

# Speak Up and Investigations Policy

## Version Control

Version No.	2.0	Policy ID	L2-EC-SU-2024-01-V2
Effective from	01/24	Last updated	09/2022
Policy Owner	VP of Corporate Finance and Risk	Date	01/01/2024
Approved by	Group CFO	Next review	01/2025

## 1. Introduction and Purpose

At Adevinta, we want to foster an environment where everyone can speak freely and respectfully. If you have a genuine concern of suspected wrongdoing or misconduct<sup>1</sup>, we want you to use your voice and speak up. We have enabled different reporting channels to support you that guarantee confidentiality, including a third party reporting platform managed by an independent party that facilitates anonymous reporting.

This procedure is part of our overall Ethics & Compliance Framework and provides guidance on how you can raise any concerns you may have about suspected misconduct, in confidence and without fear of retaliation, including how any misconduct will be investigated.

## 2. Scope

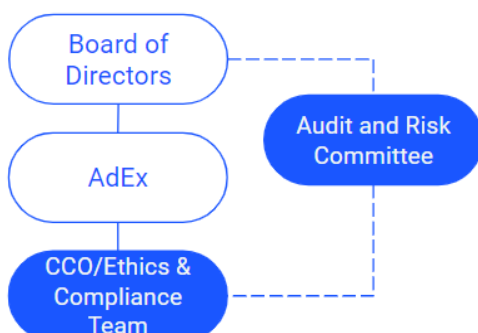
This procedure applies to:

- All Adevintans<sup>2</sup> whether permanent, temporary, part-time, or full-time.
- Third parties: anyone who had, has or will have a business relationship with Adevinta: contingent workers, contractors, subcontractors, suppliers, customers, consultants, business partners, temporary agency employees, freelance workers, etc. including former employees and job applicants.

There may be instances where this Policy is at variance with the local laws of a particular country. Where local law imposes higher standards than those set out in this Policy, the local law will prevail.

## 3. Roles and Responsibilities

Getting our Speak-up and Investigations procedure right is a blend of each person taking ownership and accountability. Therefore, it's important to understand your role.



<sup>1</sup> The terms “wrongdoing” and “misconduct” refer to any type of unethical practices, illegal activities or infringements of any applicable laws and regulations, including the ones set forth in Adevinta’s Code of Ethical Conduct and its related policies and procedures.

<sup>2</sup> Adevintans: any person employed by Adevinta ASA and its controlled subsidiaries, where Adevinta ASA controls or holds a shareholding of more than 50%.

The **Board of Directors (BoD)** bears primary responsibility for overseeing the Adevinta E&C programme and delegates responsibility for oversight and supervision of the implementation of the Ethics and Compliance Program to the Audit and Risk Committee (the “ARC”).

### **Adevinta Executive Team (AdEx)**

The Group CEO is appointed by the Board and together with the Adevinta Executive team (AdEx) are responsible for ensuring that an effective Ethics and Compliance programme is in place and that mechanisms and resources are in place to identify, monitor and manage compliance and ethical risks or issues. This include:

- creating a culture where discussing ethical and compliance issues is part of our day to day activities;
- promoting and providing a safe environment where employees and third parties are confident that they can speak up about concerns without fear of retaliation; and
- ensuring that mechanisms and resources are in place to report and investigate concerns in compliance with this procedure.

### **Chief Compliance Officer / Group Ethics and Compliance Team**

The Chief Compliance Officer | Group Ethics & Compliance Team is responsible for:

- developing and maintaining this procedure;
- managing the relationship with external parties conducting investigations;
- overseeing Speak Up and Investigation processes to ensure compliance with this procedure;
- making sure that actions are put in place and monitoring their implementation to prevent recurrence;
- provide training on this procedure as well as the Code of Ethical Conduct on a regular basis; and
- reporting to the AdEx, ARC and BoD on raised concerns & investigations as well as the overall status of the E&C Programme.
- Overseeing the imposition of corrective and/or disciplinary action for any wrongdoing/s, identified misconduct, unethical practices or infringement of any applicable laws and regulations, including the ones set forth in Adevinta’s Code of Ethical Conduct and its related Policies and procedures.

### **Adevinta Leadership team**

The Adevinta Leadership Team, including operational management both at a central or market level, is responsible on behalf of the AdEx team for:

- ensuring that all relevant employees within their areas of responsibility are aware of their obligations under this procedure;
- providing a safe environment where employees feel comfortable speaking up about matters of concern and raising any concerns relating to ethical or compliance issues; and

- ensuring a zero-tolerance policy on retaliation or intimidation against anyone who raises a concern, makes a report or cooperates in an investigation.

