SKS365 GROUP

GROUP WHISTLEBLOWING POLICY

REV.	DATE	APPROVED	NOTES
1	8/05/2023	Andrew Naudi – Sole Director	First adoption of the policy for the headquarters and the branch in Italy, Austria e Serbia.

TABLE OF CONTENT

1. INTRODUCTION AND PURPOSE

SKS365 Malta Limited as well as its Branch offices in Italy, Austria and Serbia (together "**SKS365**" or the "**Company**") intends to promote a corporate culture characterised by virtuous behaviour and a corporate governance system that prevents commission of wrongful acts, while guaranteeing a work environment in which employees can serenely report any unlawful behaviour, enabling a virtuous path of transparency and compliance with adequate ethical standards. For this reason, SKS365 recognises the importance of adopting a specific procedure governing the reporting of unlawful conduct by employees.

With regards to the Italian Branch of the Company, this Policy forms an integral part of the Organisation, Management and Control Model pursuant to Italian Legislative Decree No. 231/2001 (the "**231 Model"**).

The purpose of this Policy is to define appropriate communication channels for receipt, analysis and processing of reports of possible unlawful conduct within SKS365. The identity of whistle-blowers must always be kept confidential, and whistle-blowers must not incur any liability, be it civil, criminal, administrative or employment-related for having reported in good faith possible wrongful acts through the appropriate channels.

In particular, the Company **prohibits and condemns any act of retaliation or discrimination, direct or indirect, against anyone who reports in good faith potential unlawful conduct**, for reasons directly or indirectly related to such report, providing for appropriate sanctions, within the disciplinary system, against those who violate the measures of whistle-blower's protection. At the same time, SKS365 commits itself to apply appropriate sanctions against those who, with wilful misconduct or gross negligence, submit reports that turn out to be ungrounded.

***

With reference to any reports of unlawful conduct in the area of anti-money laundering provisions applicable in the jurisdictions where the Company operates regarding any relevant conduct carried out by retail and online players, please refer to what is regulated in section 10 "*Internal Reporting Obligations (so-called Whistleblowing)*" in the document "*Policies for Managing the Risk of Money Laundering and Financing of Terrorism*" and/or to local applicable anti-money laundering policies and procedures.

***

With refence to the employees sitting at the Serbian Branch of the Company, the application of this Policy is secondary the guidelines set out in the "**Rulebook On Internal Whistleblowing Procedure At The Employer**", the latter being the prime guidelines applicable by said employees.

***

This Whistleblowing Policy has been prepared in terms of the local regulations applicable to the jurisdictions where the Company operates, adopted as implementing measures to Directive EU 2019/1937, where applicable.

2. TERMS OF VALIDITY

This Policy is valid starting from the date of its issuance indicated on the cover page.

Any subsequent update cancels and replaces, from the date of its issuance, all previously issued versions.

3. SCOPE OF APPLICATION – ADDRESSEES AND CORPORATE FUNCTIONS INVOLVED

This Whistleblowing Policy applies to the following subjects (together, the "**Addressees**"):

- all present or former employees, present or former persons who are or were seconded to the Company, or independent collaborators of SKS365;

- any candidate for employment, only where information concerning improper practices has been acquired during the recruitment process or other pre-contractual negotiations;

- self-employed workers, freelancers, contractors, subcontractors, consultants, volunteers and trainees (including unpaid ones), who perform their activities at SKS365;

- shareholders and persons with administrative, management, control, supervisory or representative functions, as well as non-executive members of the corporate bodies, of the Company its Branches in Italy, Austria and Serbia; and

- in general, all those who, although external to SKS365 Group, work directly or indirectly on its behalf (e.g., agents, distributors, business partners, etc.).

The protections afforded in terms of this Policy shall also apply to the following persons:

- third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons;

- legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context; and

- other persons as may be specified in locally applicable laws.

In line with the above, this document is communicated to all the Addressees by appropriate means of communication, including emails, by the AML Function (as defined below) or the function/department requesting the service of an entity outside SKS365 to which this document shall be communicated. In particular, the Whistleblowing Policy is displayed and made easily visible in workplaces, including through Company's intranet, and it is as well accessible to persons who, while not attending workplaces, have a legal relationship in one of the forms referred above. It is also published in a dedicated section of the SKS365 Group website.

***

In order that protection is afforded in terms of this Policy, the disclosure must be a protected disclosure. A protected disclosure is an internal disclosure (vide para. 5) or an external disclosure (vide para. 7) of information, made in writing or in any format which may be prescribed in terms of this Policy ("**Protected Disclosure**").

Anonymous disclosures are not automatically considered as Protected Disclosures. Notwithstanding, in the event that an anonymous Internal Disclosure or External Disclosure is made, and subsequently the whistle-blower has been identified and suffers retaliation, the whistle-blower shall nonetheless qualify for the protection provided by this Policy and applicable law, provided that the conditions as set out below have been satisfied.

A disclosure is a protected disclosure if the whistle-blower:

- had reasonable grounds to believe that the information on breaches disclosed was true at time of the disclosure; and
- disclosed internally (in accordance with Article 5 of this Policy) or externally (in accordance with Article 7 of this Policy or made a public disclosure.

The protections conferred by this Policy and in terms of applicable law do not apply to a whistle-blower who knowingly discloses information which he knows or ought to reasonably know is false.

In the event that a whistle-blower has made an Internal Disclosure or External Disclosure in good faith, and it transpires that the whistle-blower was mistaken about its import or that any perceived threat to the public interest on which the disclosure was based has not materialised or that the person making the disclosure has not fully respected the procedural requirements set by this Policy, such whistle-blower shall still be afforded the protections as set out in this Policy.

***

The person bearing the role Head of the Compliance & Money laundering reporting office for Italy (the "**Head of Compliance & MLRO – Italy**" or the "**AML Function**") is appointed as the whistleblowing reporting officer and is therefore responsible for collecting the reports, acknowledging receipt and following up on the latter, including by and carrying out the preliminary examination thereof, while ensuring the confidentiality of any information concerning the whistle-blower, the individuals named in the report and the subject-matter of the report, in order to prevent potential retaliatory acts of any kind. The AML Function is also responsible for keeping the whistle-blower abreast of the progress of an internal investigation and providing feedback to the whistle-blower where deemed appropriate. The AML Function is also responsible for reporting to the Company's senior management as per the provisions included in this document.

The AML Function shall be provided annually with adequate financial and organisational resources to allow the proper carrying out the activities provided for in this Policy.

4. GENERAL PRINCIPLES

The following general principles, as more exhaustively illustrated below, govern this Policy:

1. Prohibition of retaliatory or discriminatory acts toward the Whistleblower;
2. Prohibition of making manifestly unfounded and/or defamatory Reports;
3. Duty of independence and professionalism in the handling of Reports;
4. Due process of review ensuring right of defense of the reported individuals
5. Protection of the identity of the Whistleblower and confidentiality of information;
6. Protection of the Whistleblower.

5. PROCEDURE

5.1 REPORTING

5.1.1 Scope of the facts to be reported

All the Addressees are encouraged to report actions or conducts that:

- are not in line with SKS365's values, Code of Ethics and compliance procedures (including 231 Model with regard the Italian Branch); or
- do not comply with the laws in force in the territory of the relevant Branch (either at national or EU level); or
- could significantly damage the interests of SKS365.

Th following are examples of potential facts or actions to be reported:

- a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject, e.g. in the field of public procurement and public tenders, financial services, consumer protection, protection of privacy and personal data; or
- the health or safety of any individual has been, is being or is likely to be endangered; or
- a corrupt practice has occurred or is likely to occur or to have occurred; or
- a criminal offence has been committed, is being committed or is likely to be committed; or
- a breach affecting the financial interests of the European Union as referred to in Article 325 of the Treaty on the Functioning of the European Union (TFEU) and further specified in relevant European Union measures has occurred or is likely to occur or to have occurred; or
- a breach relating to the internal market, as referred to in Article 26(2) of the Treaty on the Functioning of the European Union (TFEU), including breaches of European Union competition and State aid rules, as well as breaches relating to the internal market in relation to acts which breach the rules of corporate tax or to arrangements the purpose of which is to obtain a tax advantage that defeats the object or purpose of the applicable corporate tax law has occurred or is likely to occur or to have occurred; or
- information tending to show any matter falling within any of the preceding points has been, is being or is likely to be deliberately concealed:

***

Reports must be made in a disinterested manner and in good faith: reports provided for the mere purpose of retaliation or intimidation, or ungrounded reports made with wilful misconduct or gross negligence shall be sanctioned. In particular, sending of any communication that proves to be ungrounded on the basis of objective elements and that is, again, on the basis of objective elements, made for the sole purpose of causing unjust damage to the reported person, shall be sanctioned.

The report shall not concern complaints, claims or demands related to an interest of a personal nature (i.e., that pertain exclusively to the individual employment relationships of the whistle-blower, or regarding the employment relationship with hierarchically superordinate figures) and, therefore, shall not be used for purely personal purposes.

5.1.2 Content of the report

The report shall provide the elements enabling the receiving function to carry out the necessary checks to assess whether the report is grounded.

To this end, the content of the report shall be sufficiently circumstantiated, and, as far as possible, provide the following information, together with any supporting documentation:

(i) clear and complete description of the conduct (that may also concern the omission of a due activity) underlying the report;

(ii) circumstances of time and place in which the reported facts were committed and the related conduct;

(iii) personal details or other elements (e.g., position held, relevant Function/Area) enabling the identification of the person who allegedly carried out the reported facts;

(iv) any third parties involved or potentially damaged;

(v) indication of any other persons who may be able to provide information on the facts underlying the report;

(vi) any other information that may prove useful in establishing the reported facts.

The identity of the whistle-blower making the Protected Disclosure, and the identity of Other Protected Persons (as defined below), shall be protected at all times and any communication in relation to the alleged or actual improper practice (including the report itself and/or any communication in this regard) shall not include the identification details, or any other details, which may lead to the identification of the whistle-blower who had made the disclosure or to the Other Protected Persons. Each of the whistle-blower and Other Protected Person(s) may, separately, expressly consent in writing to the disclosure of their details.

Any reports made omitting one or more of the above-mentioned elements shall be taken into account where they are sufficiently circumstantiated to allow an effective verification and review of the reported facts, where appropriate, by means of interaction with the whistle-blower and/or the third parties indicated in the report and/or through other means.

In particular, **anonymous reports**, i.e., those lacking any element allowing for their author to be identified, are admitted where allowed by local law. However, such reports limit SKS365's ability to carry out an effective verification of the reported information. Therefore, they shall only be taken into account if adequately substantiated and detailed and concerning potential wrongdoings or irregularities deemed serious. Relevant factors for assessing anonymous reporting include the credibility of the presented facts and the possibility of verifying the truthfulness of the information about the breach on the basis of reliable sources.

5.2 CHANNELS FOR REPORTING

The report shall be submitted by any of the following means:

1. via the specific IT platform made available by the Company at the following URL: sks365.parrotwb.app;

2. on the **e-mail** address of the Head of Compliance & MLRO - Italy;

3. by **ordinary post** to the address, as per place of employment, the Company or its relevant Branch, marked as "*private and confidential*" to the attention of the Head of Compliance & MLRO - Italy;

4. by word of mouth, through recorded calls via registered telephone line by calling the number provided by the Company and/or the recorded voice messaging system made available by the Company.

With regard to reports submitted by Addressees within the Italian Branch:

- In case of reports made using channels 1) and 4), the Supervisory Board (OdV) of the Italian Branch of the Company shall receive a notification of the report;
- In case of a report made using channel 3), or if a report made using channel 2) does not CC the Supervisory Board (OdV) of the Italian Branch, the AML Function shall forward the report to the Supervisory Board (OdV) of the Italian Branch.

Moreover, upon request of the whistle-blower, the oral report can also be made through a face-to-face meeting with the Head of Compliance & MLRO - Italy, set within a reasonable time. Also in this case, with regards to reports submitted with reference to the Italian Branch, the AML Function must promptly notify the Supervisory Board (OdV) of the Italian Branch.

