TECHTARGET, INC.
CODE OF BUSINESS CONDUCT AND ETHICS

Last approved by the Board of Directors: April 24, 2026

Introduction

Purpose

The Board of Directors of TechTarget, Inc. (together with its subsidiaries, "TechTarget" or the "Company") established the Code of Business Conduct and Ethics (the "Code") to aid the Company's directors, officers (including the principal executive officer, principal financial officer, principal accounting officer or controller, or persons performing similar functions), and in making ethical and legal decisions when conducting business and performing their day-to-day duties and to avoid the appearance of improper behavior. The Company's board of directors (the "Board of Directors") is responsible for administering the Code. The Board of Directors has delegated day-to-day responsibility for administering and interpreting the Code to the General Counsel.

TechTarget expects all directors, officers, and employees, as well as covered contractors and temporary or third-party workers, (collectively, "Colleagues" or "you") to exercise reasonable judgment when conducting business and to refer to the Code frequently to ensure that they are acting within both the letter and the spirit of the Code.

TechTarget also understands that the Code will not contain the answer to every situation you may encounter or every concern you may have about conducting business ethically and legally. In these situations, or if you otherwise have questions or concerns about the Code, you are encouraged to speak with your supervisor or manager (if applicable) or, if you are uncomfortable doing that, with the Company's Human Resources Department or General Counsel, or other resources by using the channels of communications provided in the Speak Up section of the Code.

How we work at TechTarget

The Code is designed to ensure, among other things, that all Colleagues have the guidance and information needed to develop and sustain ethical, long-term and mutually beneficial connections with customers, business partners, investors, the communities in which we operate and one another. We are each responsible for ensuring we remain familiar with the Code and associated Global Policies and for completing any training provided. If any of the sections in the Code are particularly relevant to your role, you can talk to your supervisor or manager or contact the Company's Human Resources Department or General Counsel, to find out more.

Communication of Code

All Colleagues will be asked to acknowledge that they have received and read a copy of the Code when they start at TechTarget. Updates of the Code will be provided from time to time. A copy of the Code is also available on the Company's website at https://www.techtarget.com/terms-and-conditions/.

All Colleagues generally have other legal and contractual obligations to the Company. The Code is not intended to reduce or limit the other obligations that you may have including, in particular, the Company's Insider Trading and Public Communication Policy ("Insider Trading Policy"). Instead, the standards in the Code should be viewed as the *minimum standards* that are expected of you when conducting business.

The Code cannot and is not designed to cover every situation. If you are facing a dilemma, consider the following:

- **Does it meet applicable regulations and the law?**
- **Does it align with good standards of decency, morality and respect?**
- **Is it consistent with our Policies?**
- **Would I feel proud if my action became public?**

Compliance with Laws, Rules and Regulations

We seek to conduct our business in compliance with applicable laws, rules and regulations. No Colleague, regardless of position, tenure or seniority, should engage in, or instruct any other Colleague to engage in, any unlawful activity in conducting TechTarget business or in performing your day-to-day Company duties.

Working with others

Conflicts of Interest

We all have personal and professional connections or interests with people or organizations we trust, and it is natural that we turn to them when an opportunity arises. A conflict of interest occurs if these personal and professional connections or interests influence or conflict with the actions and decisions we make on behalf of TechTarget, so that we may longer be acting in TechTarget's best interests.

Conflicts of interest may arise in many situations, including the following:

- if an individual is simultaneously employed or engaged by TechTarget and another business concern, particularly a TechTarget client or business partner
- if an individual takes part in any activity that enhances or supports a competitor's position, including accepting simultaneous employment with a competitor
- if an individual or any member of an individual's immediate family gives or accepts any gift with the intent to improperly influence the normal business relationship between TechTarget and its clients or other business partners, or gives or accepts any gifts from a competitor
- if an individual or any member of an individual's immediate family holds a financial interest in an outside business concern, particularly, a TechTarget client or business partner, and
- if an individual conducts business on behalf of TechTarget with a business in which a family member is associated in any significant role.

Many factors must be considered in determining whether a conflict of interest exists, including the size and nature of the involvement; the ability to influence TechTarget's decisions; access to confidential information on either side; and the nature of the relationship between TechTarget and the outside business concern.