## All employees

All employees have a responsibility to comply with the Adevinta's Code of Ethical Conduct and associated policies and they are responsible for reporting concerns in good faith, based on reasonable suspicion, and for raising concerns through the appropriate channels in line with this procedure.

## 4. Speak Up

### A. The importance of Speaking Up

At Adevinta we look to build trust and confidence with our employees, customers, users, suppliers and other stakeholders by upholding the highest standards of ethical business conduct, acting with integrity in everything we do. Our reputation is important to us and is essential for our success

At Adevinta we **Use our Voice**; turning a blind eye to actions that are not in line with our key behaviours, our ways of working or our policies, is never the right solution.

and ability to operate today and in the future.

We serve our colleagues, customers and users best when we communicate openly, speak freely and share relevant information. If you observe or suspect any conduct that concerns you or that seems to violate our Code of Ethical Conduct and/or our policies and/or procedures, you are encouraged to speak up.

**Speak Up in good faith**, based on reasonable suspicion even if you do not have sufficient proof. However, raising malicious allegations on other employees or third parties may lead to disciplinary actions.

### *What type of concerns can be raised?*

This Speak Up procedure can be used to raise concerns about suspected misconduct, i.e. any violation to our Code of Ethical Conduct and/or any company policy or procedure, and/or any attempt to conceal a violation.

Examples of concerns that can be raised through the available speak up channels are (but not limited to):

- Fraud (including Tax fraud)
- Human and/or Labour rights violations
- Bullying or harassment
- Violations of competition laws
- Money laundering and terrorism financing

- Inadequate financial or non-financial recordkeeping
- Any form of bribery
- Conflicts of interest
- Influence peddling
- Improper use of company resources/assets
- Insider trading
- Social Fraud
- Misuse of data such a malicious use or intentional misappropriation (ie. stealing)
- Criminal offences or illegal acts
- Disclosure of confidential information
- Environmental crimes
- Issues at work that are breaking health and safety laws
- Retaliation against anyone for speaking up in good faith
- Discrimination
- Misuse of power and influence
- Sexual intimidation
- Breaches of our Diversity, Equity and Inclusion policy

This list is not exhaustive and in any case, speak up channels could be used to report any (danger to) violation of Union Law or national law, and danger to public interest, including public health, safety of persons, damage to the environment or the proper functioning of Adevinta. If you are not sure about whether to report a concern, use one of our channels described in section *B. How and When to Speak Up* to help you decide.

There are some general complaints, personal-related matters or aspects of your work that **fall out of the scope of this Policy**. These include, at least, the following cases/situations

- Grievances in relation to your employment with Adevinta, personal conflicts between employees, the way you have been treated or aspects of your work, such as the allocation of work, your working environment or conditions, issues related to employment contracts, performance related issues, or the way you are being managed – please refer to our [Global Resolving Problems Policy](#).
- Any issues raised that are the subject of a collective negotiation or consultation with a Trade Union, Staff Association or an Employee Works Council – please refer to your People Consultant via a Workday Help case
- Complaints raised by customers/users in relation to our products
- Complaints related to IT
- Learning and Development

## B. How and When to Speak Up

We encourage you to speak up as soon as possible, ideally before situations escalate or damage is done. There are several ways you can raise a concern through our reporting channels and you can use any of them.

Regardless of which reporting channel you use:

- you can be confident that your report will be taken seriously; and
- your identity (and any third party disclosed in the report) will be kept confidential.

## 1) Internal (Adevinta) channels:

- **Your Manager**

We encourage you to speak to your manager at first (unless of course the concern involves your manager) and do not keep the issue to yourself or ignore it. If after discussing the issue with your manager you believe that the concern is funded, create a case in Workday<sup>3</sup> so to ensure it goes through a thorough and standard triage process (see section 5. *Investigations procedure: what to expect if you Speak Up*).

- **Your Manager's Manager**

If you don't feel comfortable talking to your manager, you may reach out to your Manager's Manager. If after discussing the issue with your manager's manager you believe that the concern is funded, please create a case in Workday<sup>3</sup> so to ensure it goes through a thorough and standard triage process (see section 5. *Investigations procedure: what to expect if you Speak Up*).

