



# Whistleblower Protection Policy - Global

<b>Category:</b>	Global ▾		
<b>Type:</b>	Policy ▾		
<b>Applicability:</b>	Global - Coinbase, Global Inc. ▾		
<b>Document Classification:</b>	Internal ▾	<b>Unique Identifier No:</b>	254974
<b>Version:</b>	v4.3	<b>Version Effective Date:</b>	April 1, 2024
<b>Issuing Department:</b>	Legal ▾		
<b>Contact:</b>	Direct any questions regarding this Document to the Chief Legal Officer.		
<b>Document Summary:</b>	This policy establishes global standards and mechanisms for employees to report known and suspected unlawful or improper activities without fear of retaliation.		

## Table of contents

<b>1. Overview</b>	<b>2</b>
<b>2. Background</b>	<b>2</b>
<b>3. Applicability</b>	<b>3</b>
<b>4. Definitions</b>	<b>3</b>
<b>5. Statement</b>	<b>3</b>
a. What Violations Should be Reported	3
b. How to Report Violations - Whistleblowing Reporting Channel	4
c. Option for Anonymity Policy Statement	5
d. Protection of Whistleblowers	6
e. No Retaliation Policy Statement	6
<b>6. Investigation</b>	<b>7</b>
<b>7. Roles and Responsibilities</b>	<b>9</b>
<b>8. Reporting of Non-Compliance</b>	<b>9</b>
<b>Appendix A - Ireland Supplement</b>	<b>10</b>
<b>Appendix B - UK Supplement</b>	<b>13</b>
<b>Appendix C – Germany Supplement</b>	<b>15</b>

## 1. Overview

Coinbase Global Inc. and its global subsidiaries and affiliates, including Coinbase, Inc. and Coinbase Custody Trust Company, LLC (collectively “Coinbase”) expects its employees, contractors, consultants, agents, representatives, officers and members of the Coinbase board of directors (collectively referred to as “Company Member”) worldwide to observe high standards of business and personal ethics in the conduct of their duties and responsibilities. To that end, it has an open door policy and suggests that the Company Member share their questions, concerns, suggestions or complaints with someone who can address them properly and timely, without fear of reprisal or retaliation of any kind.

We have established this Whistleblower Protection Policy (“Policy”) to enable employees and other service providers to report any activity that is unlawful or otherwise violates our policies so that we can investigate and resolve potential violations as quickly and efficiently as possible.

You are encouraged to use the guidance provided by this Policy to report all known and suspected improper activities as described below. This Policy is designed to provide you with a confidential or anonymous method for reporting any improper activities.

You should understand, however, that nothing in this Policy (nor any other Coinbase policy or agreement) limits, impedes, or restricts your ability to contact, report to, or file a charge or complaint with, the Securities and Exchange Commission, or any other federal, state, or local government agency or commission (“Government Agencies”). This Policy also does not limit your ability to participate and/or assist in any investigation or proceeding that may be conducted by any Government Agencies, including providing documents or other information without notice to Coinbase. Nothing in this Policy limits your right to seek and/or receive an award for information provided to any Government Agencies or prohibits you from providing truthful information in response to a subpoena or other legal process.

If you make a whistleblower report pursuant to this Policy, or to a Government Agency, we have a responsibility to protect you, including not disclosing your identity (unless required or permitted by law) and making sure you are not subject to retaliation. This Policy is available to all Company Members internally and anyone at [coinbase.ethicspoint.com](https://coinbase.ethicspoint.com).

## 2. Background

This Policy has been adopted to supplement the [Global Code of Business Conduct and Ethics](#) and the appropriate sections of each subsidiaries’ employment policies by further emphasizing the importance of combating ethical violations in the workplace and to provide Company Members with access to a mechanism for escalating unethical behavior in confidence and without fear of retribution.

Coinbase has developed this Policy, taking into consideration the Consumer Financial Protection Act of 2010 (CFPA), Section 1057 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, 12 U.S.C. § 5567, Guidance from the New York Department of Financial Services, Guidance of Whistleblowing Programs and any other applicable local laws or regulations, including but not limited to the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law and the Protected Disclosures (Amendment) Act 2022.

