



SpeakUp Policy

Version 1, English
February 25, 2019





Table of Contents

1. About SpeakUp	2
1.1 Introduction	2
Purpose	2
Scope	2
Benefits	3
1.2 Use of SpeakUp	3
1.3 Management of concerns	4
1.4 Non-Retaliation	5
1.5 Special Country Regulations	5
Belgium	6
Canada	6
Czech Republic	6
Denmark	6
Finland	6
France	7
Hungary	7
India	7
Italy	7
Luxembourg	7
Morocco	7
Netherlands	7
Portugal	8
Romania	8
Russia	8
Slovak Republic	8
Spain	9
Sweden	9
2. Privacy Notice	9
2.1 Definitions	9
2.2 Who is processing your Personal Data and why?	9
2.3 Who can access your Personal Data?	10
2.4 How long will Capgemini keep your Personal Data?	10
2.5 What are your rights and how to exercise them?	11

NOTE: This SpeakUp Policy replaces and supersedes the SpeakUp Data Protection & Privacy Notice (version 1.2 dated October 31, 2017)



1. About SpeakUp

1.1 Introduction

Purpose

Capgemini, right from its inception, has always strived to be an ethical and humane company whose most important asset is its people. And this was always very strongly underpinned by Serge Kampf, our Group's founder. To reinforce and continue this ethical journey and ensure that Capgemini remains a workplace where team members grow and feel valued in a fair and open working environment, we have a leading-edge ethics concerns reporting and incident management tool called "SpeakUp". The SpeakUp helpline has been implemented by Capgemini to uphold its Values and protect its ethical culture; it also helps meet legal requirements in jurisdictions which have whistleblowing regulations.

SpeakUp is a voluntary, confidential web and phone-based intake system operated by Convercent, an independent service provider, and provided by Capgemini to its employees, external consultants, contractors, agency staff, customers, suppliers and business partners and those of its affiliates ("reporter").

SpeakUp is a commitment from Capgemini: to listen to your voice when you raise it in good faith; to be fair when investigating a concern, respect organizational justice, maintain confidentiality; and to protect you from any form of retaliation; a commitment which is endorsed by all members of the Board of Directors of Capgemini SE and members of the Group Executive Board (GEB) as part of their individual and collective support to the provisions of the Code of Business Ethics.

Scope

SpeakUp empowers reporters to report concerns and/or ask for advice and guidance about actions or behaviors that are:

1. not aligned with our Values, our Code of Business Ethics and related ethics & compliance policies,
2. not in compliance with applicable laws, or
3. that may significantly affect vital interests of Capgemini and its affiliates.

In certain countries, SpeakUp can only be used to report suspected violations of a more limited number of matters. To know the exact scope of matters that can be reported in your country, please refer to section 1.5 of this policy. If your concern pertains to a matter that, under local law, may not be accepted by Capgemini through SpeakUp, please contact your team leader, Ethics & Compliance Officer or a representative of the Human Resources department to report the matter.

SpeakUp is not a grievance helpline. It is not a platform to raise HR-related issues such as, but not limited to, performance review, compensation, career development and other topics of similar nature. For such issues, local grievance channels should be used.



Benefits

SpeakUp provides a simple, safe and centralized incident management system to report your concerns. Additionally, it:

- makes reporting concerns easy: anytime, anywhere, and in any language;
- ensures confidentiality and allows anonymity;
- promises prompt and systematic investigation along with time-bound and effective resolution;
- assures fairness and organizational justice and protection from retaliatory action; and
- gives an accurate overview of the ethics culture to top management.

You may contact Capgemini with any questions relating to this policy and/or the SpeakUp helpline by writing to ethics@capgemini.com.

1.2 Use of SpeakUp

Use of SpeakUp is entirely voluntary. As a reminder, the normal route for reporting a possible violation is to raise it directly to your team leader or to your Ethics & Compliance Officer or a representative of the Human Resources department; reasonable efforts would be made to ensure all concerns are captured in SpeakUp for better management of concerns. There may also be additional resources available in certain countries, such as staff representatives, grievance procedures or specific helplines.

