DESCRIZIONE / DESCRIPTION

PROCEDURE FOR REPORTING VIOLATIONS CY4GATE GROUP

SOMMARIO PAGINE / Page Summary		**Nr. Pagine**
Documento Principale / Main Document	**Frontespizio □ Indice /** Front Page + Indices	**III**
	Documento-Document	**6**
	Total	**9**

Allegati / Annex	**Titolo /** Title	**Pages**
1	INFORMATIVA PRIVACY SEGNALAZIONE DI VIOLAZIONI	4
2	VIOLAZIONI SEGNALABILI	2
	Total	
Pagine Totali / Total Pages		**15**

Cod	Rev.	Prepared by	Verified by	Approved by	Data
PR 08.6D	02	LEGALE office CY4GATE	DIR QUALITA’	DIR	02/08/23

STORIA DELLE REVISIONI E CAMBIAMENTI REVISIONS AND CHANGES HISTORY			
REVISIONE REVISION	**DATA** DATE	**AUTORE** AUTHOR	**CAMBIAMENTO** CHANGE
00	**02/08/23**	**UL**	**FIRST ISSUE**
01	**15/10/24**	**UL**	**INCLUSION OF ANONYMOUS REPORTING OPTION**
02	**17/02/25**	**UL**	**UPDATE OF PARAGRAPHS 6 AND 7**
03	**19/05/25**	**EST**	**INTEGRATION OF XTN COGNITIVE SECURITY S.R.L. INTO THE GROUP PROCEDURE**

Summary

1. PURPOSE AND SCOPE

As the parent company, CY4Gate requires that all Group companies and employees, including managers and executives, always act in accordance with its core values and Business Principles. This means acting responsibly, with integrity, and in compliance with internal policies and procedures as well as applicable laws and regulations.

CY4Gate promotes a culture of openness and transparency and encourages all stakeholders to report any instances of unlawful conduct, violations of core values and/or Business Principles, and/or breaches of Group policies. Such reports are essential to help protect personnel, the company and its values, other stakeholders, and society as a whole. Aware of the difficulty of coming forward, CY4Gate is committed to ensuring that this can be done easily and safely.

This procedure governs the whistleblowing reporting system pursuant to Legislative Decree No. 24/2023 (the "Decree"), with reference to the companies within the CY4Gate Group.

2. AFFECTED COMPANIES AND STAKEHOLDERS

This procedure applies to CY4Gate S.p.A., as well as to all companies controlled by it and meeting the requirements set forth in Article 3 of the Decree (hereinafter individually referred to as the "Company").

The procedure is addressed to all stakeholders who wish to make reports.

The term **Stakeholder** refers to any person internal or external to the CY4Gate Group (or related thereto) and may include:

- company employees, including managers and executives, interns/trainees;
- members of the Board of Directors, members of committees or bodies with control and supervisory functions;
- workers, including agency or subcontracted personnel, consultants, freelancers, and self-employed workers;
- former company employees and workers previously employed by or through the CY4Gate Group;
- candidates and job seekers, personnel in their probationary period;
- clients, suppliers and their respective subcontractors, and their personnel.

3. DEFINITIONS

For better understanding and usability of this document, the following definitions are reported as provided in Article 2 of Legislative Decree no. 24/2023:

a) **“violations”**: unlawful conduct, acts, omissions, and all behaviors described in Article 2, point a) of Legislative Decree 24/23, which harm the public interest or the integrity of the public administration or the private entity;

b) **“information on violations”**: information, including well-founded suspicions, regarding violations committed or that, based on concrete elements, could be committed within the organization with

