Whistle Blower Policy

For

AT&T Communications and AT&T Corporate Entities within the European Union

About this Policy

The Whistle Blower policy (the "Policy") aims to implement, within AT&T, (the "Company") for countries based in the European Union, the EU Directive 2019/237 of 23 October 2019, on the protection of persons who report breaches of Union law (the "Act"), and the requirements of the Local legislation adopted to implement the Act.

This Act and Local legislation require legal entities, in the private sector, employing more than 50 workers in a given member State, to implement appropriate procedures on handling whistleblowing reporting by employees or any other person mentioned under article one.

The purpose of this policy is to ensure that the persons mentioned in article General Scope:

- Made aware of internal channels, external channels, and the follow-up procedure.
- Ensure that if they make a report in relation to Activities, the Report will be taken. seriously and investigated appropriately, and that their confidentiality will be respected.
- Provide guidance as to how to raise those concerns as well as the procedure in place.
- Reassure that they should be able to raise genuine concerns without fear of reprisals and that their confidentiality will be respected unless they agree otherwise.

General scope

This Policy applies to each employee ("Employee") based in the European Union under an employment agreement with AT&T.

This Policy applies as well to anyone who acquired information on breaches in a work-related context including:

- Individuals with which the work-based relationship with AT&T has ended but who report or publicly disclose information on breaches acquired during the time of this work-based relationship.
- Individuals whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations.
- Persons having a self-employed status.

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

- Shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees.
- Any persons working under the supervision and direction of contractors, subcontractors and suppliers.

The Employee must be familiar with this Policy.

To enjoy protection under this Policy, persons making reports should have reasonable grounds to believe, considering the circumstances and the information available to them at the time of reporting, that the matters reported are true.

The procedure set forth by the present Policy is not mandatory and employees are not required to make use of it. There is no adverse consequence to an employee who chooses not to engage in the procedure. However, any abuse of the Policy may be subject to disciplinary sanctions set forth by the Company Internal Regulation.

Definitions

- '**Act**': EU Directive 2019/237 of 23 October 2019, on the protection of persons who report breaches of Union law.
- '**Anonymous**' means not including an individual's identity, functions and contact details when submitting a report or making a public disclosure.
- '**Authorized Person(s)**' are the members of the AT&T function in charge of receiving and investigating a Report and documenting the Minutes.
    - For Netherlands, the members of the AT&T function in charge of receiving and investigating a Report and documenting minutes is Steve Willis, Lead Security and Investigation.
    - For Spain, the person responsible as System Manager in charge of receiving and investigating a Report and documenting minutes is Steve Willis, Lead Security and Investigation.
- '**Breach(es)**': means acts or omissions, information as defined under the article 'what can be reported or disclosed' of the policy that: (i) are unlawful and relate to the Union acts and areas falling within the material scope referred to in article ; 'What can be reported or disclosed' or (ii) defeat the object or the purpose of the rules in the Union acts and areas falling within the material scope. Additional information about the scope as per the respective Local legislation are set out under article 'what can be reported or disclosed' and Appendix 1.
- '**Company**' refers to entities located within the European Union.
- '**External reporting'** means the oral or written communication of information on breaches to the competent authorities.
- '**Facilitator**' means a natural person who assists a person with the reporting process in a work-related context, and whose assistance should be confidential.

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

- '**Information on breaches'** means information, including reasonable suspicions, about actual or potential breaches, which occurred or are very likely to occur in the organization in which the reporting person works or has worked or in another organization with which the reporting person is or was in contact through his or her work, and about attempts to conceal such breaches.
- '**Internal reporting'** means the oral or written communication of information on breaches within the Company.
- '**Local legislation'** refers to the law aimed at improving the protection of the reporting persons/whistleblowers and any decrees adopted in relation to the law.
- '**Minutes**' are documentation of the processing of the Report.
- '**Person concerned'** means a natural or legal person who is referred to in the report or public disclosure as a person to whom the breach is attributed or with whom that person is associated.
- '**Public disclosure**' or '**to publicly disclose'** means the making of information on breaches available in the public domain.
- **'Report**' or '**to report'** means, the oral or written communication of information on breaches.
- '**Reporting person'** also referred to as a '**Whistleblower'** means a natural person who reports or publicly discloses information on breaches occurring in the context of their work-related activities, without direct financial compensation and in good faith, information relating to a crime, an offence, a threat or harm to the general interest, a violation or an attempt to conceal a violation of an international commitment regularly ratified or approved by a country, of a unilateral act of an international organization taken on the basis of such a commitment, of the European Union, law or regulation, unless local legislation decrees differently.
- '**Retaliation**' means any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person.
- **'Suspected abuse'** for Netherlands only **-** means a reporting person's suspicion of an abuse in the organisation at which he works or has worked or in another organisation if he has come into contact with that organisation through his work, in so far as the suspicion is based on reasonable grounds resulting from the knowledge gained by the employee in the service of his employer or from the knowledge obtained by the employee through his work at another business or organization. See appendix 1 for the scope of Abuse.
- '**Work-related context**' means current or past work activities with the Company through which, irrespective of the nature of those activities, persons acquire information on breaches and within which those persons could suffer retaliation if they reported such information. Please note this does not apply for France.