### **3. Applicability**

This Policy applies to Coinbase employees, applicants, interns, contractors, consultants, agents, representatives, officers, and members of the Coinbase board of directors (the “Board”) (collectively, “you” or “Company Members”).

### **4. Definitions**

**Protected Disclosure** – A disclosure of relevant information, which in the reasonable and good faith belief of a Company Member or other eligible whistleblower tends to show one or more relevant wrongdoings which comes to the attention of that individual in connection with their relationship with the Company.

**Whistleblowing** - The reporting of information or concerns, by one or more individuals or entities, that are reasonably believed in by such individual(s) or entity(s) to constitute illegality, fraud, unfair or unethical conduct, money laundering, financial irregularities, mismanagement, abuse of power, unsafe or dangerous activity, or other wrongful conduct, including any conduct that may affect the safety, soundness, or reputation of Coinbase.

### **5. Statement**

Coinbase is committed to facilitating honest, open communications and compliance with applicable laws and regulations. Our [Global Code of Business Conduct and Ethics](#) guides our everyday conduct. We have a professional responsibility to speak up and report unethical behavior. Coinbase will take all reports made under this Policy seriously.

#### **a. What Violations Should be Reported**

We ask that you follow this Policy to report good faith concerns regarding known or suspected violations of any of the following:

1. laws, governmental rules or regulations;

2. any applicable accounting rules or principles, internal accounting controls, recordkeeping obligations or auditing matters; or
3. any Coinbase policies (including our [Global Code of Business Conduct and Ethics](#) and its associated policies).

Examples of reportable conduct include but are not limited to:

- illegal conduct, such as theft, violence, discrimination, harassment and criminal damage against property;
- fraud, money laundering or misappropriation of funds;
- offering or accepting a bribe;
- financial irregularities;
- actions that endanger the health and safety of an individual;
- failure to comply with legal or regulatory requirements;
- actions which are intended to conceal or destroy information tending to show any matter falling within any of the points listed above; and
- engaging in retaliation against a person who has made a disclosure or is believed to have made or be planning to make a disclosure.

Reportable conduct generally does not include personal work-related grievances, including an interpersonal conflict between you and another Company Member or a decision relating to your employment or assignment. Personal work-related grievances do not qualify for protection under the Whistleblower Laws or this Policy and should be reported to Employee Relations or your HR Business Partner. Of course, reports related to Coinbase's existing policies on equal opportunity, anti-bullying and anti-harassment policy are reportable conduct.

Keep in mind that your reporting obligation includes complaints or reports you might get from your direct reports if you are a manager and people outside of Coinbase and complaints regarding third parties who provide services to us.

#### **b. How to Report Violations - Whistleblowing Reporting Channel**

If you believe that any violation has occurred or is occurring or you have a good faith concern regarding conduct that you reasonably believe may be a violation, you are encouraged to promptly take one or more of the following steps:

1. Report the known or suspected violation to your manager and/or supervisor or Country Head.
2. If you would prefer to speak to someone other than your manager or supervisor, you can report concerns to our Chief Legal Officer or their authorized designee or, if no

such employee at Coinbase has the Chief Legal Officer title, the most senior in-house attorney of Coinbase (the “Whistleblower Reporting Officer” or the “WRO”).

3. You can also reach a member of human resources by emailing [peopleops@coinbase.com](mailto:peopleops@coinbase.com).
4. Alternatively, ***you may report the known or suspected violation confidentially and anonymously by:***
  - i. Calling our compliance hotline toll-free at 1-844-564-3372 in the United States (international numbers available at [coinbase.ethicspoint.com](https://coinbase.ethicspoint.com)); or
  - ii. Online at [coinbase.ethicspoint.com](https://coinbase.ethicspoint.com).

You may also choose to directly contact, report to, or file a charge or complaint with, a Government Agency.

Reports can be raised verbally in the first instance but we encourage you to follow-up a verbal report in writing. In the case of a report made verbally, and upon request of the reporting person, the report can be raised by means of a physical meeting with the employer or designated person, within a reasonable period from the making of the request.