which the reporting person or the one who files a complaint to the judicial or auditing authority maintains a legal relationship pursuant to Article 3, paragraphs 1 or 2, as well as elements concerning conduct aimed at concealing such violations;
c) **"report" or "reporting"**: the written or oral communication of information regarding violations;
d) **"internal report"**: the written or oral communication of information on violations submitted through the internal reporting channel referred to in Article 4;
e) **"external report"**: the written or oral communication of information on violations submitted through the external reporting channel referred to in Article 7;
f) **"public disclosure" or "publicly disclose"**: making information on violations public through the press, electronic means, or by any means of dissemination capable of reaching a large number of people;
g) **"reporting person"**: the natural person who makes the report or the public disclosure of information on violations acquired within their work context;
h) **"facilitator"**: a natural person who assists a reporting person in the reporting process, operating within the same work context and whose assistance must be kept confidential;
i) **"work context"**: the work or professional activities, past or present, performed within the relationships referred to in Article 3, paragraphs 3 or 4, through which, regardless of the nature of such activities, a person acquires information on violations and within which they may risk retaliation in case of reporting, public disclosure, or complaint to the judicial or auditing authority;
j) **"involved person"**: the natural or legal person mentioned in the internal or external report or in the public disclosure as the person to whom the violation is attributed or as a person otherwise involved in the reported or publicly disclosed violation;
k) **"retaliation"**: any behavior, act, or omission, even only attempted or threatened, carried out because of the report, complaint to the judicial or auditing authority, or public disclosure, which causes or may cause unjust harm, directly or indirectly, to the reporting person or to the person who filed the complaint;
l) **"follow-up"**: the action taken by the entity entrusted with managing the reporting channel to assess the existence of the reported facts, the outcome of the investigations, and any measures adopted;
m) **"feedback"**: communication to the reporting person of information regarding the follow-up given or intended to be given to the report;
n) **"public sector entities"**: public administrations as per Article 1, paragraph 2, of Legislative Decree 30 March 2001, no. 165, independent administrative authorities for guarantee, supervision or regulation, public economic entities, public law bodies as per Article 3, paragraph 1, letter d), of Legislative Decree 18 April 2016, no. 50, public service concessionaires, publicly controlled companies, and in-house companies, as respectively defined by Article 2, paragraph 1, letters m) and o), of Legislative Decree 19 August 2016, no. 175, even if listed;
o) **"private sector entities"**: entities other than those falling within the definition of public sector entities, as specified in point o) of Article 2 of Legislative Decree 24/23.

4. SUBJECT OF THE REPORT

It is possible to use the internal reporting channels provided by the CY4Gate Group in accordance

with this Procedure to report situations or incidents for which there is reasonable suspicion, or evidence, of unlawful behavior and/or a violation of the Group's Policies, of which the reporting person has become aware within their work context inside the CY4Gate Group or in relation to it ("Violation")

Regarding the reportable violations, please refer to Annex 2.

The reporter must assign the reported Violation to one of the following categories:

- Bribery and corruption
- Antitrust issues
- Data protection and IT security issues
- Fraud, embezzlement, misappropriation, theft
- Human Resources (HR)
- Fair play and conflict of interest
- Environment, health, and safety
- Violation of diversity, equity, and inclusion principles
- Other

The reporter should include in the report, as specifically as possible, the following information:

- Whether they work for a company within the CY4Gate Group, and if so, which company;
- What happened;
- Who is involved: who did what, any victims, accused persons, and/or witnesses, including potential ones;
- Who is aware of the incident;
- When it happened;
- Where it happened;
- How it happened: which means or methods were used;
- If known, why it happened.

Where possible, it is advisable to attach to the report any evidence, documents, references, photos, or other relevant information that can help the report handler assess it more efficiently. If such evidence is not available, any references or suggestions on how to obtain it will still be useful.

5. LIMITATIONS

Reports must be made in good faith. Reports are considered made in bad faith when the reporter has transmitted untrue accusations with intent or gross negligence to create unjust benefits for themselves or others and/or to unfairly cause harm to the Company or one of its employees (including executives and managers).

The Company reserves the right to consider reports made in bad faith as a serious violation—not only of this procedure but also of its ethical principles—and, consequently, to take disciplinary measures against the reporter.

Reports cannot, under any circumstances, concern questions or issues related to the reporter's working conditions that do not constitute a violation, including matters related to personal grievances, disputes, performance evaluations, remuneration, working hours, or the work environment.

6. REPORTING CHANNELS

The CY4Gate Group has activated two internal channels for the submission and management of reports that guarantee the confidentiality of the identities of the reporting person, the facilitator, the person involved, or any other subjects mentioned in the report, as well as the content of the report and the related documentation.