If you do not feel comfortable raising a concern through the above-mentioned mechanisms, or if you raised a concern locally but think that it has not been handled properly, you can use SpeakUp.

Please be aware that the information you supply about yourself, your colleagues, or any aspect of the company's operations may result in decisions that affect others. Therefore, we ask that you only provide information that, to the best of your knowledge, at the time that the information is provided, is correct and factual. You will not be subject to disciplinary or adverse action by Capgemini for any report of a suspected legal or compliance violation that is made in "good faith", even if it later turns out to be incorrect. Acting in "good faith" means acting with an honest belief and intention. Please be aware, however, that knowingly providing false or misleading information will not be tolerated. Further, if it is determined that the reporter has not acted in good faith (i.e. the concern reported is found/known to be malicious or false), disciplinary action(s) may be taken against such reporters.

The information you submit will be treated confidentially except in cases where this is not possible because of legal requirements or in order to conduct a proper investigation; in any case all information will be handled sensitively.

You may remain anonymous where permitted by law. Even if you choose anonymity (partial or full), you can still opt to receive notifications about the concern by providing an email address and using your own login credentials (unique reference number which would be known only to you) that is associated with the concern:



- to track the progress of the concern
- to respond to any questions received from the investigation team

Although the dedicated investigation team will be able to communicate with you, using the 'Message' feature of the helpline, to seek additional information about your concern, they will not be able to identify you (even if you have provided your email address to receive notifications). Further, the investigation team's ability to address the concern largely depends on the information provided by you in the concern and your willingness to provide responses to any additional information requested by them; you are therefore requested to regularly login to SpeakUp to follow the status of your concern.

While SpeakUp allows anonymity, Capgemini strongly encourages reporters to disclose their identity when they report concerns as it would help address the concerns more efficiently. Additionally, it would help:

- expedite the investigation process since the investigation team has easy access to the reporter;
- protect the reporter, in case of any retaliation;
- avoid/reduce reporting of concerns done maliciously or in 'bad' faith; and
- reinforce the trust in the ethical culture of the organization.

You can report a concern or submit a question through SpeakUp by either visiting the SpeakUp portal (www.capgemini.com/speakup) or by using the local SpeakUp phone number available on the SpeakUp portal.

Know more about SpeakUp by watching the videos available on [Talent](#) (company intranet) and on the SpeakUp [portal](#).

1.3 Management of concerns

Once a concern is raised in the SpeakUp helpline, auto generated messages will be sent to (i) you, acknowledging receipt of the concern and (ii) Capgemini's Group Ethics Office notifying receipt of the concern. Group Ethics Office shall perform preliminary assessment of the concern to determine the appropriate course of action and your concern will accordingly be assigned to a dedicated team for appropriate action.

All concerns reported in SpeakUp will be dealt with thoroughly and as soon as reasonably practicable, taking into account the complexity and the nature of the concern. The dedicated team investigating the concern has the ability to reach out to the reporter (whether known or anonymous) to seek further information by asking follow-up questions using the 'Message' feature in SpeakUp. All involved stakeholders are required to cooperate during any investigation by providing requested information; failure to cooperate with an investigation is grounds for disciplinary action.

The reporter would be notified when the concern has been closed under SpeakUp; details in relation to outcome of the investigation will not be shared with the reporter considering Capgemini's obligation to keep the contents of the concern confidential.



In cases where there is a legal obligation to communicate the information to public bodies responsible for the prosecution of crimes or otherwise having jurisdiction over the matter, the dedicated team will contact the relevant competent authority having jurisdiction over the matter.

1.4 Non-Retaliation

Capgemini encourages a culture of openness where reporters can raise their genuine concerns regarding Capgemini's business practices in good faith and without fear of retaliation. Creating a safe and supportive environment where employees' views are respected, will allow employees to take personal responsibility for ensuring that our conduct is aligned with our Values and our Code of Business Ethics. It is crucial that employees who, in good faith, want to raise a concern or seek advice and guidance on an ethics or compliance concern, feel able to do so without fear of retaliation; "good faith" means that employees must act with an honest belief and intention.