The Stockholders Agreement, dated on or about the Closing Date (as defined below) (as amended from time to time, the "Stockholders Agreement"), by and among the Company, Informa PLC ("Informa") and Informa US Holdings Limited, contains provisions that address potential conflicts of interest affecting directors and officers of the Company (including the Company's subsidiaries) who also serve from time to time as directors, officers, or employees of Informa or its subsidiaries (other than the Company) ("Informa Group Associates"). The Company's Related Party Transactions Policy, adopted in accordance with the Stockholders Agreement, governs certain transactions between the Company (including the Company's subsidiaries), on the one hand, and Informa or any of its subsidiaries (other than the Company and its subsidiaries) or (solely in their capacity as such) any Informa Group Associate or other "associate" of Informa or its subsidiaries, on the other hand ("Informa Related Party Transactions"). To the extent any provision of this Code is inconsistent with the Stockholders Agreement or the Related Party Transactions Policy, the Stockholders Agreement or the Related Party Transactions Policy, as applicable, will prevail. Each individual's situation is different and evaluating a situation for a director, officer or colleague will require the consideration of many factors. Each individual is responsible for promptly reporting in writing to their supervisor or manager any transaction or relationship that reasonably may be expected to give rise to an actual or apparent conflict of interest. Additionally, the Company's General Counsel may notify the Board of Directors or appropriate committee or take other action as required.

Actual or potential conflicts of interest involving a director or executive officer should be disclosed in writing directly to the Chair of the Board of Directors who will determine whether the transaction or relationship constitutes an actual or apparent conflict of interest.

If an Informa Group Associate is subject to a particular conflict of interest involving Informa or one of its subsidiaries (other than the Company and its subsidiaries) (an “Informa Conflict of Interest”), the conflict must be addressed in accordance with the Stockholders Agreement and the Related Party Transactions Policy.

Individuals may not participate in any transaction or relationship that reasonably could be expected to give rise to a conflict of interest other than an Informa Conflict of Interest unless they first obtain specific, written approval from the Compliance Officer or, if they are a director or executive officer, the Chair of the Board or the Lead Independent Director. Individuals are not required to give notice of, or obtain approval for, Informa Related Party Transactions that are permitted under the Related Party Transactions Policy.

Corporate Opportunities

- All Colleagues owe a duty to the Company to advance its legitimate business interests when the opportunity to do so arises.

The Stockholders Agreement provides that with respect to a potential transaction or matter that may be a corporate opportunity for both (a) the Company (including the Company's subsidiaries) and (b) Informa or its other subsidiaries (an "Informa Opportunity"), unless Informa and the Company agree otherwise:

- a corporate opportunity offered to an individual who is a director but not an officer or employee of the Company and who is also an Ivory Group Associate (as defined in the Stockholders Agreement) shall belong to the Company only if the opportunity is expressly offered to that person solely in that person's capacity as a director of the Company, and otherwise the opportunity shall belong to Informa; and
- a corporate opportunity offered to an individual who is an officer or employee of the Company and who also is an Ivory Group Associate shall belong to the Company unless the opportunity is expressly offered to that person in that person's capacity as a director, officer, or employee of Informa or its subsidiaries, in which case the opportunity shall belong to Informa.

Subject to the Stockholders Agreement, each employee, officer, and director is prohibited from:

- diverting any opportunities, other than Informa Opportunities, that are discovered through the use of the Company’s property or information or as a result of their position within the Company to their own, or someone else’s benefit unless such opportunity has first been presented to, and rejected by, the Company;
- using the Company’s property or information or leverages their position within the Company for improper personal gain; and
- competing with the Company.

Anti-competitive behavior

Anti-competitive behavior can go by different names depending on your geographic region. Wherever you are in the world, however, the principles are generally consistent and are designed to ensure businesses don’t take unfair advantage in the marketplace by entering into any agreements with a third party to divide or control the marketplace, or act in such a way that could manipulate it illegally to their benefit. Anti-competition laws are often complex, so always discuss any relevant matter with our Legal team. These laws also may apply when we are engaging in sales, marketing, and advertising for our products and services, undertaking corporate development activity such as acquisitions, launching a new product, or entering a new market.