The reporting channels, together with the methods suitable to ensure the confidentiality of the information, are described below:

a. Reporting via web platform

The reporter accesses the Integrity Line webpage, reachable through a link on the company's website or directly at https://cy4gategroup.integrityline.com/, inserts a message (in Italian or English) and receives a unique identification number for the report. The system stores a copy of the message in a digital space accessible by the members of the Supervisory Body, who will manage it in accordance with these guidelines.
The reporter also has the possibility to record a voice message (the voice will be disguised), upload documents, or take a photo to support the report.
The person responsible for managing the report will provide an initial response to the reporter within the timelines specified below.
The reporter can access the web platform again and, using the unique identification number, consult the manager's response and reply even at a later time.
Anonymous reports are possible.

b. Reporting in paper form

The reporter submits the communication, drafted in paper form according to the principles contained in these guidelines, by depositing it in the dedicated mailbox located at the company's headquarters, marked with the wording "Internal Reports."
Reports must be addressed to the Supervisory Body through the following channels, depending on the company involved:

CY4gate S.p.A.
• Verbal communication to the Supervisory Body; • email: odv231@cy4gate.com (also available in the company directory); • postal mail: via Coponia 8, 00131 Roma, Italia.
RCS S.p.A.
• Verbal communication to the Supervisory Body; • email: odv@rcslab.it (also available in the company directory);; • postal mail: via Caldera 21, 20153 Milano, Italia.
Cognitive Security s.r.l
• Verbal communication to the Supervisory Body; • email: odv@xtn-lab.com(also available in the company directory);;

- postal mail : Piazza Aldo Moro 10, 35129 Padova, Italia.

The paper documentation is collected by the members of the Supervisory Body and managed in accordance with these guidelines. Anonymous reports are permitted.

c. External channel at ANAC

The Decree provides that entities in both the public and private sectors have the possibility to submit a report through an external channel. The National Anti-Corruption Authority (ANAC) is responsible for managing this channel, which guarantees, including through the use of encryption tools, the confidentiality of the identity of the whistleblower, the person involved, and the person mentioned in the report, as well as the content of the report and the related documentation..

Conditions for using the ANAC channel:

1. *If the mandatory internal channel*

- is not active

- is active but does not comply with the requirements set by the legislator regarding the subjects and methods of submitting reports

2. *The person has already made an internal report but no action was taken*
3. *The reporting person has reasonable grounds to believe that if they made an internal report*

- no effective follow-up would be given
- it could expose them to the risk of retaliation

4. *The reporting person has reasonable grounds to believe that the violation may pose an imminent or obvious danger to the public interest.*

The report can be submitted by filling out a digital form available on the homepage of the ANAC website at https://whistleblowing.anticorruzione.it/, by clicking on the “Submit a report” icon.

Reports submitted anonymously are treated as ordinary reports and cannot be equated with whistleblowing reports.

7. HANDLING OF REPORTS

Le **Reports are collected in digital and/or physical spaces accessible to the members of the Supervisory Body, and are categorized as follows:**

- Reports concerning unlawful conduct relevant under the national and EU legislation referenced in the Annex of the Decree;
- Reports concerning violations of the Organization, Management and Control Model adopted by the company pursuant to Legislative Decree 231/2001, as well as unlawful conduct relevant under the same Legislative Decree.

The report handler provides the whistleblower with an initial response within a maximum of seven (7) days from receipt of the initial message. The response confirms whether or not the reported issue constitutes a violation: if not, the whistleblower will receive appropriate explanations as well

as guidance on the appropriate reporting channel (e.g., through the HR function); if positive, the whistleblower will be informed that the report has been taken in charge and, if necessary, additional information will be requested to evaluate the case.
The report handler ensures that all reports will be managed promptly and in accordance with applicable laws as follows:

- Upon taking charge, an internal investigation is initiated to collect information on the validity of the report;
- Once the validity of the report is verified, the report handler identifies the corrective actions that will be necessary (e.g., communication to the competent company function, which may be followed by disciplinary measures, and/or communication to the competent Authorities);
- Within the final deadline of three (3) months from the opening of the report, the report handler provides the whistleblower with feedback on the validity of the report and any corrective actions taken, within the limits allowed by applicable laws regarding confidentiality, also concerning the rights of the accused person. If, after this deadline, investigations are still ongoing, the report handler is still required to provide the whistleblower with an update on the investigation status.