If you report using the above internal procedures, your report will automatically be directed to our WRO or their designated representative. In accordance with applicable law, reports will be appropriately communicated to the Board or appropriate committee (e.g., the Audit and Compliance Committee). Human resources complaints that do not involve accounting, internal accounting controls and auditing matters will be reported to our employee relations or human resources team.

You are encouraged to provide as much detail as possible regarding the subject matter of the complaint or concern. In order to better respond to any reported concerns, it would be helpful if you provide your telephone number and other contact information when making the report. However, if you prefer to remain anonymous, you may report a concern without disclosing your name or position.

If you wish to report a matter directly to our Audit and Compliance Committee, you may use the process above and indicate that the report should be escalated to the Audit and Compliance Committee. The Audit and Compliance Committee will take whatever steps it deems necessary to respond to a report that they receive, including whether to refer the matter to our WRO for investigation.

### **c. Option for Anonymity Policy Statement**

It is Coinbase’s policy to provide Company Members the means to report any perceived unethical or illegal behavior in a confidential manner. Coinbase will protect the confidentiality and anonymity of individuals where required by law and consistent with the need to carry out a thorough and comprehensive investigation. As discussed above, anonymous reports may be submitted online at

[coinbase.ethicspoint.com](https://coinbase.ethicspoint.com) or through the reporting hotline. Phone numbers for the reporting hotline are also available on the EthicsPoint site. However, anonymity may make it more difficult for us to investigate the issue or take the action we would like to take. By letting us know who you are, we can contact you directly to discuss your concerns which will help us investigate the report more efficiently and thoroughly, as well as protect you from any retaliatory actions.

#### **d. Protection of Whistleblowers**

Coinbase recognises that encouraging Company Members or other eligible whistleblowers to make disclosures benefits Coinbase. To encourage reporting, Coinbase strives to maintain an appropriate level of confidentiality of the investigation, including the identity of the whistleblower, in all workplace investigations (even where anonymity has not been requested). However, the investigative process necessarily requires discussing the report with various people. Additionally, there may be laws, rules, or regulations that apply to Coinbase that require reporting of certain violations to outside regulators or law enforcement. With this in mind, Coinbase will maintain confidentiality of the report and investigation subject to the below exceptions:

- i. If disclosing such information is necessary for:
  - the effective investigation of the relevant wrongdoing concerned;
  - the prevention of serious risk to the security of the State, public health, public safety, or the environment;
  - the prevention of crime or prosecution of a criminal offence; or
- ii. If it is otherwise necessary in the public interest or is required by any law, rule, or regulation.

When making a report, you are expected to have reasonable grounds or a good faith belief to suspect the information you are disclosing is true. You will not be subject to discipline or penalty, however, if the information turns out to be incorrect. Of course, you should not make a report in bad faith or that you know to be untrue.

#### **e. No Retaliation Policy Statement**

It is Coinbase's policy not to tolerate or take any retaliatory actions, including discharge, harassment, or discipline, against any Company Member who makes a good faith report of a reasonable belief that there has been a violation of law or Coinbase policy, including but not limited to a misappropriation of funds, even if an investigation shows that there has not been a violation.

In some cases, federal, state, and/or local law provides that retaliatory action for reporting unlawful activity is illegal. Company Members who object to or refuse to participate in a policy, practice or activity that is unlawful, fraudulent, criminal or incompatible with a clear mandate of public policy

concerning the public health, safety or welfare or protection of the environment are also protected from retaliatory action.

We do not permit any form of intimidation or retaliation by any employee, contractor, subcontractor or agent of Coinbase against you because of any lawful act done to:

1. provide information or otherwise assist in an investigation of conduct you reasonably believe is a violation of any law, rule, or regulation, or of any Coinbase policy; or
2. testify, participate in or otherwise assist in a proceeding filed or to be filed relating to a violation of any law, rule or regulation.

Any Company Member who engages in retaliatory conduct will be disciplined, up to and including termination. Outside of Coinbase and depending on the applicable law in your jurisdiction, there may be potential criminal penalties.