We should never, either directly or through an agent, enter into any agreement, in any form, with a supplier, competitor or other third party that involves:

- Fixing prices or any aspect of pricing, such as discounts or credit terms, at which we and a competitor will buy and sell products and services

- Dividing up or allocating or otherwise restricting marketplaces, territories, customers or any other definable market
- Attaching inappropriate conditions of sale
- Exchanging commercially sensitive information, including prices, costs, discounts, terms and conditions, sales, volumes or credit arrangements
- Influencing the outcome of a competitive tender or colluding with our competitors.

Colleagues should remain aware of the limits of the conversations we can have with those working for competitors, even if they are a former colleague, personal friend, or family member, and should ensure they do not share or become party to any disclosure of confidential, privileged, or commercially sensitive information, however informally. It is equally important that we should never manipulate, conceal, or misrepresent material facts at any time.

Colleagues joining TechTarget from a competitor should ensure they do not bring with them or make use of any confidential, proprietary, or commercially sensitive information from their previous employment.

Bribery and Corruption

A bribe can be anything of value, either offered or accepted, which is intended to influence an action, secure a business advantage or affect someone's professional judgment. It can be anything of value or which creates a feeling of gratitude such as cash, gifts or hospitality, vouchers, shares, charitable donations, a job offer, or an internship. It can be large and lavish, or a small facilitation payment designed to encourage someone to perform a normal job more quickly.

We have zero tolerance for all forms of bribery or corruption and are committed to complying with all applicable anti-bribery and anti-corruption laws. We expect all colleagues to act in accordance with this commitment, wherever they work and whoever they work with.

When working with public officials, we should be especially careful to ensure that everything we do or say is above reproach and cannot be misinterpreted.

If you are offered or asked for a bribe, REFUSE, and report it to the General Counsel immediately.

Gifts and Entertainment

Giving or receiving gifts and hospitality can be an important part of maintaining and developing business relationships.

Even where it is not the intent, lavish or unreasonable gifts or entertainment can appear to be a form of bribery. The appearance of corrupt activity can be enough to put our reputation at risk and lose the trust of our partners.

All gifts and entertainment must be **moderate, appropriate, occasional** and have a **genuine business purpose.**

Colleagues should never give or accept cash or a cash equivalent, such as gift vouchers, or offer or demand something in return.

Particular care needs to be taken when extending the offer or accepting any meals, refreshments, travel or hospitality of any value from government or public official. You must first discuss the matter with Legal or Compliance.

Ensure details of any gifts and entertainment, given or received, worth over $150 (or local equivalent) are accurately recorded in the expenses system including details of the recipient's name, organization and the business purpose and have your supervisor's or manager's approval.

Political contributions

Business contributions to political campaigns are strictly regulated. Accordingly, all political contributions proposed to be made with TechTarget's funds must be first approved and coordinated through the General Counsel. Individuals may make personal contributions but may not represent that they are making any such contribution on the Company's behalf.

TechTarget does not make donations to political parties, candidates or campaigns in any of the countries in which we operate. We do not engage in lobbying on our own behalf. Where we are members of any broader industry associations, these will engage with governments as representatives of industry views, and not for a single issue.

We respect the rights of Colleagues to participate in political activities and contribute to the political parties of their choice on their own time. Colleagues should never suffer discrimination because of their personal political affiliations or lack of them. Any personal political activity must take place outside work and should not use our resources or make any claim of support on TechTarget's behalf.

International Trade Sanctions

We are committed to conducting business in accordance with applicable international trade laws and sanctions.

Sanctions are measures imposed by governments and international organizations, such as the United Nations, intended to deter a range of activities, which may include political or military aggression, providing sanctuary for criminals or terrorists, developing nuclear or other weapons programs, and abusing human rights.

This means we are restricted in our dealings with certain individuals, businesses, nations, or particular industries in some countries. We are careful to ensure we comply with all applicable international sanctions and review transactions and third parties against relevant international watch lists.

Sanctions rules and restrictions are complex and change frequently. Colleagues should refer to any applicable Sanctions Policy or procedure in determining whether such restrictions apply.

Money Matters

Insider Trading

A fair stock market depends on ensuring that no-one misuses inside information to gain an unfair advantage when trading shares or securities.