Conclusion and Measures
After the conclusion of the investigation, timely and appropriate corrective measures will be taken, if and where deemed appropriate by the management of the involved Company and the HR function.
The corrective measures adopted in case of a confirmed violation may range from written warnings, coaching sessions, and/or apologies to the persons involved in the violation, to suspension or termination of the contract or employment relationship with the perpetrators of the violation, up to reporting to the competent authorities and/or any other measure relevant to the specific case.

8. CONFIDENTIALITY AND PROHIBITION OF RETALIATION

All information concerning a report, with particular regard to the identity of the whistleblower, is handled by the report manager with the highest degree of confidentiality and is shared only with the minimum number of people necessary for its management.
Under no circumstances may the Company apply any form of retaliation or threat against a whistleblower acting in good faith as a result of the report, such as, by way of example, dismissal, denial of promotion, demotion, reduction of salary, discrimination, or non-renewal of the employment contract.

9. PROTECTION OF THE ACCUSED PERSON

The accused person in a report is informed of the accusation, with due regard to the above-mentioned principle of confidentiality, within a reasonable time frame, also taking into account any need to prevent the concealment or destruction of evidence of conduct in violation of the law and/or company policies.

ANNEX 1- PRIVACY NOTICE FOR REPORTING VIOLATIONS

Who we are and what we do with your personal data?

Cy4Gate S.p.A., via Coponia, 8, Roma,

e

RCS S.p.A., Via Caldera, 21, Milano,

e

XTN Cognitive Security s.r.l, Piazza Aldo Moro 10, Padova

As data controllers, respectively, for the reports addressed to each company (hereinafter also the Controller), they are committed to maintaining the confidentiality of your personal data and ensuring the necessary protection against any event that may put them at risk of breach.
To this end, the Controller implements policies and practices regarding the collection and use of personal data and the exercise of the rights granted to you under applicable law. The Controller takes care to update the policies and practices adopted for the protection of personal data whenever necessary, and in any case in the event of regulatory or organizational changes that may affect the processing of your personal data.
The Controller has appointed a Data Protection Officer (DPO), whom you can contact if you have any questions regarding the policies and practices adopted.
You can contact the DPO of the respective company at the following addresses and contacts:

- For inquiries addressed to CY4Gate S.p.A.: dpo@cy4gate.com
- For inquiries addressed to RCS S.p.A.: dpo@rcslab.it
- For inquiries addressed to XTN Cognitive Security s.r.l : dpo@xtn-lab.com

If you choose to use the internal online channel, the Company uses an external Data Processing Manager as the operator of the Integrity Line:

EQS Group S.r.l.
Corso Vercelli, 40
20125 MILANO

How and why does the Controller collect and process your personal data?

The Controller collects and/or receives information about you, such as:

- With reference to the processing related to the disclosure of your identity, as well as any other information from which such identity can be inferred—directly or indirectly—to persons other than those authorized to receive or follow up on the reports (as provided and indicated in the Whistleblowing Procedure), this is based on your expressed consent in the forms and ways indicated in the Whistleblowing Procedure.
- In the event that you make a Report, your personal data is collected directly from you using any of the specific channels that the Controller has implemented. It is possible that during the investigation carried out according to the Whistleblowing Procedure, the Controller may collect data concerning you from third parties involved in such process.
- If you are an accused person, a witness, or a third party involved in the investigation and management process, your personal data may be collected directly from you, the person making the Report, or any of the aforementioned parties.
- Depending on the nature of the reports or investigations to be carried out, the Controller may process all or some of the following categories of personal data: identification and contact data, data relating to personal characteristics, academic and professional data, employment data, data relating to company information or social circumstances, economic, financial or insurance data, property or insurance transactions, special categories of data (e.g., health data, political opinions), judicial data (e.g., criminal records, data relating to offenses, etc.), and in general all personal data that may be included in a Report.

Your personal data will be processed for the purposes described below.

Who are the recipients?

External data processors and any further controllers:

- Supervisory Body in case the report concerns a possible relevant violation pursuant to Legislative Decree 231/01, as expressly authorized to process personal data pursuant to Articles 29 and 32 of the GDPR and Article 2 quaterdecies of Legislative Decree 196/2003;
- Report manager during the investigation and verification phase regarding the validity of the Report, in full compliance with the right to confidentiality as provided by the Procedure, as expressly authorized to process personal data pursuant to Articles 29 and 32 of the GDPR and Article 2 quaterdecies of Legislative Decree 196/2003;
- With your consent, where necessary for investigative purposes, personal data may be communicated to other CY4Gate group structures and/or functions and/or external consultants;
- For technical activities related to platform management only, your data may also be processed by third parties who, as Data Processors under Article 28 GDPR, act under the direction and control of the Controller.