Whoever receives a report which is not submitted via the channels identified above must promptly communicate same to the Head of Compliance & MLRO – Italy by means of one of the aforementioned channels, being sure to put at the disposition of the latter, the soft and hard copies that came to be in his / her possession.

In addition to the channels listed above, the channels provided by the compliance programmes adopted by SKS365 Branches on the basis of local regulations are available.

***

In the case of reports concerning any unlawful conduct realized by retail or/and online players in the area of anti-money laundering pursuant to Legislative Decree 231/2007 or any other locally applicable anti-money laundering regulations mistakenly sent to the reporting channels referred above, the AML Function shall manage the report in accordance with the provisions of the document "*Policies for the Management of the Risk of Money Laundering and Financing of Terrorism*".

5.3 ADDRESSEES OF REPORTS

The addressee of the reports is the Head of Compliance & MLRO - Italy, equipped with the necessary reporting management skills, also through dedicated training on the management of whistleblowing reports. This, however, without prejudice to the possibility that the report is sent to local compliance bodies on the basis of compliance programs adopted by relevant Branches on the basis of local regulations. In this case, the investigation activities indicated in Section 7 below are carried out directly by the local compliance body, possibly on the basis of the appropriate local procedure.

If the reported conduct concerns a member of the AML Function, the whistle-blower may forward its report directly to:

- the Supervisory Body (OdV) of the Italian Branch, in the person of its Chairman, with regards to reports submitted in respect of the Italian Branch, using the contact details provided; or
- the Legal department of the Company, using the email address of the relevant contact person.

5.4 INVESTIGATION ON THE REPORTS

Any investigation under this Policy will be conducted as sensitively and speedily as possible. Within 7 days of receipt of a report, the AML Function (or other recipient of the report, as outlined under par. 5.3 above) provides feedback to the whistle-blower on the receipt of the report and the intended timetable for investigation. The AML Function may outline this information in a written report, or he may opt to arrange a meeting with the whistle-blower. Such meeting shall be documented by the AML Function. Within three months of the date of the report, feedback shall be provided to the whistle-blower on the outcome of the investigation, making sure that the content of such feedback is not jeopardizing any action taken by the Company as a consequence of the investigation and/or any pending investigation carried out by Public Authorities on the same facts.

The AML Function (or other recipient of the report, as outlined under par. 5.3 above) preliminarily verifies the report is relevant and *prima facie* founded, if needed with the help of an external legal counsel bound to confidentiality on the activities carried out.

As part of the internal investigation conducted, the AML Function (or other recipient of the report, as outlined under par. 5.3 above) may request additional information and/or documentation from the whistle-blower. Whistle-blowers shall, as much as possible, co-operate to meet any reasonable request to clarify any facts and/or circumstances, to provide (additional) information. The lack of information or other evidence including the unwillingness of whistle-blower to cooperate with an investigation can be the reason for the AML Function (or other recipient of the report, as outlined under par. 5.3 above) deciding to conclude that the report has no factual basis.

The AML Function (or other recipient of the report, as outlined under par. 5.3 above) then registers the report by means of an identification code/name, ensuring the traceability and correct archiving of the documentation also in the subsequent stages.

The AML Function (or other recipient of the report, as outlined under par. 5.3 above) classifies reports into:

- **Non-relevant reports**: in this case, where appropriate, it shall inform the whistle-blower accordingly, addressing the latter to other Company Functions (e.g. HR, Legal) to address the items raised and close the report;

- **Reports made in bad faith**: the report is forwarded to the Head of HR for it to consider whether to commence any disciplinary procedure;

- **Substantiated reports**: if the AML Function (or other recipient of the report, as outlined under par. 5.3 above) considers that there is sufficient evidence of potentially unlawful conduct such as to allow for an investigation to be initiated, it starts the investigation phase.

The investigation phase takes the form of carrying out targeted checks on the reports, enabling the identification, analysis and evaluation of the elements confirming the reliability of the reported facts. The AML Function shall coordinate at this stage with the Legal Function and carefully evaluate the possibility to engage external professionals to assist in the investigation phase.

The AML Function (or other recipient of the report, as outlined under par. 5.3 above), in coordination with the Legal Function and external professionals, where engaged, may carry out any activity deemed appropriate, including personal hearing of the whistle-blower and any other person who may provide information on the facts reported. Indeed, the person involved may be heard, or, at his or her request, shall be heard, also by means of a paper procedure through the acquisition of written submissions and documents.

The AML Function (or other recipient of the report, as outlined under par. 5.3 above):

- Shall ensure that confidentiality requirements, as set out under Chapter 6 below, are fully complied with;

- Shall ensure that the verification be carried out in a diligent, fair and impartial manner; this implies that each person involved in the investigation must be informed – once the preliminary investigation has been completed – of the statements made and the evidence obtained against them and that they must be in a position to provide counter-arguments;

- may engage technical advisors (such as external professionals or in-house specialists of the Group) on matters that do not fall within their specific competence.

Information gathered in the course of the investigation, even when managed by third parties involved, shall be handled with the utmost confidentiality and restricted to the persons involved in the verification activities.

5.5 OUTCOME OF THE INVESTIGATION

The investigation phase may end up with:

a. **A negative outcome**, in which case the report is dismissed;

b. **A positive outcome**, in which case the AML Function (or other recipient of the report, as outlined under par. 5.3 above) shall send the outcome of the investigation to the directorship of the Company, in order to enable SKS365 to take the necessary countermeasures and adopt any disciplinary sanctions. In particular, upon completion of the verification, a report shall be issued to the directorship of the Company that:

- summarises the course of the investigation;

- sets out the conclusions reached and provides any supporting documentation;

- provides recommendations and suggests actions to be taken in relation to the breaches detected, at disciplinary and compliance level.

Feedback shall be provided to the whistle-blower at the conclusion of the investigation. However, details of the outcome of the investigation cannot be shared with the whistle-blower, in compliance with the confidentiality obligation to which the Company is bound.

5.6 REPORTING

The AML Function provides updates in relation to the reports received and the status of any open investigation:

a) quarterly - to the Supervisory Board of the Italian Branch, with regard to reports submitted by Addressees within the Italian Branch; and

b) on an annual basis - to the Board of Directors of the Company and to the individuals in charge of managing each Branch.

6. PROTECTION AND RESPONSIBILITY OF THE WHISTLE-BLOWER

CONFIDENTIALITY AND PROHIBITION OF RETALIATORY AND/OR DISCRIMINATORY ACTS

SKS365 guarantees the utmost **confidentiality** of the identity of the whistle-blower, the person involved, and the persons otherwise mentioned in the report, as well as of the content of the report and related documentation, using, to this end, criteria and communication methods suitable to protect the identity and integrity of the above-mentioned persons, also in order to ensure that the whistle-blower is not subject to any form of retaliation and/or discrimination, avoiding in any case the communication of data to third parties who are not involved in the report management process regulated by this procedure.

With the exception of cases where criminal or civil liability of the whistle-blower can be envisaged and instances where anonymity is not enforceable by law, the identity of the whistle-blower is protected in any context subsequent to the reporting.

Therefore, subject to the exceptions mentioned above, the identity of the whistle-blower may not be disclosed without their express consent, and all persons who receive or are involved in the handling of the report are obliged to protect the confidentiality of such information.

Breach of the confidentiality obligation gives rise to disciplinary liability, without prejudice to other forms of liability provided for by law.

In particular, in the framework of any disciplinary procedure brought against any person mentioned in the report, the identity of the whistle-blower may only be disclosed in cases where express consent of the whistle-blower is provided.

The same confidentiality requirements shall be applied also to the persons involved/ mentioned in the report.

***Bona fide* whistle-blowers shall be protected against any form of retaliation, discrimination or penalisation, without prejudice to any other form of protection provided for by the law.**

By way of example only, the following are considered to be form of retaliation:

- termination of employment, suspension or equivalent measures;
- downgrading or non-promotion;
- change of duties, change of place of work, reduction of salary, change of working hours;
- suspension of training or any restriction of access to training;
- negative merit notes or negative references;
- the adoption of disciplinary measures or other sanction, including fines;
- intimidation, harassment or ostracism;

- discrimination or otherwise unfavorable treatment;
- the failure to convert a fixed-term employment contract into an employment contract of indefinite duration, where the employee had a legitimate expectation of such conversion;
- the non-renewal or early termination of a fixed-term employment contract;
- damage, including to a person's reputation, particularly on social media, or economic or financial harm, including loss of economic opportunities and loss of income;
- improper listing on the basis of a formal or informal sector or industry agreement, which may result in the person being unable to find employment in the sector or industry in the future;
- the early termination or cancellation of a contract for the supply of goods or services;
- the cancellation of a license or permit;
- the request to undergo psychiatric or medical examinations.

Whistle-blowers who believe that they have been subjected to retaliatory conduct as a result of a previously made reports are encouraged to file a new report concerning the retaliation they have suffered. Moreover, they can communicate to the competent national body / authority any form of retaliation that they deemed to have suffered (see par. 7 below).

Acts taken in violation of the prohibition above shall be null and void. Whistle-blowers who have been fired as a result of whistleblowing have the right to be reinstated in their jobs and/or to get any protection granted by applicable local law.

***

Alongside the protection granted to the whistle-blower, the above-mentioned protective measures shall also be granted towards referred to as “Other Protected Persons”:

(a) facilitators (i.e., those who assist a whistleblower in the reporting process, operating within the same work context and whose assistance must be kept confidential);

(b) persons in the same work context as the whistle-blower who are related to him/her by a stable emotional or family relationship within the fourth degree;

(c) co-workers of the whistle-blower who work in his/her same work context and who have a regular and current relationship with him/her;

(d) entities owned by the whistle-blower, as well as entities operating in the same work context of the whistle-blower.

RESPONSIBILITY OF THE WHISTLE-BLOWER

As anticipated above, disciplinary sanctions may be applied to the whistle-blower making reports with malice or gross negligence, in accordance with locally applicable labor regulations. The criminal and civil liability of the whistle-blower remains unaffected.

Any forms of abuse of whistleblowing, such as manifestly opportunistic, slanderous or defamatory reports and/or made for the sole purpose of harming the reported person or other persons, as well as any other hypothesis of improper use or intentional instrumentalization of the whistleblowing channels, are also subject to disciplinary sanctions and/or liability under applicable law.

7. EXTERNAL REPORTING

In case the whistle-blower has:

- already made an internal report according to paragraph 5 above and it has not been followed up within the terms set in the same chapter; or

- reasonable grounds to believe that if he or she made an internal report, the report would not be effectively followed up or that the same report may result in the risk of retaliation;

- reasonable grounds to believe that the violation may pose an imminent or obvious danger to the public interest;

whistle-blower may make an external report ("**External Disclosure**") to the competent national body / authority set up according to local applicable law. This is also considered to be a Protected Disclosure in terms of this Policy.

The competent national bodies operating within the EU and competent for the matters addressed by this Policy are:

- ANAC – Autorità Nazionale Anticorruzione for Italy
- BAK - Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung for Austria
- Commissioner of Revenue (CfR), Financial Intelligence Analysis Unit (FIAU), Malta Financial Services Authority (MFSA), Commissioner for Voluntary Organisation (CVO), Permanent Commission Against Corruption and the Ombudsman, depending on the kind of reported facts, for Malta.

The reporting can be done in written form, through IT platforms or the other means implemented by the national body / authority, or in oral form, through telephone line and/or the recorded voice messaging system implemented by the national body / authority. The relevant national body / authority shall guarantee the utmost confidentiality of the identity of the whistle-blower, the person involved, and the person otherwise mentioned in the report, as well as the content of the report and related documentation. For the more detailed discipline, please refer to relevant local laws.

8. TRACEABILITY

The documentation used in the performance of the activities (including in the case of irrelevant reports) shall be kept by the AML Function (or other recipient of the report, as outlined under par. 5.3 above) in a special archive.

Reports and related documentation shall be retained for as long as necessary for the processing of the report, and in any case no longer than five years from the date of the communication of the final outcome of the reporting procedure, in compliance with the confidentiality obligations set forth by the relevant applicable laws.

