

Code of Conduct of the Sygnity Group Companies

The companies of the Sygnity Group (hereinafter separately referred to as a “Company” or collectively as the “Companies” or the “Capital Group”, except for cases concerning Sygnity itself, where the term “Sygnity” will be used), related parties of the Total Specific Solutions Group (hereinafter referred to as the ‘TSS Group’), are committed to conducting their business with integrity, complying with laws and standards, and ensuring that each of its employees, associates and business partners is treated with respect. The Companies are proud of their reputation as responsible and reliable business partners. This Code of Conduct of the Sygnity Group Companies (hereinafter referred to as ‘the Code of Conduct’) contains the main business standards defining the principles of ethical behavior to be observed by all associates, employees, directors and members of the management board (the ‘Representatives’).

The Companies aim to integrate in their long-term strategy and business model not only economic considerations, but also ESG: environmental, social, as well as corporate governance aspects. This approach reflects a commitment to business ethics and sustainable, responsible practices. Companies will strive to balance their economic viability with the broader interests of society and responsible organisational management.

The Code of Conduct was also created with the firm belief that Sygnity should actively contribute to sustainable development that meets the needs of the present generation without compromising the opportunities of future generations to satisfy their own needs¹. Sygnity seeks to turn this commitment into action by adopting the following *General Principles of RBC*² as a testament to its dedication to the following goals:

¹ An idea expressed in the 1987 report of the World Commission on Environment and Development (WCED) – „Our Common Future”.

² Responsible Business Conduct

- Contributing to economic, environmental and social progress to support sustainable development; □ Respecting human rights, prioritising areas affected by the company's activities.
- Promoting capacity building in the region by collaborating with local communities, including business circles, and expanding the company's activities in the domestic and foreign markets, in line with good business practices.
- Fostering human capital development by creating employment opportunities and training programmes for employees.
- Refraining from seeking or accepting exemptions not permitted by statutes or laws related to human rights, the environment, health and safety, labour, taxation, financial incentives or other areas.
- Promoting and adhering to the principles of good corporate governance, as well as developing and implementing effective governance practices, including at the Capital Group level.
- Developing and implementing effective internal control practices and management systems to build mutual trust with the communities in which Sygnity operates.
- Promoting awareness and compliance with the company's RBC policies among employees through education initiatives, including training programmes.
- Refraining from discriminatory or disciplinary action against employees who, in good faith, report instances of behaviour that violate the law, the Code of Conduct, or Sygnity's policies to the Management Board or, where appropriate, to relevant authorities.
- Conducting risk analyses within the risk management system to identify, prevent and minimise actual and potential adverse impact of Sygnity's operations, as well as to establish appropriate response strategies to any adverse effects.
- Avoiding causing or contributing to adverse impact on the issues covered by the Guidance Package referred to below in the Code of Conduct, through own actions, as well as taking appropriate steps to address such impact when it occurs.
- Striving to prevent or minimise adverse impact of Sygnity's operations, even in cases where such impact was not caused through Sygnity's direct fault, but is linked to its activities, products or services through business relationships. This policy, however, does not shift responsibility for such impact from the entity directly responsible to Sygnity, regardless of any existing business relationship between the two.
- In addition to taking appropriate measures in the event of adverse impact covered by the Guidance Package, Sygnity will, wherever possible, encourage its business partners, including suppliers and subcontractors, to adopt principles of responsible business conduct.

- The Company commits to collaborating with stakeholders to ensure their perspectives are considered during the planning and decision-making processes related to projects and activities that may significantly impact local communities.
- Sygnity pledges to refrain from any inappropriate involvement in local political activities.
- The Company will strive to support, where appropriate, collective efforts in relevant forums to promote internet freedom by upholding freedom of speech, assembly and online association.
- The Company will endeavor to support, where appropriate, initiatives by individuals or stakeholders and engage in social dialogue on responsible supply chain management, ensuring these efforts take due account of their societal and economic impacts on developing countries and align with internationally recognised standards.

The General Principles of RBC are implemented through the policies and procedures outlined in the following sections of this Code of Conduct.

A key objective of adopting the advanced regulatory framework and solutions defined in the Code of Conduct is to ensure that Sygnity adheres to the so-called Minimum Guarantees, which are essential for the Group's activities to be considered sustainable. The Minimum Guarantees are procedures adopted by Sygnity to ensure compliance with:

- **OECD Guidelines for Multinational Enterprises**, which are accessible here;
 - **UN Guiding Principles on Business and Human Rights**, which are accessible here;
 - **The principles and rights set out in the eight core conventions outlined in the Declaration of the International Labour Organization (ILO)**, which are accessible here;
 - **The principles and rights set out in the International Bill of Human Rights**, which are accessible here,
- These documents collectively form the "Guidance Package". All addressees of the Code of Conduct are encouraged to consult them via the provided links.

The Code of Conduct is the primary document governing the procedures within the aforementioned Minimum Guarantees system. It establishes the fundamental principles, mechanisms and solutions for implementing sustainable development policies that prioritise human rights, social and environmental concerns, as well as optimised corporate governance. Furthermore, it ensures compliance with applicable laws across companies from the Capital Group. Another, equally important document within the procedural system ensuring the Minimum Guarantees is the Book of Integrated Quality, Information Security and Anti-Corruption Management Systems. It outlines measures to protect the values that the Company upholds and promotes .

Business Integrity

1.1 Compliance with Laws

The Companies must comply with all laws and regulations relating to their business activities, including those of the TSS Group. Remember that you must be familiar with the applicable laws and regulations, and you can always verify your doubts and how to comply with them with your supervisor or another competent person, in particular with a representative of the Company's Legal Office. Further guidance in respect of competition laws is provided in Annex 1 - How to Avoid Anti-competitive Conduct.

1.2 Prevention of Fraud

Fraud is any dishonest activity that causes actual or potential loss to any person or entity. The Companies take zero tolerance approach to fraud and expect you to conduct your work in a reliable and honest way, not to steal or misuse the property of the Companies or your associates nor to mislead anyone to obtain private gain. Further explanations and examples are set out in Annex 2 - Prevention of Fraud.

1.3 No Corruption or Bribery

The Companies take a zero tolerance approach to bribery and corruption in all jurisdictions where the Companies are active in the business. Bribery is offering, promising, providing or receiving something of value (such as cash, gifts, favors or benefits) as an inducement or reward to gain any commercial, contractual, or personal advantage. Do not in any way (try to) bribe another person, organization or company. You shall not offer to or accept anything of value from someone if such items are beyond what could reasonably be considered ethical and within accepted business practices. Should you reckon that declining or not offering will be against business courtesies, please discuss it with your supervisor or another competent person. Further explanations and examples are set out in Annex 3 - No Corruption or Bribery.

1.4 Avoid Conflicts of Interest

Representatives must always act in the best interest of a given Company or Companies and are not permitted to engage in any activity that conflicts with their interests. A conflict of interest exists whenever a Representative's private interests interfere or appear to interfere with the interests of any of the Companies. It may arise whenever a Representative takes action or has an interest that prevents that person or appears to prevent that person from performing their duties for the Companies openly, honestly, objectively, and effectively. Further explanations are set out in Annex 4 - Avoid Conflicts of Interest.

1.5 Accurate Accounting and Reporting

All books, records, accounts and financial statements, time and expense reports should be recorded consistently and accurately, reflecting the true view and conforming to all applicable legal requirements and internal control policies. This requirement applies regardless of whether such records would disclose

disappointing results or a failure to meet anticipated profit levels. Any attempt to mask actual results by inaccurately reflecting costs or sales will not be tolerated.

1.6 Protection of Personal Information

You are expected to act in compliance with applicable privacy and data security laws, and the Data Protection Standard put in place at each Company. You should only acquire or retain personal information where it is required by law, requested by customers or required in connection with the operation of business activities of any of the Companies. Access to any such personal information is to be restricted internally to those with a legitimate need to know and you must not market, sell or otherwise disclose such personal information in any manner. Representative communications transmitted through or by computer systems of the Companies are not considered to be private and may be monitored or restricted by authorized personnel. Further explanations and examples are set out in Annex 5 - GDPR.