There are instances where Colleagues may have information about TechTarget or a third party that is not known to the investing public. Such information, referred to as "non-public" or "inside" information, may relate to, among other things: business plans; new products; mergers, acquisitions or dispositions of businesses or securities; problems facing our company or a company with which we do business; significant contracts or business relationships; significant litigation; or financial information.

If you have access to such confidential information, it should be handled carefully and never disclosed to anyone who is not authorized to have access, including family members, nor used as a basis to make recommendations to anyone about share trading nor buy or sell any company securities themselves, until such information becomes public. If the information is such that a reasonable investor would consider the information important in reaching an investment decision (i.e., material), then the person who holds the information must not buy or sell Company securities nor provide such information to others, until such information becomes public. Further, you must not buy or sell securities in any other company about which you have such material non-public information, nor provide such information to others, including family or friends until such information becomes public.

Anyone who engages in illegal insider trading (either by personally engaging in the trading or by disclosing material non-public information to others) will be subject to disciplinary action including termination.

You can find more information in our Insider Trading Policy or contact the Geneal Counsel for further assistance.

Accurate Records and Financial Integrity

The accuracy and integrity of our information, including any data relating to business operations, is essential to maintaining the trust and confidence of all our business partners, including investors. We create and maintain full and accurate records in relation to all aspects of our business and in compliance with all applicable local laws and regulations.

As a listed company whose shares are publicly traded, we must comply with all relevant financial reporting and accounting standards and regulations and ensure that the reports and documents we file with the United States Securities Exchange Commission and the other public communications we make are timely and contain fulsome, fair, accurate, complete information. Colleagues responsible for these disclosures must use sound judgment and act with honesty, ethics, and objectivity to meet this standard.

Fraud of any kind is forbidden, including falsifying expense claims, misappropriating assets, falsifying sales information or dishonestly altering or leaving company records incomplete. In addition, Colleagues should never facilitate others to evade paying tax or commit tax fraud, including other colleagues, contractors, customers and business partners.

Decision Making

We set a framework around the authorization of financial expenditure, contracts, and other commitments to safeguard our assets and protect against unauthorized transactions.

The Vendor Contract & Invoice Approval Policy, and any successor policy, describes the decision-making limits that are in place to ensure that the right people and teams are involved in these decisions and that the appropriate level of risk analysis has been completed before we enter into legal and financial commitments.

Colleagues should make themselves aware of how these limits apply to them, and which decisions are within their authority or require additional approval.

Tax

We recognize that the taxes paid by companies like TechTarget help governments provide the vital services and infrastructure from which we all benefit, and that a fair and effective tax system is in the interests of tax-payers and the community as a whole.

TechTarget takes a principled and risk-based approach to taxes, managing costs in accordance with our responsibilities to shareholders, and ensuring that we pay our taxes in full and on time, in compliance with both the letter and intent of the laws of the countries in which we operate.

Dealing with Data

Managing our information and information systems

Our information is one of our most valuable assets, and we have both legal and commercial reasons to manage and protect it, and to ensure we can meet our customers' needs and maintain their trust. Each of us has a role to play in safeguarding TechTarget's data and systems and complying with applicable laws and industry regulations.

Protection and Proper use of the Company's assets

Our business assets include our intellectual property, customer data, proprietary information, employee time, brands, funds, our facilities and offices, and other physical assets, such as laptops, phones and equipment. Loss, theft and misuse of our assets have a direct impact on our business and its

profitability. Colleagues are expected to protect any assets that are entrusted to them and take steps to ensure that they are used only for legitimate business purposes.

Confidential and Proprietary Information

Proprietary information is crucial to TechTarget's business, competitiveness, and future prospects. Colleagues must not disclose or use information without prior written permission, both during and after their employment at TechTarget, except as permitted under the Stockholders Agreement (which authorizes the sharing of information with Informa and its other subsidiaries under certain circumstances). They must also prevent unauthorized disclosures and return all proprietary information when they cease employment.

The Stockholders Agreement generally permits Informa Group Associates to share information about the Company with Informa and gives Informa the right to obtain various types of Company-related information from the Company. This Code does not prohibit disclosures to Informa that are permitted or required under the Stockholders Agreement.