Where a recorded telephone line or another recorded voice messaging system is used for reporting, subject to the consent of the reporting person, the AML Function (or other recipient of the report, as outlined under par. 5.3 above) may keep the report in the following ways:

a) by making a recording of the conversation in a durable and retrievable form; or

b) through a complete and accurate transcript of the conversation prepared by the staff members responsible for handling the report (the whistle-blower may verify, correct or confirm the contents of the transcript by his or her own signature).

When, at the request of the whistle-blower, the report is made orally in a face-to-face meeting with the personnel in charge, it shall, with the consent of the reporting person, be documented by the personnel in charge by recording on a device suitable for storage and listening or by minutes. In case of minutes, the reporting person may verify, correct and confirm the minutes of the meeting by his or her signature.

In the report archive, personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay.

***

Personal data - including special categories of data and judicial data - disclosed as part of the reporting will be processed in accordance with the provisions of the European Regulation 2016/679 on the Protection of Personal Data ("GDPR") and according to the relevant Company's policies.

9. DISCIPLINARY SYSTEM

Failure to comply with the principles and rules contained in this Policy entails the application of the disciplinary system adopted by the Company.

GRUPPO SKS365

POLICY WHISTLEBLOWING DI GRUPPO

REV.	DATA	APPROVATA	NOTE
1	8/05/2023	Andrew Naudi – Sole director	Prima approvazione della policy per l'headquarters e le branch in Italia, Austria e Serbia.

INDICE

1. PREMESSA E SCOPO

SKS365 Malta Limited e con essa le sue Branch con sede in Italia, Austria e Serbia (insieme "**SKS365**" o la "**Società**") intendono promuovere una cultura aziendale caratterizzata da comportamenti virtuosi e un sistema di corporate governance che prevenga la commissione di atti illeciti, garantendo al contempo un ambiente di lavoro in cui i dipendenti possano serenamente segnalare eventuali comportamenti illeciti, consentendo un percorso virtuoso di trasparenza e rispetto di adeguati standard etici. Per questo motivo, SKS365 riconosce l'importanza di adottare una procedura specifica per la segnalazione di comportamenti illeciti da parte dei dipendenti.

Per quanto riguarda la Branch italiana della Società, la presente policy costituisce parte integrante del Modello di organizzazione, gestione e controllo ai sensi del Decreto Legislativo 231/2001 (il "**Modello 231**").

Lo scopo di tale policy è quello di definire i canali di comunicazione appropriati per la ricezione, l'analisi e l'elaborazione delle segnalazioni di possibili comportamenti illeciti all'interno di SKS365. L'identità degli informatori deve sempre essere mantenuta riservata e gli informatori non devono incorrere in alcuna responsabilità, sia essa civile, penale, amministrativa o lavorativa, per aver segnalato in buona fede possibili atti illeciti attraverso i canali appropriati.

In particolare, la Società **vieta e condanna qualsiasi atto di ritorsione o discriminazione, diretto o indiretto, nei confronti di chiunque segnali in buona fede potenziali condotte illecite**, per motivi direttamente o indirettamente connessi alla segnalazione, prevedendo adeguate sanzioni, nell'ambito del sistema disciplinare, nei confronti di coloro che violano le misure di tutela del segnalante. Allo stesso tempo, SKS365 si impegna ad applicare sanzioni adeguate nei confronti di coloro che, con dolo o grave colpa, presentano segnalazioni che si rivelano infondate.

***

Con riferimento ad eventuali segnalazioni di comportamenti illeciti nell'ambito delle disposizioni antiriciclaggio applicabili nelle giurisdizioni in cui opera la Società relativamente a qualsiasi condotta rilevante posta in essere da attori retail e online, si rimanda a quanto disciplinato nella sezione 10 "*Obblighi di segnalazione interna (c.d. Whistleblowing)*" del documento "*Politiche di gestione del rischio di riciclaggio e finanziamento del terrorismo*" e/o alle politiche e procedure antiriciclaggio locali applicabili.

***

Con riferimento ai dipendenti in forza alla Branch di SKS365 Malta Limited con sede in Serbia, Ogranak SKS365 Malta Limited Beograd, la Policy di Whistleblowing trova applicazione in via subordinata rispetto al "Rulebook On Internal Whistleblowing Procedure At The Employer", la quale continua ad avere nei loro riguardi applicazione prioritaria.

***

La presente Policy di Whistleblowing è stata redatta in conformità alle normative locali applicabili alle giurisdizioni in cui opera la Società, adottate come misure di attuazione della Direttiva UE 2019/1937, ove applicabile.

2. TERMINI DI VALIDITÀ

La presente Policy è valida a partire dalla data di emissione indicata sul frontespizio.

Qualsiasi aggiornamento successivo annulla e sostituisce, a partire dalla data di emissione, tutte le versioni precedentemente emesse.

3. AMBITO DI APPLICAZIONE - DESTINATARI E FUNZIONI AZIENDALI COINVOLTE

La presente Whistleblowing Policy si applica ai seguenti soggetti (i "**Destinatari**"):

- tutti gli attuali o ex dipendenti, persone che sono o sono state distaccate presso la Società, o collaboratori di SKS365;

- qualsiasi candidato all'assunzione, solo nel caso in cui le informazioni relative a pratiche scorrette siano state acquisite durante il processo di assunzione o altre trattative precontrattuali;

- lavoratori autonomi, liberi professionisti, appaltatori, subappaltatori, consulenti, volontari e tirocinanti (anche non retribuiti), che svolgono la loro attività presso SKS365;

- gli azionisti e i soggetti con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, nonché i membri non esecutivi degli organi sociali, della Società o delle sue branch in Italia, Austria e Serbia;

- in generale, tutti coloro che, pur essendo esterni a SKS365 Group, operano direttamente o indirettamente per suo conto (ad esempio, agenti, distributori, partner commerciali, ecc.).

Le tutele previste dalla presente Policy si applicano anche alle seguenti persone:

- soggetti terzi che hanno rapporti con i segnalanti e che potrebbero subire ritorsioni in ambito lavorativo, come colleghi o parenti dei segnalanti;

- soggetti giuridici di cui i soggetti segnalanti sono proprietari, per i quali lavorano o con i quali sono altrimenti collegati in un contesto lavorativo; e

- altre persone, come indicato nelle leggi applicabili a livello locale.

In linea con quanto sopra, il presente documento viene comunicato a tutti i Destinatari con mezzi di comunicazione appropriati, inclusa la posta elettronica, da parte della Funzione AML (come di seguito definita) o della funzione/reparto che richiede il servizio di un'entità esterna a SKS365 a cui il presente documento deve essere comunicato. In particolare, la Whistleblowing Policy è esposta e resa facilmente visibile nei luoghi di lavoro, anche attraverso la rete interna aziendale, ed è accessibile anche a coloro che, pur non frequentando i luoghi di lavoro, hanno un rapporto giuridico in una delle forme sopra citate. Viene inoltre pubblicata in una sezione dedicata del sito web di SKS365 Group.

***

Affinché la protezione sia garantita ai sensi della presente Whistleblowing Policy, la segnalazione deve essere una segnalazione protetta. Una segnalazione protetta è una segnalazione interna (v. par. 5) o di una segnalazione esterna (v. par. 7) di informazioni, in forma scritta o in qualsiasi formato che possa essere prescritto ai sensi della presente Policy ("**Segnalazione Protetta**").

Le segnalazioni anonime non sono considerate automaticamente come Segnalazioni Protette. Ciononostante, nel caso in cui venga effettuata una segnalazione interna o esterna anonima e successivamente il segnalante venga identificato e subisca ritorsioni, il segnalante potrà comunque beneficiare della protezione prevista dalla presente Policy e dalla legge applicabile, a condizione che siano state soddisfatte le condizioni di seguito riportate.

Una comunicazione è una comunicazione protetta se il segnalante:

- aveva ragionevoli motivi per credere che le informazioni sulle violazioni divulgate fossero vere al momento dell'effettuazione della comunicazione; e
- ha effettuato una segnalazione interna (conformemente al par. 5 della presente Policy di Whistleblowing) o esterna (conformemente al par. 7 della presente Policy di Whistleblowing) o ha reso una divulgazione pubblica.

Le tutele conferite dalla presente Policy di Whistleblowing e in termini di legge applicabile non si applicano a un segnalante che comunichi consapevolmente informazioni che sa o dovrebbe ragionevolmente sapere essere false.

Nel caso in cui un segnalante abbia fatto una segnalazione interna o esterna in buona fede, e risulti che il segnalante si sia sbagliato sulla sua rilevanza o che qualsiasi minaccia percepita all'interesse pubblico su cui si basava la comunicazione non si sia concretizzata o che la persona che ha reso la segnalazione non abbia rispettato appieno i requisiti procedurali stabiliti dalla presente Policy, a tale segnalante saranno comunque garantite le tutele stabilite dalla presente Policy.

***

Il soggetto titolare del ruolo di Head of Compliance e Responsabile interno della funzione antiriciclaggio per l'Italia "**Responsabile della Funzione AML"** o sinteticamente "**Funzione AML**") è nominato responsabile delle segnalazioni di whistleblowing ed è pertanto incaricato di raccogliere le segnalazioni, darne riscontro e dare seguito a queste ultime, anche mediante l'effettuazione di un'istruttoria delle stesse, assicurando al contempo la riservatezza di tutte le informazioni riguardanti il segnalante, i soggetti citati nella segnalazione e l'oggetto della stessa, al fine di prevenire potenziali atti ritorsivi di qualsiasi natura. La Funzione AML è inoltre responsabile di tenere aggiornato il segnalante sull'andamento di un'indagine interna e di fornire un feedback al segnalante, se ritenuto opportuno. Il Responsabile della Funzione AML è anche responsabile della segnalazione all'alta direzione della Società, come previsto dalle disposizioni contenute nel presente documento.

La Funzione AML deve essere dotata annualmente di adeguate risorse finanziarie e organizzative per consentire il corretto svolgimento delle attività previste dalla presente Policy.

4. PRINCIPI GENERALI

I seguenti principi generali, illustrati in modo più esaustivo di seguito, regolano la presente Policy:

1. Divieto di atti di ritorsione o discriminatori nei confronti del Segnalante;
2. Divieto di effettuare Segnalazioni palesemente infondate e/o diffamatorie;
3. Dovere di indipendenza e professionalità nella gestione delle Segnalazioni;
4. Un giusto procedimento di accertamento che garantisca il diritto di difesa dei soggetti segnalati
5. Protezione dell'identità del Segnalante e riservatezza delle informazioni;
6. Protezione del Segnalante.

5. PROCEDURA

5.1 SEGNALAZIONE

5.1.1 Ambito dei fatti da segnalare

Tutti i Destinatari sono invitati a segnalare azioni o comportamenti che:

- non sono in linea con i valori, il Codice Etico e le procedure di compliance di SKS365 (incluso il Modello 231 per quanto riguarda la Branch Italiana); o
- non sono conformi alle leggi in vigore nel territorio della Branch interessata (a livello nazionale o dell'UE); oppure
- potrebbero danneggiare in modo significativo gli interessi di SKS365.

I seguenti sono esempi di potenziali fatti o azioni da segnalare:

- una persona non ha adempiuto, non sta adempiendo o è probabile che non adempia a un obbligo giuridico a cui è soggetta, ad esempio nel campo delle procedure ad evidenza pubblica, dei servizi finanziari, della tutela dei consumatori, della protezione della privacy e dei dati personali; o
- la salute o la sicurezza di un individuo è stata, è o può essere messa in pericolo; oppure
- si è verificata o è probabile che si verifichi o si sia verificata una pratica di corruzione; oppure
- è stato commesso, è in corso o potrebbe essere commesso un reato; oppure
- si è verificata o è probabile che si verifichi o si sia verificata una violazione degli interessi finanziari dell'Unione europea di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea (TFUE) e ulteriormente indicata nelle pertinenti misure dell'Unione europea; oppure
- si è verificata, o è probabile che si verifichi o si sia verificata, una violazione relativa al mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea (TFUE), comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni relative al mercato interno in relazione ad atti che violano le norme sull'imposta sulle società o ad accordi il cui scopo è ottenere un vantaggio fiscale che vanifichi l'oggetto o lo scopo della normativa applicabile in materia di imposta sulle società; oppure
- informazioni tendenti a dimostrare che una questione che rientra in uno dei punti precedenti è stata, è in corso o è probabile che venga deliberatamente occultata:

***

Le segnalazioni devono essere effettuate in modo disinteressato e in buona fede: saranno sanzionate le segnalazioni effettuate a mero scopo di ritorsione o intimidazione, o quelle prive di fondamento effettuate con dolo o colpa grave. In particolare, sarà sanzionato l'invio di qualsiasi comunicazione che risulti infondata sulla base di elementi oggettivi e che sia, sempre sulla base di elementi oggettivi, effettuata al solo scopo di arrecare un danno ingiusto alla persona segnalata.