- **Compass Team (Workday Help) or your local HR contact (People Consultants)**

If you feel your Manager (or Manager's Manager) isn't the right person to help, you may reach out to our HR team, either the Compass Team or your HR contact (People Consultants) by creating a case in Workday.<sup>3</sup>

- **Group Ethics and Compliance Team**

You can also report suspected misconduct to the Group Ethics and Compliance Team at [groupethicscompliance@adevinta.com](mailto:groupethicscompliance@adevinta.com). For legal compliance matters, like for example Corporate Governance, or Antitrust and Competition, you can also contact your Local Legal Counsel. They can advise you of the best course of action and help you to create the case in Workday<sup>3</sup>.

Any concerns raised through a different channel will need to be immediately referred to one of the aforementioned channels to ensure it is subject to the Speak Up process described within this Policy.

## 2) Speak Up Channel managed by an independent party: online, by phone or in person

If you feel unsafe or uncomfortable sharing your concern with anyone internally, you genuinely believe that the matter cannot be dealt with through the available channels, or you simply would like to report your concerns anonymously, you can use our [Speak Up](#) channel **managed by an independent (external to Adevinta) party**. Reports can be made online or by phone in your native language.

- To raise a concern **online** through our external Speak Up channel, please visit the [Wave](#) website to see all details and instructions.

---

<sup>3</sup> See Appendix 1 that describes how to log a case in Workday

- To raise a concern through our external Speak Up channel **by phone**, please call the Speak Up Line in your country (free of charge). This Line is operated by a third party. Please check [Wave](#) website for the correct phone number and further instructions.
- To raise a concern **in person** you can use our network of External Trusted Persons: please visit the Adevinta Speak up channel [Wave](#) website for details on how to contact them. They can organise an in-person meeting within the next seven days of your first contact.

**Third parties** should also use any of these reporting channels since they do not have access to the Internal (Adevinta) reporting channels. Full details can be found on our external [website](#).

If you make a report verbally, we will document it as a complete transcript of the conversation depending on your consent. We will then confirm the transcript with you. You can make changes so that it accurately captures the issue you would like to report. If you decide to now provide your consent to a transcript, we will summarise the conversation and confirm it with you.

### C. Information that needs to be provided

When you raise a concern, it will be helpful to include the following elements to support the investigation:

- any relevant background or history
- the reason for the concern
- description, as accurate as possible, of the reported concern
- the name/s of people involved, dates of the occurrence of the reported concerns, places and other relevant information
- any documents that may support your report.

We don't expect you to have all the answers. It's our job to look into the matter to decide if there is cause for concern. It is not a problem if your genuine concern later turns out to be mistaken or misguided; no disciplinary measures or other steps will be taken against you.

### D. Reporting concerns to external parties

Competent national and EU Authorities have set up external independent and autonomous reporting channels (see [Appendix 2](#) of this Policy) for employees to report concerns. You are always free to choose the channel through which you report an issue, may it be through official external channels or our internal channels. However, we strongly encourage you to raise concerns internally through one of the available channels without fear of retaliation. All our internal channels are a safe way for voicing concerns and by Speaking Up internally.

### **Use of Social Media**

Using social media to report a concern can interfere and compromise investigations into workplace wrongdoing and have serious implications for our Company, for the persons involved and possibly also for yourself. Refer to the [Social Media Guidelines Do's and Don'ts](#) and our Code of Ethical Conduct for guidance on how to use social media channels.

## **E. Protection of people involved in investigations**

### *Confidentiality*

We know that in these kinds of situations, confidentiality and anonymity can be important. This means that information about your concern will only be shared with a limited number of people on a strict need-to-know basis. We will ensure, as far as legally possible, to keep your reporting and identity confidential, and we will let you know if we are not able to maintain this confidentiality prior to the disclosure (unless the disclosure could hinder an ongoing judicial investigation). See the section on data protection below on information disclosure.

Breaches in confidentiality will be liable to disciplinary actions.

Anyone who is in possession of any information pertaining to a report is required to keep strict confidentiality.

### *Anonymity*

If you want to stay anonymous, you can share your concerns through our external Speak Up channel. However, please consider that not revealing your identity could make the investigation more difficult, and even in some cases not possible. We encourage you to disclose your identity if you raise a genuine concern, knowing that you will be protected from retaliation of any sort.

### *Data protection*

Upholding data privacy is an integral part of our business. We are committed to respecting individuals' rights when using their data. When pursuing a specific issue, personal data collection and retention is kept to a minimum and will be handled in accordance with the GDPR or any applicable privacy laws.

