



Whistleblowing procedure

Language versions

SUMMARY OF THE VERSIONS

English Version	2
Version Française.....	25
Deutsche Version	49
Versione Italiana	73
Nederlandse Versie	97
Slovenska Verzija	121
Svensk Version	144
中文版	167



Whistleblowing procedure

December 2025_V1

Summary

I.Introduction	3
1. Purpose of the internal whistleblowing system	3
2. Reminder of the legal framework	3
3. Scope.....	3
II.The collection of ethical alerts	4
1. Conditions for the admissibility of an ethical alert	4
Who can file a report?	4
How can you benefit from whistleblower status and the associated legal protection?	4
What facts can be reported?	5
2. How to submit a report.....	6
3. Content of the report.....	7
4. Anonymous reports	7
5. External channels	7
III.Handling of internal ethical alerts.....	7
1. Acknowledgment of receipt of the report	7
2. Review of the admissibility of the report.....	7
3. Conducting the internal investigation	8
4. Decision-making and closure of the investigation.....	9
IV.Protection and guarantees offered.....	10
1. General principles	10
2. Information	10
3. Protection in criminal, civil, and social matters	10
4. Limited data retention period	11
5. Confidentiality and security	11
6. Protection of personal data	12
V.Reporting.....	12
VI.Updating the procedure.....	12
Appendix 1: Summary	13
Appendix 2: List of countries with local whistleblowing procedure	14
Appendix 3: Illustrations of behaviors or misconducts covered by the whistleblowing procedure.....	15
Appendix 4: Privacy Policy.....	19

I. Introduction

1. Purpose of the internal whistleblowing system

As part of the Rexel Group's Ethics & Compliance policy, as described in particular in its Ethics Guide, its Responsible Supplier Charter, and its Anti-Corruption Code of Conduct, the Rexel Group has established an internal whistleblowing system..

The Rexel Group's internal whistleblowing system allows any employee, as well as third parties with whom the Rexel Group has a relationship, to report situations that violate the law, the Rexel Group's Ethics Guide, or its Anti-Corruption Code of Conduct.

The purpose of this procedure is to describe the process for collecting and handling ethical alerts within the Rexel Group.

A summary of the procedure is attached to **Appendix 1**.

2. Reminder of the legal framework

As the holding company of the Rexel Group is incorporated in France, the procedure was established in accordance with the following French laws:

- The Sapin II Law of December 9, 2016, on transparency, anti-corruption, and economic modernization;
- The "duty of vigilance" law of March 27, 2017, relating to the duty of vigilance of parent companies and contracting companies;
- The "Waserman" Law of March 21, 2022, aimed at improving the protection of whistleblowers, and its implementing decree of October 3, 2022.

The procedure is also based on a number of publications by the French Anti-Corruption Agency (AFA) and the French Data Protection Authority (CNIL):

- The AFA's recommendations;
- The practical guide "Internal Anti-Corruption Investigations" published in March 2023 by the AFA and the French Financial Prosecutor's Office;
- The CNIL's "professional alerts" reference document, initially published in 2019 and updated in 2023.

More generally, the collection and processing of reports is carried out in accordance with applicable laws and regulations, and this procedure may be updated as necessary to reflect legislative developments and best practices.

If a local law or regulation offers more protective rules for whistleblowers than this procedure, the local provisions shall prevail. However, where this procedure provides greater protective guarantees, the Rexel Group will apply them voluntarily to the extent permitted by applicable law.

3. Scope

This procedure is intended to be implemented in all Rexel Group entities. It will be amended, as required, to reflect any changes in laws and regulations.

This procedure is supplemented in certain countries within the Rexel group by local procedures. These specify the applicable legal requirements and, as the case may be, the channels available locally (see Appendix 2).

The author of a report can therefore choose the reporting channel of their choice (group or local). The applicable procedure will then be that corresponding to the chosen channel. Depending on the nature and severity of the reported behavior or misconducts, an alert made via the local channel may be forwarded to the group and vice versa.

This procedure applies to all Rexel Group employees (regardless of their role, position, or department) and third parties with whom the Rexel Group has a relationship. It covers the collection and processing of internal alerts by the Rexel Group and, more specifically:

- Their submission;
- Their receipt;
- The assessment of their admissibility;
- The main internal investigation steps
- The closure of the case.

II. The collection of ethical alerts

1. Conditions for the admissibility of an ethical alert

Who can file a report?

The Rexel Group's internal alert system is open to the following persons:

- Rexel Group employees (permanent, fixed-term, apprentices, interns)
- External or temporary employees (temporary workers, consultants, etc.)
- Job applicants
- Former employees
- Shareholders, partners, and holders of voting rights at the general meeting
- Members of the administrative, executive committee , or supervisory bodies
- Any third-party employees with whom the Rexel Group has a relationship (e.g., customers, suppliers, service providers, etc.).

The internal whistleblowing system is open to all Rexel Group entities and is available in the Group's main languages: English, German, Chinese, French, Italian, Dutch, Swedish, and Slovenian.

How can you benefit from whistleblower status and the associated legal protection?

To be considered a whistleblower and benefit from the protection provided by law, you must meet the legal definition of a whistleblower, namely by fulfilling all the following criteria, unless otherwise provided by applicable local law:

- Be a natural person;
- Not receive any direct financial compensation for the report;
- Act in good faith;

- If the reported facts were obtained outside of a professional context, have personal knowledge of the reported facts.

What facts can be reported?

The Rexel Group's internal whistleblowing system allows reports to be made on facts that may constitute the following categories of behavior or misconduct:

- A crime or offense
- A threat to or harm to the public interest
- A violation, or attempted concealment of a violation of national, European, or international laws and regulations
- A breach of, or situation contrary to, the Rexel Group's Ethics Guide or Anti-Corruption Code of Conduct
- Serious risks related to the Rexel Group's activities that could harm human rights, fundamental freedoms, people's health and safety, or the environment

Examples of behaviors or misconducts to be reported may include:

- Corruption, including any violation of the Anti-Corruption Code of Conduct
- Harassment (psychological or sexual)
- Discrimination
- Health, hygiene, or safety (e.g. risk to physical or mental integrity)
- Human rights (other than discrimination, privacy and harassment)
- Conflict of interest
- Anti-competitive practices
- Environment (e.g. pollution, management of waste)
- Tax fraud
- Financial or accounting fraud
- Insider trading
- Fictitious jobs
- Personal data/IT security

Appendix 3 illustrates some of these types of behaviors or misconducts.

Reports relating to categories not listed above do not fall within the scope of this procedure. Similarly, facts, information, or documents, regardless of their form or medium, whose disclosure is prohibited by provisions relating to national defense secrecy, medical secrecy, secrecy of judicial deliberations, secrecy of judicial investigations or inquiries, or attorney-client privilege are excluded from this procedure. Where applicable, the author of the report will be informed and redirected to the persons competent to deal with the reported facts.

2. How to submit a report

The author of a report has several channels for submitting alerts:

- The online reporting platform accessible at: <https://www.rexel.com/en/rexel-group-ethics-alert>.
- Additional reporting channels that may exist at group or local country level.

There is no hierarchy between channels. The author of a report may use any channel at their disposal.

Regardless of the channel used, the person(s) responsible for collecting reports are hereinafter referred to as "**Internal Manager(s)**".

The online reporting platform

The author of a report may issue an alert, including anonymously, on the online reporting platform accessible at: <https://www.rexel.com/en/rexel-group-ethics-alert>

This is a dedicated, free platform available 24/7.

It is hosted in the European Union by an external service provider (EY) that implements strict measures to ensure data security and confidentiality. It should be noted that the employees of this service provider are not involved in the processing of reports and do not have access to the information exchanged.

This platform allows direct communication with the recipient of the alert via chat. It also allows the author of the report to send documents supporting the facts.

The link to this platform is available on the Group's websites: <https://www.rexel.com/en/rexel-group-ethics-alert> and <https://ethique.rexel.com/en/>, as well as on the intranet sites for the Rexel Group entities.

Additional reporting channels

Internal employees of the Rexel Group may submit a report in writing or verbally to one of the following Internal Managers: (i) the local compliance manager (legal or compliance department), (ii) the local Human Resources Department, (iii) the Group Compliance Department, or (iv) the Group Human Resources Department.