La segnalazione non deve riguardare reclami, pretese o richieste relative a un interesse di natura personale (cioè che riguardino esclusivamente i singoli rapporti di lavoro del segnalante o il rapporto di lavoro con figure gerarchicamente sovraordinate) e, pertanto, non deve essere utilizzata per scopi puramente personali.

5.1.2 Contenuto della segnalazione

La segnalazione deve fornire gli elementi che consentano alla funzione ricevente di effettuare i controlli necessari per valutare la fondatezza della segnalazione.

A tal fine, il contenuto della segnalazione deve essere sufficientemente circostanziato e, per quanto possibile, fornire le seguenti informazioni, unitamente a qualsiasi documentazione di supporto:

(i) descrizione chiara e completa del comportamento (che può riguardare anche l'omissione di un'attività dovuta) alla base della segnalazione;

(ii) circostanze di tempo e di luogo in cui sono stati commessi i fatti segnalati e la relativa condotta;

(iii) dati anagrafici o altri elementi (ad esempio, posizione ricoperta, funzione/area di pertinenza) che consentano di identificare la persona che avrebbe compiuto i fatti segnalati;

(iv) eventuali terzi coinvolti o potenzialmente danneggiati;

(v) indicazione di eventuali altre persone in grado di fornire informazioni sui fatti alla base della segnalazione;

(vi) qualsiasi altra informazione che possa risultare utile per stabilire i fatti segnalati.

L'identità del segnalante che effettua la Segnalazione Protetta e l'identità degli Altri Soggetti Protetti (come definiti di seguito) saranno sempre protette e qualsiasi comunicazione in relazione alla presunta o effettiva pratica scorretta (compresa la segnalazione stessa e/o qualsiasi comunicazione al riguardo) non dovrà includere i dati identificativi o qualsiasi altro dettaglio che possa portare all'identificazione del segnalante che ha effettuato la segnalazione o degli Altri Soggetti Protetti. Ciascuno dei Segnalanti e delle altre persone protette può, separatamente, acconsentire espressamente per iscritto alla divulgazione dei propri dati.

Le segnalazioni che omettono uno o più dei suddetti elementi saranno prese in considerazione qualora siano sufficientemente circostanziate da consentire un'effettiva verifica e revisione dei fatti segnalati, se del caso, attraverso l'interazione con il segnalante e/o i terzi indicati nella segnalazione e/o con altri mezzi.

In particolare, le **segnalazioni anonime**, cioè prive di qualsiasi elemento che consenta di identificarne l'autore, sono ammesse laddove consentito dalla legge locale. Tuttavia, tali segnalazioni limitano la possibilità di SKS365 di effettuare una verifica efficace delle informazioni riportate. Pertanto, saranno prese in considerazione solo se adeguatamente motivate e dettagliate e riguardano potenziali illeciti o irregolarità ritenute gravi. I fattori rilevanti per la valutazione delle segnalazioni anonime includono la credibilità dei fatti presentati e la possibilità di verificare la veridicità delle informazioni sulla violazione sulla base di fonti affidabili.

5.2 CANALI PER LA SEGNALAZIONE

La segnalazione può essere presentata alternativamente:

1. tramite l'apposita piattaforma informatica messa a disposizione dalla Società e resa accessibile al seguente URL: sks365.parrotwb.app;

2. all'indirizzo **e-mail** aziendale del Responsabile interno della Funzione AML;

3. tramite **posta ordinaria** all'indirizzo, a seconda dei casi, della Società o della branch di riferimento, avendo cura di distinguere la corrispondenza con la dicitura "*privato e riservato*" e di porre la stessa all'attenzione del Responsabile interno della Funzione AML;

4. oralmente, tramite l'apposito sistema di messaggistica vocale registrato all'uopo fornito dalla Società medesima.

Le segnalazioni attinenti alla Branch Italiana sono prontamente inoltrate dalla Funzione AML all'Organismo di Vigilanza, per l'eventuale seguito di competenza.

Inoltre, su richiesta del segnalante, la segnalazione orale può essere effettuata anche attraverso un incontro di persona con il Responsabile interno della Funzione AML, fissato entro un termine ragionevole. Anche in questo caso, per quanto riguarda le segnalazioni attinenti alla Branch Italiana, la Funzione AML deve darne tempestiva comunicazione all'Organismo di Vigilanza (OdV) della Branch Italiana.

Chiunque riceva una segnalazione effettuata al di fuori dei canali di comunicazione sopra elencati è tenuto a comunicarlo prontamente al Responsabile interno della Funzione AML mediante uno dei suddetti canali, avendo cura di mettere a disposizione di quest'ultimo la documentazione digitale o cartacea di cui sia entrato in possesso.

Oltre ai canali sopra elencati, sono disponibili i canali previsti dai programmi di compliance adottati da SKS365 in conformità alle normative locali.

***

Nel caso di segnalazioni relative a comportamenti illeciti posti in essere in materia di antiriciclaggio ai sensi del D.lgs. 231/2007 o di qualsiasi altra normativa antiriciclaggio applicabile a livello locale erroneamente inviate ai canali di segnalazione di cui sopra, la Funzione AML provvede a gestire la segnalazione secondo quanto previsto dal documento "*Politiche di gestione del rischio di riciclaggio e di finanziamento del terrorismo*".

5.3 SOGGETTI DEPUTATI A RICEVERE LE SEGNALAZIONI

Il soggetto deputato alla ricezione delle segnalazioni è il Responsabile interno della Funzione AML, dotato delle necessarie competenze di gestione delle segnalazioni, anche attraverso una formazione dedicata alla gestione delle segnalazioni di whistleblowing. Ciò, tuttavia, non pregiudica la possibilità che la relazione venga inviata agli organismi di compliance locali sulla base dei programmi di compliance adottati dalle Branch interessate sulla base delle normative locali. In tal caso, le attività di indagine indicate nella successiva Sezione 5.4 sono svolte direttamente dall'organismo di compliance locale, eventualmente sulla base dell'apposita procedura locale.

Se la condotta segnalata riguarda un membro della Funzione AML, il segnalante può inoltrare la segnalazione direttamente:

- all'Organismo di Vigilanza, nella persona del suo Presidente, in relazione alle segnalazioni attinenti alla Branch Italiana, utilizzando i recapiti appositamente comunicati; o
- all'ufficio legale della Società, utilizzando l'indirizzo e-mail del responsabile di tale funzione.

5.4 INDAGINE SULLE SEGNALAZIONI

Qualsiasi indagine ai sensi della presente Policy sarà condotta nel modo più delicato e rapido possibile. Entro 7 giorni dalla ricezione della segnalazione, la Funzione AML (o altro destinatario della segnalazione, come indicato al precedente par. 5.3) fornisce un riscontro al segnalante in merito alla ricezione della segnalazione e alla tempistica prevista per l'indagine. La Funzione AML può delineare queste informazioni in una relazione scritta, oppure può scegliere di organizzare un incontro con il segnalante. Tale incontro deve essere documentato dalla Funzione AML. Entro tre mesi dalla data della segnalazione, dovrà essere fornito al segnalante un riscontro sull'esito dell'indagine, assicurandosi che il contenuto di tale riscontro non pregiudichi eventuali azioni intraprese dalla Società a seguito dell'indagine e/o eventuali indagini in corso svolte da Autorità Pubbliche sui medesimi fatti.

La Funzione AML (o altro destinatario della segnalazione, come indicato al precedente par. 5.3) verifica preliminarmente che la segnalazione sia rilevante e *prima facie* fondata, se necessario con l'ausilio di un consulente legale esterno tenuto alla riservatezza sulle attività svolte.

Nell'ambito dell'indagine interna condotta, la Funzione AML (o altro destinatario della segnalazione, come indicato al precedente par. 5.3) può richiedere al segnalante ulteriori informazioni e/o documentazione. I segnalanti devono, per quanto possibile, collaborare per soddisfare qualsiasi ragionevole richiesta di chiarire fatti e/o circostanze, di fornire informazioni (aggiuntive). La mancanza di informazioni o di altre prove, compresa la riluttanza del segnalante a collaborare a un'indagine, può essere il motivo per cui la Funzione AML (o un altro destinatario della segnalazione, come indicato al precedente paragrafo 5.3) decide di concludere che la segnalazione non ha basi concrete.

La Funzione AML (o altro destinatario della segnalazione, come indicato al precedente par. 5.3) provvede quindi a registrare la segnalazione tramite un codice/nome identificativo, garantendo la tracciabilità e la corretta archiviazione della documentazione anche nelle fasi successive.

La Funzione AML (o altro destinatario della segnalazione, come indicato al precedente par. 5.3) classifica le segnalazioni in:

- **Segnalazioni non rilevanti**: in quest'ipotesi, se del caso, informerà il segnalante, indirizzandolo ad altre Funzioni aziendali (ad es. Risorse Umane, Ufficio Legale) per affrontare i punti sollevati e chiudere la segnalazione;

- **Segnalazioni in malafede**: la segnalazione viene inoltrata al responsabile delle risorse umane affinché valuti se avviare una procedura disciplinare;

- **Segnalazioni circostanziate**: se la Funzione AML (o altro destinatario della segnalazione, come indicato al precedente par. 5.3) ritiene che vi siano sufficienti evidenze di comportamenti potenzialmente illeciti tali da consentire l'avvio di un'indagine, avvia la fase investigativa.

La fase di indagine si concretizza nell'esecuzione di controlli mirati sulle segnalazioni, che consentono di individuare, analizzare e valutare gli elementi che confermano l'attendibilità dei fatti riportati. In questa fase, la Funzione AML si coordinerà con la Funzione Legale e valuterà attentamente la possibilità di coinvolgere professionisti esterni per assistere nella fase di indagine.

La Funzione AML (o altro destinatario della segnalazione, come indicato al precedente par. 5.3), in coordinamento con la Funzione Legale e con i professionisti esterni, ove incaricati, può svolgere ogni attività ritenuta opportuna, compresa l'audizione personale del segnalante e di ogni altro soggetto che possa fornire informazioni sui fatti

segnalati. Infatti, la persona coinvolta può essere ascoltata, o, su sua richiesta, sarà ascoltata, anche mediante una procedura cartacea attraverso l'acquisizione di osservazioni e documenti scritti.

La Funzione AML (o altro destinatario della segnalazione, come indicato al par. 5.3):

- deve garantire il pieno rispetto dei requisiti di riservatezza, come indicato al capitolo 6;

- deve garantire che la verifica sia condotta in modo diligente, equo e imparziale; ciò implica che ogni persona coinvolta nell'indagine deve essere informata – una volta completate le indagini preliminari – delle dichiarazioni rese e delle prove acquisite a suo carico e che deve essere in grado di fornire controdeduzioni;

- può avvalersi di consulenti tecnici (come professionisti esterni o specialisti interni al Gruppo) su questioni che non rientrano nelle sue competenze specifiche.

Le informazioni raccolte nel corso dell'indagine, anche se gestite da soggetti terzi coinvolti, saranno trattate con la massima riservatezza e limitate alle persone coinvolte nelle attività di verifica.