The Group prohibits retaliation against anyone for raising or helping address a concern. Any form of retaliation is grounds for disciplinary action, up to and including dismissal in accordance with the applicable legislation.

If you witness or face any retaliation, it is important that you report it immediately; contact us through the 'message' functionality on SpeakUp portal or by writing to us at ethics@capgemini.com

1.5 Special Country Regulations

There are no specific restrictions for the following countries (as of February 25, 2019): Argentina, Australia, Austria, Brazil, China, Columbia, Germany, Guatemala, Hong Kong, Ireland, Japan, Malaysia, Mexico, New Zealand, Norway, Philippines, Poland, South Africa, Saudi Arabia, Singapore, Switzerland, Taiwan, United Arab Emirates, United Kingdom, United States of America, Vietnam.

Throughout much of the European Union and surrounding areas, concerns can only be reported relating to limited topics - typically accounting, auditing, bribery, competition law, discrimination and harassment and environment, health, hygiene, and safety matters. Further, some countries restrict concerns such that only employees in key or management functions may be the subject of a concern.

Any issues or concerns relating to topics not permitted by law to be reported via the SpeakUp helpline should be reported directly to your team leader or Ethics & Compliance Officer or a representative of the Human Resources department as appropriate for the subject matter of the possible violation.

In some countries, anonymous reports may not be permitted under the law except under extremely restrictive circumstances.



Belgium

- SpeakUp may only be used to report on internal matters relating to bribery, finance, accounting and auditing.

Canada

- For Capgemini and its Canadian affiliates' employees:
 - SpeakUp may only be used by employees who do not belong to either The Power Workers Union or The Society of United Professionals.
 - Employees who are members of either The Power Workers Union or The Society of United Professionals should raise their concerns by reporting them directly to the Ethics & Compliance officer for Canada, and not the SpeakUp helpline.

Czech Republic

- Concerns can only be reported in relation to:
 - possible irregularities such as
 - unfair competition;
 - bribery or corruption within the business of Capgemini;
 - conflicts of interest;
 - insider trading;
 - the commission of a criminal offence;
 - serious cases of
 - accounting, auditing or banking matters; or
 - vital Capgemini interests being affected;
 - in case of a serious threat to the health or safety of any team member; or
 - harassment or discrimination.

Denmark

- Concerns can only be reported relating to offences which entail misconduct or suspected serious misconduct that may impact the vital interests of the company or significant impacts to a person's health or life, such as e.g., economic crime (including bribery, fraud, forgery and similar offences) as well as irregularities in the areas of accounting and auditing, internal controls or financial reporting, anti-competition and insider trading but also cases of environmental pollution, serious violations of occupational safety rules and serious offences against an employee such as for instance violence or sexual offences.
- Any other issues or concerns that could affect Capgemini, such as cases of mental bullying, collegial difficulties, incompetence, absence, and breach of smoking and alcohol policies and workplace rules on the use of e-mails/internet, etc. should be reported directly to your team leader, Ethics & Compliance Officer or to a representative of the Human Resources department.

Finland

- Concerns can only be reported relating to offences or misconduct in relation to accounting, internal accounting controls or auditing, banking and financial crime or bribery.



France

- Concerns can be reported relating to:
 - crime, or misdemeanor;
 - serious and manifest violation of any international commitment ratified or approved by France;
 - serious and manifest violation of a unilateral act taken by an international organization on the ground of an international commitment regularly ratified;
 - serious and manifest violation of law or regulation;
 - or serious threat or damages to general interest. In such a case the reporter must have personal knowledge of the threat or the damage to the general interest;
 - conduct or situation violating provisions in the Code of Business Ethics and/or in the Group Anti-Corruption Policy relating to bribery and influence peddling.
- Disclosure of matters involving national defense, confidential medical issues or legal privilege are excluded from the scope of protection and cannot be disclosed.