The Human Resources Department (local or Group) usually collects reports of violations of labor law or inappropriate behavior at work (harassment, discrimination, health, hygiene, or safety, etc.).

The local compliance officer or Group Compliance Department usually collects reports of violations of the law, the Ethics Guide, the Anti-Corruption Code of Conduct, and Rexel Group compliance procedures, etc.

When a report is made verbally, it may be received by telephone and, at the request of the person making the report and at her/his choice, during a videoconference or a physical meeting organized no later than twenty (20) business days after receipt of the request. Verbal reporting is transcribed in writing.

Employees may, in any event, seek the advice of their direct or indirect line manager and share any concerns they may have, except where the line manager themselves is the alleged author of the conduct in question. If, following such a discussion, it appears that these concerns fall within the scope of this procedure, the line manager must encourage the employee to make a report via the channels indicated above or by contacting the local Legal or Compliance Department or the local Human Resources Department.

3. Content of the report

The author of a report must present the facts and information that are the subject of their report in a precise and objective manner, in order to enable the alert to be handled.

Where possible, they should support their report by:

- indicating the date(s) on which and place(s) where the reported facts occurred, the entity concerned, and the identity and position of the person(s) involved;
- providing a detailed description of the facts with specific and factual information directly related to the subject of the alert, regardless of its form or medium.

4. Anonymous reports

It is preferable for the author of a report to identify themselves, in particular to simplify the conduct of the investigation. However, the author of a report may choose to make an anonymous report, as provided for in the online reporting platform, provided that (i) the seriousness of the facts is established and (ii) the factual elements are sufficiently detailed.

5. External channels

Subject to compliance with applicable local regulations, it should be noted that the author of a report also has the option of making an external report to (i) the competent authority, (ii) the ombudsman, (iii) the judicial authority, or (iv) any relevant local or international institution, body or agency competent to receive such reports. Reporters may file external reports either directly with an authority or after filing a report with the Rexel Group.

III. Handling of internal ethical alerts

1. Acknowledgment of receipt of the report

When the report is received on the online reporting platform or through traditional channels, the Internal Manager (the person responsible for collecting reports as defined above) acknowledges receipt of the alert within seven (7) business days of its receipt.

Acknowledgment of receipt does not constitute acceptance of the alert.

2. Review of the admissibility of the report

Each alert received is subject to a preliminary analysis by the Internal Manager to ensure that it falls within the scope of the procedure and ensure its admissibility.

This verification, which may necessitate communicating with the author or the report, focuses in particular on the following points:

- **The status of the author as a "whistleblower":** in particular, that they are acting in good faith and without seeking direct financial compensation.
- **The nature of the report:** that it does indeed fall within one of the categories of reports covered by the procedure.

- **The content of the report:** that the information and facts reported are objective and sufficiently detailed to allow an investigation to be opened.
- **The existence of protected secrets:** that the report does not reveal facts covered by national defense secrecy, medical secrecy, judicial deliberation secrecy, judicial investigation or inquiry secrecy, or attorney-client privilege.

The decision on admissibility is made by the Internal Manager. The author of a report is informed of the inadmissibility of their report, if applicable, and the reasons for this decision.

In any event, the Internal Manager must provide an initial response within three (3) months. The Rexel Group is not required to process the alert within this time frame, but must inform the author of the report of the actions planned or already taken to assess the validity of the alert and remedy the situation reported.

The alert will be treated in complete confidentiality.

Depending on the nature and seriousness of the facts reported, the alert may be handled by the Rexel Group Ethics Committee. The Rexel Group Ethics Committee is an ad hoc committee set up within Rexel Développement whose role is to handle the most serious alerts reported by Rexel employees or third parties with whom Rexel has a relationship.

The Rexel Group Ethics Committee is composed of three permanent members:

- the General Secretary,
- the Group Human Resources Director, and
- the Ethics & Compliance Director

3. Conducting the internal investigation

Objectives and management of the internal investigation

The time required to process an alert varies and depends on the complexity of the facts reported and the nature of the information provided.

The objective of the internal investigation is to verify the accuracy and materiality of the reported facts. The alert is investigated using methods (interviews, data searches, etc.) that may vary depending on the context and nature of the subject.

This investigation may be conducted by:

- (i) the local Human Resources Department;
- (ii) the local Compliance or Legal Department;
- (iii) the Group Compliance Department;
- (iv) the Group Human Resources Department;
- (v) the Rexel Group Ethics Committee, depending on the nature and severity of the reported facts

(hereinafter referred to as the "**Investigation Manager**").

In any event, the Investigating Manager will lead the internal investigation into the alert. Information relating to the existence and content of the alert will only be disclosed to the persons in charge of the investigation to the extent strictly necessary.

When an alert is filed, Rexel Group guarantees the independence of the investigation process. Before launching an internal investigation, it is verified that none of the individuals involved in investigating the alert are directly or indirectly affected by the reported facts or have any connection of interest with the individuals involved. If a risk of conflict of interest is identified, the employee concerned is immediately removed from the process and replaced. This principle of independence is an integral part of Rexel's ethics and compliance system and aims to ensure rigorous, impartial, and credible management of all alerts received.

Seizure of emails, documents, or computer media

The internal investigation may require the review and processing of emails or any computer media belonging to one or more employees. Before seizing or freezing any email accounts or computer media, the Investigation Manager must request authorization, as defined by local procedure (e.g. the Group Ethics Committee, local General Counsel or local Data Protection Correspondent) to seize and retain these emails for investigation purposes.

Guest expert

When the situation warrants it, the Investigation Manager may decide to invite one or more people to join him or her within the specific framework of handling a specific alert, particularly if accounting, financial, technical, or IT expertise is required.

The Investigation Manager may thus decide to seek assistance in his or her mission from an expert Rexel employee, such as the Internal Audit Department, the Finance Department, the Purchasing Department, a country or zone management team, or any other person within the Rexel Group whom the Investigation Manager deems competent and necessary, or from a duly qualified external service provider.

The expert's assignment shall automatically end upon completion of all verification or processing operations related to the alert for which the Investigation Manager requested their assistance, or upon simple request by the Investigation Manager.

The invited expert is subject to the same confidentiality obligations as the Internal Manager and the Investigation Manager.

4. Decision-making and closure of the investigation

If the facts are not proven, the alert is closed and the author of the report is informed.

If the facts are proven, based on the findings of the investigation, the Investigation Manager will determine whether violations of the law, the Ethics Guide, or the Anti-Corruption Code of conduct have occurred and, if so, will recommend corrective actions and/or appropriate sanctions.

The person who made the report is informed of the closure of the investigation in writing.

The person concerned is also informed of the closure of the investigation. When, after investigation, the breach is found to be serious and proven, disciplinary action, up to and including dismissal, may be taken against the person concerned by the relevant management, depending on the nature and seriousness of the alleged facts.

IV. Protection and guarantees offered

1. General principles

All investigations will be conducted fairly and in full compliance with applicable local laws and regulations. In all cases, the Rexel Group will ensure that the principle of presumption of innocence is respected for the individuals concerned.

The whistleblowing system can only function on the basis of information provided in good faith. Any report made in bad faith—i.e., with the sole intention of causing harm—may be subject to disciplinary action, up to and including dismissal.

2. Information

The whistleblower will be informed within seven (7) business days of receipt of their report.

Within a reasonable period of time not exceeding three (3) months from the acknowledgment of receipt of the report, the author of the report is informed in writing of the measures envisaged or taken to assess the accuracy of the allegations and, where appropriate, to remedy the subject matter of the report, as well as the reasons for these measures. Where the allegations are inaccurate or unfounded, or where the report has become irrelevant, the author of the report shall be informed in writing of the closure of the case.

Any person implicated in an admissible alert will be informed of the nature of the allegations concerning them. However, in the event of precautionary measures necessary to prevent the destruction of evidence relating to the alert, the person concerned by the alert will only be informed after these measures have been taken, as per the applicable laws.

The person targeted by a report may not, under any circumstances, obtain disclosure from the Rexel Group, on the basis of their right of access, of the identity of the person who made the report.

It is specified that the level of information provided may vary depending on applicable local laws.