5.5 ESITO DELL'INDAGINE

La fase di indagine può concludersi con:

a. **Esito negativo**, nel qual caso la segnalazione viene archiviata;

b. **Esito positivo**: in tal caso la Funzione AML (o altro destinatario della segnalazione, come indicato al precedente par. 5.3) trasmetterà l'esito dell'accertamento all'Organo amministrativo della Società, al fine di consentire a SKS365 di adottare le necessarie contromisure e le eventuali sanzioni disciplinari. In particolare, al termine della verifica, sarà emessa una relazione all'Organo amministrativo della Società che:

- riassume l'iter dell'indagine;

- espone le conclusioni raggiunte e fornisce l'eventuale documentazione di supporto;

- fornisce raccomandazioni e suggerisce azioni da intraprendere in relazione alle violazioni rilevate, a livello disciplinare e di compliance.

Al termine dell'indagine, il segnalante riceverà un feedback. Tuttavia, i dettagli dell'esito dell'indagine non possono essere condivisi con il segnalante, in ottemperanza all'obbligo di riservatezza cui è tenuta la Società.

5.6 FLUSSI INFORMATIVI

La Funzione Antiriciclaggio fornisce aggiornamenti in relazione alle segnalazioni ricevute e allo stato delle indagini aperte:

a) trimestralmente - all'Organismo di Vigilanza della Filiale italiana, con riferimento alle segnalazioni presentate dai Destinatari all'interno della Filiale Italiana; e

b) su base annuale - al Consiglio di amministrazione della Società e ai responsabili della gestione di ciascuna Filiale.

6. PROTEZIONE E RESPONSABILITÀ DEL SEGNALANTE

RISERVATEZZA E DIVIETO DI ATTI DI RITORSIONE E/O DISCRIMINATORI

SKS365 garantisce la massima **riservatezza** sull'identità del segnalante, del soggetto coinvolto e dei soggetti altrimenti indicati nella segnalazione, nonché sul contenuto della segnalazione e della relativa documentazione, utilizzando, a tal fine, criteri e modalità di comunicazione idonei a tutelare l'identità e l'integrità dei suddetti soggetti, anche al fine di garantire che il segnalante non sia oggetto di alcuna forma di ritorsione e/o discriminazione, evitando in ogni caso la comunicazione dei dati a terzi non coinvolti nel processo di gestione della segnalazione disciplinato dalla presente procedura.

Ad eccezione dei casi in cui sia ipotizzabile una responsabilità penale o civile del segnalante e dei casi in cui l'anonimato non sia previsto dalla legge, l'identità del segnalante è protetta in qualsiasi ambito successivamente alla segnalazione.

Pertanto, fatte salve le eccezioni di cui sopra, l'identità del segnalante non può essere rivelata senza il suo esplicito consenso e tutte le persone che ricevono o sono coinvolte nella gestione della segnalazione sono tenute a proteggere la riservatezza di tali informazioni.

La violazione dell'obbligo di riservatezza dà luogo a responsabilità disciplinare, fatte salve le altre forme di responsabilità previste dalla legge.

In particolare, nell'ambito di qualsiasi procedura disciplinare avviata nei confronti di una persona menzionata nella segnalazione, l'identità del segnalante può essere rivelata solo in caso di consenso esplicito del segnalante.

Gli stessi requisiti di riservatezza si applicano anche alle persone coinvolte/ menzionate nella segnalazione.

I segnalanti in buona fede devono essere protetti da qualsiasi forma di ritorsione, discriminazione o penalizzazione, fatta salva ogni altra forma di tutela prevista dalla legge.

A titolo puramente esemplificativo, sono considerate forme di ritorsione le seguenti:

- Il licenziamento, la sospensione o misure equivalenti;
- Il declassamento o la non promozione;
- Il cambio di mansioni, il cambio di sede di lavoro, la riduzione della retribuzione, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla formazione;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o altre sanzioni, comprese le multe;
- l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o il trattamento altrimenti sfavorevole;

- la mancata conversione di un contratto di lavoro a tempo determinato in un contratto di lavoro a tempo indeterminato, quando il lavoratore aveva una legittima aspettativa di tale conversione;

- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a tempo determinato;

- danni, compresi quelli alla reputazione di una persona, in particolare sui social media, o danni economici o finanziari, compresa la perdita di opportunità economiche e di reddito;

- un inserimento improprio nell'elenco sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità di trovare un impiego nel settore o nell'industria in futuro;

- la risoluzione anticipata o l'annullamento di un contratto per la fornitura di beni o servizi;

- l'annullamento di una licenza o di un permesso;

- la richiesta di sottoporsi a esami psichiatrici o medici.

I segnalanti che ritengono di aver subito una condotta ritorsiva a seguito di una segnalazione fatta in precedenza sono incoraggiati a presentare una nuova segnalazione relativa alla ritorsione subita. Inoltre, possono comunicare all'organismo/autorità nazionale competente qualsiasi forma di ritorsione che ritengano di aver subito (cfr. par. 7).

Gli atti compiuti in violazione del divieto di cui sopra sono nulli. I segnalanti che sono stati licenziati a seguito di whistleblowing hanno il diritto di essere reintegrati nel loro posto di lavoro e/o di ottenere qualsiasi protezione garantita dalla legge locale applicabile.

***

Oltre alla protezione concessa al segnalante, le misure di protezione di cui sopra sono concesse anche nei confronti degli "Altri Soggetti Protetti":

(a) facilitatori (ossia coloro che assistono il segnalante nel processo di segnalazione, operando nello stesso contesto lavorativo e la cui assistenza deve essere mantenuta riservata);

(b) persone che si trovano nello stesso contesto lavorativo del segnalante e che sono legate a lui da un rapporto affettivo o familiare stabile entro il quarto grado;

(c) i colleghi del segnalante che lavorano nel suo stesso contesto lavorativo e che hanno con lui un rapporto regolare e corrente;

(d) entità di proprietà del segnalante, nonché entità che operano nello stesso contesto lavorativo del segnalante.

RESPONSABILITÀ DEL SEGNALANTE

Come anticipato in precedenza, le sanzioni disciplinari possono essere applicate al segnalante che effettua segnalazioni con dolo o grave colpa, in conformità con le normative sul lavoro applicabili a livello locale. La responsabilità penale e civile del segnalante rimane inalterata.

Eventuali forme di abuso del whistleblowing, quali segnalazioni palesemente opportunistiche, calunniose o diffamatorie e/o effettuate al solo scopo di danneggiare il segnalato o altri soggetti, nonché ogni altra ipotesi di

utilizzo improprio o di intenzionale strumentalizzazione dei canali di whistleblowing, sono altresì soggette a sanzioni disciplinari e/o responsabilità ai sensi della normativa vigente.

7. SEGNALAZIONE ESTERNA

Nel caso in cui il segnalante abbia:

- già effettuato una segnalazione interna ai sensi del precedente paragrafo 5 e questa non ha avuto seguito nei termini previsti dallo stesso capitolo; oppure
- ragionevoli motivi per ritenere che, se facesse una segnalazione interna, questa non avrebbe un seguito efficace o che la stessa segnalazione potrebbe comportare il rischio di ritorsioni;
- ragionevoli motivi per ritenere che la violazione possa rappresentare un pericolo imminente o evidente per l'interesse pubblico;

il medesimo segnalante può effettuare una segnalazione esterna ("**Segnalazione Esterna**") all'ente / autorità nazionale competente istituito in conformità alla legge locale applicabile. Anche questa è considerata una Segnalazione Protetta ai sensi della presente Policy di Whistleblowing.

Gli organismi nazionali operanti nell'ambito dell'Unione Europea e aventi competenze in relazione alla materia oggetto della presente Policy di Whistleblowing sono:

- ANAC - Autorità Nazionale Anticorruzione per l'Italia
- BAK - Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung per l'Austria
- Commissioner of Revenue (CfR), Financial Intelligence Analysis Unit (FIAU), Malta Financial Services Authority (MFSA), Commissioner for Voluntary Organisation (CVO), Permanent Commission Against Corruption (Commissione permanente contro la corruzione) e l'Ombudsman, a seconda del tipo di fatti segnalati, per Malta.

La segnalazione può avvenire in forma scritta, attraverso le piattaforme informatiche o gli altri mezzi implementati dall'organismo/autorità nazionale, o in forma orale, attraverso il sistema di messaggistica vocale registrata implementato dall'organismo/autorità nazionale. L'organismo/autorità nazionale competente deve garantire la massima riservatezza dell'identità del segnalante, della persona coinvolta e di quella altrimenti menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione. Per una disciplina più dettagliata, si rimanda alle leggi locali in materia.

8. TRACCIABILITÀ

La documentazione utilizzata nello svolgimento delle attività (anche nel caso di segnalazioni non pertinenti) sarà conservata dalla Funzione AML (o da altro destinatario della segnalazione, come indicato al precedente par. 5.3) in un apposito archivio.

Le segnalazioni e la relativa documentazione saranno conservate per il tempo necessario all'evasione della segnalazione e comunque non oltre cinque anni dalla data di comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza previsti dalla normativa vigente in materia.

Qualora per la segnalazione venga utilizzato un sistema di messaggistica vocale registrato, previo consenso del segnalante, la Funzione AML (o altro destinatario della segnalazione, come indicato al precedente par. 5.3) può conservare la segnalazione nei seguenti modi:

a) effettuando una registrazione della conversazione in forma durevole e recuperabile; oppure

b) attraverso una trascrizione completa e accurata della conversazione redatta dai membri del personale incaricati di gestire la segnalazione (il segnalante può verificare, correggere o confermare il contenuto della trascrizione con la propria firma).

Quando, su richiesta del segnalante, la segnalazione viene fatta oralmente in un incontro di persona con il personale incaricato, essa, con il consenso del segnalante, viene documentata dal personale incaricato mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto o mediante verbalizzazione. In caso di verbale, il segnalante può verificare, correggere e confermare il verbale della riunione con la propria firma.

Nell'archivio delle segnalazioni, i dati personali che non sono manifestamente rilevanti per il trattamento di un rapporto specifico non saranno raccolti o, se accidentalmente raccolti, saranno cancellati senza indebito ritardo.

***

I dati personali - comprese le categorie particolari di dati e i dati giudiziari - comunicati nell'ambito della segnalazione saranno trattati in conformità alle disposizioni del Regolamento europeo 2016/679 sulla Protezione dei Dati Personali ("GDPR") e secondo le relative politiche aziendali.

9. SISTEMA DISCIPLINARE

L'inosservanza dei principi e delle regole contenute nella presente Policy comporta l'applicazione del sistema disciplinare adottato dalla Società.

SKS365 GROUP

PRAVILNIK O UNUTRAŠNJEM UZBUNJIVANJU

BR.	DATUM	ODOBRIO	NAPOMENA
1	8/05/2023	Andrew Naudi - direktor	Prvo usvajanje pravilnika za sedište kompanije kao i za ogranke u Italiji, Austriji i Srbiji

SADRŽAJ

1. UVOD I SVRHA

SKS365 Malta Limited i njeni ogranci u Italiji, Austriji i Srbiji (u daljem tekstu "**SKS365**" ili "**Kompanija**") imaju nameru da promovišu korporativnu kulturu koja se karakteriše profesionalnim ponašanjem i korporativnim upravljačkim sistemom koji sprečava činjenje nezakonitih radnji, istovremeno garantujući radno okruženje u kojem zaposleni mogu mirno da prijave svako nezakonito ponašanje, omogućavajući profesionalan tok transparentnosti i usklađenosti sa odgovarajućim etičkim standardima. Iz tog razloga, SKS365 prepoznaje važnost usvajanja specifičnog pravilnika koji uređuje prijavljivanje nezakonitog ponašanja od strane zaposlenih.

Što se tiče italijanskog ogranka kompanije, ovaj pravilnik predstavlja integralni deo Modela organizacije, upravljanja i kontrole u skladu sa italijanskim Zakonskim dekretom br. 231/2001 (tzv. ,,**Model 231**").