Proprietary information includes:

- Corporate: Plans, strategies, policies, negotiations, litigation.
- Marketing: Strategies, customer/prospect details, market analyses.
- Financial: Performance data, debt arrangements, equity structure, sales data.
- Operational/Technological: Manuals, software, designs, procedures, inventions.
- Personnel: Organizational structure, resumes, compensation, evaluations.
- Personal Data: Identifiable information about colleagues, members, and partners
- Third party: Information received in confidence by TechTarget from a client or other third parties.

We are dedicated to protecting this information through robust data protection and privacy policies. Colleagues must secure confidential information against loss, unauthorized access, and misuse, and only use personal data as necessary for their job roles, adhering to our policies and laws. Every Colleague has a responsibility to take proactive and thoughtful measures to secure any confidential or proprietary information, including material non-public information, and to safeguard such information against data loss, unauthorized access or exposure, and misuse.

Colleagues who have access to personal data may access, use and share such data only to the extent necessary and relevant to fulfil their assigned job responsibilities and in accordance with the Company's policies and applicable laws and regulations.

Any suspected theft or unauthorized access to personal data must be reported to the Privacy and Data Protection Officer. All Colleagues should refer to their applicable employment-related agreements and Company policies and procedures for more detail on their obligations with respect to confidential and proprietary information and other related matters. For questions about personal data, consult the Legal Department.

Intellectual Property: Patents, Copyrights and Trademarks

Subject to the Stockholders Agreement, any intellectual property you create or develop during your employment with us is considered the Company's property, except where state law or a formal written agreement specifies otherwise. We ask that you promptly disclose any such intellectual property to us and assist in securing the necessary protections, including patents, copyrights, and trademarks. For detailed information on your obligations regarding intellectual property, please refer to your applicable employment-related agreements and related Company policies and procedures.

Intellectual property that an Informa Group Associate develops in performing employment-related obligations for Informa or another subsidiary of Informa belongs to Informa and not to the Company. This Code does not prohibit disclosures to Informa that are permitted or required under the Stockholders Agreement.

Privacy and Personal Data

We respect the right individuals have to privacy and are committed to managing and protecting personal information and data responsibly and in accordance with all applicable data privacy laws and regulations.

We collect and use personal information for a wide range of business purposes, including Colleague payroll and benefit information, recruitment, marketing and sales, author and supplier payments, and customer invoicing.

Colleagues who are responsible for collecting, managing or using any personal data, whether this is from colleagues, customers or business partners, should ensure they follow these key principles:

- Do not collect sensitive personal information, such as data on an individual's health, unless you have first consulted with the Privacy and Data Protection Officer
- Consider data privacy implications when any new processing activity is being planned
- Market compliantly: collect and maintain all necessary rights, permissions or authorizations to use the data
- Ensure confidentiality and security: keep personal data secure to protect against accidental loss, theft, or transfer
- Be accountable: ensure you understand the laws and regulations that apply to you and any data you manage
- Respect individuals' rights: inform them about the data that is being collected and its purpose
- Use personal information responsibly: ensure the data is accurate, relevant, not excessive and not held for longer than is necessary

If you believe there has been a potential or actual data breach, **immediately** report it in accordance with applicable Company policies and procedures.

Marketing and Advertising

The marketing and advertising we engage in and the related services we provide to our customers connects people and communities across the world with knowledge. We strive to ensure that all these communications show integrity and reflect generally accepted contemporary standards of good taste and decency, both locally and globally. We are responsible for ensuring the impact of our marketing is evaluated from the perspective of the target audience and do not knowingly market to vulnerable groups, such as children or support those who do, or produce, host or distribute content that is disrespectful of human life or promotes hatred, violence or discrimination.

Our people and communities

Health, Safety and Security

As a business, we aim to cause zero harm, and each of us has a part to play in ensuring the health, safety and security of ourselves, colleagues, customers, business partners, and the communities in which we operate.

All Colleagues have the right to come home from work healthy and safe, and for that reason, each of us is responsible for understanding and following the health and safety laws and regulations that apply to any offices, events or external locations visited as part of work.

