also be revealed in connection with legal proceedings regarding the reported matter.

9.9 If the Whistleblower has deliberately revealed his or her identity in connection with a publication of the reported matter, the special considerations regarding the protection of the Whistleblower's identity are not applicable. In such cases, information on the Whistleblower's identity may be passed on pursuant to the rules under the General Data Protection Regulation.

9.10 Other information from the report, i.e., information not revealing the Whistleblower's identity, will only be disclosed to persons outside the whistleblower unit as part of a follow-up on the report or for the purpose of preventing a potential offence in relation to the issues described in section 3.4.

9.11 If the whistleblower unit collects additional information in connection with the processing of the report, such information is not covered by the provisions of the Whistleblower Act, such as the special duty of confidentiality. Such information will thus be subject to the general rules on the person concerned's right of access pursuant to Section 22 of the Danish Data Protection Act. Therefore, the duty of confidentiality only pertains to the information contained in the reports.

10 EXTERNAL WHISTLEBLOWER SYSTEMS

10.1 A Whistleblower who intends to submit a report under the Arrangement may instead - if the conditions are otherwise fulfilled in this respect - choose to file the report through the external whistleblower system of the Danish Data Protection Agency, e.g., if the Whistleblower fears retaliation. The external whistleblower system of the Danish Data Protection Agency can be reached through https://whistleblower.dk/indberet.

10.2 It is emphasized that the Whistleblower is free to choose to submit a report through the Arrangement or through the external whistleblower system of the Danish Data Protection Agency.

11 DATA SECURITY AND DATA STORAGE

11.1 Netcompany Banking Services will register all reports received under the Arrangement. The registration takes place in accordance with the provisions of the Whistleblower Act. Reports are stored as long as necessary and proportionate in order to comply with the requirements imposed by Danish law.

11.2 Netcompany Banking Services and Plesner will process all information reported through the Arrangement, including information on persons reported through the Arrangement, in accordance with applicable law in force at any time.

11.3 All reports will be stored properly, and it will only be possible for relevant persons of the whistleblower unit to access the information.

11.4 If the report is falling outside the scope of the Arrangement, the Whistleblower will be informed in this respect, and the report will be closed in the Arrangement. In case a report falls outside the scope of the Arrangement - but does otherwise not appear to be unfounded, the whistleblower unit will obtain the Whistleblower's consent to forward the report to Netcompany Group's Chief People Officer. Before giving his or her consent, the Whistleblower will be informed of any possible consequences that may arise in this respect.

11.5 In principle, reports will be deleted from the Arrangement 45 days after Netcompany Banking Services has finalized the processing, unless Netcompany Banking Services has legitimate reasons to continue the storage, e.g., if required by other legislation, or if there is reason to believe that the report may be corroborated by subsequent reports on the same matter.

11.6 If the matter is reported to the police or another authority, the reported case will be closed in the Arrangement immediately after the case has been closed by the authorities in question.

11.7 If - on basis of the collected data - a disciplinary sanction is implemented against the person concerned, or if there are other grounds justifying and requiring the continued storage of the data on the person concerned, such data will be stored, where an employee is involved, in the employee's personnel file.

11.8 Otherwise, the information is stored in accordance with Netcompany Banking Services' deletion policy.

12 QUESTIONS

12.1 If you have any questions regarding this Whistleblower Policy, you are welcome to contact Anders Poulsen, General Counsel (Legal) at apo@netcompany.com or +45 45 30 47 45 72.

13 REVIEW AND AMENDMENT

13.1 The Board of Directors shall annually review, and if relevant update, the Whistleblower Policy.

14 PUBLICATION

14.1 The Whistleblower Procedures will be published on Netcompany's website.

This Whistleblower Policy has been updated on or before: *October 2025*