Adevinta will at all times protect the privacy and identity of users who choose to report wrongdoing or misconduct and will guarantee the anonymity of those who choose to make a report without revealing their identity.

If you wish to know more details about the processing of your personal data and the guarantees adopted by Adevinta to protect your privacy when using the Speak Up tool, please check the Adevinta Speak Up Privacy Policy ([Appendix 3](#)).



## Non-Retaliation

We want to foster an environment where everyone can speak freely and respectfully. If you have a genuine concern relating to suspected wrongdoing, we want you to use your voice without fear of retaliation.

Any form of threat or retaliation will not be tolerated. Retaliation against people who raise concerns or anyone involved in an investigation will be treated as a breach of our Code of Ethical Conduct and may lead to disciplinary action. You will be protected from any retaliation during and after a submission of report either internally or externally following the process described in section “*How and when to Speak Up*” and “*Reporting concerns to External Parties*”. You will not be protected, however, if you maliciously raise a concern that you know is false.

In case of a disclosure of the suspected misconduct, you will be protected as long as you have previously reported this via Speak Up channels mentioned in section “*How and when to Speak Up*” or externally as described in section “*Reporting concerns to External Parties*” above whereas you have with reasonable grounds that the information reported was true at the moment of disclosure.

If you receive any retaliation or notice any retaliation against anyone else for raising a concern in good faith about suspected misconduct, please report this via one of our Speak Up channels. This will be treated like any other Speak Up report and in line with this procedure.

Retaliation can take many forms and should be understood as any threat or attempt of disadvantage. We have included some examples in [Appendix 4](#). Watch out for any sign and report it immediately.

## 5. Investigations procedure: what to expect if you Speak Up

Adevinta takes every report of possible misconduct seriously. This investigation procedure aims to provide transparency in the way we investigate concerns received through any of our Speak Up channels.

### Timeline

If you raise a concern through any of the speak-up channels, you will receive a confirmation of receipt within 7 working days.

We will carry out an initial review, and if appropriate, the issue will be further investigated. Closure of the matter can be expected within 3 months, including an answer and/or feedback to you in relation to the submitted report. If a case is considered complex or additional investigations are required, it can take longer to investigate. In such a case, the additional time required will not exceed 3 months (up to 6 months in total).

### Initial review

Once a concern has been received, there is a thorough triage process to determine whether:

- the concern raised is a misconduct issue that needs further review and investigation under this procedure; or
- the concern raised needs to be referred to HR or another department because it doesn't fall within the scope of this procedure (see section A. *The importance of Speaking Up*).

At this stage, we may ask you for additional information.

All information about issues raised will be kept secure, in a durable and retrievable form, so that it can be used as evidence where appropriate.

All cases received via Workday or the external Speak Up channels will be logged into a CMS (case management system that serves as the complete register of all speak up cases in Adevinta):

- cases received via Workday: a selected group of People Consultants will perform an initial triage of the case and log it in CMS if deemed as an Speak Up case. You will be informed of the outcome of the triage process.
- cases received via the Speak Up Channel managed by an independent party will be automatically logged into CMS.

Once the cases are in CMS, an independent external party will perform the initial review of the case and convene the Ethics & Compliance Committee (the "E&C Committee" or the "Committee") to decide next steps. The People Consultant that received your case will act as intermediary and will keep you updated of the progress of the case in Workday.

Having a completely independent third party external to Adevinta performing the initial review and supervising the assignment of the investigator/s ensures objectivity and non-bias during the process.

## Review and Investigation

The Ethics & Compliance Committee is composed of senior Adevinta members and chaired by the external party, who ensures the right individuals are involved based on the nature of the concern or investigation. If a member/s of the Committee is/are mentioned in the report, they will guarantee that this/these individual/s are excluded from the Committee when convened.

The Ethics & Compliance Committee is responsible for reviewing all incoming reports, cases or compliance related concerns, and agreeing on the next steps or actions to be taken. If the Committee considers that an investigation is required, an appropriate investigator will be assigned to the case. Who is assigned will depend on the nature of the case and the seniority of the people involved in the incident. This could be a dedicated investigations manager within the Group Ethics & Compliance team, a senior member of the People/HR team, the Legal team, or an external party.