1.7. Insider Trading

Sygnity S.A. ('Sygnity'), is a Company listed on the Warsaw Stock Exchange. Buying and selling stocks of Sygnity based on inside information is unlawful, and therefore, Representatives and related persons should not engage in these activities. In addition to the above, during specific periods of the year, Representatives will not be allowed to sell or purchase stocks by the applicable laws. Public disclosure of confidential business or financial data is generally prohibited as it may affect the price of Sygnity's stock. Prior to full public disclosure, Representatives may not discuss or disclose information on important events concerning the Companies and their related parties; this includes social conversations, among family or friends, with third parties or other Representatives if such persons have no need to know the information. Giving a 'tip' to someone else based on inside information is illegal. Both the discloser and the person given the 'tip' may be subject to significant criminal and civil penalties if securities are traded based on a disclosure of inside information. Further guidance is provided in Annex 6 - Disclosure, Confidentiality and Insider Trading Policy.

1.8 Disclosure of Information

Any confidential information concerning the Companies' business or finances may not be disclosed to the public or communicated to the press without prior consultation with the Companies. Furthermore, every Representative should refrain from disclosing information, by any means of communication, that may harm the image of the Companies or any of their Representatives. You may not disclose any confidential information regarding the Companies, their customers and suppliers. Always take care to keep such information confidential.

1.9 Dealing with Suppliers (Business Partners)

The Companies must select their suppliers based on an objective comparison of evaluation criteria, including business conditions, reputation, or operation sustainably and reliably. Detailed terms and conditions of

establishing cooperation are regulated in the Procurement Procedure and Principles for Contractors of the Sygnity Group Companies.

1.10 Responsible Work Conduct

The IT and communication systems of the Companies are built for business purposes. The capacity, software and security are not designed for private purposes and any use for private purposes should be limited as much as reasonably possible. Representatives must always use their best efforts to protect the assets of the Companies, including facilities, computer equipment, and any other physical property, from unauthorized use, loss, theft or misuse. All assets should be used for legitimate business purposes only and not for personal benefit. The use of any funds or assets of the Companies for any unlawful or improper purpose is strictly prohibited. Claims for travel and expenses must be fair and should only relate to the business activity of the Companies. Further guidance is provided in Annex 7 - Responsible Work Conduct and Annex 7a – AI Policy.

1.11 Responsible Work Environment

Companies continuously strive to improve health and safety aspects within their work environment. Each Representative is responsible for creating and maintaining an inclusive workplace culture in which all individuals are respected and that is free of harassment, bullying and discrimination. Gaining an advantage over others through manipulation, concealing the truth, insider trading, misrepresentation or other dishonest behavior is not acceptable. The Companies also do not tolerate the use of drugs or other prohibited substances, as well as the consumption of alcohol during or the inappropriate consumption of alcohol outside working hours if this affects the performance of employee duties. Further guidance is provided in Annex 8 - Responsible Work Environment.

1.12 Corporate Responsibility

The Companies are obliged to act responsibly in the areas of energy, waste, purchasing, personnel, health and safety. Representatives are also required to comply with this commitment.

1.13 Proper Authorizations and Approvals

In all matters that require it, you must obtain appropriate approval based on the regulations in force in the Companies. The above is the basis for ethical behavior in a business environment. This requirement is not intended to restrict business initiative, but to reduce the risks associated with inadequate representation and commitment of the Companies.

1.14 Due diligence

Sygnity conducts a detailed analysis of the Companies' impact on the protected values and rights of stakeholders, while also assessing how the environment affects both the Companies and Sygnity itself. This analysis is part of the double materiality process and is based on due diligence procedures. On this basis, an

ESG risk map is created, identifying the areas with the highest priority (key aspects of negative impact). Conclusions from this analysis are incorporated into Sygnity's risk management system, which is a crucial component of corporate governance. The Company is committed to continuously updating the risk management system, including ESG-related matters. To ensure compliance with the Minimum Guarantees, it is essential that the risk management system takes into account both Sygnity's impact on the environment and the environment's impact on Sygnity, enabling the mapping of priority areas based on mutual impact.

The protection of the rights and values outlined in the Guidance Package is achieved, for example, through the implementation of a due diligence process consisting of six steps as defined in the OECD Guidelines Part II:

- Incorporating RBC Issues into Sygnity's policies and compliance system (including the Code of Conduct) and ensuring adherence to due diligence principles;
- Identifying actual or potential negative impact on RBC issues;
- Preventing, halting or mitigating negative impact;
- Monitoring implementation and outcomes;
- Communicating how any instances of negative impact are addressed;
- Enabling appropriate corrective actions.

In response to the requirement to integrate RBC issues into policies and the compliance system, the Code of Conduct establishes a set of rules of conduct for all individuals employed at Sygnity (whether under an employment contract or through civil law contracts, such as contracts for a specific work or services) at all levels. Along with related documents, the Code of Conduct governs Sygnity's operations in areas such as: ethics management (including policies against corruption, bribery and other abuses, as well as policies on fair competition), the whistleblowing system, social engagement and dialogue with stakeholders (including social policy), human resources management policies, and the protection of human rights (covered within the human resources (HR) policies, including data protection and corporate confidentiality, prevention of discriminatory practices, harassment, conflict of interest in professional activities, as well as acceptable forms of hospitality and the offering/accepting of gifts).

In implementing these procedures, Sygnity adheres to the principle of 'do no serious harm' (DNSH), meaning it strives to protect specific values or rights in a way that does not harm other rights or values.

At the procedural level, due diligence in responsible business conduct within the Capital Group is reflected in a compliance system tailored to the Capital Group's operations and business model. This system, based on the Code of Conduct, policies, procedures, other regulations and solutions, ensures compliance with the principles, values and rights outlined in such documents as the Guidance Package.

The Companies aim to promote the principles and values outlined in the Code of Ethics throughout the supply chain, including in cooperation with suppliers (business partners). This is reflected in the implementation and dissemination of the Code of Conduct to the business partners of the Sygnity Group Companies, as well as, where possible, the inclusion of relevant contractual clauses requiring compliance with the principles outlined in the Code of Conduct. Entities that do not respect the principles and rights outlined in the Guidance Package are identified and removed from the supply chain (including the indirect supply chain) on an ongoing basis.

The implementation of corporate regulations and a system for reporting violations, as well as ongoing awareness-raising efforts among employees through educational and training activities, make it possible to effectively address any actions that violate the principles and values outlined in the Guidance Package. Sygnity continuously monitors potential violations to prevent them. To this end, Sygnity has adopted a procedure for reporting irregularities related to corruption or conflicts of interest, which describes the steps employees and their supervisors must follow in case of questionable situations.

One example of due diligence measures in ensuring compliance with RBC issues is Sygnity's readiness to cooperate with the National Contact Point (NCP). The OECD National Contact Point was established to promote and ensure compliance with the OECD Guidelines. NCPs are also responsible for handling complaints related to the operations of companies that violate the OECD Guidelines. NGOs or trade unions can report violations of the OECD Guidelines to the NCP, which, in such a case, is required to investigate the issue and, if valid, initiate a mediation process between the company and the affected parties.

Another organisation whose work is taken into account by Sygnity is the Business & Human Rights Resource Centre (B&HRRC). The B&HRRC is committed to promoting human rights in business and eliminating abuses. It focuses on empowering partners and allies, as well as undertaking activities to ensure that businesses respect and support human rights and are held accountable for any violations in this respect.

As part of the conducted analysis of compliance with the Minimum Guarantees, Sygnity ensures adherence to the principles of cooperation with the National Contact Point outlined in the OECD Guidelines Part II. This includes being subject to final accountability, meaning the absence of a final ruling against the companies in the Sygnity Group for violating the principles and rights set out in the Guidance Package.

1.15 Identification of and dialogue with stakeholders

Sygnity operates within a specific environment and cares about its relationship with it. Sygnity's environment encompasses various factors and processes that significantly influence its activities. Sygnity's immediate environment includes its suppliers, subcontractors, customers, competitors, industry organisations, shareholders, financial institutions and local communities. Sygnity's environment can present both opportunities and risks, and therefore must be carefully considered when developing the company's strategy

and objectives. To this end, Sygnity makes every effort to understand its environment and keep track of changes in order to identify emerging risks, improve relationships and meet stakeholder expectations. This is achieved through the process of stakeholder mapping and double materiality (impact) studies.