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

What can be reported or disclosed

What can be reported as Breaches or disclosed is set out in Article 2 of the Act.

See Appendix 1 for further details of reportable events under respective Local legislation.

The Policy shall not affect the application of Union or national law relating to any of the following: protection of classified information; protection of legal and medical professional privilege, secrecy of judicial deliberations, rules on criminal procedure and any other areas set out by the Local legislation.

For Netherlands, the Reporting Person can consult an advisor from the House for Whisteblowers if he/she has a Suspicion of Abuse. He/she can also consult the Whistleblowers Authority for advice if he has a Suspicion of Abuse or for obtaining general information about dealing with Suspected Abuse.

How to make a Report

A person can raise a Report with AT&T using the following channels:

I. As an internal channel the Authorized Person, local HR Country Manager can be contacted directly (IHR Connect (att.com))
II. Calling Asset Protection Client Services 7 x 24-hour hotline on +1 908 658 0380 (this route should be used if the Reporting person wishes to remain anonymous)
III. Sending an email to rm-wb-reporting@intl.att.com
IV. Desktop Reporting tool available to all employees and contractors with access to an AT&T computer (right click on the desktop)
V. Via voicemail message system (when an agent is not available)

Specifically, for:

- Czech Republic a Reporting person must make a Report by:
  - contacting the designated persons who are: Katerina Orlitova and Slavka Hurtikova, either by:
    - Email: katerina.orlitova@intl.att.com / slavka.hurtikova@intl.att.com
    - Telephone: Katerina Orlitova +42 05187 23636, Slavka Hurtikova +42 05187 23193
    - In Person at: 2 Palachova Nemesti, Brno, Czech Republic 62500, by requesting to raise an in-person Report which will occur within a reasonable period of time, but no later than 14 days from the day on which the person requested it.
- Netherlands, in addition to the 4 options set out in the present article, a Reporting Person can also request an onsite interview at an agreed location.
- Spain, in addition to the 4 options set out in the present article, a Reporting Person can also make a Report by postal mail at AT&T, Calle López de Hoyos 35, Madrid – 28002, Spain or request an onsite interview that will occur at AT&T, Calle López de Hoyos 35, Madrid – 28002, Spain within a maximum period of 7 days from the receipt of the request.

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

With respect to the content of the Report:

- For Czech Republic, a Report must contain the whistleblower's name, surname and date of birth or other details allowing the Reporting person to be identified.
- For Spain, the Reporting Person may indicate an address, email, or safe place for receiving notifications.

If the Reporting Person wishes to remain anonymous, as and if allowed by the Local legislation, they should use option II, the Asset Protection Client Services 7 x 24hr hotline. Calls to this hotline are not screened or recorded and callers are not obliged or required to provide their contact details. For Czech Republic a Reporting Person must use option Ia. above to raise a report and contact the designated person(s) either by email, telephone or in person.

Any person raising a Report must state they are reporting an incident under the Whistle Blower Policy for AT&T Communications and AT&T Corporate employees based in the European Union. The reporting person will receive an acknowledgement of receipt of their report.

An investigation case will be opened and an associated reference number provided to the reporting person within 7 calendar days of the receipt of the report. This reference will be used for all future communication with AT&T relating to the report.
An Authorized person(s) will be assigned to the investigation case for review. They will contact the reporting person as soon as possible to:

(i) Discuss the Report in further detail.
(ii) Outline the investigation process and set expectations.
(iii) Discuss updates and timing of events.

No attempt will be made to identify a Reporting Person who wishes to remain anonymous during the investigation.