The investigation itself will focus on an objective analysis of the case and will be performed under strict confidentiality. If needed, outside experts such as legal consultants, forensics, etc. will be engaged to support the investigation. Details of the case, your identity and the identity of anyone

else mentioned in the report, will be kept confidential throughout and after the investigation and will be only shared on a need-to-know basis. As a principle, the report in the CMS should only be accessed by the independent third party, the Ethics & Compliance Committee, and the investigator(s) who are relevant to the specific case whereas they are obliged to maintain the confidentiality of the information. During the investigation, you may be contacted to provide feedback or further information.

If you become involved in an investigation, you should cooperate and answer questions in an honest manner. Lying, delaying, interfering with or refusing to cooperate with an investigation may lead to disciplinary action.

All parties involved, including the accused, are entitled to confidentiality. If you participate in or learn about an investigation, you must keep the matter confidential, otherwise you may interfere in the investigation.

## Resolution and root-cause analysis

There are two possible outcomes of any issue raised:

- If we find misconduct has taken place, appropriate measures will be taken. This could include corrective and/or disciplinary action for those involved, or informing the relevant authorities if deemed necessary.

The Group Ethics and Compliance team is responsible for making sure that actions are put in place and for monitoring their implementation to prevent future recurrence of a similar situation.

- If after investigating your concern, we conclude that misconduct has not taken place, the file will be closed and the resolution documented.

We will confirm in writing the outcome to you within three months of when you raised the issue, unless you have been informed of any delay with the resolution. However, for confidentiality reasons and in order not to disrupt or prejudice the investigation, we may not be able to tell you about all the measures taken to resolve the issue.

If you believe that your concern or a concern raised against you has not been handled appropriately or that an investigation has not been performed correctly, you should inform the Group Ethics and Compliance team, who will get in touch with you to find the best way to proceed.

## Reporting

The Group Ethics & Compliance Team is responsible for providing regular information on the number of reports received, the status of the investigations and the outcome of those concluded (including the status of action plans put in place to prevent recurrence). Reporting will be provided at least bi-annually to the Adevinta Executive Team, Audit & Risk Committee and Board of Directors.

## Assurance

The Internal Audit department is responsible for performing regular assurance activities on the effectiveness of the whistleblowing procedures, to ensure that appropriate investigation protocols are in place and to ensure that there is adequate management reporting to relevant governance groups; such as the board or the ARC.

## 6. Communication and awareness

The AdEx Team, together with the Leadership Team, is responsible for building awareness of Speak Up and Investigations, and for making sure adequate processes are in place to ensure compliance.

The Group Ethics and Compliance team is responsible for the implementation, communication and training of this procedure to ensure that employees and third parties are willing to report any suspected misconduct and understand the legal protection that is conferred upon them.

## 7. Non-compliance

Any breach of this Policy (e.g. any form of retaliation, breaches in confidentiality, privacy breaches) will be investigated, and may result in corrective and/or disciplinary action. These can include, but are not limited to, the following (always subject to any local laws and regulations):

- verbal warning;
- written warning;
- postponement of promotion;
- suspension without pay;
- termination of employment; and/or
- reporting to authorities.

## Appendix 1: How to log a Speak Up Case in Workday

**1** Go to Workday and find the Hep App.

**2** At the bottom of the page, you will see the option to create a case.

**3** Choose the case type "Employee Relations" and provide details of the case.

## Appendix 2: External reporting channels

The list of external independent and autonomous reporting channels for employees to report concerns includes, but is not limited to, the following:

Country	External Reporting Channel	Description
Belgium	De Belgische Mededingingsautoriteit	A government agency that protects economic competition by enforcing relevant legislation, called competition laws
	De Gegevensbeschermingsautoriteit	An independent body that ensures that the basic principles of personal data protection are properly observed
	De Autoriteit voor Financiële diensten en Markten	An institution that oversees the Belgian financial sector. It is the successor of the former Banking, Finance and Insurance Commission (CBFA)
	De Sociale Inlichtingen en Opsporingsdienst	A strategic body that, based on the knowledge and insights of the relevant departments and scientific support, develops a vision for combating social fraud and translates it into concrete strategies
Netherlands	Huis voor Klokkeluiders	An organisation in the Netherlands, established in 2016 to provide advice and support to reporters of abuses related to their work, so-called whistleblowers. It was established on the basis of the House for Whistleblowers Act
	De Autoriteit Consument en Markt (AP)	A Dutch independent public regulator charged with overseeing competition, telecommunications and consumer law
	De Nederlandsche Bank N.V. (DNB)	The Dutch conduct-of-business regulator of the financial markets (working closely together with the AFM)
	Autoriteit Financiële Markten (AFM)	The Dutch conduct-of-business regulator of the financial markets and has existed since March 1, 2002. The AFM is the legal successor of the Stichting Toezicht Effectenverkeer.
France	CNIL	Reports must concern a breach of the regulations on personal data protection (“RGPD”, “Loi Informatique et Libertés”, etc.), including cybersecurity
	Judicial Authority	For example: to the Public Prosecutor for crimes or misdemeanours