In addition, Sygnity follows the principle of stakeholder engagement, which involves active collaboration with relevant stakeholders. This can take various forms, including surveys, meetings or consultations. Meaningful stakeholder engagement is characterised by two-way communication and good intentions of both parties. It is also flexible and ongoing, often involving collaboration with relevant stakeholders before decisions are made. Engagement from both sides means that Sygnity and its stakeholders can share their opinions, present their views and listen to alternative opinions in order to reach mutual understanding. It also allows stakeholders to participate in the development and implementation of activities related to Sygnity's commitment to responsible business conduct. Both Sygnity and its stakeholders are expected to act in good faith. This means the Company genuinely seeks to understand how its operations affect the interests of relevant stakeholders. It also means Sygnity is committed to addressing any negative impact it may cause or contribute to, while stakeholders are expected to be transparent about their interests, intentions and concerns. Positive engagement means that Sygnity actively seeks feedback from those affected by its decisions. It is important to engage with relevant stakeholders or those whose rights may potentially be affected before making any decisions. The Company aims to do so by providing all necessary information to relevant stakeholders or persons whose rights may be affected in a timely manner, enabling them to make informed decisions related to Sygnity's actions and their impact on them. This also implies fulfilling commitments, taking action to address negative impact on affected stakeholders or persons whose rights may potentially be violated, and taking remedial action when Sygnity has caused or contributed to harm. These actions align with the six due diligence steps mentioned in section 1.14 above.

1.16 Speak Up!

Each Representative is required to read the Code of Conduct and has the right to ask questions, obtain advice and express concerns about its content. Anyone with knowledge of possible, suspected or known violations of the Code of Conduct must report it to their supervisor or through one of the Speak Up channels. Further guidance is provided in Annex 9 - Speak Up!

The Companies do not tolerate any retaliation against Representatives who in good faith seek advice or report behavior that is in breach of the Code of Conduct. Any breaches of the Code of Conduct, including failure to report breaches, may lead to the initiation and conduct of appropriate proceedings relating to such breaches.

Code of Conduct

Annex 1 – How to Avoid Anti-competitive Conduct

Companies are obliged to comply with fair competition laws when conducting their business. Price fixing or even informal arrangements between competitors to share particular customer groups are strictly prohibited. Certain competition regulations may also apply to competing companies within the Sygnity Group or the TSS Group.

Communicating information to a competitor's representative about our current (price) policies, planned activities or even recent commercial decisions also constitutes a breach of competition laws.

Such situations can occur during day-to-day work and meetings with competitors. Talking to competitors is always very risky and if you choose to do so, it is your responsibility that no confidential information is exchanged. You should make it clear in any conversation that you refuse to disclose or receive confidential information even though such an information exchange may appear tempting or even useful for business.

The penalties for violations of the competition principles are significant and are imposed on the companies involved and the individual infringing competition laws. Penalties imposed on companies in Europe can be as high as 10% of the previous year's group revenues.

There are areas related to competition that are not always clear-cut and explicit, e.g., cooperation with competitors regarding selected customers or issues concerning exclusivity offered by a given supplier, distributor or customer. Doubts in this respect can only be resolved after careful analysis of legal and financial issues. Decisions in such cases always require prior consultation with a supervisor or other competent person, including, in particular obtaining legal advice. Another aspect of competition law is the control of companies that have a strong position in a particular market. If a company has a very strong position in a particular market (partial monopoly or dominance), in that case, the freedom to operate may be restricted by some of the competition laws. Market dominance usually occurs when it is possible to set our terms of business without considering the competition.

EXAMPLE:

What should you do when a competitor (even a former associate, friend or relative) provides you with information about his/her company?

Tell them that you are not authorized to talk about customers/suppliers, the state of negotiations with customers/suppliers and or about negotiation strategy. It is however permissible to talk about end customers' satisfaction with the supplier. In any dealings with competitors, you must always remember that you are not entitled to exchange information that might cause us or our competitor to adjust our financial strategy, prices, product portfolio, production process, etc. to a given situation or even to consider doing so.

Q&A

- Question 1: I received confidential business information about a competitor. What should I do?

It is decisive where the information comes from. If, for instance, the customer voluntarily provides you with information about the terms and conditions of your competitor, you can use such information in your price negotiations. If such information is however received from a competitor, the principles explained in the examples above apply. Generally, you are not allowed to use such information. Immediately speak to your supervisor about the situation.

- Question 2: I am participating in a working group in which representatives of competitors also participate. I sometimes pick up relevant information at these events. What can I do with this information?

The principles explained in the examples above apply. In personal conversations, you must reject such information exchange. You are not allowed to use such information. Immediately speak to your supervisor about the situation.

- Question 3: A group of entities has requested greater price reductions, in return for which all (new) members of this group will use our software. Can I give such a discount?

Contact your supervisor and also the Company's Legal Office for prior legal advice before agreeing on a discount with the customer.

- Question 4: An employee of a competitor asks me if the information he/she has about our commercial practice is correct. What should I do?

In this situation, you must distance yourself from the conversation and make it clear that you do not want to take part in such an exchange of information. Even a simple 'confirmation' that a piece of information is correct is a serious breach of competition principles, as it constitutes an exchange of confidential information. This also applies to other confidential information related to customers,

prices, turnover, sales results, production capacity, investment, innovation and technology. There are known cases of judgments by competition authorities that have found the sharing of information about competitors' business practices by customers to be an infringement of the law.

Code of Conduct

Annex 2 – Prevention of Fraud

Fraud is a dishonest act to gain an advantage and includes, inter alia, deception, concealment of the truth or forgery. Fraud can be committed by one person as well as by more persons acting in collusion. Both internal and external entities, including suppliers or customers, may be involved in fraud. The Companies do not tolerate any actions leading to the commission of fraud by their Representatives and business partners. Such conduct generally leads to the immediate termination of the relationship with such an entity. Involvement of customers, suppliers or other entities in fraudulent activities is unacceptable.

All managers are responsible for identifying the risks of fraud, implementing appropriate control measures and for continuously reviewing the effectiveness of the measures put in place in relation to the units or areas they manage. They should also be aware of the types of fraud risks that may arise in their area of responsibility and must inform their staff that they should be alert to any signs of fraud. Representatives who detect or suspect the commitment of fraud must report it immediately through the appropriate channel indicated in the Annex – Speak Up!

EXAMPLE:

A representative has selected a specific supplier as this supplier provides it certain benefits or a kick back fee to be paid in person.

This is considered to be theft because apparently, the purchase price for the Companies could have been lower than the contracted price. This constitutes a material breach which may result in the immediate dismissal of the Representative involved in such activities.

Q&A

- Question 1: I suspect a work colleague of fraud and want to know what I must do.

Report the situation via the channel <https://gojira.sygnity.pl/sygnalista/> or to the persons indicated in the Annex – Speak Up! If you suspect that fraud is being committed, do not discuss it with any of the people involved and do not try to verify the situation yourself. The person informed of the situation will consider it and take appropriate measures.

- Question 2: I suspect my supervisor to be involved in a fraud scheme and want to know what action to take.

Report the situation via the channel <https://gojira.sygnity.pl/sygnalista/> or to the persons indicated in the Annex – Speak Up! The matter will be dealt with in an objective manner.

- Question 3: Will there be consequences for me if I misjudged the situation?

Companies appreciate their Representatives being committed to the Companies' interests and willing to raise concerns regarding suspicious situations. The ability to investigate and prevent fraud depends on prompt and confidential reporting. You will of course not be affected by creating awareness for fraudulent conduct where in hindsight your judgement proved to be incorrect. It is of course never allowed to accuse someone intentionally without a justifiable reason.

- Question 4: A customer requires me to amend an invoice inconsistently with the actual situation to be able to book the expenses to its benefit. Is this allowed?

This is never allowed. This is considered as helping a customer with committing fraud.

Code of Conduct

Annex 3 – No Corruption or Bribery

Companies conduct their business worldwide and their Representatives are subject to anti-bribery and corruption laws applicable in all countries of operation. The payment of bribes is strictly prohibited at all times and without exception, even if certain exceptions are legally permitted in certain countries.

What conduct is considered bribery?