3. Protection in criminal, civil, and social matters

Whistleblowers are reminded that, subject to locally applicable regulations:

- They are not civilly liable for damages caused as a result of their report or disclosure, provided that their report was made in accordance with the applicable provisions and that the author of a report had reasonable grounds to believe, at the time of making the report, that the report or public disclosure of all of this information was necessary to safeguard the interests at stake.
- They shall not be criminally liable for obtaining or accessing information that is publicly reported or disclosed, provided that such obtaining or accessing does not constitute a separate criminal offense under locally applicable regulations. Where such obtaining or accessing constitutes a separate criminal offense, the locally applicable rules on criminal liability shall apply.
- They cannot be punished, dismissed, discriminated against (particularly in terms of remuneration, training, promotion) or subjected to reprisals or a threat or attempt to apply such measures for reporting or disclosing information in accordance with regulations, provided that the report was made in good faith.

Under the same conditions, individuals who have facilitated the reporting of a whistleblower or who are associated with them may not be subject to retaliatory measures, threats, or attempts to resort to such measures.

The Rexel Group does not tolerate any form of retaliation, threats, or attempts to resort to such measures against whistleblowers and their relatives, such as harassment.

4. Limited data retention period

Reports may only be retained for as long as is strictly necessary and proportionate to their processing and to the protection of their authors, the persons they concern, and any third parties they mention, taking into account the time required for any additional investigations. However, data relating to reports may be retained beyond this period, provided that the individuals concerned are neither identified nor identifiable.

There are several systems for archiving ethical alerts:

- **Inadmissible alerts** (alerts that do not fall within the scope of application, are not serious, are unsubstantiated, are made in bad faith, etc.): these are deleted as soon as possible or archived and anonymized.
- **For admissible alerts:**
 - when the report is not followed by disciplinary or legal proceedings, the Rexel Group ensures that all elements of the report file that could identify the author of the report, as well as those of the persons concerned, are destroyed within a maximum period of two (2) months from the end of the verification or investigation operations;
 - in cases where the investigation leads to legal proceedings or disciplinary sanctions, the elements of the file are duly retained for the necessary period, until the statute of limitations expires (six (6) years) or all avenues of appeal have been exhausted. Then, once the prescribed period has expired, this data is destroyed or archived and anonymized.

5. Confidentiality and security

The Rexel Group takes all necessary precautions to preserve the confidentiality and security of data during its collection, processing, communication, or storage.

Subject to locally applicable regulations, the procedures implemented to collect and process reports guarantee strict confidentiality regarding the identity of the authors of the report, the persons targeted by the report, and the information collected by the persons responsible for collecting and processing the report.

In this regard:

- The information communicated is limited to those persons who have a legitimate need to know in order to process the alert.
- All persons involved in the management of alerts are trained and subject to an obligation of confidentiality. In particular, they undertake not to use the data for improper purposes and to comply with the limited data retention period in accordance with applicable law.
- The online reporting platform is secure and alerts submitted to it can only be viewed by authorized persons. This system also allows employees who wish to remain anonymous to use this channel.

- Whistleblower identity may be disclosed to judicial authorities if required by law.
- Information that could identify the person implicated in a report may not be disclosed, except to the judicial authorities, once the validity of the alert has been established.
- Within Rexel Group entities, the departments generally involved in handling alerts are aware of the confidential nature of the identity of the author and the persons implicated.

6. Protection of personal data

As part of the whistleblowing system, the Rexel Group may collect and process personal data, in particular data relating to the author of a report and the person(s) implicated. A detailed information notice in **Appendix 4** sets out the conditions under which data is collected, processed, stored, and archived.

V. Reporting

The Group Compliance Department reports once a year on the number of alerts, their type, and the actions taken following their receipt, limiting itself to data that is strictly necessary and proportionate to the justification for the communication.

VI. Updating the procedure

The Rexel Group reserves the right to modify, supplement, or update this procedure at any time in order to adapt it to changes in legislation, regulations, case law, or the Group's internal needs. Any updates will be made in accordance with applicable local laws and regulations.

Employees, suppliers, and other stakeholders concerned will be informed of the changes by appropriate means (internal communication, email, intranet publication, direct information to suppliers, etc.), in accordance with local legal requirements.

The current and authoritative version of this procedure will be published and made available on the Rexel Group websites, on the Group intranet and on the online reporting platform.

Contact

Company: Rexel Développement

Address: 13 boulevard Fort de Vaux 75017 Paris (France) – *For the attention of the Group Compliance Department.*

Email address: compliance@rexel.com

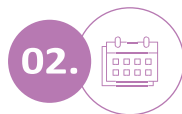
Report a situation

If you suspect or are aware of a violation of the law, the Ethics Guide, or the Anti-Corruption Code of Conduct, report it!



Who can raise an alert?

All Group employees and third parties may use the ethics line.



When to raise an alert?

When you know about or suspect a **violation of the law or our ethics principles**.

This may include:

- acts of corruption;
- a violation of human rights;
 - harassment or discrimination;
 - fraud, etc.



How to raise an alert?

1. Use the **online Rexel ethics line** (weblink below)
 - available 24/7;
 - available in all of the Group main languages.
2. Use the **whistleblowing system set up locally**.
3. Contact the **Legal or Compliance Department or the Human Resources Department (group or local)**



Is it confidential?

Yes, and you can also send an **anonymous** report



Who processes this alert?

For the Group: the Ethics Committee.

For the local system: see local procedure.



Am I protected?

You must raise the alert in good faith and without any direct financial compensation.
In this case, you are protected.



Further

Visit : <https://www.rexel.com/en/ethical-alert/>

Appendix 2: List of countries with local whistleblowing procedure

This procedure is supplemented in certain countries by local procedures, which set out the applicable legal requirements and, as the case may be, the channels available locally.

Local channel information is listed below. Please consult the local procedure for the most up-to-date details.

- **Australia:**
 - o Rexel STOPline disclosure service (operated by an independent external service provider):
Telephone: 1300 30 45 50
Facsimile: Rexel Holdings Australia (C/- the STOPline) 03 9882 4480
Email: rexel@stopline.com.au
On-line: <https://rexel.stoplinereport.com/>
Mail: Rexel Holdings Australia
C/- the STOPline
Locked Bag 8
HAWTHORN VIC 3122
- **Canada:** you may contact the Ethics Committee.
- **Germany:**
 - o E-Mail: whistleblowing@rexel.de
 - o Mail:
Rexel Germany GmbH & Co.
KG - z. Hd. Frau Nicole Steuer | General Counsel
Ridlerstr.5780339 München
- **Ireland**
 - o You may contact the HR Department, Whistleblowing Officer, Chief Executive Officer or our external whistleblower hotline operated by Safecall
Safecall
0800 915 1571
rexel@safecall.co.uk
www.safecall.co.uk/report
- **Italy:**
 - o <https://report.whistleb.com/rexel>
- **Netherlands:** you may contact the Ethics Correspondent.
- **Sweden:**
 - o <https://whistleblow.vismadraftit.se/rexel-sverige-ab>
 - o Telephone: 08-556 214 14.
- **United Kingdom**
 - o You may contact the HR Department, Whistleblowing Officer, Chief Executive Officer or our external whistleblower hotline operated by Safecall
Safecall
0800 915 1571
rexel@safecall.co.uk
www.safecall.co.uk/report
- **USA**
 - o Compliance Email: ethics@rexelusa.com
 - o Compliance Helpline: 1-800-714-8774

Appendix 3: Illustrations of behaviors or misconducts covered by the whistleblowing procedure