Hungary

- Refer local SpeakUp policy applicable for Hungary.

India

- Refer local SpeakUp policy applicable for India.

Italy

- Concerns can be reported about violations of Capgemini's Code of Business Ethics and/or of the organizational and management model pursuant to Legislative Decree 231/01.

Luxembourg

- SpeakUp may only be used to report on internal matters relating to accounting, internal accounting controls, banking matters and bribery.

Morocco

- Concerns can only be reported relating to competition law, conflict of interests, insider trading, theft, fraud, assets misappropriation, irregularities in accounting, auditing or banking matters, improper financial reporting, bribery, sexual harassment, and discrimination.

Netherlands

- Concerns must relate to violation of laws, a danger to public health, a danger to the safety of persons or the environment or a threat to proper performance of the organization as a result of inappropriate acts or omissions.
- Concerns can only be reported relating to abuses within the organization you are working for or with which you are in contact during the course of your work.



- Any issues or concerns relating to other matters that could affect Capgemini – including general HR grievances and concerns relating to the Policy for Inappropriate Behavior (Beleid ongewenste omgangsvormen) – should be reported directly to your team leader, the confidential advisor, Ethics & Compliance Officer or to a representative of the Human Resources department.

Portugal

- Concerns can only be reported relating to bribery, financial, accounting and auditing matters.
- Anonymous reports are not permitted under the law; however, your personal information will be treated confidentially.
- Additionally, only employees in key or management functions may be reported upon.

Romania

- Concerns can only be reported in relation to:
 - possible irregularities such as
 - unfair competition;
 - bribery or corruption within the business of Capgemini;
 - conflicts of interest;
 - insider trading;
 - the commission of a criminal offence;
 - serious cases of
 - accounting, auditing or banking matters; or
 - vital Capgemini interests being affected;
 - in case of a serious threat to the health or safety of any team member; or
 - harassment or discrimination.

Russia

- Concerns submitted should relate to the performance of working duties by employees and their behavior at work and should not contain details of employees' private life, otherwise whistleblowers may be held liable for an unauthorized disclosure of private life secrets.

Slovak Republic

- Concerns can only be reported in relation to:
 - possible irregularities such as
 - unfair competition;
 - bribery or corruption within the business of Capgemini;
 - conflicts of interest;
 - insider trading;
 - the commission of a criminal offence;
 - serious cases of
 - accounting, auditing or banking matters; or
 - vital Capgemini interests being affected;



- in case of a serious threat to the health or safety of any team member; or
- harassment or discrimination.

Spain

- Concerns can only be reported relating to breach of laws or violations of Capgemini's Code of Business Ethics and policies, e.g., bribery, financial, accounting and auditing matters.

Sweden

- Concerns can only be reported with respect to serious irregularities relating to financial, accounting, internal accounting controls, auditing, bribery and banking and financial crime matters as well as other serious misconduct/infractions impacting the vital interests of the company or threats to a person's health or life.
- Additionally, only employees in key, management or leading functions may be reported upon.

2. Privacy Notice

2.1 Definitions

"Personal Data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Data Subjects" means the natural person whose Personal Data are processed.

"Binding Corporate Rules" or **"BCR"** means Personal Data protection policies which are adhered to by a controller or a processor established on the territory of a Member State for transfers of Personal Data to a controller or a processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

"EU Model Clauses" means the standard contractual clauses adopted by the European Commission for the transfer of Personal Data from data controllers located in the European Union to data controllers or data processors established outside the European Union or European Economic Area.

"Supervisory Authority" means the public authority responsible for monitoring the application of the applicable data protection laws and regulations.