Anti-bribery laws prohibit persons or companies from the offering, promising or paying a bribe to a public official or person in the private sector to influence this person in his/her (official) acts or function. Likewise, it is prohibited to solicit or accept a bribe. A 'bribe' may consist of any advantage or benefit that has value. Small payments or benefits are therefore not per se excluded. The mere offering or promising of a bribe is prohibited. The bribe does not have to be paid or accepted. The person offering, promising or soliciting the bribe does also not necessarily have to be the recipient of the bribe (indirect payments are also prohibited). Anti-bribery laws vary from country to country and may cover the liability not only of the person directly involved in giving the bribe but also of those involved in giving, approving or ordering or covering up the practice. Most anti-bribery laws relate to the giving or promise of a bribe in return for a specific act or omission by the person being bribed. What matters is whether the influence is exercised to obtain or maintain a business or business advantage - for example:

(a) granting of a license, permit or awarding an assignment in circumstances where it may not otherwise be granted, (b) deciding not to continue or initiate an investigation regarding an act of wrongdoing committed by the company or (c) providing confidential information to a company. It is not required that the intended recipient of the bribe is directly involved in awarding or directing the business advantage. The use of such a person's influence to establish a certain result may be sufficient.

Representatives (or someone on their behalf, or a family member thereof) must not:

- give, promise to give, offer a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given;
- give, promise to give, offer a payment, gift or hospitality to a government official, agent or representative to 'facilitate' or expedite a routine procedure;
- accept payment from a third party that you know, or suspect is offered with the expectation that it will create a business advantage for them;

- accept a gift or hospitality from a third party if you know or suspect that it is offered or provided with an expectation that a business advantage will be provided in return;
- threaten or retaliate against another worker who has refused to commit a bribery offence or who has raised concerns under this Code of Conduct.

Corporate hospitality and promotional expenses, gifts and entertainment

Hospitality and promotional expenditure as well as offering and accepting gifts and entertainment are not considered bribery (a) if reasonable and proportionate as regards the value and timing, the impression conveyed to third parties and the type of gift or entertainment, and (b) there is no intention to induce a person to improperly perform his/her function, to secure a business advantage or not.

As a general rule, you should never offer or accept a gift or entertainment **in excess of PLN 200 per quarter** or the local currency equivalent. If a gift gives you an uncomfortable feeling and/or you would not feel comfortable if all your work colleagues would know of it, you should never accept such a gift. Hospitality and promotional or other business expenditure which seeks to improve the image of any of the Companies, to present the products and services offered by the Companies or to establish relations, is recognized as an important part of doing business. However, the recipient of any gift and/or hospitality should not be given the impression that he/she is under an obligation to confer any business as a result of the hospitality itself or that his/her independence will be affected by receiving any such hospitality.

Representatives must consider whether in all the circumstances the gift or hospitality is reasonable, proportionate and appropriate, including the following considerations:

- what is the intention of the gift or hospitality is;
- whether there is any secrecy involved;
- the value of the gift/hospitality (the higher the value, the less likely it is to be appropriate); and
- how the gift or hospitality would reflect on the Companies if the details were made public.

Circumstances that are usually acceptable include:

- occasional lunches and dinners with existing and prospective customers and suppliers, unless to be considered disproportionate;
- occasional attendance at sports, theatre and other cultural events, unless to be considered disproportionate; and
- gifts with a value not exceeding PLN 200 per quarter or other small promotional items.

Circumstances that are not acceptable include:

- gifts of cash or a cash equivalent;
- gifts in your name, not in the name of the Companies;
- secret gifts; and
- any gifts given to or received from suppliers, government officials or representatives to obtain or retain an improper advantage.

As a general rule lunch/dinner invitations may be accepted if (i) they are not disproportionate/decadent; (ii) the costs are not substantially exceeding the cost you would be prepared to pay privately for a lunch/dinner, and (iii) if this does not occur too frequent. Anything that does not meet these requirements must always be consulted with your supervisor.

If you receive a gift, hospitality and/or entertainment with a value exceeding PLN 200 per quarter you must consult with your supervisor before accepting it. In case you have any doubts about the appropriateness of hospitality, entertainment or a gift that you intend to offer or accept, you must always consult your supervisor first.

Facilitation payments and lawful government payments

The Companies prohibit all facilitation payments. Facilitation payments are small payments that are not prescribed by the written regulations in a certain country and are made to secure or expedite the performance of a routine governmental action (e.g., customs clearance). Payments to public officials that are prescribed by written regulations of the official's country, such as fees and payments for various government services, are not prohibited. Payments on top of such legally required amounts are strictly forbidden.

Liability for and prevention of bribery

The Companies could be held liable for bribery by associated persons acting on their behalf. The Companies, therefore, require that business partners acting on their behalf, such as agents and representatives, comply with all applicable anti-bribery laws. All existing and future business partners must be selected with bribery risks in mind and the appropriate contractual agreements should be made with these parties to avoid bribery risks. This investigation as well as its results of it must be documented. Detailed principles of cooperation with partners and suppliers have been regulated in the 'Principles for contractors of the Sygnity Group Companies' and in the regulations of ISO 37001, an anti-corruption management system implemented in the Companies. Any problems and doubts should be reported to a supervisor or other competent person.

EXAMPLE:

You have received a Christmas gift from a supplier. Although the gift is not exceptionally disproportionate you sense that the supplier expects you to award it a contract in the future.

You must inform your supervisor about such a situation. You may consider the possibility of politely refusing the gift. If you keep the gift, you should not award the supplier a contract without the prior approval of your supervisor.

Q&A

- Question 1: After a long integration process, the supplier offers our entire team to join its company on one of its company trips. May we accept this invitation?

No, you may not accept it. Such a trip is disproportionate as it is of high value. You should also not accept any trips from customers under any circumstances.

- Question 2: I received from a supplier a bottle of wine worth more than EUR 50. May I accept it?

No, you may not accept it.

- Question 3: We invite a few directors of a valued customer for drinks and dinner every year. Is this allowed?

Corporate hospitality aimed at maintaining a good relationship with customers is allowed. However, no undue influence may be exerted, and any impression of bribery must always be avoided. For example, you should not treat the directors to dinner with costs substantially exceeding the cost you would be prepared to pay privately for a dinner.

Code of Conduct

Annex 4 – Avoid Conflicts of Interest

What is a conflict of interest?

Representatives are expected to avoid any actual or suspected conflict between the interests of the Companies and their interests. The Companies recognize that you are part of a family, have friends, act in volunteering jobs, and have specific personal responsibilities and interests. A conflict of interest can arise when you take actions or have personal interests that can interfere with your performance for the Companies. You should always inform your supervisor of any direct relationship with entities that may enter into a contract with any of the Companies if you are directly involved in the award or management of such a contract.

Some common examples of conflicts of interest are:

- Having a financial interest in a company that competes with or does business with any of the Companies;
- Holding a position as a director, representative, employee or consultant of an enterprise that competes with or does business with any of the Companies;
- Taking personal advantage or having a related third party taking advantage of an opportunity that any of the Companies could benefit from;
- Diverting a business opportunity for any of the Companies for his or her benefit or using his or her position in any of the Companies to do business with or give preferential treatment to a friend or relative (or a company with which the friend or relative has a significant relationship); and
- Using funds, facilities, personnel or other assets of the Companies for personal benefit or the benefit of related third parties.

Full disclosure

You are required to disclose to your supervisor each actual or suspected conflict of interest situation in which you are directly or indirectly involved. You need to make this disclosure as soon as you become aware of facts giving rise to the actual or apparent conflict of interest.

Guidelines

If you are unsure as to whether a given situation creates a conflict of interest, raise the issue with your supervisor. Whilst it is impossible to describe every circumstance where a conflict of interest may arise, the following guidelines will help you avoid conflicts of interest:

- a. never allow your personal or financial interests to interfere with your work for any of the Companies;
- b. always be able to satisfactorily explain your decision to your supervisor and your associates;
- c. always involve at least two persons in the event of any conflict of interest, to ensure an objective view of the matter in question;
- d. do not employ someone you personally know who will work under your authority, unless you have been given proper permission to do so; and
- e. even the least likely conflict of interest may turn out to be real!

EXAMPLES:

1. **One of your family members owns a financial interest in an entity that wants to do business with any of the Companies and you are involved in the decision making process.**

This is a clear issue that should be raised with your supervisor, who will decide what measures should be taken to eliminate your involvement with this company.

2. **You work in the procurement department of the Companies. Your brother works in the sales department of a competitor. He proposed to start up a new business combining your and his knowledge**

The knowledge that you have obtained during your work for the Companies is considered the intellectual property of the Companies and may not be used by you for your benefit or the benefit of your family members.

Q&A

- Question 1: A good friend of mine works for a company that could be an important customer for any of the Companies. He asks me if this Company would be interested in selling to the benefit of his company. What should I do?