Categories	Scope
Corruption	Within the framework of applicable local laws and regulations and the Group's anti-corruption policies: corruption refers to the exchange, directly or through a third party, of benefits (money, gifts, invitations, services, connections, etc.) in exchange for performing or refraining from performing an act related to a function or mandate. It may take the form of a person proposing or offering a benefit in order to obtain a favor (active corruption) or a person soliciting or accepting a benefit in return for a service (passive corruption). Corruption can involve both public and private actors, distorts competition, undermines the transparency of decisions, and exposes the individuals and organizations involved to sanctions and prosecution.
Harassment	Harassment refers to repeated behavior or a single serious act that undermines a person's dignity, safety, or working conditions. It manifests itself in words, gestures, attitudes, or actions intended to intimidate, humiliate, isolate, threaten, or degrade the situation of an employee or third party in connection with professional activity. Harassment can take a psychological form, such as derogatory remarks, deliberate isolation, overloading or depriving someone of work resources, ostracism, spreading rumors, or systematic belittlement. It can also take a sexual form. Sexual harassment is characterized by unwanted sexual behavior or comments that are repeated or constitute a single serious incident, which undermine a person's dignity or create an intimidating, hostile, degrading, or humiliating work environment. This includes, among other things, persistent advances, comments about the body, requests for sexual favors, non-consensual physical gestures or contact, or the dissemination of sexual images without consent. Harassment, whether moral or sexual, is unacceptable and the perpetrators are liable under applicable local laws.
	Discrimination in the workplace involves treating someone unfavorably based on criteria prohibited by law such as origin, gender, family status, etc., or any other characteristic protected by local law. Discrimination can, for example, result

Discrimination	in unequal treatment in access to employment, working conditions, training, mobility, or any other situation related to professional activity. It can take the form of recruitment, evaluation, promotion, assignment, or dismissal decisions that disadvantage a person without objective justification based on the requirements of the position. At the workplace, discrimination can take two forms: - Direct discrimination. In this case, the perpetrator deliberately makes a decision based on discriminatory criterion that is prohibited by law. Indirect discrimination. In this case, the perpetrator makes a decision that appears neutral but ultimately disadvantages certain people over others. For example, internal regulation only allow men to remain in the company after the age of 50. This therefore constitutes indirect discrimination based on gender and age.
Health/Safety	Any serious infringement or risk to health and safety at work. Safety at work refers to all measures and practices aimed at protecting the physical and mental integrity of people in their workplace by reducing the risk of accidents, injuries, and occupational illnesses. This includes identifying and assessing risks, implementing technical and organizational safeguards, training and informing employees, and putting in place prevention, intervention, and emergency response measures. Compliance with these obligations contributes to a safe working environment that complies with local requirements.
Human Rights (other than discrimination and harassment)	Any serious infringement or risk to human rights and fundamental freedoms recognized at the national and international level, as well as any violation of applicable local requirements in this area. This includes, but is not limited to, situations involving principles such as respect for freedom of association and expression, access to decent and safe working conditions, and the possibility for those concerned to have access to legal remedies.
Conflicts of interest	A conflict of interest is a situation in which a person's personal interests, whether financial, family, friendship, political, or related to other benefits, are likely to influence, or appear to influence, their judgment or decisions in the course of their duties within the Rexel Group. This is not necessarily a fault or an illegal act, but a risk of bias that compromises the expected impartiality. This risk of bias may be sufficient to undermine the confidence of those concerned, alter the quality of decisions, and damage the organization's reputation. A conflict of interest may be actual (already present), potential (likely to arise), or apparent (perceived by third parties). The whistleblowing system is not intended to replace the conflict of interest reporting procedure defined by the Rexel Group.

Anti-competitive practices	Anti-competitive practices refer to corporate behavior that impairs free competition and harms other market players (customers, suppliers, competitors). They include formal or informal agreements between competitors to coordinate prices, commercial terms, the allocation of markets, territories or products, or to limit supply or boycott certain partners. They also include situations of abuse of a dominant position (e.g., driving out a rival, imposing predatory prices or unjustified tied sales), influencing the resale price charged by distributors, and exchanging non-public strategic information that could influence market behavior (such as plans, marketing data, or capacities). These practices are prohibited by competition rules and are subject to significant penalties.
Environment	Any situation where applicable environmental requirements are not met, or where a significant risk or damage to the environment is identified, whether within the company or among its partners in the value chain. This covers pollution prevention, responsible use of resources, and safe management of substances and waste, in accordance with regulatory obligations and internal standards.
Fraud	Any situation involving concealment, deception, or manipulation intended to obtain an undue advantage or evade obligations, whether fiscal, financial, or accounting. This includes, for example, falsifying documents or records, misrepresenting financial information, concealing income or assets, or any scheme designed to circumvent applicable rules, either within the company or in its value chain.
Insider trading	Insider trading is the act of buying, selling, or recommending financial instruments using or relying on non-public privileged information about an issuer or its securities. It also includes the illegal disclosure of such information to third parties. Such conduct confers an unfair advantage in the markets and is strictly prohibited and punishable by law.
Fictitious jobs	A fictitious job is a situation where a person is paid for a position or tasks that are not actually performed, or that do not exist, in order to obtain an unfair advantage. This may involve a total absence of actual work, fictitious duties, or nominal assignment to a department without any real contribution, within the company or via third parties.
	Any situation where personal data or IT systems are not protected in accordance with laws and internal rules, exposing individuals or the company to the risk of unauthorized access, use, disclosure, modification, or destruction. This covers the lawful and minimized collection and processing of data, system security (access controls,

Personal data protection / IT security	encryption, backups), incident and breach management, and the confidentiality and integrity of information throughout its lifecycle, including at service providers. Personal data is any information that directly or indirectly identifies a natural person (e.g., name, contact details, identifiers, photo, location data, or other elements relating to their identity or personal life).
--	--

PRIVACY POLICY

—

WHISTLEBLOWING SYSTEM

Version 12/2025

The Rexel Group has established a professional whistleblowing system that allows its employees and third parties with whom the Rexel Group has a relationship to report unlawful acts or misconduct. The scope of the system is described in the Whistleblowing Procedure, available on the [rexel.com](https://www.rexel.com) website.

 Under this system, a Rexel entity may collect and process data about you. Data confidentiality is the foundation of our relationship of trust. Therefore, we take the protection of your personal data seriously in the course of our business activities.

This policy outlines the Rexel Group's commitments to personal data protection and. The following notice also allows you to learn about your rights and the conditions under which your personal data is collected, processed, stored, and archived.

Who are we?

REXEL DEVELOPPEMENT SAS, a simplified joint-stock company under French law, with its registered office at 13, Boulevard du Fort de Vaux, Paris, registered with the Paris Trade and Companies Register under number 480 172 840, is the data controller.

The entity within the Group that has an employment contract with, or collaborates with the author of the report is also a data controller.

They determine the purposes and means of processing your data.

They are referred to in this policy as "Rexel," "we," or "Data Controllers."

EY Poland acts as a processor for the processing carried out on the online alert platform.

How do we process your data in the context of the alert system?

The table below details:

- (i) why we process your personal data,
- (ii) what types of data we process, and
- (iii) the legal basis for processing your data.

Purpose 1	Type of data
Collect and process alerts reporting acts that violate the law, or the anti-Corruption Code of conduct covered by the whistleblowing system (see the Whistleblowing Procedure) <u>Sub-purposes:</u> - Centralized management of professional reports (receiving and handling alerts, setting up a secure channel, storing and retaining information, ensuring security) - Processing of professional reports (conducting internal investigations, assessing the relevant facts) - Decision-making and implementation of appropriate measures upon closure of the report (notification and implementation of measures) - Statistical monitoring and improvement of the whistleblowing system - Exercise or defend rights in legal proceedings	As part of the system, the following categories of data may be processed: - Identity data (first and last name, contact details), professional data (position, employer, place of work) of the person making the report (unless the report is anonymous) and any other information voluntarily provided by them - Identity data (first and last name, contact details), professional data (position, employer, place of work) of the persons implicated - Identity data (first and last name, email address), professional data (position, employer, place of work) of persons involved or consulted in the collection or processing of the alert, and facilitators and persons in contact with the whistleblower - Sensitive data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, sex life or sexual orientation) where strictly necessary in order to exercise or defend legal rights (Article 9.2.f of the GDPR) or for reasons of substantial public interest (Article 9.2.g of the GDPR) - Data relating to criminal convictions and offenses or related security measures where strictly necessary and in accordance with Article 10 of the GDPR - Information collected in the course of fact-checking - Reports on verification operations - Data relating to the follow-up to the report
Legal basis for the processing of your data Legal obligation to implement a whistleblowing system: in particular Articles 8.I.B and 17 II of the Sapin II law and Article L. 225-102-4 of the Commercial Code, as well as any equivalent law relating to the protection of whistleblowers, the fight against corruption, or the duty of vigilance.	