Nothing in this Policy in any way prohibits or is intended to restrict or impede non supervisory employees from discussing the terms and conditions of their employment with co-workers or union representatives/exercising protected rights under Section 7 of the National Labor Relations Act/exercising protected rights to the extent that such rights cannot be waived by agreement, or otherwise disclosing information as permitted by law.

## **6. Investigation**

As soon as reasonably possible, Coinbase will investigate and respond to all reported complaints regarding potential violations and take appropriate action(s). Upon learning of conduct requiring further review, qualified investigators will complete thorough investigations in a timely and impartial manner in accordance with Coinbase's Internal Workplace Investigations Policy and process.

### **a. Procedures for Investigating Concerns / Complaints**

The assigned investigator will keep a record of being made aware of the Company Member or other eligible whistleblower's concern and of the subsequent action(s) taken. Coinbase recognises that a disclosure is presumed to be a Protected Disclosure until the contrary is proven and the motivation for making the disclosure is irrelevant.

The investigator may choose to investigate the matter themselves or request that the matter be investigated by another party, either internally or externally.

While the particular circumstance of each Protected Disclosure may require different investigation steps, for each concern raised the investigator will:

- Follow a fair process;



- Send the reporting party a written acknowledgement of receipt of their concern as soon as practicable, but not later than within 7 days of receipt;
- Carry out a preliminary inquiry, including meeting with the reporting party if that is requested, to determine whether a full investigation is necessary and/or if it needs to be referred to an outside body (e.g. a Regulator or The Central Bank of Ireland, An Garda Síochána).
- If, on completion of the preliminary inquiry, the concern is judged to be without *prima facie* substance or merit, the concern may be dismissed and the whistleblower will be informed of this decision;
- Ensure that all investigations are undertaken as quickly as possible without affecting the quality and depth of those investigations, generally not exceeding 3 months from acknowledgement of receipt of the protected disclosure;
- Maintain confidentiality and maintain compliance with GDPR;
- Keep, as appropriate, all relevant parties informed as to the progress of the investigation and as to when it is likely to be concluded;
- Draft a written report detailing the complaint and findings and determining the validity of the complaint; and
- Provide the written report to the person who commissioned it.

When investigating a complaint, consideration is given to identifying and managing potential conflicts of interest. This includes scrutiny for possible conflicts involving senior management and the Board. A conflict may arise if an employee who handles or manages a whistleblowing matter, works on the investigation of a matter, or is among the group to whom the matter will be escalated or reported:

- a. is the subject of a complaint;
- b. is a possible witness to or source of information about the conduct at issue in a complaint; or
- c. supervises, reports to, or has some other close relationship to the subject of the allegation or the whistleblower (if known).

If you are making a disclosure concerning an executive or member of the Board, you may report as follows:

- CEO and executive Leadership - report to the Chair of the Board
- Board member - report to the Chair of the Board
- Chair of the Board - report to the Deputy Chair of the Board

Reasonable conclusions will be reached based upon the evidence collected. If misconduct is found, Coinbase will take appropriate remedial measures in response. Corrective action may include, for example: training, referral to counseling, or disciplinary action ranging from a verbal or written warning to termination of employment, depending on the circumstances.

The investigation will be handled in as confidential a manner as possible consistent with a full, fair, and proper investigation.

You should not conduct your own independent investigation into any suspected violations; instead make your complaint or report by following the procedures in this Policy. The WRO will review and coordinate the investigation and resolution of all complaints and reports of a suspected violation, as well as ensure that corrective action is taken, as necessary and appropriate.

When the investigation is complete, Coinbase will notify the reporting party. Note that Coinbase may not be able to disclose details of the investigation nor the outcome of the investigation.

## 7. Roles and Responsibilities

The roles and responsibilities in relation to the requirements and information set forth in this Document are as follows:

Role	Responsibility
All Company Members	Report believed illegal or otherwise improper conduct via the mechanisms outlined in the policy, including anonymous reporting options if desired.
Complaint Recipients	Receive, review, refer, process, or handle protected disclosures as required by the policy.
Whistleblower Reporting Officer (WRO)	Receive and respond to reports of reportable conduct from a whistleblower.
Investigator	Carry out an investigation of a whistleblower report.

