BNP Paribas Netherlands

PERSONAL DATA PROTECTION NOTICE FOR THE WHISTLEBLOWING PROCESS

This Data Protection Notice provides you with transparent and detailed information relating to the protection of your personal data processed by BNP Paribas SA or an entity of BNP Paribas located in the Netherlands ("**BNP Paribas**") referred to as ''we'' or "us". Please see Appendix 1 for an overview of the BNP Paribas entities established in the Netherlands that use this notice to inform you about the processing of your personal data.

The purpose of this Data Protection Notice is to inform you of the personal data we collect about you; the reasons why we use and share such data; how long we keep the data; what your rights are (as to the control and management of your data) and how you can exercise your personal data rights.

This Notice is drafted based on all applicable laws and regulations, including Dutch law.

Processing operations in the context of whistleblowing:

Personal data are processed to:

- collect and process whistleblowing alerts;
- carry out the necessary checks, investigations and analyses in the context of the whistleblowing process;
- define the follow-up to be given to the whistleblowing report/alert;
- ensure the protection of data subjects; and
- exercise or defend legal rights.

Which types of alerts could be escalated? The alerts could be escalated to whom?[1]

Under our whistleblowing system, the whistleblower can report several types of Alerts:

- Compliance/Professional ethics alerts can be routed to:
  - BNP Paribas SA as the "Group"
  - Business Line/Function in which the violation took place
  - Local entity in which the violation took place
- Financial Sanctions alerts are automatically routed to the dedicated group channel at BNP Paribas SA
- HR/Respect for persons alerts are routed to:
  - Business Line/Function to which the person(s) in question is assigned.

Therefore, depending on the location of the whistleblower, the entity to which the whistleblower routes the Alert and the type of Alerts, the alert could be handled by BNP Paribas SA and/or any other entity of the BNP Paribas Group. Consequently, BNP Paribas SA and the entities relying on the Navex tool to ensure a consistent approach are all acting as data controller. For entities established in the

[1] Please refer to appendix 2 for an overview of HR and Compliance related alerts.

European Economic Area (EEA), these controllers are acting as joint controllers. The EEA includes all EU countries plus Liechtenstein, Norway and Iceland.

1. ARE YOU SUBJECT TO THIS NOTICE?

This notice is addressed to all natural persons (you) whose personal data are processed within the framework of the whistleblowing alert including mainly:

- The whistleblowers regardless of the channel of the alert
- Targeted persons
- Persons requested to provide information on the alert (witnesses for instance)
- Persons mentioned in the investigation/alert

2. WHICH PERSONAL DATA DO WE COLLECT AND FURTHER PROCESS?

Personal data (i.e. any information that identifies or allows BNP Paribas to identify you) collected and otherwise processed through the Navex tool, or collected through other media (email, form, phone, in person, instant messages) and any other data held by BNP Paribas or transmitted by a third party will generally be related to:

- identity and contact details of the whistleblower: **only** if the alert mentions such information. The whistleblower could decide to report the alert anonymously or not. If the alert is made anonymously, we will not collect any of the above data (neither identity nor contact details);
- facts (suspected or witnessed) relating to a natural person mentioned in the alert, including any piece of information or evidence provided with the alert;
- identity, functions and contact details of people mentioned in the alert (identity of the targeted person, the identity of any witnesses to the alleged misconduct or other third parties involved in the case, persons subject to the alert, persons involved in the alert management, enabler persons in connection with the whistleblower);
- if the alert is made verbally: a recording of the conversation in a permanent and retrievable form or a complete and accurate written account of such conversation;
- elements relating to a natural person collected in the context of investigation, which includes any information needed to investigate the alleged misconduct;
- reporting elements on investigation operations; and
- actions to be taken/already taken in relation with people mentioned in the alert to either protect them and/or stop the wrongdoings.