Purpose 2	Type of data
Collect and process alerts reporting acts that violate the Ethics Guide <u>Sub-purposes:</u> - Centralized management of professional reports (receiving and handling alerts, setting up a secure channel, storing and retaining information, ensuring security) - Processing of professional reports (conducting internal investigations, assessing the relevant facts) - Decision-making and implementation of appropriate measures upon closure of the report (notification and implementation of measures) - Statistical monitoring and improvement of the whistleblowing system - Exercise or defend rights in legal proceedings	As part of the system, the following categories of data may be processed: - Identity data (first and last name, contact details), professional data (position, employer, place of work) of the person making the report (unless the report is anonymous) and any other information voluntarily provided by them - Identity data (first and last name, contact details), professional data (position, employer, place of work) of the persons implicated - Identity data (first and last name, email address), professional data (position, employer, place of work) of persons involved or consulted in the collection or processing of the alert, and facilitators and persons in contact with the whistleblower - Sensitive data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, sex life or sexual orientation) where strictly necessary in order to exercise or defend legal rights (Article 9.2.f of the GDPR) or for reasons of substantial public interest (Article 9.2.g of the GDPR) - Data relating to criminal convictions and offenses or related security measures where strictly necessary and in accordance with Article 10 of the GDPR - Information collected in the course of fact-checking - Reports on verification operations - Data relating to the follow-up to the report
Legal basis for the processing of your data	
Legal basis: Legitimate interest in processing ethical alerts that are not covered by a legal obligation.	

Who are the recipients of your data?



The personal data we collect, as well as any data collected subsequently, is intended for us in our capacity as data controller.



We ensure that only authorized persons have access to this data.

Internally:

- Those responsible for collecting and processing alerts, namely:
 - Members of the Rexel Group Ethics Committee
 - Authorized members of the legal or compliance Department at the Group and local levels
 - Authorized members of the Human Resources Department at the Group and local levels
- Authorized members of the Audit and Internal Control Department at the Group and local levels to ensure the effectiveness of internal controls and governance
- When justified by the situation, other internal personnel may have access to the data, particularly when accounting, financial, legal, technical, or IT expertise is required.

Externally:

- Our advisors
- Our brokers and insurers
- Our auditors
- The competent authorities (judicial, administrative, and regulatory bodies), in accordance with applicable regulations
- Our service providers, and more specifically EY Poland, which provides us with the online reporting platform.

These recipients are located in the European Union.

How long do we keep your data?

Situations	Retention period
Inadmissible alerts (not falling within the scope of application, not serious in nature, lacking information, made in bad faith, etc.)	Deletion or archiving and anonymization as soon as possible
Admissible alert but dismissed (not followed by disciplinary or legal proceedings)	Deletion or anonymization and archiving within two (2) months
Alerts giving rise to disciplinary or legal proceedings	Data retention until the end of the proceedings and appeals. After this period, deletion or anonymization and archiving.

What are your rights?



In accordance with personal data protection laws, you have the following rights:

- right of access: you can access the information we hold about you and obtain a copy of it;
- right of rectification: you can have any inaccurate data concerning you modified, completed, updated, or deleted;
- right to object: you can object to us processing your data, unless there are legitimate and compelling reasons for us to process it;
- right to erasure: you may request that we erase data concerning you within the limits of the conditions set out in Article 17 of the GDPR;
- right to data portability: you may retrieve your data in order to transfer it to another organization or for personal use;
- right to restriction of processing;
- right to formulate specific and general guidelines concerning the storage, erasure, and communication of your data after your death.

Any person who is the subject of a report will be informed as soon as possible (within one month at the latest) following the recording, whether computerized or not, of data concerning them in order to enable them to exercise their rights. However, if such information is likely to seriously compromise the objectives of the processing and, in particular, the conduct of the investigation (for example, if there is a risk of evidence being destroyed), then this information may be deferred and will only be provided once any risk has been eliminated.

The person who is the subject of a report may not, under any circumstances, obtain from the data controller, on the basis of their right of access, information concerning the identity of the Author of the Report or any other person involved in the investigation.

If you do not receive a response, or if you consider the response to be unsatisfactory, or if you believe that the processing of your data does not comply with legal and regulatory provisions, you may contact the competent supervisory authority.

How to exercise your rights?



By written request to our Data Protection Officer:

Countries	Entities	Address
Austria	COMTECH IT-SOLUTIONS GMBH	datenschutz@rexel.at
	Rexel Austria GmbH	datenschutz@rexel.at
Belgium	Rexel Belgique SA	gdpr@rexel.be
France	Cordia	donnees.personnelles@francofa-eurodis.fr
	Rexel Développement SAS / Rexel Group	data.protection@rexel.com
	Rexel France SAS	donnees.personnelles@rexel.fr
	Bizline	data.protection@rexel.com
	Gigamedia	data.protection@rexel.com
	Sofinther SAS	donnees.personnelles@sofinther.fr
	Espace Elec SAS	donnees.personnelles@espace-elec.fr
	Esabora Digital Services SAS	dataprotection-rda@rexel.fr
	Francofa Eurodis	donnees.personnelles@francofa-eurodis.fr
	Freshmile Services SAS	donnees.personnelles@rexel.fr
	ITESA	donnees.personnelles@rexel.fr
Germany	REXEL GERMANY BETEILIGUNGS GMBH	Datenschutzbeauftragter@rexel.de
	Rexel Germany GmbH & Co KG	Datenschutzbeauftragter@rexel.de
	REXEL GERMANY VERWALTUNGS GMBH	Datenschutzbeauftragter@rexel.de
Italy	Rexel Italia S.p.A	dataprotection@rexel.it
	Tecno-Bi S.r.l.	dataprotection@rexel.it
	Comm-Tech S.r.l.	dataprotection@rexel.it
Ireland	M. Kelliher 1998	data.protection@rexel.ie
	Rexel Industrial Solutions	data.protection@rexel.ie
Luxembourg	Rexel Luxembourg SA	gdpr@rexel.be
Netherlands	Rexel Nederland B.V	AVG@rexel.nl
	Wasco Group B.V.	AVG@rexel.nl
	Wasco Holding B.V.	AVG@rexel.nl
	Wasco Groothandels Greop B.V.	AVG@rexel.nl
	Wasco Distributlecentrum B.V.	AVG@rexel.nl
Slovenia	Rexel d.o.o.	dpc@rexel.si
Sweden	Rexel Sverige AB	dataskydd@rexel.se
Switzerland	ELEKTRO-MATERIAL AG	datenschutz@e-m.ch
	Rexel 3S	data.protection@rexel.com
UK	Rexel (UK) Ltd.	data.protection@rexel.co.uk



Procédure d'alerte Décembre 2025_V1

Sommaire

I. Introduction	3
1. <u>Objet du dispositif d'alerte interne</u>	3
2. <u>Rappel du référentiel juridique</u>	3
3. <u>Champ d'application</u>	3
II. Le recueil des alertes éthiques	4
1. <u>Conditions de recevabilité d'une alerte éthique</u>	4
<u>Qui peut émettre un signalement ?</u>	4
<u>Comment bénéficier du statut du lanceur d'alerte et de la protection légale associée ?</u>	5
<u>Quels faits peuvent faire l'objet d'un signalement ?</u>	5
2. <u>Les modalités de recueil d'un signalement</u>	6
3. <u>Contenu du signalement</u>	7
4. <u>Signalement anonyme</u>	7
5. <u>Canaux externes</u>	7
III. Le traitement des alertes éthiques internes	8
1. <u>Accusé de réception du signalement</u>	8
2. <u>Examen de la recevabilité du signalement</u>	8
3. <u>Conduite de l'enquête interne</u>	9
4. <u>Prises de décision et clôture de l'enquête</u>	10
IV. Protection et garanties offertes	10
1. <u>Principes généraux</u>	10
2. <u>Information</u>	10
3. <u>Protection en matières pénale, civile et sociale</u>	11
4. <u>Conservation des données limitées dans le temps</u>	11
5. <u>Confidentialité et sécurité</u>	12
6. <u>Protection des données à caractère personnel</u>	12
V. Reporting	13
VI. Mise à jour de la procédure	13
Annexe 1 : Synthèse	14
Annexe 2 : Liste des pays avec une procédure d'alerte locale	15
Annexe 3 : Exemples de comportements ou manquements visés par la procédure d'alerte	15
Annexe 4 : Politique de protection des données personnelles	19

I. Introduction

1. Objet du dispositif d'alerte interne

Dans le cadre de la politique Ethique & Conformité du groupe Rexel telle que décrite notamment dans son Guide d’Ethique, sa Charte Fournisseur Responsable et son Code de conduite anti-corruption, le groupe Rexel a mis en place un dispositif d’alerte interne.