## 8. Reporting of Non-Compliance

Non-compliance with this Document may result in disciplinary action up to and including termination. Known instances of a violation of this Document must be reported to the Chief Compliance Officer.

## **Appendix A - Ireland Supplement**

### **1. Overview**

This appendix supplements the general Whistleblower Protection Policy applicable to Coinbase Global, Inc. and its subsidiaries.

### **2. Applicability**

This appendix seeks to give effect to the Protected Disclosures (Amendment) Act 2022. This Act updates the Protected Disclosures Act 2014 and transposes the EU Whistleblowing Directive into Irish Law. This legislation aims to protect Workers in all sectors who disclose relevant information which in the reasonable belief of the Worker, tends to show a relevant wrongdoing has been, is being or is likely to be committed and that the information came to the attention of the Worker in connection with his/her employment. The Act also seeks to provide whistleblowers protection against penalisation, including dismissal, by their employer for having made a Protected Disclosure. Coinbase is of the view that it is important to have a mechanism in place to enable the Worker to voice concerns in an effective manner and this Policy sets out how concerns can be reported and how they will be handled.

### **3. Definitions**

- 3.1. **“Worker”** – refers to all employees (current or former), those in Central Bank of Ireland pre-approved controlled functions (“PCF”) roles, contractors, trainees / interns, agency staff, officers, trainees, volunteers, board members, shareholders, unpaid trainees or job applicants and directors of Coinbase, Inc. - Dublin Branch, Coinbase Ireland Limited, Coinbase Custody International Limited, Coinbase Europe Limited or any other individual working in Ireland.

### **4. Statement**

#### **a. Whistleblowing Concerns**

All whistleblowing concerns should be reported internally in the first instance. This will afford Coinbase the opportunity to investigate and manage any issues itself, and prevent unnecessary reputational damage where, after investigation, it is found that concerns have not been validated. Coinbase does however recognise a Whistleblower’s entitlement to make disclosures externally when internal procedures have been exhausted and/or the whistleblower is not satisfied with the outcome of the initial investigation or as may be required by law.

#### **b. Concerns Covered Under this Policy**

This Policy is designed to enable Workers to raise concerns in relation to any relevant information that they may have about actual, or potential, malpractice or relevant wrongdoing. While it is impossible to

provide an exhaustive list of all such activities, the following are examples of relevant wrongdoings which Workers should report:

- Criminal offence / activity that has been, is being, or is likely to be committed;
- Failure to comply with legal obligations;
- Miscarriage of justice;
- Actions which endanger the health and safety of any individual;
- Actions which cause damage to the environment;
- Unlawful or otherwise improper use of funds or resources of a public body, or of other public money;
- An act or omission by or on behalf of a public body which is oppressive, discriminatory, grossly negligent or constitutes gross mismanagement; or
- Actions which are intended to conceal or destroy information tending to show any matter falling within any of the points listed above.

It should also be noted that disclosures raised prior to the introduction of the Act are protected under the legislation.

### **c. Reporting**

Given the seriousness of the concerns which fall under the scope of this Policy, and the importance Coinbase places on such issues, all whistleblowing concerns are to be reported directly to HR and/or the local CEO.

If, for any reason, the whistleblower considers it inappropriate to refer the matter to HR and/or the local CEO, his/her concerns can be made known to the Chief Legal Officer of Coinbase Inc.

The contact details for each are as follows:

- HR Representative in Ireland (can be reached through [peopleops@coinbase.com](mailto:peopleops@coinbase.com))
- Local CEO or Country Manager (can be found on [the Company Intranet](#))
- Chief Legal Officer - Coinbase, Inc. (can be found on [the Company Intranet](#))
- You can also raise a report through our third-party reporting services provider, EthicsPoint, via telephone by calling 00-800-222-55288 (UIFN) or 1-800-550-000 (at the English prompt dial 844-564-3372) or online at [coinbase.ethicspoint.com](https://coinbase.ethicspoint.com). Reports through Ethicspoint can also be made anonymously.