In case the information is needed for the processing of the alert, we may receive and otherwise process personal data related to your ethnic origins, political opinions, religious or philosophical beliefs, data concerning your sexual orientation, biometric and genetic information, health data and information on criminal convictions and offences. Also, we may process this data if it is made public by you and necessary for the purposes for which it is intended.

In any case, received and collected personal data will only be stored and otherwise processed if this is strictly necessary to understand, verify, clarify, and resolve alerts.

3. WHO DO WE COLLECT PERSONAL DATA FROM?

To process the alert and investigate the alleged facts, personal data are collected directly from the whistleblower, the concerned BNP Paribas entity and in certain circumstances other sources. Personal data is sometimes collected (if related to the alert) from public sources, such as:

- publications/databases made available by official authorities
- websites/social media pages of legal entities or business clients containing information that you have disclosed (e.g. your own website or social media page when it is public and authorized by terms and conditions of the social network)
- public information, such as information published in the press

Personal data may also be collected from third parties, such as:

- other BNP Paribas Group entities
- law firms
- our clients
- our business partners
- external Investigations experts
- witnesses

4. ON WHAT LEGAL GROUND(S) DO WE PROCESS YOUR PERSONAL DATA?

4.1 To comply with our regulatory obligations

In order to comply with our legal obligations as set out in the Dutch Whistleblower Protection Act, all internal and external staffs are able to raise an alert concerning:

- a breach or a risk of breach of Union law; or
- an act or omission in which the public interest is at stake in:
    - a breach or a risk of breach of a legal requirement or internal rules which contain a specific obligation established by BNP Paribas on the basis of legal requirement, or
    - a danger to the safety of persons, to damage to the environment or to the proper functioning of BNP Paribas as a result of improper acts or omissions.

If you report an alert concerning another type of wrongdoing (not mentioned above) or if you choose to report your alert to another entity than the entity where the violation took place, the legal basis for the processing of your personal data is our legitimate interest.

4.2 To fulfil our legitimate interest

BNP Paribas is particularly committed to the development and well-being of its employees and to provide them with a motivating work environment in which everyone is treated with respect, dignity and fairness. Our commitment is to report any proven or suspected violation of the BNP Paribas Code of Conduct in connection with the request made by employees. BNP Paribas wants also to strengthen

the protection of whistleblowers, in particular by allowing them to report alert(s) and acts of retaliation due to this alert, through a direct access channel ensuring their anonymity.

- In order to do so, we will process personal data in order to collect all whistleblowing alerts, carry out the necessary checks, investigations and analyses defining the follow-up to be given to the report and ensuring the protection of data subjects and exercise or defend legal rights.
- We collect personal data to process alerts relating to any unethical behavior and any violation of the BNP Paribas Code of Conduct.

The legal basis for the processing is represented by the pursuit of the legitimate interest of the BNP Paribas or third parties, represented by the right to defense itself but also its employees and by the interest in guaranteeing the effectiveness and efficiency of our internal control, also in order to prevent and effectively combat fraudulent, illegal or irregular conduct.

In any case, our legitimate interests remain proportionate, and we verify according to a balancing test, that your interests and fundamental rights are preserved. Should you wish to obtain more information about such balancing test, please contact us using the contact details in Appendix 1 of this Notice.

4.3 Based on your prior consent

When an alert is made through a verbal conversation (either by phone or face-to-face), our legal obligations require making either a recording or a transcript of the conversation. Recording the conversation is only allowed if you provide us with your prior consent. When a transcript is made, you will be given the opportunity to review, correct and sign it for validation.

Please note: when you provide your consent for recording of the conversation used to report an alert, this consent only relates to the recording. Should you exercise your right to withdraw your consent (see section 8.7 for more information), this will only affect the recording and not the whistleblowing process itself.