Svrha ovog pravilnika je definisanje odgovarajućih komunikacionih kanala za prijem, analizu i obradu izveštaja o mogućim nezakonitim postupcima unutar SKS365. Identitet lica koja podnose izveštaj uvek mora biti držan u tajnosti, a ta lica ne smeju snositi nikakvu odgovornost, bilo građansku, krivičnu, administrativnu ili radno-pravnu, zbog prijavljivanja mogućih nezakonitih postupaka na odgovarajući način i iz dobrih namera.

Kompanija **zabranjuje i osuđuje svaki čin osvete ili diskriminacije, direktno ili indirektno, protiv bilo koga ko u dobroj nameri prijavljuje moguće nezakonite postupke**, zbog razloga direktno ili indirektno povezanih sa takvom prijavom, obezbeđujući odgovarajuće sankcije, unutar disciplinskog postupka, protiv onih koji krše mere zaštite lica koja prijavljuju. Istovremeno, SKS365 se obavezuje da primenjuje odgovarajuće sankcije protiv onih koji s namerom ili grubom nepažnjom podnose izveštaje koji se ispostave kao neutemeljeni.

***

U vezi sa bilo kojim izveštajima o nezakonitim postupcima u području odredbi protiv sprečavanja pranja novca koje se primenjuju u jurisdikcijama gde kompanija posluje u vezi sa bilo kojim relevantnim postupcima koje sprovode igrači u objektima i onlajn igrači, molimo vas da se uputite na ono što je regulisano u poglavlju 10 ,,Obaveze internog izveštavanja (takozvano prijavljivanje nepravilnosti)" u dokumentu ,,Politike za upravljanje rizikom pranja novca i finansiranja terorizma" i/ili lokalno primenljive pravilnike i postupke protiv sprečavanja pranja novca.

***

U odnosu na zaposlene koji rade u srpskom ogranku kompanije, primena ovog pravilnika je sekundarna u odnosu na smernice date u ,,Pravilniku o proceduri o internom uzbunjivanju kod Poslodavca'', pri čemu su smernice u ovom pravilniku primarne koje primenjuju navedeni zaposleni.

***

Ovaj Pravilnik o unutrašnjem uzbunjivanju je pripremljen u skladu sa lokalnim propisima primenljivim u zemljama u kojima kompanija posluje, u skladu sa Direktivom EU 2019/1937, gde je primenljiva. Direktiva EU 2019/1937 predviđa zaštitu uzbunjivača u Evropskoj uniji i ima za cilj da uspostavi zajednički standard za zaštitu uzbunjivača u celoj EU.

2. USLOVI VAŽENJA

Ovaj Pravilnik stupa na snagu i primenjuje se od datuma navedenog na naslovnoj strani.

Bilo kakvo kasnije ažuriranje poništava i zamenjuje, od datuma njegovog usvajanja, sve prethodne usvojene verzije.

3. OBLAST PRIMENE – ADRESE I KORPORATIVNE FUNKCIJE KOJE SU UKLJUČENE U PROCEDURU

Ovaj Pravilnik o unutrašnjem uzbunjvanju odnosi se na sledeće subjekte (zajedno ,,Adresate''):

- sve trenutne ili bivše zaposlene, trenutne ili bivše osobe koje su ili bile angažovane u Kompaniji, ili nezavisne saradnike SKS365;

- bilo kog kandidata za zaposlenje, samo ako se informacije o nepravilnim postupanjima steknu tokom procesa zapošljavanja ili drugih predugovornih pregovora;

- samozaposlene radnike, slobodne saradnike, izvođače radova, podizvođače, konsultante, volontere i pripravnike (uključujući neplaćene), koji obavljaju svoje aktivnosti u SKS365;

- akcionare i osobe sa administrativnim, menadžerskim, kontrolnim, nadzornim ili predstavničkim funkcijama, kao i članove korporativnih tela koji nemaju ovlašćenje za upravljanje u Kompaniji i njenim ograncima u Italiji, Austriji i Srbiji;

- uopšteno, sve one koji, iako su van SKS365 Grupe, rade direktno ili indirektno u njeno ime (npr. agenti, distributeri, poslovni partneri itd.) (zajedno, "**Adresati**").

Zaštita koja se pruža u skladu sa ovim pravilnikom takođe se odnosi na sledeće osobe:

- treće osobe koje su povezane sa osobama koje podnose izveštaje i koje bi mogle biti izložene osveti u kontekstu rada, kao što su kolege ili srodnici osoba koje podnose izveštaje;

- pravna lica koja su u vlasništvu osobe koje podnose izveštaje, za koja rade ili su na drugi način povezani u kontekstu rada;

- druge osobe koje su navedene u lokalno primenljivim zakonima.

U skladu sa navedenim, ovaj dokument se putem odgovarajućih sredstava komunikacije, uključujući e-poštu, dostavlja svim adresatima, od strane AML sektora ili funkcije/odeljenja (kao što je definisano u nastavku) koje zahtevaju uslugu entiteta van SKS365, kome će biti dostavljen ovaj dokument. Posebno, Pravilnik o unutrašnjem uzbunjivanju se prikazuje i lako je vidljiv na radnim mestima, uključujući kroz internet kompanije, a dostupna je i osobama koje, iako ne prisustvuju radnom mestu, imaju pravni odnos u jednoj od gore navedenih formi. Takođe se objavljuje u posebnom delu veb-sajta SKS365 Grupe.

***

Da bi se zaštitio u skladu s ovim Pravilnikom, uzbunjivanje mora biti zaštićeno uzbunjivanje. Zaštićeno uzbunjivanje je interno uzbunjivanje (čl. 5) ili eksterno uzbunjivanje (čl. 7), izraženo pismeno ili u bilo kom drugom formatu koji je propisan u skladu s ovim Pravilnikom (,,**Zaštićeno otkrivanje**").

Anonimna uzbunjivanja se ne smatraju automatski Zaštićenim uzbunjivanjem. Međutim, u slučaju da je anonimno interno ili eksterno otkrivanje informacija učinjeno, a kasnije je otkriven identitet osobe koja je otkrila informacije i ta osoba je podvrgnuta osveti, ta osoba će i dalje imati pravo na zaštitu koju pruža ovaj Pravilnik i primenljivi zakoni, pod uslovom da su ispunjeni uslovi navedeni u nastavku.

Uzbunjivanje je zaštićeno uzbunjivanje ako je uzbunjivač:

- imao razumne razloge da veruje da su informacije o kršenjima tačne u vreme uzbunjivanja; i
- izneo je interno (u skladu sa članom 5 ovog Pravilnika) ili eksterno (u skladu sa članom 7 ovog Pravilnika) uzbunjivanje, ili je javno objavio uzbunjivanje.

Zaštita koju pruža ovaj Pravilnik i srodni zakoni ne odnosi se na uzbunjivača koji namerno otkriva informacije koje zna ili bi trebao očigledno znati da su lažne.

U slučaju da je uzbunjivač dobronamerno izneo interno ili eksterno uzbunjivanje, a ispostavi se da je uzbunjivač bio u zabludi u vezi sa njegovim značajem ili da se bilo koja uočena pretnja za javni interes na kojoj se zasnivalo uzbunjivanje nije materijalizovala, ili da osoba koja je iznela uzbunjivanje nije u potpunosti poštovala proceduralne zahteve utvrđene ovim Pravilnikom, takav uzbunjivač će i dalje biti zaštićen u skladu sa ovim Pravilnikom.

***

Osoba koja je imenovana za menadžera sektora za izveštavanje o usklađenosti poslovanja i sprečavanja pranja novca za Italiju (menadžer sektora za usklađenost poslovanja i sprešavanje pranja novca u Italiji ili ,,**AML sektor**"), je imenovana za lice kome se prijavljuje unutrašnje uzbunjivanje i odgovorno je za prikupljanje izveštaja, potvrdu o prijemu i praćenje prijave, uključujući i preliminarnu proveru, uz obezbeđivanje poverljivosti informacija koje se odnose na osobu koja je prijavila, osobe koje su imenovane u izveštaju i predmet prijave, kako bi se sprečili potencijalna osvetnička delovanja svake vrste. AML sektor je takođe odgovorno za informisanje lica koje prijavljuje o napretku unutrašnje istrage i davanje povratnih informacija, gde se smatra potrebnim. Menadžer sektora za sprečavanje pranja novca takođe je odgovoran za izveštavanje višeg menadžmenta kompanije u skladu sa odredbama koje čine ovaj dokument.

AML sektoru će se godišnje obezbediti adekvatni finansijski i organizacioni resursi kako bi se omogućilo pravilno sprovođenje aktivnosti predviđenih ovim Pravilnikom.

4. OPŠTI PRINCIPI

Sledeći opšti principi, kao što je detaljnije opisano u nastavku, regulišu ovaj Pravilnik:

1. **Zabrana osvete ili diskriminacije prema uzbunjivaču;**
2. **Zabrana podnošenja očigledno neosnovanih i/ili klevetničkih prijava;**
3. **Obaveza nezavisnosti i profesionalnosti u postupanju s prijavama;**
4. **Poštovanje procesa pregleda koji osigurava pravo na odbranu osoba prijavljenih za nepravilnosti;**
5. **Zaštita identiteta uzbunjivača i poverljivosti informacija;**
6. **Zaštita uzbunjivača.**

5. PROCEDURA

5.1 PRIJAVLJIVANJE

5.1.1 Obeležja činjenica koje treba prijaviti

Svi Adresati se ohrabruju da prijave postupke i ponašanja koja:

- nisu u skladu sa vrednostima, Kodeksom etike i procedurama usklađenosti poslovanja SKS365 (uključujući Model 231 u pogledu italijanske filijale); ili
- ne poštuju zakone koji su na snazi na teritoriji odgovarajućeg ogranka (bilo na nacionalnom ili nivou EU); ili
- bi mogli značajno oštetiti interese SKS365.

U nastavku su primeri potencijalnih činjenica ili postupaka koje treba prijaviti:

- osoba nije ispunila, ne ispunjava ili je verovatno da neće ispuniti bilo koju zakonsku obavezu na koju je obavezna, npr. u oblasti javne nabavke i javni tenderi, finansijskih usluga, zaštite potrošača, zaštite privatnosti i ličnih podataka; ili
- zdravlje ili bezbednost bilo kog pojedinca je ugroženo, bilo da se dešava ili verovatno će se desiti; ili
- dogodila se ili je verovatno da će se dogoditi koruptivna delatnost; ili
- izvršeno je krivično delo, izvršava se ili je verovatno da će se izvršiti; ili
- dogodio se ili verovatno će se dogoditi prekršaj koji utiče na finansijske interese Evropske unije, kako je navedeno u članu 325 Ugovora o funkcionisanju Evropske unije (UFEU) i dalje specificirano u relevantnim merama Evropske unije; ili
- prekršaj koji se odnosi na unutrašnje tržište, kako je navedeno u članu 26(2) Ugovora o funkcionisanju Evropske unije (UFEU), uključujući prekršaje u vezi sa pravilima Evropske unije o konkurenciji i državnoj pomoći, kao i prekršaje u vezi sa unutrašnjim tržištem u odnosu na postupke koji krše pravila korporativnog poreza ili aranžmane čiji je cilj da se dobije poreska prednost koja narušava suštinu ili cilj primenljivog zakona o korporativnom porezu, dogodio se, dešava se ili je verovatno da će se desiti; ili
- informacije koje ukazuju na bilo koju od prethodnih tačaka su bile, jesu ili će verovatno biti namerno prikrivene.

***

Prijave moraju biti sačinjene na nepristrasan način i sa dobrom namerom: prijave koji su dostavljene isključivo u svrhu osvete ili zastrašivanja, ili neosnovane prijave napravljene sa namernom greškom ili grubom nepažnjom će biti sankcionisane. Posebno, slanje bilo kakve komunikacije koja se ispostavi kao neosnovana na osnovu objektivnih elemenata i koja je, opet, na osnovu objektivnih elemenata, napravljena samo u cilju uzrokovanja nepravedne štete prijavljenoj osobi, biće sankcionisane.

Prijave se ne smeju odnositi na pritužbe, zahteve ili zahteve vezane za lični interes (tj. koji se odnose isključivo na individualni odnos i zaposlenje uzbunjivača, ili u vezi sa zaposlenjem odnosno sa hijerarhijski nadređenim licima) i, stoga, ne smeju se koristiti u isključivo lične svrhe.