Report the situation and relationship to your supervisor and keep him/her fully informed of the deal and each step in the process. However, since it can result in an important customer for the Company there is no need to say no to the (potential) customer beforehand unless the dealing would be on non-commercial terms.

- Question 2: I am asked by a good friend to provide advice to his/her company that is in direct competition with the Companies. Although he/she seeks only technical advice, which seems not to be commercially sensitive, I am not sure what to do.

When considering a such request, always involve your supervisor. Your supervisor will ensure that your question is considered objectively. In addition, be aware that information sharing between competing businesses is in many cases forbidden due to competition laws. For more information, see Annex 1 – How to Avoid Anti-competitive Conduct.

Code of Conduct

Annex 5 – GDPR

What is GDPR?

The EU General Data Protection Regulation ('GDPR') covers the data protection legislation that governs how companies manage such data. GDPR applies to any company that manually or automatically processes personal data. 'Processing' means any operation performed on personal data, such as collection, usage, storage, transfer, dissemination or erasure. Even if a company processes data on behalf of another entity, it is still bound by the provisions of the GDPR.

What is personal data, e.g., of customers and employees?

Personal data refers to any information that relates to an identified or identifiable individual. This can include:

- name and surname
- address and phone number
- location
- income and banking information
- ... and more

Personal data that has been de-identified, or pseudonymized, but that can still be used to re-identify a person also falls under the scope of the GDPR. However, personal data that has been rendered irreversibly anonymous in such a way that the individual is no longer identifiable is not considered to be personal data and thus not governed by the GDPR.

Possible penalties

If the Company does not comply with the provisions of the GDPR, it faces a fine of up to 4% of its annual global revenue from the previous financial year (whereby TSS Group's ultimate shareholders Topicus.com Inc. or Constellation Software Inc. ('CSI') may be included in the calculation of the above fine) or EUR 20 million, whichever is higher. Other penalties may also be applied to the Companies, such as a ban on the processing of personal data, which may lead to the interruption of the business continuity of the penalized Company.

How do I comply with GDPR?

Data protection is extremely important, and everyone should comply with the GDPR, both when it comes to internal data (e.g., employees) and external data (e.g., end customers).

To be compliant with the GDPR, you must comply with the Personal Data Protection Standard in force at the Companies and follow the basic principles of data processing:

- Always enter into a personal data processing agreement (or further entrustment agreement) with customers and suppliers;
- Always create an appropriate processing register for the process/entrustment agreement;
- Ensure that personal data is only processed for the purpose agreed with the data owner, e.g., for the performance of the master agreement;
- Ensure that you have authorized the right people to process the data and that only they have access to the data (data is protected);
- Ensure that personal data is not transferred to unauthorized persons and/or is not used for purposes that have not been agreed with the data owner;
- If you need to transfer/disclose personal data for purposes agreed with the owner of the personal data, ensure that this is done in a secure, protected manner and by applicable laws.

Each Company has a policy on how data (internal and external) is used and protected in a particular case. Make sure you are aware of this policy and know how to comply with it. You should not allow unauthorized disclosure of personal data, but if this occurs, you should report the situation to the relevant Company as soon as possible. Any data protection incidents should be reported to iod@sygnity.pl or iod@sygnitysbs.pl within 6 hours of their (suspected) occurrence; to do so, you should contact your supervisor, who will inform the Data Protection Officer ('DPO') and the relevant managers. For the avoidance of doubt, if any manager receives information about any (possible) incident, he/she is obliged to report it immediately as described above.

EXAMPLES:

1. **You have sent an email with the wrong attachment which contains personal data to an employee from the finance department.**

Although your colleague is used to working with confidential information this is a breach of the GDPR. You must inform the recipient of the email and request him/her to delete your email and attachment. Also, you must inform your manager.

2. **You lost your USB stick which contains the personal data of your customers. You did not protect the USB stick with a password.**

Nevertheless, you should immediately report it to your manager, to your IT contact person and iod@sygnity.pl or iod@sygnitysbs.pl. Even though the USB stick is password protected this loss may still qualify as a data breach which needs to be reported.

Q&A

- Question 1: Our software generates certain data which includes personal data. A company offered us a monthly fee for providing such data to them. May we sell this data?

No. Personal data may not be processed for purposes which are not agreed upon by the owner of the personal data. You may only sell this data if all the people to whom this data relates have agreed in writing to this specific purpose.

- Question 2: My work colleague asked me to forward a CV to him/her by email. May I do so?

You may only do so if it is necessary for this colleague to see such a CV for the specific purpose for which you received such data. Plus, you always need to make sure that this kind of confidential documents are deleted from all media (including all email folders and trash folders on your computer) when the purpose to have this data is no longer there.

- Question 3: I left my laptop at the airport. What should I do?

You have to immediately report this to your supervisor and IT contact person.

- Question 4: I forgot that I had printed documents which contain the personal data of our employees. As a result, these documents were present on the printer the whole day and I don't know if people have seen them. What should I do?

You have to immediately report this to your supervisor. All possible breaches of data confidentiality must be reported.

Code of Conduct

Annex 6 – Disclosure, Confidentiality and Insider Trading Policy

Definitions

„**Sygnity**” means Sygnity S.A.

„**Insider trading**” refers to an employee, officer or director of Sygnity or any of its direct or indirect affiliates or subsidiaries, purchasing or selling or otherwise monetizing securities of Sygnity while in possession of undisclosed Material Information.

‘**Material Information**’ means a fact, change or event that would reasonably be expected to affect the market price of the securities of Sygnity.

‘**Tipping**’ refers to disclosure of Material Information to third parties, other than (i) if required by applicable law, or (ii) if such disclosure is made as the necessary course of business to a person who has a duty of confidentiality to Sygnity or its affiliates.

‘**Management Board**’ means Members of the Management Board of Sygnity.

How do I comply?

1. Anyone possessing Material Information which has not been disclosed to the public must maintain its confidentiality and refrain from Insider Trading or Tipping.
2. Only Members of the Management Board are authorized to disclose Material Information to the media, analysts, stockholders and the public.
3. Prospectuses, management information circulars, interim financial statements, annual financial statements, the related MD&A, and all related press releases must be reviewed and approved in advance by the Management Board of Sygnity.
4. If any Material Information is undisclosed, the Management Board shall promptly disclose the Material Information to the public as required by applicable law.

5. Any employee who becomes aware of undisclosed Material Information should promptly disclose that information to the Management Board.
6. Employees, officers and directors of Sygnity or its direct or indirect subsidiaries may be required by law not to purchase, sell or otherwise monetize securities of Sygnity during 30 calendar days prior to the announcement of the interim financial report (an interim report is both a half-yearly report and a quarterly report) or the year-end report (this period is referred to as the 'Closed Period').
7. Any person failing to comply with this provision may be punished by a penalty appropriate to the situation.

EXAMPLES:

1. **You read certain rumors on the internet in respect of Sygnity that you know are not true. You want to set things straight and respond with the right information.**

Do not discuss or post any information relating to Sygnity or any of its subsidiaries or trading in securities on the internet chat rooms, newsgroups, bulletin boards, web logs or other electronic media available to the public as you may possibly disclose information that is not publicly available yet.

2. **Sygnity is working on a really large acquisition. Therefore, you assume that the value of Sygnity's stocks will increase once the acquisition is completed. In anticipation of this transaction, you are already buying additional stocks of Sygnity.**

This is not allowed as you have possession over material information that other stockholders do not have. Besides violating the insider trading policy, you may also violate security or securities trading regulations and may become subject to large fines or imprisonment.

Q&A

- Question 1: I want to buy or sell stocks of Sygnity outside a Black Out Period but am not fully sure whether I may be in the possession of certain Material Information that may not be publicly known to the market yet. Am I allowed to trade?

If you have any doubts, please contact the Director of the Sygnity Management Board Office (before trading securities).

- Question 2: I receive a phone call from a financial analyst from a large financial institution/bank with some questions about our business. Am I allowed to provide some general information that is already publicly known to the market?

No. You are not allowed to share any information with external parties as any information will have to be shared in a consistent manner and by applicable policies. Therefore, disclosures shall only be made to third parties by the Management Board.