Country	External Reporting Channel	Description
	French anti-corruption agency	For breaches of probity
	Tracfin	For any suspicious financial behaviour
	Defender of the rights (Le Défenseur des droits)	Institution that is responsible for orienting whistleblowers towards the relevant authorities to ensure that the facts reported are remedied
	A comprehensive list of authorities can be found following this <a href="#">link</a> .	
Italy	Anti Corruption Authority (ANAC)	An Italian independent administrative authority tasked with combating corruption in the country
Germany	External channel at the Federal Financial Supervisory Authority (BaFin)	An external channel at the German financial markets regulator
	External channel at the Federal Cartel Office (Bundeskartellamt)	An external channel at the German independent public regulator that is charged with overseeing competition, telecommunications and consumer law
	External channel at the Federal Office of Justice (Bundesamt für Justiz)	An external channel at the government department that protects the principles of justice
Spain	Comisión Nacional del Mercado de Valores (CNMV) – National Securities Market Commission	Agency responsible for the financial regulation of the securities markets
	Comisión Nacional de Mercados y Competencia (CNMC) – National Commission on Markets and Competition	Independent competition regulator responsible for enforcing competition law
	Agencia Española de Protección de Datos (AEPD) – Spanish Data Protection Agency	Independent agency of the government of Spain which oversees the compliance with the legal provisions on the protection of personal data
	Banco de España (BdE) – Bank of Spain	Central bank of the country and national competent authority for banking supervision within the Single Supervisory Mechanism

Country	External Reporting Channel	Description
	Agencia Estatal de Administración Tributaria (AEAT) – Spanish Tax Administration Agency	The taxation authority/revenue service of Spain
	Intervención General de la Administración del Estado (IGAE) – Office of the Comptroller General of the State Administration	Internal supervisory agency, dependent on the Ministry of Finance, with the task of supervising the state public administration and of managing the public accounts
	Guardia Civil (GC) – Civil Guard	The oldest law enforcement agency in Spain, one of the two national police forces
	Cuerpo Nacional de Policía (CNP) – National Police Corps	The other national police force
	Organización de Consumidores y Usuarios (OCU) – Consumers and Users Organization	Non-profit organisation and independent association dedicated to inform consumers and defend their rights
	Oficina Nacional de Lucha contra el Fraude – National Anti-Fraud Office	Body mandated with protecting Spain's financial interests
	Fiscalía Especial contra la Corrupción y la Criminalidad Organizada (Fiscalía Anticorrupción)	Special State Attorney Office dependent on the Ministry of Justice dedicated to investigate economic and financial crimes within the national territory



## Appendix 3: Adevinta Speak Up Privacy Policy

### Disclaimer:

- Note that when reporting via the Speak Up tool, the anonymity of the reporter is guaranteed. Adevinta has engaged an independent service provider to facilitate this anonymous process. The below Privacy Policy is applicable to the process once Adevinta has received a complaint report containing personal data in relation to a Reported Individual, and only to the Reporter if the Reporter chose to forego the option of staying anonymous.

### 1. The purpose of this Privacy Policy

This Privacy Policy explains what personal data Adevinta collects, why and how it is collected, and how it is managed during and after the 'Speak Up' process. In law, Adevinta ASA and any Adevinta Group company – as the case may be – is ultimately responsible for how your information is used (the "Controller").

This Privacy Policy is applicable to all Adevinta's internal reporting channels, regardless of whether you raise a concern to your manager, your manager's manager, the Compass Team (Workday Help) or your local HR contact, the Group Ethics and Compliance Team, or whether you use the [Speak Up reporting channel](#) managed by an independent party.

In this regard, you should be aware that regardless of the channel you choose, Adevinta will maintain the confidentiality of your identity as far as legally possible. In this regard, if you wish to make a report completely anonymously, you must use the [Speak Up tool](#).

Should you decide to use the [Speak Up tool](#), you are contacting a service which is provided for Adevinta by an independent organisation (People Intouch B.V), who will respect your privacy in how they work with your information, as indicated in their [Privacy Notice](#) applicable for the use of the tool.