5.1.2 Sadržaj prijave

Prijava treba da obezbedi elemente koji omogućavaju imenovanom licu koje prima prijavu da izvrši potrebne provere i proceni da li je prijava osnovana.

U svrhu toga, sadržaj prijave treba da bude dovoljno jasno opisan, i, koliko je to moguće, da pruži sledeće informacije, zajedno sa svom pripadajućom dokumentacijom:

(i) jasan i potpun opis ponašanja (koje može takođe da se odnosi na propuštanje adekvatnih aktivnosti) koje leži u osnovi prijave;

(ii) okolnosti koje se odnose na vreme i mesto u kojima su se dogodili prijavljeni događaji i ponašanja na koja se navedeno odnosi;

(iii) lični podaci ili drugi elementi (npr. zauzeta pozicija, relevantna funkcija/oblast) koji omogućavaju identifikaciju osobe koja je navodno izvršila prijavljene događaje;

(iv) bilo koja treća strana koja je bila uključena ili potencijalno oštećena;

(v) naznaka bilo kojih drugih osoba koje bi mogle da pruže informacije o događajima koji su osnova prijave;

(vi) bilo koje druge informacije koje bi mogle biti korisne u utvrđivanju prijavljenih činjenica.

Identitet osobe koja podnosi zaštićenu prijavu, kao i identitet drugih zaštićenih osoba (kako su definisane u nastavku), biće zaštićen u svakom trenutku, i bilo kakva komunikacija u vezi sa navodnom ili stvarnom neprikladnom praksom (uključujući sam izveštaj i/ili bilo koju drugu komunikaciju u vezi s tim) neće uključivati identifikacione podatke ili bilo koje druge detalje koji bi mogli dovesti do identifikacije osobe koja je podnela prijavu ili drugih zaštićenih osoba. Svako od lica koje podnosi zaštićenu prijavu i druge zaštićene osobe može, pojedinačno, izričito dati pismenu saglasnost za otkrivanje svojih podataka.

Sve prijave koji izostave jedan ili više od gorenavedenih elemenata biće uzete u obzir ako su dovoljno opisane da omoguće efikasnu proveru i pregled prijavljenih činjenica, ako je to prikladno, putem interakcije sa osobom koja je podnela prijavu i/ili trećim stranama naznačenim u prijavi i/ili putem drugih sredstava.

Posebno, **anonimne prijave**, odnosno one kojima nedostaju neki elementi koji omogućavaju identifikaciju autora, prihvataju se ukoliko to dozvoljava lokalni zakon. Međutim, takvi izveštaji ograničavaju sposobnost SKS365 da izvrši efikasnu proveru prijavljenih informacija. Stoga će se takvi izveštaji uzeti u obzir samo ako su adekvatno potkrepljeni i detaljni, a odnose se na potencijalne nepravilnosti ili nepravilnosti koje se smatraju ozbiljnim. Relevantni faktori za procenu anonimne prijave uključuju verodostojnost prikazanih činjenica i mogućnost provere istinitosti informacija o povredi na osnovu pouzdanih izvora.

5.2 KANALI ZA PRIJAVU

Prijava se podnosi na bilo koji od sledećih načina:

1. putem posebne IT platforme koju je kompanija učinila dostupnom na sledećoj URL adresi: sks365.parrotwb.app;

2. na e-mail adresu menadžera za usklađenost poslovanja i sprečavanje pranja novca – Italija;

3. redovnom poštom na adresu prema mestu zaposlenja, kompanije ili njenog ogranka, označeno kao ,,privatno i poverljivo'' za menadžera za usklađenost poslovanja i sprečavanje pranja novca – Italija;

4. usmeno, putem snimljenih poziva putem registrovane telefonske linije pozivom na broj koji je kompanija obezbedila i/ili snimanjem glasovne poruke putem sistema koji je kompanije učinila dostupnim.

U vezi sa izveštajima podnetim od strane Adresata unutar italijanskog ogranka:

- U slučaju prijava koje su podnete putem kanala 1) i 4), Nadzorni odbor (OdV) italijanskog ogranka kompanije će dobiti obaveštenje o izveštaju;

- U slučaju prijava koje su podnete putem kanala 3), ili ako prijava podneta putem kanala 2) ne sadrži kopiju za Nadzorni odbor (OdV) italijanskog ogranka, AML sektor će proslediti izveštaj Nadzornom odboru (OdV) italijanskog ogranka.

Osim toga, na zahtev lica koje je podnelo prijavu, usmena prijava može biti izvršena i putem sastanka licem u lice sa menadžerom za usklađenost poslovanja i sprečavanje pranja novca – Italija, u razumnom roku. Takođe u ovom slučaju, u vezi sa prijavama koje su podnete od strane adrese unutar italijanskog ogranka, AML sektor mora odmah obavestiti nadzorni odbor italijanskog ogranka.

Ko god primi izveštaj koji nije dostavljen preko gore navedenih kanala mora odmah obavestiti menadžera za usklađenost poslovanja i sprečavanje pranja novca – Italija putem jednog od gore navedenih kanala, vodeći računa da ga stavi na raspolaganje u originalu kao i fotokopirano, u svemu kao što ih je on primio.

Pored navedenih načina, dostupni su i načini koji su propisani procedurama usklađenosti poslovanja, a koje su usvojili ogranci SKS365 na osnovu lokalnih propisa.

***

U slučaju prijave koja se odnosi na nezakonito ponašanje ostvareno od strane igrača u objektima i/ili online u području sprečavanja pranja novca u skladu sa Zakonskim dekretom 231/2007 ili drugim lokalno primenjivim propisima o sprečavanju pranja novca i finansiranju terorizma, koji su slučajno poslati na prijavne kanale gore navedene, AML sektor će upravljati prijavom u skladu s odredbama dokumenta ,,Pravilnik za upravljanje rizikom pranja novca i financiranja terorizma".

5.3 ADRESE PRIJAVLJIVANJA

Primalac prijave je menadžera za usklađenost poslovanja i sprečavanje pranja novca – Italija, koji poseduje potrebne veštine upravljanja prijavama, takođe prošao je i sveobuhvatnu obuku o koordinisanju prijava o unutrašnjem uzbunjivanju. Međutim, ne dovodeći u pitanje mogućnost da se prijava pošalje lokalnim telima za usklađenost s obzirom na programe usklađenosti koje relevantni ogranci usvajaju na temelju lokalnih propisa. U tom slučaju, aktivnosti istraživanja navedene u poglavlju 7 u nastavku sprovodi lokalno telo za usklađenost, po mogućnosti na temelju odgovarajućeg lokalnog postupka.

Ako prijavljeno ponašanje uključuje člana AML sektora, uzbunjivač može podneti prijavu direktno:

- Nadzornom organu (OdV) italijanskog ogranka, u vidu njenog direktora, u vezi sa izveštajima podnetim u vezi sa italijanskim ogrankom, koristeći date kontakt podatke;
- Pravnom odeljenju Kompanije, korišćenjem e-mail adrese relevantne osobe za kontakt.

5.4 ISTRAŽIVANJE PRIJAVA

Svaka istraga u skladu sa ovim Pravilnikom sprovodiće se na osetljiv i najbrži mogući način. U roku od 7 dana od prijema prijave, AML sektor (ili drugo lice koje je prijavu primilo, kako je opisano u paragrafu 5.3 gore) pružiće povratnu informaciju uzbunjivaču o prijemu prijave i nameravanim vremenskim okvirima za istragu. AML sektor može potvrditi ovu informaciju u pisanom izveštaju ili može organizovati sastanak sa uzbunjivačem. Takav sastanak dokumentovaće će AML sektor. U roku od tri meseca od datuma izveštaja, pružiće se povratna informacija uzbunjivaču o ishodu istrage, pri čemu se osigurava da sadržaj takve povratne informacije ne ugrožava bilo koju akciju koju je kompanija preuzela kao posledicu istrage i / ili bilo koju istragu koju sprovode javna tela na istim činjenicama.

AML sektor (ili drugo lice koje je prijavu primilo, kako je opisano u paragrafu 5.3 gore) preliminarno proverava opravdanost i primarnu utemeljenost prijave, ako je potrebno uz pomoć spoljnog pravnog savetnika koji je obavezan da čuva poverljivost aktivnosti koje obavlja.

Kao deo interne istrage koja se sprovodi, AML sektor (ili drugo lice koje je prijavu primilo, kako je opisano u paragrafu 5.3 gore) može zatražiti dodatne informacije i / ili dokumentaciju od uzbunjivača. Uzbunjivači će, koliko god je to moguće, sarađivati kako bi udovoljili bilo kom razumnom zahtevu za razjašnjenje bilo kojih činjenica i / ili okolnosti, kako bi pružili (dodatne) informacije. Nedostatak informacija ili drugih dokaza, uključujući nevoljnost uzbunjivača da sarađuju u istrazi, može biti razlog da AML sektor (ili drugo lice koje je prijavu primilo, kako je opisano u paragrafu 5.3 gore) odluči da zaključi da prijava nema faktičku osnovu.

AML sektor (ili drugo lice koje je prijavu primilo, kako je naznačeno u tački 5.3 gore) zatim registruje prijavu putem identifikacionog koda / imena, osiguravajući praćenje i pravilno arhiviranje dokumentacije i u kasnijim fazama.

AML sektor (ili drugo lice koje je prijavu primilo, kako je navedeno u stavu 5.3 gore) klasifikuje izveštaje u:

- **Nerelevantne izveštaje**: u ovom slučaju, gde je neophodno, obaveštava se uzbunjivač u skladu sa tim i upućuje se na druge funkcije kompanije (npr. HR, Pravna služba) da se bave pitanjima koja su pokrenuta, gde je to primereno, i zatvara se prijava;

- **Prijave podnete iz loše namere**: prijave se prosleđuje rukovodiocu HR-a kako bi razmotrio da li treba pokrenuti neki disciplinski postupak;

- **Opravdani izveštaji**: ako AML sektor (ili drugo lice koje je prijavu primilo, kako je navedeno u stavu 5.3 gore) smatra da postoji dovoljno dokaza o potencijalno nezakonitom ponašanju koje omogućava pokretanje istrage, započinje se faza istrage.

Faza istrage podrazumeva sprovođenje ciljanih provera prijava, omogućavajući identifikaciju, analizu i procenu elemenata koji potvrđuju pouzdanost prijavljenih činjenica. AML sektor će u ovoj fazi koordinirati sa pravnim odeljenjem i pažljivo razmotriti mogućnost angažovanja eksternih stručnjaka za pomoć u fazi istrage.

AML sektor (ili drugo lice koje je prijavu primilo, kako je navedeno u tački 5.3 gore), u koordinaciji sa pravnim odeljenjem i eksternim stručnjacima, ukoliko su angažovani, može sprovoditi bilo koju aktivnost koja se smatra

adekvatnom, uključujući lično saslušavanje uzbunjivača i bilo koje druge osobe koja može pružiti informacije o prijavljenim činjenicama. Osoba koja je uključena u istragu može biti saslušana ili, na njihov zahtev, će biti saslušana, takođe putem pisane procedure putem prikupljanja pisanih podnesaka i dokumenata.

AML sektor (ili drugo lice koje je prijavu primilo, kako je navedeno u stavu 5.3 gore):

- Mora da obezbedi puno poštovanje zahteva za poverljivost, kako je opisano u Poglavlju 6 ispod;

- Mora da se pobrine da se provera sprovede na brižan, pravičan i nepristrasan način; to podrazumeva da se svaka osoba koja učestvuje u istrazi obavesti - kada se preliminarna istraga završi - o izjavama koje su protiv njih iznete i dokazima koji su prikupljeni protiv njih, i da moraju biti u stanju da pruže svoje protivargumente;

- Može angažovati tehničke savetnike (kao što su eksterni profesionalci ili interni stručnjaci Kompanije) za pitanja koja ne spadaju u njihovu specifičnu nadležnost.