The management of the Report and consequent, including regulatory, obligations

Personal data will be processed for:	The processing is based on:
Managing the received report and carrying out the necessary investigations related to the reported matter;;	Legal obligation, with specific reference to the provisions contained in Legislative Decree No. 24 of March 10, 2024 (“Implementation of Directive (EU) 2019/1937 of the European Parliament and of the Council of October 23, 2019, on the protection of persons who report breaches of Union law and provisions concerning the protection of persons who report breaches of national regulations”);
Ensuring protection against retaliation towards any individual involved in related activities, in particular whistleblowers (except for the exceptions indicated in the Whistleblowing Procedure);	Legal obligation.
Adoption of corrective measures or any other action related to specific inappropriate/unlawful behavior (e.g., reporting to competent authorities);	Legal obligation.
Fulfilling legal and regulatory obligations to which the Controller is subject;	Legal obligation.
For security activities — detection and notification of data breaches.	Legal obligation.

Transfer of data outside the European Union

No. Personal data will be processed within the European Economic Area.

Cybersecurity activities related to the prevention of data breaches

Purpose	Legal basis
Implementation of procedures for detection	Compliance with legal obligations (detection

and notification of personal data breaches (data breach).	and notification of data breach events).

How, where, and for how long are your data stored?

HOW

Il Data processing is carried out using paper documents or IT procedures by authorized internal or external personnel. These individuals have access to your personal data only to the extent necessary to perform the processing activities related to you. Your data, especially those belonging to special categories, are processed separately from others, including by means of pseudonymization or aggregation methods that do not allow easy and immediate identification of you.
The Data Controller periodically reviews the tools through which your data (including special categories of data — such as health status, ethnic origin, political opinions, etc.) are processed and the security measures in place, updating them as needed. The Controller also ensures, including through authorized data processors, that no unnecessary personal data are collected, processed, archived, or stored, or that the purposes for processing have been fulfilled. It verifies that the data are kept with integrity and authenticity guarantees and are used only for the actual processing purposes. These periodic checks allow the Controller to assess the strict relevance, non-excessiveness, and indispensability of the data in relation to the ongoing or terminated relationship, service, or assignment.
The Controller implements adequate technical measures to guarantee data protection and confidentiality. For reports made through the web platform, your data will be stored in a specifically protected and encrypted database using the most advanced technology.

Where

Data are stored in paper, IT, and electronic archives located within the European Economic Area, with specific security measures ensured.

For how long

Personal data collected and processed in relation to a report are retained for a maximum period of five (5) years from the date of receipt of the report. After this period, personal data will be permanently deleted or anonymized, except where retention is necessary for legal defense purposes. In any case, one (1) year after your report, personal data related to the report will be deleted from the platform.
The Company recommends that you do not submit or communicate personal data that are manifestly unnecessary for the processing of a report; if such data are incidentally collected, the Company will delete them immediately.

What are your rights?

You have rights that allow you to maintain control over your data at all times.

In particular, at any time and free of charge, without specific formalities, you may request to:

- **Access:** obtain confirmation of the processing carried out by the Controller, access your personal data, and know their origin (if not collected directly from you), the purposes and objectives of the processing, the recipients of the data, the retention period, or the criteria to determine it;
- **Rectification:** update or correct your personal data to ensure accuracy and completeness;

- **Erasure:** delete your personal data from databases and archives (including backups), for example, if no longer necessary for the processing purposes or if the processing is unlawful, provided the legal conditions apply; and in any case if the processing is not justified by another legitimate reason;
- **Restriction of processing:** limit the processing of your data in certain circumstances, for example, if you contest its accuracy, for the time needed by the Controller to verify accuracy. You must be informed within a reasonable time when the restriction period ends or the cause for restriction ceases, and thus the restriction is lifted;
- **Data portability:** obtain a copy of your personal data in a commonly used electronic format when the processing is based on a contract, consent, and performed with automated tools, to transmit it to another Controller.