2.2 Who is processing your Personal Data and why?

Capgemini Service SAS and affiliates of Capgemini SE (together referred to as "Capgemini"), through the SpeakUp helpline capture and further process Personal Data to investigate a concern submitted by the reporter. The processing of Personal Data is carried out by Capgemini in its legitimate interest to uphold its Values and protect its ethical culture by



fostering an open, transparent and safe working environment and to comply with legal obligations in certain countries which have whistleblowing regulations.

The Personal Data and information you share and which may be processed by Capgemini include: (i) your name, your contact details and whether you are employed by Capgemini; (ii) the name and other personal data of the persons you name in your report if you provide such information (e.g., description of functions and contact details); and (iii) a description of the alleged misconduct as well as a description of the circumstances of the incident, which may contain Personal Data.

2.3 Who can access your Personal Data?

The Personal Data and information you provide will be stored in a secure database which is located on servers hosted and operated by a third-party service provider, Convercent, in Ireland. Convercent has entered into contractual commitments with Capgemini to secure the information you provide in accordance with applicable law.

For the purpose of processing and investigating your concern and subject to the provisions of applicable local laws, the Personal Data and information you provide shall be communicated to Capgemini's Group Ethics Office, which shall perform a first review of your concern. Depending on the Group Ethics Office's assessment, your concern will be assigned to a dedicated team for appropriate action whereby the Personal Data and information you provided may be accessed and, further processed by the relevant personnel of Capgemini, including Ethics, Human Resources, Finance, Internal Audit, Legal, management, external advisors (e.g., legal advisors), and, in limited circumstances, by technical staff at Convercent.

As a result, the Personal Data and information you provided in your concern may be transferred to Capgemini's affiliates and/or third parties located outside of the European Union ("**EU**").

Where the Personal Data and information are transferred to Capgemini affiliates, such transfer shall be covered by Capgemini's Binding Corporate Rules ("**BCR**"), ensuring an appropriate level of protection to the Personal Data. For more information on the BCR: <https://www.capgemini.com/resources/capgemini-binding-corporate-rules/>

In addition, your Personal Data may be accessed from the United States of America for maintenance purposes, in which case such transfer shall be framed by the EU Model Clauses, ensuring an adequate level of protection to the Personal Data.

Personal Data and information you provide may also be disclosed to the police and/or other enforcement or regulatory authorities for investigation purposes.

2.4 How long will Capgemini keep your Personal Data?

Where your concern falls outside the scope of SpeakUp, Personal Data contained in the concern will be redacted immediately upon such assessment.



Where your concern falls into the scope of the SpeakUp helpline, Personal Data you provided will be kept for:

- Two (2) months maximum after closing the concern in SpeakUp tool, or
- The duration of the disciplinary or judicial procedure where applicable,
- Except that if the data is required in the event of a potential lawsuit against the Company, it will be kept for the duration of the statute of limitations regarding the potential lawsuit.

2.5 What are your rights and how to exercise them?

As a Data Subject you can request to access, rectify or erase your Personal Data. You may also object to the processing of your Personal Data, or request that it be restricted. In addition, you can ask for the communication of your Personal Data in a structured, commonly used and machine-readable format.

If you wish to exercise those rights, please contact Capgemini's Global Data Protection Officer by sending an email to the following address: dpocapgemini.global@capgemini.com Please note that you also have the right to lodge a complaint before a Supervisory Authority and/or before the competent court of law.

Capgemini will promptly notify any person who is the subject of a concern as to the status of their concern, except where such notification must be delayed to preserve evidence. The subject of the concern has the right to access information relating to the concern (with the exception of data that may allow to identify the reporter) and to request correction of his/her Personal Data that may be inaccurate or incomplete in accordance with applicable law.

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in over 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Learn more about us at www.capgemini.com



People matter, results count.

This message is intended only for the person to whom it is addressed. If you are not the intended recipient, you are not authorized to read, print, retain, copy, disseminate, distribute, or use this message or any part thereof. If you receive this message in error, please notify the sender immediately and delete all copies of this message.

This message contains information that may be privileged or confidential and is the property of the Capgemini Group. Copyright © 2019 Capgemini. All rights reserved.