Code of Conduct

Annex 7 – Responsible Work Conduct

Company assets and funds

All property of the Companies may only be used for the intended business purposes. This includes but is not limited to: a. physical assets such as office equipment, tools, technical equipment and IT equipment; b. software, intellectual property rights and confidential information; and c. company funds, bank accounts and other resources of the Companies. You must use the property of the Companies only for the intended business purposes and guard it against misuse, loss or theft. Funds of the Companies may only be used for business purposes implemented by the Companies and may never be used for private purposes. It is not permitted to combine business expenses such as lunches and travel trips with personal holidays with family members or friends without the prior written consent of your supervisor.

Use of IT and communication

IT systems, software and all means of electronic communication belonging to any of the Companies, including the internet, shall be primarily used for business purposes and in the Company's interest. The capacity for communications, antivirus software and licenses are implemented for business use and not for private use. Though some proportionate personal use of these systems may be inevitable, such use should be limited as much as possible and may never interfere with the intended business purposes. IT systems must never be used in any way that leads to the storage of information that violates applicable laws, that can be used to harass other employees or third parties, or other inappropriate behavior. Only if there are justifiable suspicions that you do not act in accordance with this Code of Conduct or applicable legislation, the Companies reserve the right to monitor your use of the IT systems and electronic communications by applicable laws.

Responsible use of IT does also involve IT security. Every Representative must always use all IT systems responsibly. This consists of for example:

- Never click on suspicious links in emails without consulting the person you received it from or the IT department;
- Always use strong passwords which are not easy to guess or crack;

- Always comply with internal authorization schemes before transferring money;
- Always make sure before sending an email that any attached document is the document you wanted to send;
- Never use your company laptop to visit websites with inappropriate content and/or download files from websites which are to be considered high-risk.

Intellectual property

The Companies have developed or purchased licenses for valuable intellectual property, including inventions, product names, software, engineering drawings, and confidential information for its business operation. You must strictly comply with the applicable intellectual property laws and license conditions. Unauthorized use or disclosure of the intellectual property of any of the Companies is forbidden and the intellectual property right of third parties must be fully respected.

EXAMPLES:

- 1. You are the coach of the soccer team of your child and urgently need to send a mailing to various sponsors for the next soccer tournament.**

It is not allowed to use the company email service for this. Your company email address contains the trade name of your company, and such email interferes with the business purposes of this name. This can damage the image or reputation of any of the Companies. These mailings should be done with your private email address outside office hours.

- 2. Representative provides its children with office supplies to do their homework.**

This is not allowed.

- 3. Representative downloads illegal software to prepare a business presentation.**

This endangers the safety of the IT- systems of the Companies and breaches third-party intellectual property rights.

Q&A

- Question 1: You receive an email, apparently from an associate, containing all kinds of confidential information. The email turned out not to be intended for you but another person within the company. What should you do?

Delete the message permanently so that the personal data contained in it cannot be further used. Inform the work colleague who sent the message. Communicate the situation to your supervisor and the DPO. The DPO will give you further instructions on how to proceed.

- Question 2: What if a device is stolen during a break-in (from home, car)?

Never leave a business laptop unattended in a car or public place. Make sure your laptop and storage media are protected with the latest encryption software and are password protected. Always lock your computer when you are not working on it. Seek advice from the IT department before saving any data on an external device. If your laptop is stolen, report it immediately to your supervisor and the IT department.

- Question 3: I am planning to work some days from home. I always drink coffee at work, but I know that I am out of coffee beans at home. Am I allowed to take some coffee beans from work?

No, you are not. This is considered to be theft.

- Question 4: I have travelled to another country for a business meeting. After the meeting, I get informed that the flight back is delayed, and I will have to stay another day abroad. Can I receive compensation?

No, you cannot. It was the company that paid for your flight and therefore the compensation belongs to the company as well.

Code of Conduct

Appendix 7a – Generative AI Policy (updated September 2025).

Sygnity and its subsidiaries are part of the TSS Group and are committed to fostering a culture of collaboration

and innovation. Generative AI (i.e., a category of AI that generates output from the data it was trained on) has emerged as a game-changing technology, which has great potential to benefit Companies and enable employees and associates to achieve new levels of success.

Companies are involved in managing the existing risks posed by the use of generative AI, including their ability to maintain appropriate information security measures, protect intellectual property rights, and ensure the accuracy and integrity of their work. Tools such as generative AI must always be used responsibly to limit the possibilities of exposing the Company to any, including unintended adverse consequences.

This policy aims to establish guidelines for the proper use of generative AI by all employees and associates of each of the Sygnity Group Companies.

Policy scope and introduction

General

This policy is intended to help employees and associates of the Companies to effectively and responsibly use of generative AI tools so we can innovate

while addressing the necessary ethical and legal issues. **Failure to comply with the rules resulting from this policy may result in legal action being taken against the employee or co-worker, including termination of the contract between him or her and the Company.**

Policy Application Guidelines

For guidance on disclosure and other questions related to the application of the policy, please consult with your manager or legal department. A commitment to transparency of use and responsible use of generative AI is critical to our organization and continued growth together.

Policy changes

Generative AI is a vast and growing technology space, and access to and use of generative AI platforms may be restricted in the future. The Company reserves the right to make changes to this policy whenever it deems it appropriate.

Applying the policy

This policy applies to all employees and associates of the Companies and others who have access to Company Data (as defined below). This policy applies to the use of generative AI tools (both publicly available and licensed by the Company) by employees and associates of the Company as part of their roles within each Company. The Company's employees may use generative AI applications in addition to other tools on which they rely to provide services to our clients, only in accordance with this policy. Examples of publicly available generative AI tools include chatbots like ChatGPT, Bard, and Bing, and image generators like DALLE2 and Midjourney. The Company may also acquire commercial solutions that use generative AI. A list of generative AI tools that have been verified by the Company can be found in Appendix A.

Be advised that the list of generative AI tools may change in time. Change of the list do not require Board of Directors resolution. All generative AI tools must approved in compliance with procedures stated in Appendix B.

Should you have some concerns about current list, please ask IT Service Center (CUI).

Definition of Company Data

The term "**Company Data**" should be interpreted broadly for the purposes of this policy and includes, at a minimum, the following: all of the Company's business information and all personal data (of employees, officers, contractors, consultants, customers, companies to be acquired, users or others) that any of the Company's systems have access to and that is collected, used, processed, stored, shared, distributed, transmitted, disclosed, destroyed or removed by any of the Company's systems; all proprietary information and intellectual property (including, but not limited to, source code, designs, schematics, product plans, product specifications, market analysis, reports, strategy documents, financial information, internal communications, customer lists, customer files, customer contact information, customer agreements, first, internal or confidential data of the customer or a third party, and any non-public information of the Company). Company Data includes information in written, electronic, audio, video or any other form or medium.

The Company's policy on the use of generative AI; Dos and don'ts

Account

If your work for the Company involves the use of generative AI tools licensed by the Company, then you may not use your personal account for the duties you perform at the Company in conjunction with such tool.

Confidential information

You should not include any personal, sensitive, proprietary, or confidential information in your communications to an AI generative application, such as ChatGPT, unless a detailed risk assessment has been conducted with respect to the use of such information and which risk assessment has been approved by the assigned Member of the Company's Board of Directors. (Note: Such data includes source code, confidential customer information and documents, passwords and other credentials, protected health information, employee materials, names, addresses, likenesses, information from documents marked "Confidential", "Sensitive" or "Proprietary", or any other non-public information owned or processed by the Companies that may be useful to competitors or harmful to the Company if disclosed).

Integration and assignment

Generative AI-based tools or AI-generated results should not be incorporated or integrated into the Company's commercial software products and offerings unless: (i) a detailed risk assessment has been conducted with respect to the use of such tools and which risk assessment has been approved by the assigned Member of the Company's Board of Directors, or (ii) the tool is listed in Exhibit A. In such cases, all employees of the Company shall be required to provide **they must** clearly and distinctly identify and/or label all AI-generated content in the internal documentation, including the source generative AI application. The research, implementation, development or incorporation into the Company's products or services of any functionality that in any way may be considered generative artificial intelligence must be approved in advance by the assigned Member of the Company's Board of Directors in accordance with the procedures set out in this Artificial Intelligence Policy or is listed in Exhibit A.