4.4 Specific case of sensitive data and criminal data

In the context of alert management, we may process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data or data concerning a natural person's sex life or sexual orientation, only if:

- the processing is necessary for the establishment, exercise or defense of legal claims
- the processing is necessary for reasons of substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Moreover, we may process personal data relating to criminal convictions and offences, or related security measures only under the control of official authorized staff members of BNP Paribas or when

the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

5. WHO HAS ACCESS TO YOUR PERSONAL DATA AND TO WHOM IS IT DISCLOSED?

In BNP Paribas whistleblowing platform, alerts will be processed by either HR (human resource-related alerts) or Compliance (all remaining alerts). An alert could be reported alternatively through 3 channels, depending on the whistleblower's choice:

- At entity level
- At business line level
- At Group level

5.1 Sharing of information within the BNP Paribas Group

To fulfill the purposes set out above, we may share your personal data with internal duly authorized whistleblowing referents (HR / Compliance), in order to conduct investigations, on a need-to know-basis. For the sole purposes of checking or processing the alert, personal data may also be shared with other BNP Paribas entities, provided that access authorizations are documented and that access to the various processing operations is subject to traceability measures.

5.2 Disclosing information outside the BNP Paribas Group

In order to fulfil some of the purposes described in this Data Protection Notice, we may disclose from time to time your personal data to third parties, including:

- other service providers and their authorized subcontractors performing services on our behalf;
- local or foreign financial, tax, administrative, criminal or judicial authorities, regulators, arbitrators or mediators, law enforcement, state agencies or public bodies, where we are required to disclose personal data pursuant to:
    - their request
    - defending or responding to a matter, action or proceeding
    - complying with a regulation or guidance from a competent authority
    - certain regulated professionals such as lawyers, notaries, medical staff for the processing of an alert under specific circumstances (e.g. litigation, audit, etc.).

The transfer of personal data to third parties pursuant to this section 5.2 is subject to the prior signing of a Non-Disclosure Agreement.

6. INTERNATIONAL TRANSFERS OF PERSONAL DATA

During the processing of your personal data in the context of the whistleblowing process, we may transfer your personal data to recipients outside the European Economic Area (EEA). It concerns possible transfers to the following recipients:

- The whistleblowing tool is managed by our external service provider, Navex Global UK Limited (Navex). Some of Navex's support teams are located in the United States (US). When these support teams are engaged, your personal data may be transferred to the US.
- Whistleblowing alerts covering violations of sanctions or embargoes are escalated to the compliance team of BNP Paribas New York Branch. This escalation results in a transfer of your personal data to the US.

We have appropriate safeguards in place to protect your personal data. The contracts with both recipients in the US contain Standard Contractual Clauses (SCCs) to ensure an adequate level of protection. To receive a copy of these SCCs and/or more information about them, you can send a written request as outlined in section 10 of this notice.

7. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We will retain your personal data for as long as it is required to comply with applicable legislation or to achieve the purpose for which they were collected or otherwise processed. Specifically, the following retention periods are applied:

- Personal data related to inadmissible whistleblowing reports will be erased no later than 2 monhts from the date of the decision to close the alert.
- Personal data related to admissible whistleblowing reports will be erased 5 years after the communication of the final outcome of the whistleblowing procedure, unless retention for a longer period is required for claim or litigation purposes
- Personal data related to admissible whistleblowing reports related to sanctions will be erased 10 years after the closure of the alert.

8. WHAT ARE YOUR RIGHTS AND HOW CAN YOU EXERCISE THEM?

You have specific rights as a 'data subject' under Chapter III of the General Data Protection Regulation GDPR[2], in particular the right to access, your personal data and to rectify them in case your personal data is inaccurate or incomplete. Where applicable, you have the right to erase your personal data, to restrict the processing of your personal data and to object to the processing.

If you wish to exercise the rights listed below, please send a letter or e-mail to your contact as referred in the contact list available in Appendix 1 of this Data Protection Notice. You can exercise your rights with the entity to which you have chosen to report the alert.

8.1 You can request access to your personal data

If you wish to have access to your personal data, we will provide you with a copy of the personal data you requested as well as information relating to their processing.