Any reports you raise and the information you are willing to share will be passed on to specialist teams within Adevinta ASA and/or the relevant Adevinta Group company for investigation, action and resolution. The information you submit will be treated confidentially and where the law or the investigation requires information to be shared, this will be done sensitively.

In this regard, upholding data privacy is an integral part of our business. Adevinta is committed to respecting individuals' rights when using their data. When pursuing a specific issue, personal data collection and retention is kept to a minimum and will be handled in accordance with the GDPR or any applicable privacy laws.

## 2. Contact details of the Data Privacy team and Data Protection Officer

If you have any questions regarding this Privacy Policy, please email us at [privacy@adevinta.com](mailto:privacy@adevinta.com).

## 3. What categories of personal data are processed?

Depending on the nature of the reported incident, it is unpredictable which kind of data categories may be processed. In this regard, the following categories may be processed:

### *Data of incident reporter*

- Contact details (name, job title, address, email address, phone number, company, country), in case the incident is not reported on an anonymous basis.
- Content of the reported incident: depending upon the nature of the allegation or concern, this could include a description of behaviour, activities in relation to Adevinta, location and time of incident, or other data which is relevant to the allegation or concern.

### **Additional specific data processed if you report your concern via Speak Up tool:**

- Session cookie: if an incident is reported by using the web-portal (see also the Privacy Statement for the web portal, which is hosted and administered by the external service provider (Processor).
- Voice: only if the concern is reported via [phone call](#). In this regard, transcript is provided to Adevinta and to the independent party managing the Speak Up channel, as the recorded voice is only accessible by the processor People Intouch B.V., the provider of the Speak up tool.

### *Data of person subject to incident reporting*

- Contact details (name, job-title, address, email-address, phone number, company, country).
- Content of the reported incident: depending upon the nature of the allegation or concern, this could include a description of behaviour, activities in relation to Adevinta, location and time of incident, or other data which is relevant to the allegation or concern.
- Measures taken as a response to the reported incident.

### *Data of (potential) witnesses*

- Contact details (name, job-title, address, email-address, phone number, company, country)
- Role of such witness in the reported incident
- Data the witness provides to Adevinta in the context of the investigation

### *Data of investigators and individuals responsible for measures*

- Contact details (name, job-title, address, email-address, phone number, company, country)

As any compliance concern can be raised through the different 'Speak Up' channels, the previous list is not exhaustive. Special categories of data may also be processed if it is relevant to the reported incident, such as race, ethnic origin, trade union membership, philosophy, or religion, sexual life or orientation, health or financial information relating to individuals. For instance, a safeguarding case may reveal sexual orientation, ethnic origin or religion data.

## 4. Purposes of the data processing

Purposes of the data processing	Legal Basis
Gather further information regarding the reported incident or concern.	Legal obligations and Adevinta's legitimate interest to learn about any compliance incidents within the organisation and to stop any inappropriate/illegal behaviour by taking any appropriate decisions after conducting a comprehensive and rigorous investigation of the facts.
Learn about potential compliance risks in Adevinta, identify misconduct, illegal acts, or protect those with whom we work.	
Take appropriate action where necessary to address the reported incident: administration and clarification of responsibilities. This may include the establishment, exercise or defence of legal claims by Adevinta.	
Identify any person who is subject to an incident report, and who may not act in accordance with applicable laws or internal policies.	Legal obligations and Adevinta's legitimate interest is to identify any person within its organisation – or within any third party related to Adevinta whatsoever – who may not act in accordance with applicable laws or internal policies and to contact such persons or use their contact details during the course of the appropriate investigation.
Identify any potential witness willing to contribute to clarify the facts related to the reported incident.	Legal obligations and Adevinta's legitimate interest is to document the investigation process in order to evidence its correctness.
Document all steps during the investigation and solve the case properly.	Legal obligations and Adevinta's legitimate interest is to identify persons who can contribute to the clarification of a reported incident.

Purposes of the data processing	Legal Basis
Update the incident reporter regarding the way in which Adevinta is dealing with the Speak Up process, should the incident reporter decide not to stay anonymous.	The reporter's consent, should the reporter decide to report non-anonymously and agree to submit his/her/their personal contact details.
Make referrals to the authorities, if appropriate.	Adevinta's legal obligation to bring to the attention of the relevant authorities the commission of a potential criminal offence.
Produce statistical data to create appropriate reports.	Adevinta's legitimate interest to analyse the cases for statistical purposes and to report compliance cases so that relevant management can comply with its obligations to ensure an effective compliance system at Adevinta.