Investigation of a Report by Authorized Persons

The Authorized Persons must:

- Acknowledge receipt of the Report to the reporting person within seven calendar days of the receipt
- Provide the Reporting person with a diligent follow-up
- Overall, will provide feedback in a reasonable timeframe which will not exceed three months from the acknowledgement of receipt or if no acknowledgement was sent to the Reporting Person, feedback will be provided three months from the expiry of the seven-day period after the Report was made.
    - For Czech Republic, the Authorized person will provide the feedback within 30 days from the date of receipt of the Report, unless the Authorized person have provided prior notice to the reporting person to extend the initial period up to twice and each time by up to 30 days.
    - For Spain, in case of special complexity, the period to provide feedback can be extended up to a maximum of three additional months.
- Inform the Reporting person that he/she may make an external report.

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

Any and all communication among the Authorized Persons and the Reporting person shall be made through the specified email address by means of encrypted messages.

If a Reporting Person requests a face-to-face meeting or a videoconference, the authorised person will meet with the person at the earliest convenience for both parties. For France this meeting should take place within twenty working days after receipt of the request.

The Minutes, established by the Authorized Persons, must contain and are strictly limited to, the following records:

- The identity, functions and contact details of the employees of the AT&T function acting as Authorized Persons and of the employees of other AT&T functions assisting the Authorized Persons
- Date of receipt of the Report; closing date of the review of the Report and date of notification or the latter results to the Reporting person in case of a non-Anonymous Report as well as to the Person subject to the Report
- The identity, functions and contact details of the Reporting person; a comment will be included in the Minutes in case the Report is Anonymous
- The identity, functions and contact details of the Person subject to the Report;
- The facts reported;
- The evidence gathered to verify the facts reported;
- The process for verifying how the Report was completed;
- The follow-up given to the Report.

The Report will be closed when the allegations are inaccurate or unfounded, or when the report has become moot. The procedure provides that the author of the Report is informed in writing of the closure of the file.

Record keeping of the Reports

All information relating to the investigation, including communications, will be kept by the Authorised person and saved in a case file.

The Authorised person will conduct an investigation in line with current best practices and procedures and adhering to the Act and the Local legislation

Any Report made orally is kept as follows:

- When collected, with the consent of the Reporting Person over a recorded telephone line or other recorded voicemail system, either by recording the conversation on a durable and retrievable medium or by transcribing it in full
- When collected over an unrecorded telephone line or other unrecorded voice mail system, establishing an accurate record of the conversation

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

- When it is collected in the context of a videoconference or a physical meeting, by establishing, with the consent of its author, either a recording of the conversation on a durable and recoverable medium, or a precise Report.

The Reporting Person has the possibility of checking, correcting and approving the transcription of the conversation or the minutes by affixing his signature. Recordings, transcripts and minutes may only be kept for the time strictly necessary and proportionate to the processing of the Report and the protection of their authors, the persons they target and the third parties they mention.

A copy of the document will be made available to the Reporting person upon request.

Archiving and retention period of the Report after investigation

Reports will be stored for no longer than it is necessary and proportionate for the purposes of investigating the report, including compatible purposes as stated in this Policy and to comply with the requirements of the Act and the Local legislation.

- For Germany, will be kept for a period of 3 years after the end of the procedure. Documents may however be kept longer if required by the local legislation and as long as necessary and proportionate.

In addition, Data relating to Reports:

- for France: may be kept beyond this period, provided that the natural persons concerned are neither identified or identifiable.
- For Czech Republic, will be kept for a period of 5 years from the date of receipt of the notification.

- When disciplinary proceedings or legal proceedings are instituted against the Person Concerned or the Reporting Person, the data relating to the Report and the Minutes shall be kept by the Authorized Persons until the end of these proceedings.
- Data, relating to a Report that is declared inadmissible, will be destroyed or archived without delay as soon as received by the Authorized Persons in case they do not fall under the scope of the procedure after anonymization.
- When no disciplinary or judicial procedures are instituted, the data relating to the Report will be destroyed or archived after anonymization by the Authorized Persons within two months from the closing of the review of the Report.

For however long, Personal Data is Processed, AT&T will use appropriate security measures consistent with Data Privacy Laws.