Le dispositif d’alerte interne du groupe Rexel permet à tout collaborateur, ainsi qu’aux tiers avec lesquels le groupe Rexel est en relation de signaler des situations contraires à la loi, au Guide d’Ethique, ou au Code de conduite anti-corruption du groupe Rexel.

L’objet de cette procédure est de décrire le processus de recueil et de traitement des alertes éthiques par le groupe Rexel.

Un résumé de la procédure est joint en **Annexe 1**.

2. Rappel du référentiel juridique

La holding du groupe Rexel étant constituée en France, la procédure a été établie dans le respect des lois françaises suivantes :

- La Loi dite « Sapin II » du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique ;
- La loi dite « devoir de vigilance » du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre ;
- La Loi dite « Wasserman » du 21 mars 2022 visant à améliorer la protection des lanceurs d’alerte ainsi que son décret d’application du 3 octobre 2022.

La procédure s’appuie également sur un certain nombre de publications de l’Agence Française Anticorruption (AFA) et de la Commission Nationale de l’Informatique et des Libertés (CNIL) :

- Les recommandations de l’AFA ;
- Le guide pratique « Les enquêtes internes anticorruption » publié en mars 2023 par l’AFA et le Parquet national financier ;
- Le référentiel « alertes professionnelles » de la CNIL initialement publié en 2019 et mis à jour en 2023.

Plus généralement, le recueil et le traitement des signalements sont menés en conformité avec les lois et réglementations applicables, et cette procédure pourra être mise à jour au besoin pour refléter les évolutions législatives et les meilleures pratiques.

Si une loi ou une réglementation locale offre des règles plus protectrices que la présente procédure pour le lanceur d’alerte, les dispositions locales prévalent. En revanche, si la présente procédure accorde des garanties plus protectrices, le groupe Rexel les appliquera à titre volontaire dans les limites permises par le droit applicable.

3. Champ d’application

La présente procédure a vocation à être déclinée dans l’ensemble des entités du groupe Rexel. Elle sera modifiée, le cas échéant, afin de refléter toute évolution législative et réglementaire.

Cette procédure est complétée dans certains pays du groupe Rexel par des procédures locales. Ces dernières précisent les conditions légales applicables, et le cas échéant, les canaux disponibles localement (voir **Annexe 2**).

L'auteur d'un signalement peut ainsi choisir le canal de signalement de son choix (groupe ou local). La procédure applicable sera alors celle correspondant au canal choisi. Selon la nature et la gravité du comportement ou manquement signalé, une alerte effectuée via le canal local peut être renvoyée au groupe et vice et versa.

La présente procédure s'applique à l'ensemble des collaborateurs du groupe Rexel (quel que soit leur rôle, position ou département) et les tiers avec lesquels le groupe Rexel est en relation. Elle porte sur le recueil et le traitement des alertes internes par le groupe Rexel et plus particulièrement sur :

- Leur émission ;
- Leur réception ;
- L'analyse de leur recevabilité ;
- les principales étapes de l'enquête interne;
- La clôture du dossier.

II. Le recueil des alertes éthiques

1. Conditions de recevabilité d'une alerte éthique

Qui peut émettre un signalement ?

Le dispositif d'alerte interne du groupe Rexel est ouvert aux personnes suivantes :

- Les collaborateurs du groupe Rexel (CDI, CDD, alternants, stagiaires)
- Les collaborateurs extérieurs ou occasionnels (intérimaires, consultants, etc.)
- Les candidats à l'embauche
- Les anciens salariés
- Les actionnaires, associés et titulaires de droits de vote au sein de l'assemblée générale
- Les membres de l'organe d'administration, du Comité de direction ou de l'organe de surveillance
- Tout collaborateur de tiers avec lequel le groupe Rexel est en relation (ex : clients, fournisseurs, prestataires, etc.).

Le dispositif d'alerte interne est ouvert à l'ensemble des entités du groupe Rexel et est disponible dans les langues principales du groupe : anglais, allemand, chinois, français, italien, néerlandais, suédois et slovène.

Comment bénéficier du statut du lanceur d'alerte et de la protection légale associée ?

Pour être considéré comme un lanceur d'alerte et bénéficier de la protection prévue par la loi, il est nécessaire de répondre à la définition du lanceur d'alerte prévue par la loi, en réunissant les critères cumulatifs suivants, sauf disposition contraire d'une loi locale applicable :

- Être une personne physique

- Ne tirer aucune contrepartie financière directe du signalement, sauf si une loi locale l'autorise expressément.
- Être de bonne foi
- Si les faits signalés ont été obtenus en dehors d'un cadre professionnel, avoir personnellement eu connaissance des faits signalés

Quels faits peuvent faire l'objet d'un signalement ?

Le dispositif d'alerte interne du groupe Rexel permet de signaler des faits susceptibles de constituer l'un des comportements ou manquements suivants :

- Un crime ou un délit
- Une menace ou un préjudice pour l'intérêt général
- Une violation ou une tentative de dissimulation d'une violation des lois et règlements nationaux, européens ou internationaux
- Un manquement ou une situation contraire au Code de conduite anti-corruption ou au Guide d'Ethique du groupe Rexel
- Des risques d'atteintes graves liés aux activités du groupe Rexel envers les droits humains, les libertés fondamentales, la santé et la sécurité des personnes, ainsi que l'environnement

A titre d'exemples, les comportements ou manquements à signaler peuvent inclure :

- Corruption, y compris toute violation du Code de conduite anti-corruption
- Harcèlement (moral ou sexuel)
- Discrimination
- Santé, hygiène ou sécurité (par exemple, risque pour l'intégrité physique ou mentale)
- Droits de l'homme (autres que la discrimination, le harcèlement ou le respect de la vie privée)
- Conflit d'intérêts
- Pratique anticoncurrentielle
- Environnement (par exemple, pollution ou gestion des déchets)
- Fraude fiscale
- Fraude financière ou comptable
- Délit d'initié
- Emplois fictifs
- Données personnelles / sécurité informatique

L'Annexe 3 illustre certains de ces comportements ou manquements.

Les signalements portant sur des catégories non visées ci-dessus n'entrent pas dans le champ d'application de la présente procédure. De même, sont exclus de la présente procédure les faits, informations ou documents, quel que soit leur forme ou leur support, dont la révélation ou la divulgation est interdite par les dispositions relatives au secret de la défense nationale, au secret médical, au secret des délibérations judiciaires, au secret de l'enquête ou de l'instruction judiciaires ou au secret professionnel avocat/client. Le cas échéant, l'auteur du signalement en sera informé et redirigé vers les personnes compétentes pour traiter les faits signalés.

2. Les modalités de recueil d'un signalement

L'auteur d'un signalement dispose de plusieurs canaux de recueil des alertes :

- La plateforme de signalement en ligne accessible à l'adresse : <https://www.rexel.com/fr/alerte-ethique-du-groupe-rexel> ;
- Les canaux additionnels de signalement qui peuvent exister au niveau groupe ou local.

Il n'existe pas de hiérarchie entre les canaux. L'auteur d'un signalement peut utiliser n'importe quel canal à sa disposition.

Quel que soit le canal utilisé, la(les) personne(s) en charge du recueil des signalements sont ci-après désignée(s) comme « **Responsable(s) interne(s)** ».

La plateforme de signalement en ligne

L'auteur d'un signalement peut émettre une alerte, y compris de manière anonyme, sur la plateforme de signalement en ligne accessible à l'adresse : <https://www.rexel.com/fr/alerte-ethique-du-groupe-rexel> .

Il s'agit d'une plateforme dédiée, gratuite, disponible 24h/24 et 7j/7.

Elle est hébergée dans l'Union Européenne par un prestataire externe (EY) qui met en œuvre des mesures strictes pour assurer la sécurité et la confidentialité des données. Il est précisé que les salariés de ce prestataire n'interviennent pas dans le traitement des signalements et n'ont pas accès aux informations échangées.