Disclosure

Except in cases where translation support or transcription is performed, all Company employees must disclose the use of generative AI in any material created within the organization. You should inform your supervisor about the use of generative AI to perform a task, regardless of the extent of such use. When presenting or submitting a work that includes AI-generated content, you must clearly identify the specific sections or elements that were created or influenced by generative AI technologies. the use of generative AI must be confirmed and the content generated by AI should be clearly indicated. For example: "The content used in this report is from ChatGPT." Under no circumstances should the work generated by the generative AI tool be presented as your own original work.

Public/viral risks

You should always assume that **any** information or data you provide to the AI generative tool will be made public and that you or the Company will be identified as the source of the disclosure. Such inadvertent disclosure may have legal consequences, including a breach of the Company's contractual obligations or applicable laws. Therefore, you should also exercise caution when using any non-confidential information, as

it may become associated with the Company and lead to the disclosure of information in respect of which we would not like to become publicly known.

Use of Company data

You should not use Company data in generative AI communications or upload Company data to such applications unless a detailed risk assessment has been carried out with respect to the use of such Company data and which risk assessment has been approved by the assigned Member of the Company's Board of Directors. The use of generative AI as part of, or in connection with, any offering that our customers will access and enter their communications into (e.g., a front-end AI application to facilitate searches of a product knowledge base) must obtain prior approval from the assigned Member of the Company Board of Directors, and the AI technology must be managed and controlled by the Company and located behind the Company's firewall.

Risk of inaccuracy

It is common for generative AI to make errors or create content that is biased, outdated, false, misleading, or factually contradictory. Any work produced using generative AI should be checked against reliable, manmade, independent sources. You are responsible for the accuracy and completeness of your work.

Annex A

The Company has reviewed some of the generative AI tools listed below. The use of any of the tools listed in this Appendix or other tools not listed must always comply with (i) the Company's policy on the use of generative AI and (ii) the guidelines for the use of the tool in question.

Generative AI tools tested by the Company:

1. GitHub Copilot business subscription (paid version, purchased by Sygnity)
2. Microsoft 365 Copilot (paid subscription, purchased by Sygnity)
3. Microsoft Teams Premium (purchased by Sygnity)
4. Stack AI (purchased by Sygnity)
5. Law Insider (Pro/Enterprise Access subscription purchased by Sygnity or TSS)

Appendix B:

TSS generative AI approval application

Read the offers, conditions and purpose of the proposed tool. Consider whether it complies with the Company's policies (including the Code of Conduct and Generative AI Policy) and any other obligations (e.g., customer agreements that may contain restrictions on the use of customer data). Consult with the assigned Board Member and ask them to sign it.

Please fill out the form below and request that a fully completed copy be sent to: (i) TSS Legal, (ii) the responsible GM of your BU, and (iii) TSS SCF Governance.

Tool/Platform Name	<i>[Insert Name]</i>
Terms and conditions	<i>[Insert link or send file separately]</i>
Briefly describe what the tool/platform is used for and how it will be used:	
Inputs <i>Unless otherwise indicated, please answer the following questions as Y/N based on the review of the terms. This refers to the "inputs" (information, hints, etc.) that we will enter into the Generative AI (TSS) tool.</i>	
What type or type of input is being entered into the tool/platform?	
Do we (TSS) remain the owner of all inputs?	
Does the input remain private to us (TSS)?	
Are the inputs used to update/improve their models?	
Is the input further transmitted to other AI tools/platforms? If so, what are they?	
Does the tool/platform comply with applicable data protection laws (e.g. GDPR) for the processing of personal or sensitive data?	
Is the tool/platform compatible with the recognized security standards (e.g. SOC 2, ISO 27001) to protect data integrity and confidentiality?	

<p>Go out Answer the following questions as Y/N based on the review of the conditions. This refers to the "results," which is the information we get from the Generative AI tool and want to use it.</p>	
Does TSS own the information generated?	
Are there any restrictions on use (i.e. can it be used commercially)?	
Other	
Have you identified any other caveats in the terms and conditions?	<i>[Please indicate any concerns or questions based on the initial assessment that they would like to see considered by approvers]</i>
AI impact/risk assessment	<i>[Please add a generative AI impact/risk assessment that assesses the potential ethical, legal, and safety implications of using the suggested generative AI tools in the specific context of the project and describes the steps taken to comply with the TSS AI Principles when using such generative AI tools.]</i>
I confirm that the tool/platform will only be used in accordance with the TSS Generative AI Policy.	

[BUSINESS UNIT NAME]

[Name of the person filling out this form]

[Date]

[Name: assigned Board Member]

[Date]

[Name: Business Unit Director]

[Date]

Code of Conduct

Annex 8 – Responsible Work Environment

Health and Safety

The Companies are committed to ensuring that your workplace is healthy, safe and accident-free. The Companies require their Representatives to strive to ensure these conditions as well. Never take actions that could jeopardize your health and safety or that of any other person, even if such actions could improve work. The Companies do not tolerate any form of violence in the workplace.

Diversity and Inclusion

Diversity embraces individual differences and unique characteristics such as personality, beliefs, values, gender, nationality, race, ethnic origin, age, religion, disability, sexual orientation, marital status and political preference. Inclusion recognizes and values people's differences to enrich work environments and enable optimal performance. It involves investment in understanding and eliminating bias, creating a working culture that accepts and respects everyone. In an inclusive environment, everyone is encouraged to thrive and be the best they can be.

Diversity and inclusion are vital to realize positive results for our business. By implementing our diversity and inclusion culture, Total Specific Solutions aims to create a diverse and inclusive workforce recognizing human rights and equal opportunities for our people.

The Companies wish to create work environment that mirrors the diversity of the society where all employees and coworkers feel welcome and safe, can be themselves and receive space and recognition to use their talents in development and customers' success.

We apply diversity and inclusion rules in all areas such as leadership, HR, research & development, sales and any other Companies operation activities.

No harassment and discrimination

The Companies do not tolerate harassment of any kind, including on the grounds of race, color, religion, gender, sexual orientation, national origin, age, disability or any other type of behavior that is hostile, disrespectful, abusive and/or humiliating. Harassment or discrimination can take many forms, such as verbal, visual or physical. Such conduct will not be tolerated. Employment with a given Company is based solely upon individual merit and qualifications directly related to your job. If you or your work colleague are being harassed or

discriminated against, report the situation to your supervisor or another person through the appropriate channel in accordance with the annex – Speak Up! which describes other forms of contact.

No workplace bullying

Workplace bullying is behavior by one person or a group of people that makes the targeted person feel humiliated or ridiculed. Workplace bullying can take many forms, such as verbal, visual, digital or physical. The Companies do not tolerate any form of workplace bullying. Detailed rules for dealing with such cases are described in each Company's Internal Anti-Bullying and Discrimination Policy. If you or your work colleague are the target of bullying, report the situation to your supervisor or report it to another person through the appropriate channel in accordance with the annex – Speak Up! which describes the appropriate forms of contact.

Equal opportunity

To be a leader in our business, we must be flexible, innovative, and creative and have the ability to accommodate other people's points of view. The Companies strive for equal opportunities for their Representatives, including recruitment, promotion, compensation, training and development. We expect our management persons to exercise leadership in this field by role-modelling appropriate behavior.

No drugs or alcohol

The Companies do not tolerate any use of drugs or other prohibited substances, or the consumption of alcohol during working hours or the inappropriate consumption of alcohol outside working hours if this affects the performance of the employee's duties.

EXAMPLES:

- 1. A Representative does not want to promote a female to Managing Director as the job requires leading a difficult management team and from the representative's point of view, the successor lacks dominant leadership style.**

However, this is not a justified reason to prevent this promotion since assessment shows that leadership skills are developed and one should be selected based on those leadership capabilities, and not personal preferred leadership style(s).

- 2. A Representative displays a screen saver with a cartoon that contains a harsh statement about religion.**

Such a display will be seen as discriminatory and will not be tolerated. Refer respectfully to any religion that your associates may profess.

3. A Representative notices that the breath of their work colleague regularly smells of alcohol. The Representative tries to discuss this with their colleague, but the conversation gets nowhere.

The Representative should report to his or her supervisor or another person through the appropriate channel in accordance with the annex – Speak Up! which describes the appropriate forms of contact. Alcohol consumption can seriously affect an associate's actions and put him/her and other Representatives at risk.

Q&A

- Question 1: I suspect that our company does not comply with fire safety regulations, which could potentially be very dangerous. My supervisor does not want to make sure all fire safety regulations are complied with, because this might put our targets at risk. What should I do?