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

Confidentiality

The company ensures that:

- The internal channels available for receiving Reports are designed, established and operated in a secure manner that guarantee that the confidentiality of the identity of the Reporting Persons, as well as any third party mentioned in the Report, is protected. This includes any information from which the identity of the Reporting Person may be directly or indirectly deduced.
- Data will not be shared with non-authorized persons.
- Authorized persons will make every effort to ensure confidentiality.
- Authorized persons will receive regular specific training, including training related to data protection.

Elements likely to identify the Reporting Person may only be disclosed with their consent. Information may be disclosed only where this is a necessary and proportionate obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, including with a view to safeguarding the rights of defense of the person concerned.

Reporting persons shall be informed before their identity is disclosed unless such information would jeopardize the related investigations or judicial proceedings. When informing the Reporting persons, the competent authority shall send them an explanation in writing of the reasons for the disclosure of the confidential data concerned.

Data protection

This Policy provides information in furtherance of notice and transparency obligations under data privacy laws, including the processing of certain personal data, the entities which will have access to personal data, and for how long personal data will be retained. This Policy should be read in furtherance of the AT&T Most of World Employee Privacy Notice. In additional support of personal data protection:

- The Company will not collect personal data when it is not relevant for the handling of a specific report. If accidentally collected, the Company will delete the data without undue delay.

- Data collected about any person concerned when investigating a report will not be included when provisioning personal data in response to an Employee Data Subject's request to ensure no adverse effect is occurring to the rights and freedoms of the reporting person. Further information about an Employee Data Subject's rights may be found at the Employee Data Subject Right to Access Request Submission Guidelines link on IHR OneStop. Former employees, applicants and others who have performed work for AT&T may contact the International Human Resources mailbox.

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

Reporting externally

Persons identified under article – General scope can make a report after having first reported through internal reporting channels, or by directly reporting through external reporting channels.

They can make a Report before the relevant European authorities.

In addition: the Reporting person can choose to make an external report to the competent authority.

- for France as designated by the decree, to the Defender of Rights (Defenseur des droits) or to the judicial authority.
- For Germany, Federal Office of Justice (*Bundesamt für Justiz*) or if relevant the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht*) and the Federal Cartel Office (*Bundeskartellamt*).
- For Czech Republic, the Ministery of Justice
- For Netherlands, (1°) the Netherlands Authority for Consumers and Markets; (2°) the Dutch Authority for the Financial Markets; (3°) the Data Protection Authority; (4°) De Nederlandsche Bank N.V.; (5°) the Authority; (6°) the Health and Youth Care Inspectorate; (7°) the Dutch Healthcare Authority; (8°) the Authority for Nuclear Safety and Radiation Protection; and (9°) organisations and administrative authorities, or units thereof, designated by an order in council or a ministerial order which have tasks or powers in one of the areas referred to in Article 2, paragraph 1 of the directive.
- For Spain, to the Independent Informant Protection Authority (Autoridad Independiente de Protección del Informante)

Measures of protection

The Company will not tolerate any victimization or any form of retaliation.

Persons mentioned in article General Scope, and who made a report, will qualify for protection under this Policy if they have reasonable grounds to believe that the information on breaches reported was true at the time of reporting and that such information fell within the scope of what can be reported under this Policy.

The measures of protection set out in this Article apply to the Reporting person as well as to facilitators, persons connected with the reporting persons who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons; legal entities that the reporting persons own, work for, or are otherwise connected within a work-related context.

In addition:

- for France: After having made an external report, whether or not preceded by an internal report and if not appropriate measure has been taken in response to this report on the expiry of the period for feedback mentioned by law or, when an authority has been seized, at the end of a period fixed by decree in Council of State; or immediately when they publicly discloses information obtained in the context of his professional

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

activities in case of imminent or manifest danger to the general interest, in particular when there is an emergency situation or a risk of irreversible damage

The protections are:

- Identity protection
- Protection from detrimental acts or omissions
- Protection against any victimization, any form of retaliation including any threats of retaliation or attempts of retaliation, examples include, but are not limited to:
  - Watching work or attendance more closely than that of other employees, without justification
  - Bullying, which involves repeated intimidation or humiliation, or derogatory or insulting remarks
  - Social isolation (ostracism), e.g., exclusion from corporate or team events or meetings
  - Unsupported negative performance evaluations or disciplinary action or negative work certificate
  - Inequity in compensation, working conditions, or job opportunities
  - Discrimination, disadvantageous or unfair treatment or harassment
  - Threats or warnings
  - Termination, suspension or illegal withdrawal of benefits, including leaves of absence
  - Dismissing, layoff, refusing a promotion or demoting an employee without just reason
  - Altering the employee's position or duties to their disadvantage
  - Withholding training

Company will provide any other measure of protection required by the Act or Local legislation.