Informacije prikupljene tokom istrage, čak i kada su prikupljene od strane trećih strana, moraju biti tretirane sa najvećom poverljivošću i ograničene na osobe koje su uključene u verifikacione aktivnosti.

5.5 ISHOD ISTRAŽIVANJA

Faza istraživanja može rezultirati:

a. **Negativnim ishodom**, u tom slučaju se prijava odbacuje;

b. **Pozitivnim ishodom**: u tom slučaju AML sektor (ili (ili drugo lice koje je prijavu primilo, kako je opisano u par. 5.3 gore) šalje ishod istrage direktorima društva, kako bi SKS365 mogao preduzeti potrebne protivmere i usvojiti disciplinske sankcije. Posebno, nakon završetka verifikacije, izveštaj će se dostaviti direktorima društva koje:

- sažima tok istraživanja;

- navodi zaključke koje je postiglo i pruža potrebnu dokumentaciju;

- daje preporuke i predlaže mere koje treba preduzeti u vezi s otkrivenim prekršajima, na nivou disciplinskih sankcija i usklađenosti.

Povratne informacije će se dati osobi koja je podnela prijavu nakon zaključenja istrage. Međutim, detalji ishoda istrage ne mogu se deliti s osobom koja je podnela prijavu, u skladu s obavezom poverljivosti na koju je društvo obavezno.

5.6 IZVEŠTAVANJE

AML sektor pruža nove informacije u vezi s primljenim prijavama i statusom bilo koje otvorene istrage:

a) kvartalno - Nadzornom odboru italijanskog ogranka u vezi sa prijavama koje su podnesena od Adresaata unutar italijanskog ogranka; i

b) jednom godišnje - Upravnom odboru društva i osobama koje su zadužene za upravljanje svakim ogrankom.

6. ZAŠTITA I ODGOVORNOST UZBUNJIVAČA

POVERLJIVOST I ZABRANA OSVETNIČKIH I/ILI DISKRIMINATORNIH RADNJI

SKS365 garantuje najveću poverljivost identiteta osobe koja podnosi prijavu, osoba koja su uključene i osoba koje se inače spominju u prijavi, kao i sadržaja prijave i povezane dokumentacije, koristeći, u tu svrhu, kriterijume i metode komunikacije pogodne za zaštitu identiteta i integriteta gorespomenutih lica, kako bi se osiguralo da osoba koja podnosi prijavu ne bude izložena bilo kakvoj vrsti osvete i/ili diskriminacije, izbegavajući u svakom slučaju komunikaciju o podacima sa trećim stranama koje nisu uključene u proces upravljanja prijavom koja je regulirana ovim postupkom.

S izuzetkom slučajeva u kojima se može predvideti krivična ili građanska odgovornost osobe koja podnosi prijavu i slučajeva u kojima anonimnost nije predviđena zakonom, identitet osobe koja podnosi prijavu je zaštićen u bilo kojem kontekstu nakon podnošenja prijave.

Stoga, osim u slučajevima izuzetaka navedenih gore, identitet osobe koja prijavi nepravilnosti se ne može otkriti bez njenog izričitog pristanka, a sve osobe koje primaju ili su uključene u rukovanje prijavom obavezne su štititi poverljivost takvih informacija.

Kršenje obaveze poverljivosti dovodi do disciplinske odgovornosti, bez obzira na druge oblike odgovornosti predviđene zakonom.

Posebno, u okviru bilo kog disciplinskog postupka pokrenutog protiv bilo koje osobe navedene u prijavi, identitet osobe koja prijavi nepravilnosti se može otkriti samo u slučajevima gde postoji izričit pristanak te osobe.

Iste zahteve za poverljivost treba primeniti i na osobe koje su uključene/ navedene u prijavi.

,,***Bona fide" uzbunjivači će biti zaštićeni od bilo koje vrste osvete, diskriminacije ili kažnjavanja, bez ugrožavanja bilo koje druge forme zaštite predviđene zakonom.***

Kao primeri, sledeći postupci smatraju se vidovima osvete:

- prestanak radnog odnosa, suspenzija ili ekvivalentne mere;
- degradiranje sa postojeće pozicije ili sprečavanje napredovanja na više pozicije;
- promena radnih obaveza, radnog mesta, smanjenje plate, promena radnih sati;
- suspenzija obuke ili bilo kakva ograničenja pristupa obuci;
- negativne ocene ili negativne reference;
- usvajanje disciplinskih mera ili drugih sankcija, uključujući novčane kazne;
- pretnje, zlostavljanje ili izopštavanje;
- diskriminacija ili drugi nepovoljni postupci;
- nemogućnost potpisivanja ugovora o radu na neodređeno vreme, gde je radnik imao opravdana očekivanja za takvo potpisivanje;

- Neobnavljanje ili rani prestanak ugovora o radu na određeno vreme;

- Oštećenje, uključujući i štetu po reputaciju ličnosti, naročito na društvenim mrežama, ili ekonomske i finansijske štete, uključujući gubitak ekonomskih prilika i gubitak prihoda;

- Neprikladno uvrštavanje u formalne ili neformalne sektorske ili industrijske sporazume, što može dovesti do toga da osoba ne bude u mogućnosti da pronađe zaposlenje u sektoru ili industriji u budućnosti;

- Rani prekid ili otkazivanje ugovora o snabdevanju roba ili usluga;

- Otkazivanje dozvole ili dozvole za rad;

- Zahtev za psihijatrijskim ili medicinskim pregledom.

Uzbunjivači koji smatraju da su zbog toga pretrpeli odmazdu, ohrabruju se da podnesu novu prijavu u vezi sa osvetom koju su pretrpeli. Takođe, oni mogu da obaveste nadležno nacionalno telo/organ o bilo kojoj vrsti osvete koju smatraju da su pretrpeli (videti pasus 7 ispod).

Radnje preduzete u suprotnosti sa zabranom iznad su ništavne. Uzbunjivači koji su otpušteni zbog otkrivanja nepravilnosti imaju pravo na povratak na svoja radna mesta i/ili da dobiju zaštitu koju daje lokalni zakon.

***

Pored zaštite koja se pruža uzbunjivaču, gorenavedene zaštitne mere će se takođe pružiti osobama koje se nazivaju "Druge zaštićene osobe":

(a) posrednicima (tj. onima koji pomažu uzbunjivaču u procesu prijavljivanja, deluju unutar istog radnog odnosa i čija pomoć mora biti poverljiva);

(b) osobama koje su u istom radnom odnosu kao i uzbunjivač i koje su s njim/ njom u stabilnom emocionalnom ili porodičnom odnosu u četvrtom stepenu srodstva;

(c) saradnicima uzbunjivača koji su u istom radnom odnosu kao i on/ona i koji s njim/ njom imaju redovan i trenutni odnos;

(d) subjektima koje poseduje uzbunjivač, kao i subjektima koji deluju u istom radnom odnosu kao i uzbunjivač.

ODGOVORNOST UZBUNJIVAČA

Kao što je već najavljeno, disciplinske sankcije mogu se primeniti na uzbunjivača koji podnosi prijave s namerom ili grubom nepažnjom, u skladu s lokalno primenjivim radno-pravnim propisima. Kaznena i građanska odgovornost uzbunjivača ostaje netaknuta.

Bilo koje oblike zloupotrebe unutrašnjeg uzbunjivanja, kao što su očito oportunističke, klevetničke ili uvredljive prijave i/ili napravljene samo radi nanošenja štete prijavljenoj osobi ili drugim osobama, kao i bilo koja druga hipoteza nepravilne upotrebe ili namerne instrumentalizacije kanala za unutrašnje uzbunjivanje, takođe podležu disciplinskim sankcijama i/ili odgovornosti u skladu sa primenjivim zakonom.

7. EKSTERNA PRIJAVA

U slučaju da je uzbunjivač:

- već podneo internu prijavu u skladu sa gorenavedenim poglavljem 5 i da nije obrađena u okviru roka utvrđenog u istom poglavlju; ili

- postoje opravdani razlozi da veruje da ako bi podneo internu prijavu, prijava ne bi bila efikasno obrađena ili da bi ista prijava mogla da dovede do rizika od osvete;

- postoje opravdani razlozi da veruje da bi prekršaj mogao da predstavlja očiglednu ili neposrednu opasnost po javni interes;

uzbunjivač može da podnese spoljnu prijavu („**spoljna prijava**") nadležnom nacionalnom telu/organu u skladu sa lokalno primenljivim zakonom. Ovo se takođe smatra zaštićenom prijavom u smislu ovog Pravilnika.

Nadležna nacionalna tela koja deluju u okviru EU I koja su nadležna za pitanja koja su tema ovog pravilnika su:

- ANAC – Autorità Nazionale Anticorruzione za Italiju
- BAK - Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung za Austriju
- Commissioner of Revenue (CfR), Financial Intelligence Analysis Unit (FIAU), Malta Financial Services Authority (MFSA), Commissioner for Voluntary Organisation (CVO), Permanent Commission Against Corruption and the Ombudsman, u zavisnosti od vrste prijavljenih činjenica, za Maltu.

Prijavu je moguće podneti u pisanom obliku, putem IT platformi ili drugih sredstava koje je implementiralo nacionalno telo/organ, ili u usmenom obliku, putem telefonske linije i/ili sistema za snimanje glasovne poruke implementiranog od strane nacionalnog tela/organizacije. Nadležno nacionalno telo/organizacija će garantovati najveću moguću tajnost identiteta uzbunjivača, osobe koja je uključena u prijavu i osobe koja je inače pomenuta u prijavi, kao i sadržaja prijave i pripadajuće dokumentacije. Za detaljnije propise, molimo da se upoznate sa relevantnim lokalnim propisima.

8. PRAĆENJE TRAGA

Dokumentacija korišćena u obavljanju aktivnosti (uključujući i nepovezane prijave) biće čuvana od strane AML sektora (ili drugog lica koje je prijavu primilo, kako je navedeno u tački 5.3 gore) u posebnom arhivu.

Prijave i pripadajuća dokumentacija čuvaće se onoliko dugo koliko je potrebno za obradu prijave, a u svakom slučaju ne duže od pet godina od datuma saopštavanja konačnih rezultata postupka prijavljivanja, u skladu sa obavezama o poverljivosti propisanim relevantnim važećim zakonima.

Gde se za prijavljivanje koristi snimljeni telefonski poziv ili drugi snimljeni sistem za glasovne poruke, uz saglasnost osobe koja prijavljuje, AML sector (ili drugo lice koje je prijavu primilo, kako je navedeno u tački 5.3 gore) može čuvati prijavu na sledeće načine:

a) pravljenjem snimka razgovora u trajnoj i formi koja se može ponoviti; ili

b) putem potpuno i tačno sastavljenog prepisa razgovora koji su pripremili članovi osoblja odgovorni za rukovanje prijavom (osoba koja je prijavila nepravilnost može potvrditi, ispraviti ili potvrditi sadržaj transkripta svojim potpisom).

Kada se prijava, na zahtev osobe koja je prijavila nepravilnost, iznosi usmeno u sastanku licem u lice sa osobljem zaduženim za rukovođenje prijavom, ona će, uz saglasnost osobe koja prijavljuje, biti dokumentovana od strane osoblja zaduženog za rukovođenje, snimanjem na uređaju pogodnom za skladištenje i slušanje ili zapisnikom. U slučaju zapisnika, osoba koja prijavljuje može potvrditi, ispraviti i potvrditi zapisnik sastanka svojim potpisom.

U arhivi prijava, lični podaci koji su očigledno nebitni za rukovanje određenom prijavom se neće prikupljati ili, ako su slučajno prikupljeni, biće obrisani bez odlaganja.

***

Lični podaci - uključujući posebne kategorije podataka i sudske podatke - otkriveni kao deo prijave biće obrađeni u skladu sa odredbama Evropske regulative 2016/679 o zaštiti ličnih podataka ("GDPR") i u skladu sa relevantnim pravilnicima kompanije.

9. DISCIPLINSKE MERE

Nepoštovanje principa i pravila sadržanih u ovom Pravilniku podrazumeva primenu disciplinskih mera koje je usvojila kompanija.