- We must understand health, safety and security considerations when planning any new projects, events, or business travel
- We should follow the support and advice given,

Colleagues have a responsibility to call out any unsafe behavior or safety hazards that are seen. If there is immediate risk, get the activity stopped where possible and report to your supervisor or manager.
Security processes help to safeguard our offices from unwanted visitors, protect our events and equipment and form part of all our working lives.

We should always:

- Respect and follow any security or access processes in place at an event location or office
- Listen to advice about local security issues
- Ensure that the security of colleagues, customers and communities is integral to any event or project planning

Responding to Unexpected Events and Emergencies

Unexpected events can impact any business. Careful planning is undertaken to try to ensure work can continue safely and effectively wherever we are and whatever has happened. Business continuity plans and processes are put in place to assist this and ensure we stay secure and connected, and colleagues have a responsibility to stay up to date with these. In addition, be aware of any emergency procedures, such as fire or earthquake response processes, for your office and any other office or event location you may be visiting. Look after any visitors hosted at the office or location where you work, make them aware of any relevant processes and support them if anything happens

Consumption of Drugs and Alcohol

Alcohol and drugs can lead to reduced effectiveness, impaired judgement and increased health and safety risks. We are all expected to demonstrate responsible behavior and act in a way that will not have a detrimental effect on our reputation, violate the law, impact the safety of others or cause inappropriate conduct. The use of illegal drugs in our offices, company events, or while travelling on TechTarget business is strictly prohibited.

Respect at Work

All Colleagues should feel that they and their contributions are respected and valued at work. To support this, we are committed to providing a working environment in which all Colleagues feel included and are able and encouraged to participate.

We do not tolerate any behavior that undermines this commitment or makes anyone feel unsafe or unwelcome, including discrimination, bullying, harassment and sexual harassment.

This commitment is not limited to our offices. Colleagues who habitually work away from the rest of their team, either at a different location or from a home office, should not feel unsupported or unequal because of their place of work.

We encourage Colleagues to report any behavior that they genuinely believe to be improper, unethical, or inappropriate and we have zero tolerance for any form of retaliation for raising such concerns.

As a provider of specialist products and services to a global and diverse customer base, it is an essential part of our success that we recruit and retain an international colleague base with a broad range of skills, experiences, and ideas.

Our commitment to this equality of opportunity informs all aspects of how we operate, from recruitment, developing and promoting colleagues, to the opportunities and forums on offer, and how we go to market.

We aim to ensure that Colleagues are treated equally, based on each person's skills, abilities, and performance, and that employment decisions are not based on any legally-recognized class, personal characteristic, or status, such as sex, race, color or ethnicity, national origin, ancestry, citizenship, gender expression or identity, sexual orientation, religion, age, marital or parental status, or physical or mental disability.

Labor and Employment

TechTarget and all colleagues are required to comply with the relevant laws regarding labor and employment in the countries in which we operate. These laws include, but are not limited to, equal

employment opportunity, harassment and discrimination, and safety and health. For more detailed information related to labor and employment, you should consult your Employee Handbook.

Modern Slavery and Child Labor

We believe that the practice of using modern slavery, child, and forced labor has no part in any business or supply chain, and we seek to eliminate it from our supply chains. This includes all forms of labor where the choice to work or not work has been removed, or where children's rights and freedoms have been affected including:

- Forced labor by using physical or mental threats, such as threats to loved ones
- Domestic servitude
- Debt bondage, where workers cannot pay off debts incurred to do the work, such as excessive agency or accommodation fees
- Removal of freedom to leave by withholding identity documents or moving workers to a place they cannot afford to leave
- Child labor, especially where children lose access to education and play, or the work is heavy, illegal or dangerous
- Human trafficking

More information on what we do can be found in TechTarget's Modern Slavery Statement, which is updated annually.

Monitoring Compliance and Disciplinary Action

Disciplinary measures for violations of the Code may include, but are not limited to, counselling, oral or written reprimands, warnings, probation or suspension with or without pay, demotions, reductions in salary, termination of employment or service and restitution.

The Company's management shall periodically report to our Board of Directors on these compliance efforts including, without limitation, periodic reporting of alleged violations of the Code and the actions taken with respect to any such violation.