In addition, in case the reports include special categories of data that are relevant for the investigation of the case, the legitimate basis shall be (i) the consent of the reporter or, as the case may be, (ii) the necessity of such processing in accordance with paragraph 9.2 (b) of the GDPR.

## 5. Recipient or categories of recipients of the personal data

Adevinta and any Adevinta Group company affected by the incident report.

**As the case may be:** external legal counsels, relevant authorities (Police, Courts, Tax Authorities), supervising authorities (e.g. Data Protection authorities), administrative bodies.

**External service suppliers related to the Speak Up channel:**

- **Processor:** provider of the Speak Up tool, and responsible for the transcription of reports made via phone call. For more information, please check [People Intouch's Privacy Statement](#).
- **Independent party (external to Adevinta):** provides triage process services, to determine whether the concern raised is a misconduct issue that needs further review and investigation. Having a completely independent third party external to Adevinta performing the initial review and supervising the assignment of the investigator/s ensures objectivity and non-bias during the process.

## 6. Duration of the data processing

The personal data included in the incident report will be processed for the maximum period of time established and/or permitted in the relevant applicable whistleblowing and data protection

regulations, as long as such personal data are relevant to pursue the clarification of the facts during the investigation, without prejudice to the extension of this processing period in cases where the investigation is being carried out by the appropriate department or staff, who may continue to process the data until the resolution of the case. In such cases, Adevinta has a legitimate interest to store the data for a longer period than the aforementioned (e.g. defending against or pursuing legal claims).

Any personal data pertaining to the registered reports will be removed in case it is no longer necessary to fulfil the obligations of applicable laws and regulations.

Additionally, with regard to the Speak Up channel:

- Case data in the SpeakUp System will be anonymized by People Intouch after 14 days, once the case is closed. It is kept for 14 days on the back-up system.
- Soundfiles: voice recordings will be automatically deleted by People Intouch 24 hours after confirmation of receipt by Adevinta the transcript or summary in the Case Management System has been received. It is kept for 5 days on the back-up system.
- Session cookie data on the Speak Up website will be deleted by People Intouch after two (2) hours.

## 7. Data Protection rights

You have certain rights in relation to your personal information such as the right to be informed, the right of access, correcting or erasing your information, the right to restrict processing, the right to data portability, and the right to complain. For more information on your rights use the contact details at the bottom of this Policy.

Adevinta will guarantee the aforementioned rights, without ever revealing the identity of the incident reporter. Likewise, Adevinta will ensure that the persons affected by an incident report and its resulting investigation can find out as soon as possible the facts that are alleged against them, so that they can duly defend their interests, and therefore this information must be provided to them after a prudent period of time during which the preliminary investigation of the facts is carried out.

## Appendix 4: Examples of retaliation<sup>4</sup>

- suspension, lay-off, dismissal or equivalent measures;
- demotion or withholding of promotion;
- transfer of duties, change of location of place of work, reduction in wages, change in working hours;
- withholding of training;
- a negative performance assessment or employment reference;
- imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;
- coercion, intimidation, harassment or ostracism;
- discrimination, disadvantageous or unfair treatment;
- failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;
- failure to renew, or early termination of, a temporary employment contract;
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
- blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;
- early termination or cancellation of a contract for goods or services;
- cancellation of a licence or permit;
- psychiatric or medical referrals;
- a written reprimand;
- libel or slander;
- a fine as referred to in Article 650 of Book 7 of Dutch Civil Code.

---

<sup>4</sup> This list is not exhaustive. It is an extract from 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 based on the Wet Bescherming Klokkensluiders.

## Related Documents

Document <i>(add hyperlink to doc name)</i>	Description
<a href="#">Code of Ethical Conduct</a>	Sets out the basic requirements for business conduct.
<a href="#">Global Resolving Problems Policy</a>	Sets out the approach to resolving employee problems.
<a href="#">Global Maintaining Standards Policy</a>	Sets out the standards of behaviour and performance.

## Document Control

Version No.	Change summary	Reviewed by	Date
1.0	N/A	VP Corporate Finance & Risk Chief Financial Officer	09/22
2.0	Alignment to EU Whistleblowing Directive	VP Corporate Finance & Risk Chief Financial Officer	01/24