Measures of support

If the reporting person is a Company employee and suffers retaliation, he/she will be entitled to support through the Employee Assistance Program (EAP). In addition, meQuilibrium is also available to employees, their families or officers and is a stress management website and mobile app designed to help discover simple techniques to build resilience when facing stressful thoughts and situations.

Support is also available to a reporting person, as well as to facilitators, persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons; legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context, will also be provided measures as required by the Act or Local legislation.

Availability and Entering into Force

This Policy is available on-line on the intranet and internet sites of the Company to ensure employees, external and occasional contributors have access.

The present Policy is valid and effective, for an indefinite period of time.

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

Contacts

If you have any questions about this policy, please contact @AskCompliance

Published: April 2022
Amended: December 2023

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of
AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

APPENDIX 1

1. Material scope as per the Act

Chapter I Scope, Definitions and conditions for protections Article 2 – Material Scope	This Directive lays down common minimum standards for the protection of persons reporting the following breaches of Union law: (a) breaches falling within the scope of the Union acts set out in the Annex that concern the following areas: (i) public procurement; (ii) financial services, products and markets, and prevention of money laundering and terrorist financing; (iii) product safety and compliance; (iv) transport safety; (v) protection of the environment; (vi) radiation protection and nuclear safety; (vii) food and feed safety, animal health and welfare; (viii) public health; (ix) consumer protection; (x) protection of privacy and personal data, and security of network and information systems (b) breaches affecting the financial interests of the Union as referred to in Article 325 TFEU and as further specified in relevant Union measures; (c) breaches relating to the internal market, as referred to in Article 26(2) TFEU, including breaches of Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law.

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

	2. This Directive is without prejudice to the power of Member States to extend protection under national law as regards areas or acts not covered by paragraph 1.

2. Material scope as set out in Local legislations

In addition to article 2 of the Act, Local legislations also set out that the following can be reported.

Czech Republic Act No. 171/2023 Coll. *Protection of Whistleblowers Act*	A Reporting person may make a Report about an activity which: - has the characteristics of a criminal offence; - has the characteristics of an offense for which the law sets a fine rate, the upper limit of which is at least CZK 100000 - violates the Local legislation.
France Law 2022-401 of March 21, 2022	A Reporting person may make a Report regarding information about a crime, a misdemeanour, a threat or harm to the general interest, a violation or an attempt to conceal a violation of an international commitment duly ratified or approved by France, of a unilateral act of an international organization taken on the basis of such a commitment, of European Union law, or of a law or regulation.
Germany Law 2023 n140, law to improve the protection of whistleblowers and to implement the directive on the protection of persons who report violations of Union law Part 1 – General rules &2 Material scope**.**	A Reporting person may make a Report about: - violations that carry a criminal penalty; - violations that can be penalized with a fine, in so far as the violated provision aims to safeguard (i) the physical integrity and health of a person or (ii) workers' rights and their representative bodies; - other violations against specific acts of European or German law; - violations of public procurement law, financial services supervision, and of specific tax provisions or the attempt to avoid specific tax provisions; - violations of the Digital Markets Act.
Spain Law 2/2023, of February 20, regulating the protection of people	A reporting person may make a Report about an actions or omissions that may constitute a serious or very serious criminal or administrative offenses under Spanish law and in any case, those involving financial loss to the

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.

who report on regulatory violations and the fight against corruption, Title I Purpose of the law and scope of application, article 2 Material scope of application.	Spanish Treasury and Social Security.
The Netherlands Dutch Whistleblower Protection Act Chapter 1 – General Provisions &1 Definitions	A reporting Person may make a Report in case of a suspected Abuse. Under the Local legislation, an Abuse means a Breach as defined under the article Definitions of the Policy but also a breach or risk of a breach of Union law, or b) an act or omission with regard to which the public interest is at stake in connection with: (1°) a breach or risk of a breach of a statutory regulation or of internal rules that impose a specific obligation and have been established by an employer on the basis of a statutory regulation; or (2°) a risk to public health, public safety or the environment, or an improper act or omission that jeopardises the proper functioning of the public services or an undertaking.

© 2022 AT&T Intellectual Property. AT&T and Globe logo are registered trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks are the property of their respective owners.