Cette plateforme permet de communiquer directement avec le destinataire de l'alerte via un chat. Elle permet également à l'auteur du signalement d'envoyer des documents étayant les faits.

Le lien vers cette plateforme est disponible sur les sites internet du groupe : <https://www.rexel.com/fr/alerte-ethique-du-groupe-rexel> et <https://ethique.rexel.com/> ainsi que sur les sites intranets des entités du groupe Rexel.

Les canaux additionnels de signalement

Les collaborateurs internes du groupe Rexel peuvent émettre un signalement par écrit ou par oral auprès de l'un des Responsables Internes suivants : (i) le responsable local de la conformité (Direction juridique ou conformité), (ii) la Direction des Ressources Humaines locale, (iii) la Direction conformité groupe ou (iv) la Direction des Ressources Humaines groupe.

La Direction des Ressources Humaines (locale ou groupe) recueille en général les signalements révélant des infractions aux dispositions du code du travail ou des comportements inappropriés au travail (harcèlement, discrimination, santé, hygiène ou sécurité, etc.).

Le responsable local de la conformité ou la Direction conformité groupe recueille en général les signalements révélant des violations à la loi, au Guide d'Ethique, au Code de conduite anti-corruption et aux procédures de conformité du groupe Rexel, etc.

Lorsqu'un signalement est effectué par oral, il peut être reçu par téléphone et, sur la demande de l'auteur du signalement et selon son choix, lors d'une visioconférence ou d'une rencontre physique organisée au plus tard vingt (20) jours ouvrés après réception de la demande. Le signalement oral est reporté à l'écrit.

Les collaborateurs peuvent en tout état de cause solliciter l'avis de leur supérieur hiérarchique, direct ou indirect, et lui faire part de leurs éventuelles préoccupations, sauf dans l'hypothèse où il est lui-

même l’auteur du comportement incriminé. Si, à l’issue d’un tel échange, il apparaît que ces préoccupations relèvent du champ d’application de la présente procédure, le supérieur hiérarchique doit encourager le collaborateur à effectuer un signalement via les canaux indiqués ci-dessus ou en contactant la Direction juridique ou conformité locale ou la Direction des ressources humaines locale

3. Contenu du signalement

L’auteur d’un signalement doit exposer de manière précise et objective les faits et informations faisant l’objet de son signalement, de manière à ce que l’alerte puisse être traitée.

Dans la mesure du possible, il étatera son signalement :

- en indiquant la (les) dates et lieu(x) des faits dénoncés, l’entité concernée, l’identité et la fonction de la ou des personnes en cause ;
- en fournissant une description détaillée des faits avec des informations précis et factuels en lien direct avec l’objet de l’alerte, quels que soient leurs formes ou leurs supports.

4. Signalement anonyme

Il est préférable que l’auteur d’un signalement s’identifie, notamment afin de simplifier la conduite de l’enquête. Cependant, l’auteur d’un signalement peut choisir de faire un signalement anonyme, comme la plateforme de signalement en ligne le lui permet, sous réserve que (i) la gravité des faits soit établie et que (ii) les éléments factuels soient suffisamment détaillés.

5. Canaux externes

Sous réserve du respect des règles impératives applicables localement, il est rappelé que l’auteur d’un signalement dispose également de la possibilité d’effectuer un signalement externe auprès de (i) l’autorité compétente, (ii) du défenseur des droits, (iii) de l’autorité judiciaire, ou (iv) toute institution, organe ou organisme national ou transnational compétent pour recueillir cette alerte.

L’auteur d’un signalement peut faire ce signalement externe, soit directement auprès d’une autorité soit après avoir effectué une alerte auprès du groupe Rexel.

III. Le traitement des alertes éthiques internes

1. Accusé de réception du signalement

Lorsque le signalement est reçu sur la plateforme de signalement en ligne ou via les canaux traditionnels, le Responsable interne (la personne en charge du recueil des signalements comme défini ci-avant) accuse-réception de l'alerte dans les sept (7) jours ouvrés de sa réception.

L'accusé de réception ne vaut pas recevabilité de l'alerte.

2. Examen de la recevabilité du signalement

Chaque alerte reçue fait l'objet d'une analyse préliminaire par le Responsable interne afin de s'assurer qu'elle entre bien dans le champ d'application de la procédure et qu'elle soit donc recevable.

Cette vérification, qui peut nécessiter un échange avec l'auteur de l'alerte, porte notamment sur les points suivants :

- **La qualité de « lanceur d'alerte » de l'auteur** : notamment qu'il agit de bonne foi et sans recherche d'une contrepartie financière directe ;
- **La nature du signalement** : qu'il concerne bien l'une des catégories de signalement visées par la procédure ;
- **Le contenu du signalement** : que les informations et faits signalés sont objectifs et suffisamment détaillés pour permettre d'ouvrir une enquête ;
- **L'existence de secrets protégés** : que l'alerte ne révèle pas des faits couverts par le secret de la défense nationale, le secret médical, le secret des délibérations judiciaires, le secret de l'enquête ou de l'instruction judiciaire ou le secret professionnel avocat/client.

La décision de recevabilité est prise par le Responsable interne. L'auteur d'un signalement est informé de l'irrecevabilité de son signalement, le cas échéant, et les raisons justifiant cette position.

En tout état de cause, le Responsable interne doit apporter une première réponse dans un délai de trois (3) mois. Le groupe Rexel n'est pas tenu de traiter l'alerte dans ce délai, mais d'informer l'auteur du signalement sur les actions envisagées ou déjà prises pour évaluer la réalité de l'alerte et remédier à la situation signalée.

L'alerte sera traitée en toute confidentialité.

Selon la nature et la gravité des faits signalés, l'alerte pourra être traitée par le Comité Ethique du groupe Rexel. Le Comité Ethique du groupe Rexel est un comité ad hoc constitué au sein de la société Rexel Développement dont le rôle est de traiter les alertes les plus graves signalées par les collaborateurs de Rexel ou les tiers avec lesquels Rexel est en relation.

Le Comité Ethique du groupe Rexel est composé de trois membres permanents :

- le Secrétaire Général,
- le Directeur Groupe des Ressources Humaines,
- le Directeur Ethique & Conformité

+

3. Conduite de l'enquête interne

Objectifs et pilotage de l'enquête interne

Le délai de traitement d'une alerte est variable et dépend de la complexité des faits rapportés et de la nature des éléments fournis.

L'objectif de l'enquête interne est de vérifier l'exactitude et la matérialité des faits remontés. L'instruction de l'alerte est réalisée selon des moyens (entretiens, recherches de données, etc.) qui peuvent varier selon le contexte et la nature du sujet.

Cette enquête peut notamment être conduite par :

- (vi) la Direction des Ressources Humaines locale ;
- (vii) la Direction juridique ou conformité locale ;
- (viii) la Direction conformité groupe ;
- (ix) la Direction des Ressources Humaines groupe ;
- (x) le Comité Ethique du groupe Rexel, selon la nature et la gravité des faits signalés

(ci-après désigné le « **Responsable de l'enquête** »).

En tout état de cause, le Responsable de l'enquête pilotera l'enquête interne afférente à l'alerte. Les informations relatives à l'existence et au contenu de l'alerte ne sont communiquées que dans la limite du strict nécessaire aux personnes en charge de l'enquête.

Lorsqu'une alerte est déposée, Rexel garantit l'indépendance du processus d'enquête. Avant le lancement de l'enquête interne, il est vérifié qu'aucune des personnes amenées à instruire l'alerte ne soit concernée, directement ou indirectement, par les faits signalés ou n'ait de lien d'intérêt avec les personnes mises en cause. Si un risque de conflit d'intérêts est identifié, le collaborateur concerné est immédiatement écarté du processus et remplacé. Ce principe d'indépendance fait partie intégrante du dispositif d'éthique et de conformité de Rexel, et vise à garantir une gestion rigoureuse, impartiale et crédible de toutes les alertes reçues.

Saisie des emails, documents ou supports informatiques

L'enquête interne peut nécessiter la revue et le traitement d'emails ou de tout supports informatiques d'un/de collaborateur(s). Avant toute saisie, gel de boîte emails ou de supports informatiques, le Responsable de l'enquête doit demander l'autorisation, comme décrit dans la procédure locale applicable (par exemple au Comité Ethique groupe, la Direction juridique ou conformité locale ou le correspondant Données Personnelles local) de saisir et de conserver ces emails à des fins d'enquête.