Concerns can be raised verbally in the first instance but should be followed up in writing.

### **d. Post-Investigation & Appeal**

Subject to legal constraints and where deemed appropriate, the whistleblower and others involved in the investigation may be informed of the general outcome and actions taken/or to be taken, but will not generally be entitled to receive a copy of the investigator's report. If the investigation concludes that wrongdoing has occurred, those persons responsible for the wrongdoing may request a copy of the

report. In all instances, a copy of the investigator's report and actions taken will be sent to the Chief Legal Officer. Should the whistleblower not be satisfied with the outcome/actions taken, the whistleblower may re-submit their concern in writing to the CEO of Coinbase Global, Inc. This resubmission should include an outline of the whistleblower's concerns regarding the first process, its outcome and/or the actions taken. The CEO will review the whistleblower's concerns and the investigator's report and will decide whether the actions taken were appropriate or if further action is required.

**e. Obligations of Pre-Control Functions ("PCFs")**

The Act acknowledges that the Central Bank of Ireland's ("CBI") Fitness & Probity Regime, introduced under the Central Bank Reform Act 2010 and enhanced under the Central Bank (Supervision & Enforcement) Act 2013, obliges the holders of 'Pre-Approval Controlled Function' roles to disclose to the CBI, as soon as practicable, alleged breaches of financial services legislation and information which the PCF believes will be of material assistance to the CBI. Persons holding PCF roles can make disclosure in writing and submit same directly to the CBI either by email or post:

- E-mail: [Protecteddisclosures@centralbank.ie](mailto:Protecteddisclosures@centralbank.ie)
- Post: PCF Disclosure Desk, Central Bank of Ireland, Iveagh Court, Block D, Harcourt Road, Dublin 2.

## **Appendix B - UK Supplement**

### **1. Overview**

This appendix supplements the general Whistleblower Protection Policy applicable to all Coinbase Global, Inc. entities.

### **2. Reporting**

If you decide to make a disclosure to The Financial Conduct Authority (FCA) rather than to Coinbase, the following matters can be reported to the FCA:

- the conduct of funds, markets, firms and individuals subject to Financial Services and Markets Act 2000 (including banks, building societies, consumer credit and investment or insurance businesses)
- competition affecting financial markets in the UK and about the operation of mutual societies registered by the FCA under relevant legislation
- the conduct of electronic money issuers (for the purposes of Electronic Money Regulations 2011)
- the conduct of Payment Services Providers (for the purposes of the Payment Services Regulations)
- the operation of small UK Alternative Investment Fund Managers registered under regulation 10 of the Alternative Investment Fund Managers Regulations 2013
- the functioning of financial markets
- money laundering, financial crime, and other serious financial misconduct, in connection with activities regulated by the FCA
- the conduct of self-regulatory organisations (in relation to regulation 2 of the Oversight of Professional Body Anti-Money Laundering and Counter Terrorist Financing Supervision Regulations 2017)
- the conduct of persons who are supervised contributors within the meaning of Article 3(1)(10) of Regulation (EU) no. 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds
- the conduct of persons who are Miscellaneous BM persons within the meaning of regulation 5(2) of the Financial Services and Markets Act 2000 (Benchmarks) Regulations 2018)
- the conduct of persons subject to functions conferred on the Financial Conduct Authority under Regulation (EU) No 648/2012 on OTC derivatives, central counterparties and trade repositories

Coinbase Global, Inc.  
**Internal**

---

Financial Conduct Authority (FCA)  
Intelligence Department (ref PIDA)  
12 Endeavour Square  
London  
E20 1JN

Tel: 020 7066 9200

Fax: 020 7676 9727

Email: [whistle@fca.org.uk](mailto:whistle@fca.org.uk)

Website: [www.fca.org.uk/site-info/contact/whistleblowing](http://www.fca.org.uk/site-info/contact/whistleblowing)

## **Appendix C – Germany Supplement**

### **1. Overview**

This appendix supplements the Coinbase Global Whistleblower Protection Policy which is applicable to Coinbase Global Inc. and its subsidiaries.