Speaking Up and Asking Questions

Communication Channels

You are encouraged to proactively ask questions, seek guidance, and report suspected violations of the Code and other policies and procedures, or suspected violation of applicable laws, rules, or regulations arising during the course of business or occurring on our property.

Seeking Guidance

The best starting point for advice on ethics-related issues or reporting potential violations is your supervisor or manager. However, if the conduct in question involves your supervisor or manager, or you do not believe that it will be dealt with properly, or if you would otherwise feel more comfortable raising the matter through another resource, please use the channels provided below.

If you believe that potential misconduct has taken place, may be taking place, or may be about to happen you are obligated to bring the matter to the attention of the General Counsel by any of the following methods:

- In writing (which may be done anonymously) addressed to the Code of Business Conduct and Ethics/General Counsel, c/o TechTarget, Inc., 275 Grove Street, Newton, MA 02466, USA;
- By e-mail to legal@techtarget.com (anonymity cannot be maintained);
- By phoning the General Counsel at (617) 431-9875 (anonymity cannot be maintained);
- Via Speak Up, by phoning our whistleblowing line (which may be done anonymously) at (+1 (844) 408-0253); during this phone call, the Colleague should identify the subject matter of their

concern, question or complaint and/or the practices that are alleged to constitute a violation of the Code, providing as much detail as possible; or
- Via Speak Up, by submitting information through our third-party whistleblower website/mobile websites: www.techtarget.ethicspoint.com (website) or https://techtarget.navexone.com/ (mobile website).

Nothing in this Code prevents you from reporting potential violations of law to relevant government authorities.

Reporting Accounting and Similar Concerns. Any concerns or questions regarding potential violations of the Code, any other company policy or procedure or applicable law, rules or regulations involving accounting, internal accounting controls, or auditing matters, or if the officer or employee does not feel that he or she can discuss the matter with the General Counsel, may also be directed to the Audit Committee or a designee of the Audit Committee. Officers and colleagues may communicate with the Audit Committee or its designee:

- In writing (which may be done anonymously) to: Chair of the Audit Committee, c/o TechTarget, Inc., 275 Grove Street, Newton, MA 02466; or
- By e-mail to the Chair of the Audit Committee to auditchair@techtarget.com (anonymity cannot be maintained).

Misuse of Reporting Channels. Colleagues must not use these reporting channels in bad faith or in a false or frivolous manner. Further, colleagues should not use these reporting channels to report grievances that do not involve the Code or other ethics-related issues.

Anonymity

When reporting suspected Code violations, we hope you feel able to tell us who you are to facilitate a proper investigation. However, anonymous reports are also accepted in countries where it is legal.
If you choose to remain anonymous, the Company will try to protect your confidentiality, subject to legal requirements. It is generally difficult to investigate a report and act on the information you provide where your identity remains unknown, so anonymous reports should include as many details as possible, such as when and where the incident occurred, who was involved, and any witnesses, to allow for effective evaluation and investigation.

No Retaliation

The Company expressly forbids any retaliation against anyone who, acting in good faith, reports suspected misconduct. Anyone who participates in retaliation is subject to disciplinary action, including termination. For further assistance, please contact:

- Human Resources Department
- Legal Department

Waivers and Amendments

No waiver of any provisions of the Code for the benefit of a director or an executive officer (which includes without limitation, for purposes of the Code, the Company's principal executive, financial and accounting officers) shall be effective unless (i) approved by the Board of Directors or designated committee, and (ii) if applicable, such waiver is promptly disclosed to the Company's stockholders in accordance with applicable United States securities laws and/or the rules and regulations of the exchange or system on which the Company's shares are traded or quoted, as the case may be. Any waivers of the Code for other colleagues may be made by the General Counsel, the Board of Directors or, if permitted, designated committee.

All amendments to the Code must be approved by the Board of Directors or designated committee and, if applicable, must be promptly disclosed to the Company's stockholders in accordance with applicable United States securities laws and/or the rules and regulations of the exchange or system on which the Company's shares are traded or quoted, as the case may be.

Effective Date

The Code shall be effective as of the Closing Date (as defined in that certain Agreement and Plan of Merger, dated as of January 10, 2024, by and among the Company, Informa US Holdings Limited, and the other parties thereto).