If a person responsible for management does not take the appropriate actions, report this immediately through the appropriate channel in accordance with the Annex – Speak Up! which describes the appropriate forms of contact. Prevention of dangerous conditions will always prevail over meeting targets.

- Question 2: My colleague regularly makes sexual-orientated comments about my appearance. I feel highly uncomfortable working with this person. What should I do?

First of all, discuss the situation with your supervisor and if he/she does not help you then report it to the competent person through the channels indicated in the Annex – Speak Up!

- Question 3: After work, I attended a gathering with the rest of my team. One of the people made several unwelcome advances towards me. What should I do?

Unwelcome advances are never acceptable. If you are comfortable doing so, try to discuss the situation with the person professionally and respectfully. It is also a good idea to consult the relevant person in this area, e.g., the person in charge of the Human Resources Office or the persons indicated in the Annex – Speak Up! This will enable you to determine the next steps.

- Question 4: Whenever I ask my supervisor a question, my supervisor publicly mocks me and questions my qualifications. What do I do?

This behavior may be considered bullying, and at a minimum is disrespectful and inconsistent with our Code of Conduct. Report the case through one of the channels indicated in the Annex – Speak Up!

- Question 5: I was in the lunch room with my colleagues, just having a casual conversation, and one of them commented on another colleague that I found offensive. How do I handle this situation?

If you are comfortable doing so, professionally address the situation with the employee who commented to another colleague. If you do not feel comfortable addressing the situation yourself, need guidance or you are concerned that additional steps should be taken, then you should report the case through one of the channels indicated in the Annex – Speak Up!

- Question 6: When organizing an annual business unit event for employees, should you consider the relevant religious days of these employees?

Answer 6: Yes, to make people feel welcome and included it is pleasant to take all religions within the company into consideration.

Code of Conduct

Annex 9 – Speak Up!

Further information

What is the purpose of this annex?

The purpose of this Annex is to enable you to learn how you can report incidents of inappropriate behavior without fear of any retaliation.

Your responsibilities

We expect you to always act in accordance with the law and our Code of Conduct. Wherever laws, regulations or self-regulatory agreements are more restrictive, they prevail. We expect everyone to promote a culture of openness, in which we all feel comfortable raising questions, dilemmas and concerns regarding the interpretation of, or adherence to, this Code of Conduct.

Those in management positions have greater responsibilities: they must play a vital role in maintaining our reputation and good name necessary for the Company's business. You are expected to lead by example and create a transparent and open environment, in which concerns, or suspicions can be raised without fear of retaliation.

What to do when in doubt?

The Code of Conduct does not cover every situation that may occur, so you must also use common sense and professional judgement. If you are in doubt about what to do, ask yourself the following questions:

- Does it feel like it is the right thing to do?
- Is it legal and does it seem consistent with our values and our Code of Conduct?
- Will it be positively received in our Company or Companies?
- Would I still accept full responsibility for this decision if I read about this in the media?

If you answer in the negative to any of these questions, seek advice and discuss the issue with the appropriate person.

SPEAK UP

Do you have a concern about a possible violation of the Code of Conduct? Speak up! Remaining silent can only worsen the situation and undermine trust. When you honestly and truthfully raise a concern, you help to protect the Company, your workplace, and ultimately you, your colleagues and associates. So Speak Up! Raise any concern you have through appropriate Speak Up channels. All reporting is done on a confidential and/or anonymous basis and it is up to you to decide if you wish to submit it anonymously.

How to Speak up?

Our Code of Conduct allows you to raise concerns about suspected misconduct through a variety of channels either verbal or in writing. This document does not replace any regular reporting lines or complaints procedures within your business unit. If this solution is not an option, please pass on your report to us through one of the Speak Up channels. Remember that the Companies have appointed a Compliance Officer who is an additional contact person for reporting inappropriate behavior, e.g., if you do not want to discuss it with your supervisor. The Compliance Officer will speak to you in confidence and inform you of the next steps. Remember that you can also report concerns to any other local external institutions that have been legally formalized in your country, to do so you don't have to report any of your concerns internally first.

Other regulations regarding reporting irregularities

No matter which Company is your employer, or you cooperate with you can also report any irregularities based on:

1. The Procedure for anonymous reporting of irregularities – implemented in Sygnity as a publicly listed company, based on the provisions of the Act of 29 July 2005 on public offerings and conditions governing the introduction of financial instruments to organised trading, and on public companies, which defines the rules, method and procedures for anonymous reporting by employees and coworkers to a designated member of the Management Board, and in special cases – the Supervisory Board, violations of law.
2. Regulations regarding internal reports in Sygnity – which implements provisions for the protection of whistleblowers, based on Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of EU law.

Non-retaliation

No one will face retaliation if refusing to act in accordance with the provisions of the Code of Conduct. No one will suffer any consequences for raising concerns in good faith about compliance with the Code of Conduct. Any form of retaliation against you for speaking up will not be tolerated. Retaliation against whistleblowers is treated as a violation of this Code of Conduct and may lead to an appropriate investigation of that person.

Disciplinary Measures

A violation of the law and/or our Code of Conduct can have serious consequences for our Companies and the individuals involved, including you. The same goes for turning a blind eye to any such violation. You may be subject to an investigation and consequently to the sanctions envisaged by law. Companies may also face financial consequences and their reputation may be compromised. Violations of the law and/or the Code of Conduct may lead to action as envisaged by law, including dismissal. Using a third party or other means to bypass this Code of Conduct is never allowed.

What kind of information do you need to provide?

When reporting (in person, in writing, online or by phone), please provide as much detailed information as you can to enable our company to assess and investigate your concern, such as:

- The background, history and reason for the concern
- Names, dates, places and other relevant information
- Any documents that may support the reporting

What should you do if you do not have all the information?

We encourage you to speak up as soon as possible, ideally before the situation gets out of hand and/or damage is done. It is always better to discuss upfront than to report afterwards. If you know about or suspect misconduct, speak up with the facts that you have. We do not expect you to have all the answers and you are certainly not expected to prove that your concern is well founded. Let our Companies look into the matter to determine if there is a reason for concern. Never investigate the matter yourself and do not seek evidence to build a strong case. We guarantee that no disciplinary measures or other steps will be taken against you if your genuine concern later turns out to be mistaken or misguided.

Confidentiality

All reporting is done confidentially. This means that information about your concern will only be shared with a limited number of people on a strict need-to-know basis. Information will only be disclosed outside this small group if we are required to do so by law or an important public interest is at stake. In principle, we are obliged to inform the implicated person that a complaint has been filed against him/her, but your identity will not be disclosed. You can help us protect confidentiality by being discreet and not discussing your report with your colleagues or anyone else. You can share your concerns anonymously. We do however encourage you to reveal

Sygnity

Business Solutions

your identity as it is more difficult, and in some circumstances even impossible, for us to investigate reports that are made anonymously.

SPEAK UP CHANNELS

CONCERNED ABOUT MISCONDUCT



WITH WHOM CAN I TALK TO?



IF POSSIBLE, START WITH THE PERSON YOU SUSPECT OF MISCONDUCT

OR

TALK TO YOUR DIRECT SUPERVISOR OR
TALK TO THE COMPLIANCE OFFICER (FEMALE)

OR

TALK TO THE HR OFFICE DIRECTOR (FEMALE)

OR

TALK TO A LEGAL ADVISER (FEMALE OR MALE)

1. You can also report through the <https://gojira.sygnity.pl/sygnalista/> channel
2. In case of reports submitted based on “Regulations regarding internal reports in Sygnity” you can also report irregularities *via* below mentioned e-mail addresses:
 - sygnalista_zarząd@sygnity.pl
 - sygnalista_rada_nadzorcza@sygnity.pl
 - or *via* a paper report to be put in the dedicated mailbox placed in the Sygnity’s office in Warsaw.
3. At Sygnity Business Solutions S.A. you can submit your application via email:
 - compliance@sygnitysbs.pl;
 - or *via* a paper report to be put in the dedicated mailbox placed in the Sygnity Business Solutions office in Zielona Góra.

**WE UNDERSTAND IT IS NOT ALWAYS EASY TO RAISE
CONCERNS ABOUT POSSIBLE MISCONDUCT BUT WE DO
ENCOURAGE YOU TO CONTACT US.**

SPEAK UP!

**ANY CONCERN WILL BE DEALT WITH APPROPRIATELY AND
CONFIDENTIALLY.**