The Data Controller must act without undue delay and, in any case, no later than one month from the receipt of your request. This period may be extended by two further months if necessary, taking into account the complexity and number of requests received. In such cases, the Controller will inform you within one month of receiving your request and provide the reasons for the extension.

For any further information and to submit your request, please write to the following addresses:

- For inquiries addressed to CY4Gate S.p.A.: cy4gate@pec.it
- For inquiries addressed to RCS S.p.A.: etm@pec.rcslab.com
- For inquiries addressed to XTN Cognitive Security s.r.l : ikstn@pec.it

How and when can you object to the processing of your personal data?

For reasons related to your particular situation, you may object at any time to the processing of your personal data if it is based on legitimate interests, by sending your request to the following addresses:

- For inquiries addressed to CY4Gate S.p.A.: cy4gate@pec.it
- For inquiries addressed to RCS S.p.A.: etm@pec.rcslab.com
- For inquiries addressed to XTN Cognitive Security s.r.l : ikstn@pec.it

You have the right to request the deletion of your personal data if there is no overriding legitimate reason for retaining it compared to the reason that gave rise to your request..

To whom can you submit a complaint?

Without prejudice to any other administrative or judicial action, you may submit a complaint to the Data Protection Authority, unless you reside or carry out your work activities in another EU Member State. In that case, or if the violation of data protection regulations occurs in another EU country, the competent supervisory authority established there will be responsible for receiving and handling the complaint.

ANNEX 2 REPORTABLE VIOLATIONS

Legislative Decree No. 24/2023 establishes that information regarding violations, including well-founded suspicions, of national and European Union laws that harm the public interest or the integrity of the public administration or private entity committed within the organization of the entity with which the whistleblower or complainant has a qualified legal relationship as defined by the legislator, can be the subject of reporting, public disclosure, or complaint.
Information about violations may also concern potential violations not yet committed, which the whistleblower reasonably believes may occur based on concrete evidence. Such evidence may also include irregularities and anomalies (indicative signs) that the whistleblower believes could lead to one of the violations foreseen by the decree.

Examples of reportable (alleged or proven) violations concerning serious incidents related to:

- Core values, business principles, policies, or procedures of the CY4Gate Group;
- Crimes;
- Competition and antitrust laws;
- Discrimination, racism, intimidation;
- Sexual harassment;
- Other human rights violations (e.g., modern slavery/forced labor, child labor);
- Health and safety matters and environmental issues;
- Fraud or misappropriation of company assets;
- Disclosure of confidential information, including personal data;
- Conflicts of interest;
- Violations of the Organizational, Management, and Control Model adopted pursuant to Legislative Decree 231/2001;
- Failure to comply with obligations imposed by laws or regulations (including improper financial and accounting practices), including any violation of European Union law.

Specifically, violations of European Union law concern the following areas:

- Public procurement;
- Financial services, products and markets, and prevention of money laundering and terrorist financing;
- Product safety and compliance;
- Transport safety;
- Environmental protection;
- Radioprotection and nuclear safety;
- Food and feed safety, animal health and welfare;
- Public health;
- Consumer protection;
- Protection of privacy and personal data and security of networks and information systems;
- Violations harming the financial interests of the Union pursuant to Article 325 of the Treaty on the Functioning of the European Union (TFEU), as further specified in relevant Union measures;
- Violations affecting the internal market pursuant to Article 26(2) of the TFEU, including violations of EU rules on competition and State aid, as well as violations related to the internal market concerning acts that violate rules on corporate taxation or agreements aimed at obtaining a tax benefit that frustrates the purpose of the applicable corporate tax law.

D.lgs. n. 24/2023 art. 1 c. 2
WHAT CANNOT BE SUBJECT TO REPORTING, PUBLIC DISCLOSURE, OR COMPLAINT

- Disputes, claims, or requests related to personal interests of the whistleblower or the person who has filed a complaint with the judicial authority that relate exclusively to their individual employment or public employment relationships, or to their employment relationships with their hierarchical superiors.
- Reports of violations already mandatorily regulated by European Union or national acts indicated in Part II of the annex to the decree or by national acts implementing the European Union acts indicated in Part II of the annex to Directive (EU) 2019/1937, even if not indicated in Part II of the annex to the decree.
- Reports of violations concerning national security, as well as public procurement related to defense or national security matters, unless such matters fall within the relevant derived European Union law.

.