8.2 You can ask for the correction of your personal data

Where you consider that your personal data is inaccurate or incomplete, you can request that such

[2] Regulation (EU) 2016/679

personal data be modified or completed accordingly.

8.3 You can request the deletion of your personal data

If you wish, you may request the deletion of your personal data, to the extent permitted by law.

8.4 You can object to the processing of your personal data based on legitimate interests

If you do not agree with a processing activity based on a legitimate interest, you can object to it, on grounds relating to your particular situation, by informing us precisely of the processing activity involved and the reasons for the objection. We will cease processing your personal data unless there are compelling legitimate grounds for continuing to do so or it is necessary for the establishment, exercise or defence of legal claims.

8.5 You can request the restriction of the processing of your personal data

If you wish, you may request the (temporary) restriction of the processing of your personal data, to the extent permitted by law.

8.6 You can request the portability of your personal data

Where legally applicable, you have the right to have the personal data you have provided to us be returned to you or, where technically feasible, transferred to a third party.

8.7 You can withdraw your consent

Where you have given your consent for the processing of your personal data, you have the right to withdraw your consent at any time.

If you wish to exercise the rights listed above, please send a letter or e-mail to your contact as referred in the contact list in Appexdix 1 of this Data Protection Notice.

8.8 How to file a complaint with your Data Protection Authority

In addition to the rights mentioned above, you may lodge a complaint with the competent supervisory authority , which is usually the one in your place of residence.

9. HOW CAN YOU KEEP UP WITH CHANGES TO THIS DATA PROTECTION NOTICE?

In a world of constant regulatory and technological changes, we may need to regularly update this Data Protection Notice. We invite you to review the latest version of this Data Protection Notice online on this website (the website you are visiting now).

10. HOW TO CONTACT US?

If you have any questions relating to our use of your personal data under this Data Protection Notice, you can contact our Data Protection Officer using the contact details below:

BNP Paribas
Data Protection Officer
Postbus 10042

1001 EA Amsterdam

Email: bnpp.nl.dpo@bnpparibas.com.

Appendix 1 BNP Paribas Entities covered by this Data Protection Notice

Controller	Contact details
Cardif-Assurances Risques Divers S.A., NL	- HR: nlhrm@bnpparibascardif.com - Compliance: nl_compliance@bnpparibascardif.com
Cardif Assurance Vie S.A., NL branch	
BNP Paribas Cardif B.V.	

Appendix 2 Overview of HR and Compliance related alerts

Type of alert on HR related	Type of alert on Compliance related
Professional behaviors contrary to the provisions relating to "Respect for persons" (e.g. discrimination, harassment, etc.); these reports fall under the Group HR Policy (RHG0063)	Acts of corruption and influence peddling or any other infringement pertaining to probity
Infringement of the rules of professional ethics (e.g. conflict of interests)	Infringement of the rules of financial security (e.g. money laundering, terrorist financing, non-compliance with sanctions and embargoes regulations)
Violation of human rights and fundamental freedoms, damage to the health and safety of persons or to the environment committed by a Group's Entity or by its supplier or the subcontractor of a supplier within the framework of an established commercial relationship with the Group or one of its Entities (e.g. suspicion about the use of child labor by the sub-contractor of a supplier)	Acts of fraud (e.g. use of erroneous information in the setting up of a credit file or misappropriation of funds). However, frauds or suspicions of fraud identified in internal control activities must not be reported in the whistleblowing framework, but according to the usual declaration or reporting processes. The same applies to cases of purely external fraud (e.g. bank card fraud, phishing, etc.)
	Anti-competitive practices (e.g. abuse of dominant position)
	Breach of market integrity (e.g. market abuse)
	Infringement of the rules for the protection of interests of clients (e.g. charging commissions without informing the client, undue or excessive arbitration in an account under delegated management, etc.)
	Unauthorized communication of confidential information, theft or leakage of data
	A serious violation of BNP Paribas policies regarding suppliers.
	A serious violation of BNP Paribas policies regarding the use of social media.