### **2. Applicability**

This appendix takes into account specific requirements of the [German Whistleblower Protection Act](#) (“Hinweisgeberschutzgesetz”, “HinSchG”).

### **3. Information on external reporting procedures**

At the federal level, an external reporting center is located at the German Federal Office of Justice (“Bundesamt für Justiz”, “BfJ”). It is responsible for reports unless in particular the Federal Financial Supervisory Authority (“Bundesanstalt für Finanzdienstleistungsaufsicht”, “BaFin”) or German Federal Cartel Office (“Bundeskartellamt”) as further external reporting centers are responsible for specific reports (please refer to more detailed information below).

For information purposes please note that each German federal state can set up its own external reporting center for reports concerning the respective state administration and the respective local authorities (Section 20 HinSchG). In addition, the German federation sets up a further external reporting center for external reports that concern the external reporting center at the BfJ (Section 23 (I) HinSchG).

#### a) [External reporting center BfJ](#), Section 19 HinSchG

The external reporting center at the BfJ mainly deals with the following wide-ranging topics:

- Criminal law (“Strafrecht”)
- Regulatory offence law (“Ordnungswidrigkeitenrecht”), insofar as the violated regulation serves to protect life, body or health or to protect the rights of the employees or their representative bodies
- Product safety and conformity
- Traffic safety
- Protection of the environment
- Radiation protection and nuclear safety
- Food and feed safety, animal health and animal welfare
- Public health
- Consumer protection
- Protection of privacy and personal data as well as security of network and information systems
- Public procurement



- Tax law for corporations and commercial partnerships
- Protection of the financial interests of the European Union
- State aid
- Other internal market regulations (European Union regulations on the free movement of goods, persons, services and capital)
- Statements made by civil servants that constitute a breach of the duty of loyalty to the constitution

The external reporting center at the BfJ deals also with reports concerning the external reporting centers of the i) German federal states, ii) BaFin and iii) Bundeskartellamt (please refer to Section 23 (II) HinSchG).

b) [External reporting center BaFin](#), Section 21 HinSchG

The external reporting center at the BaFin mainly deals with breaches of supervisory law.

The BaFin supervises:

- Banks
- Financial service providers
- Payment and e-money institutions
- Private insurance companies
- Pension funds
- Capital management companies
- Securities trading

The BaFin also ensures that the companies it supervises comply with the applicable requirements for the prevention of money laundering and terrorist financing and takes care of collective consumer protection in the area of financial services.

c) [External reporting center Bundeskartellamt](#), Section 22 HinSchG

The external reporting center at the Bundeskartellamt mainly deals with breaches connected to competition law. For more detailed information please refer to the linked website above.

d) Information on external reporting procedures

Please refer to the linked websites of the [BfJ](#) and the further external reporting centers mentioned above for more detailed information related to external reporting procedures (Subsection 3 HinSchG) and relevant reporting procedures of bodies, institutions or other agencies of the European Union.

#### **4. Documentation of the reports**

Section 11 HinSchG requires a detailed process for the documentation of the whistleblowing reports.

The reports must be documented in a permanently retrievable manner in compliance with the confidentiality requirement (Section 8 HinSchG).

a) Reports by voice transmission

In the case of telephone messages or messages by means of another form of voice transmission: a permanently retrievable audio recording or complete and accurate transcript (verbatim protocol) are only allowed with the consent of the person providing the information (whistleblower). If no such consent has been given, the report must be documented by a summary of its content (content protocol) to be prepared by the person responsible for processing the report.

b) Reports by meeting

In case of a reporting within the framework of a meeting pursuant to Section 16 (III) HinSchG: with the consent of the reporting person, a complete and accurate record of the meeting can be made and kept. The record can be made by creating an audio recording of the conversation in a permanently retrievable form or by a verbatim protocol of the meeting to be prepared by the person responsible for processing the report.

The reporting person shall be given the opportunity to review the protocol, correct it if necessary and confirm it by signature or in electronic form. If an audio recording is used to make a protocol, it shall be deleted as soon as the written protocol is completed.

The documentation must be deleted three years after the completion of the process, unless legal requirements require otherwise.