Expert invité

Lorsque la situation le justifie le Responsable de l'enquête peut décider d'inviter une ou plusieurs personnes à le rejoindre dans le cadre déterminé du traitement d'une alerte spécifique, notamment en cas de besoin d'expertise comptable, financière, technique ou informatique.

Le Responsable de l'enquête peut ainsi décider de se faire assister dans sa mission d'un ou de salariés Rexel expert, tel que la Direction de l'audit interne, la Direction financière, la Direction des achats, une Direction de pays ou de zone ou de toute autre personne au sein du groupe Rexel que le Responsable de l'enquête juge compétent et nécessaire, ou d'un prestataire externe dûment qualifié.

La mission de cet/ces expert(s) prend fin automatiquement lors de la clôture de l'ensemble des opérations de vérification ou de traitement de l'alerte pour l'examen de laquelle il a été sollicité par le Responsable de l'enquête ou sur simple demande de ce dernier.

Le ou les expert(s) invité(s) sont soumis aux mêmes obligations de confidentialité que le Responsable interne et le Responsable de l'enquête.

4. Prises de décision et clôture de l'enquête

Si les faits ne sont pas avérés, l'alerte est clôturée et l'auteur du signalement en est informé.

Si les faits sont avérés sur la base des constatations de l'enquête, le Responsable de l'enquête déterminera si des violations à la loi, au Guide d'Éthique ou au Code de conduite anti-corruption ont eu lieu et, le cas échéant, recommandera des actions correctives et/ou les sanctions appropriées.

L'auteur du signalement est informé de la clôture de l'enquête par écrit.

La personne visée est également informée de la clôture de l'enquête.

Lorsque, après enquête, le manquement constaté est grave et avéré, une sanction disciplinaire pouvant aller jusqu'au licenciement pourra être prise à l'encontre de la personne visée par la hiérarchie concernée, en fonction de la nature et de la gravité des faits reprochés. .

IV. Protection et garanties offertes

1. Principes généraux

Toute enquête se déroulera de manière équitable et dans le plein respect de la législation et des réglementations locales applicables. En tout état de cause, le groupe Rexel veille au respect du principe de présomption d'innocence des personnes visées.

Le dispositif d'alerte ne peut fonctionner qu'à partir d'informations communiquées de « bonne foi ». Tout signalement effectué de mauvaise foi — c'est-à-dire avec pour seule intention de nuire — peut faire l'objet de sanctions disciplinaires, pouvant aller jusqu'au licenciement.

2. Information

L'auteur du signalement est informé dans un délai de sept (7) jours ouvrés de la réception de son signalement.

Dans un délai raisonnable n'excédant pas trois (3) mois à compter de l'accusé de réception du signalement, l'auteur du signalement est informé par écrit des mesures envisagées ou prises pour évaluer l'exactitude des allégations et, si cela est approprié, remédier à l'objet du signalement ainsi que sur les motifs de ces mesures. Lorsque les allégations sont inexactes ou infondées ou lorsque le signalement est devenu sans objet, l'auteur du signalement est informé par écrit de la clôture du dossier.

Toute personne mise en cause dans le cadre d'une alerte admissible sera informée de la nature des allégations la concernant. Toutefois, en cas de mesures conservatoires nécessaires pour prévenir la destruction de preuves relatives à l'alerte, la personne visée par l'alerte n'est informée que postérieurement à l'adoption de ces mesures, conformément aux dispositions légales en vigueur.

La personne visée par une alerte ne peut en aucun cas obtenir communication par le groupe Rexel, sur le fondement de son droit d'accès, de l'identité de l'auteur du signalement.

Il est précisé que le niveau d'information fourni pourra varier en fonction des lois locales applicables.

3. Protection en matières pénale, civile et sociale

Il est rappelé à l'auteur d'un signalement que, sous réserve de la réglementation localement applicable :

- Il n'est pas civilement responsable des dommages causés du fait de son signalement ou sa divulgation dès lors que son signalement a été fait dans le respect des dispositions applicables et que l'auteur d'un signalement avait des motifs raisonnables de croire, lorsqu'il y a procédé, que le signalement ou la divulgation publique de l'intégralité de ces informations était nécessaire à la sauvegarde des intérêts en cause.
- Il n'est pas responsable pénalement en ce qui concerne l'obtention des informations qui sont signalées ou divulguées publiquement, ou l'accès à ces informations, à condition que cette obtention ou cet accès ne constitue pas, en vertu de la réglementation localement applicable une infraction pénale autonome. Au cas où cette obtention ou cet accès constitue une infraction pénale autonome, les règles de responsabilité pénale applicables localement s'appliquent.
- Il ne peut pas être sanctionné, licencié, faire l'objet d'une mesure discriminatoire (notamment en matière de rémunération, formation, promotion) ou d'une mesure de représailles, ni de menace ou de tentative de recourir à ces mesures, pour avoir signalé ou divulgué des informations dans le respect de la réglementation, dès lors que le signalement a été effectué de bonne foi.

Dans les mêmes conditions, les personnes ayant facilité le signalement de l'auteur d'un signalement ou en lien avec lui ne peuvent faire l'objet de mesures de représailles, ni de menaces ou de tentatives de recourir à ces mesures.

Le groupe Rexel ne tolère aucune forme de représailles, de menaces ou de tentative de recourir à ces mesures contre les auteurs d'un signalement et leurs proches, tel que le harcèlement.

4. Conservation des données limitées dans le temps

Les signalements ne peuvent être conservés que le temps strictement nécessaire et proportionné à leur traitement et à la protection de leurs auteurs, des personnes qu'ils visent et des tiers qu'ils mentionnent, en tenant compte des délais d'éventuelles enquêtes complémentaires. Des données relatives aux signalements peuvent toutefois être conservées au-delà de cette durée, à la condition que les personnes physiques concernées n'y soient ni identifiées, ni identifiables.

Il existe plusieurs régimes d'archivage des alertes éthiques :

- **Concernant les alertes non recevables** (alerte n'entrant pas dans le champ d'application, n'ayant pas de caractère sérieux, non étayée, effectuée de mauvaise foi, etc.) : elles sont supprimées dans les meilleurs délais ou archivées et anonymisées.
- **Concernant les alertes recevables :**
 - lorsque le signalement n'est pas suivi d'une procédure disciplinaire ou judiciaire, le groupe Rexel veille à la destruction de tous les éléments du dossier de signalement de nature à permettre l'identification de l'auteur du signalement, ainsi que celles des personnes visées,

dans un délai maximal de deux (2) mois à compter de la clôture des opérations de vérification ou de l'enquête ;

- dans les cas où l'enquête aboutit à une procédure judiciaire ou disciplinaire, les éléments du dossier sont dûment conservés pendant la période nécessaire, jusqu'à acquisition de la prescription (six (6) ans) ou épuisement des voies de recours. Puis, une fois le délai prescrit, ces données sont détruites ou archivées et anonymisées.

5. Confidentialité et sécurité

Le groupe Rexel prend toutes précautions utiles pour préserver la confidentialité et la sécurité des données à l'occasion de leur recueil, de leur traitement, de leur communication ou de leur conservation.

Sous réserve des réglementations locales applicables, les procédures mises en œuvre pour recueillir et traiter les signalements garantissent une stricte confidentialité de l'identité des auteurs du signalement, des personnes visées par celui-ci et des informations recueillies par les personnes chargées du recueil et du traitement du signalement.

A cet égard :

- Les informations communiquées sont limitées aux seules personnes qui ont un besoin légitime d'en connaître pour assurer le traitement de l'alerte.
- Toutes les personnes impliquées dans la gestion des alertes sont formées et astreintes à une obligation de confidentialité. Elles s'engagent notamment, à ne pas utiliser les données à des fins détournées, à respecter la durée de conservation limitée des données conformément à la loi applicable.
- La plateforme de signalement en ligne est sécurisée et les alertes qui y déposées ne peuvent être consultées que par des personnes habilitées. Ce dispositif permet par ailleurs aux collaborateurs qui souhaitent conserver leur anonymat de privilégier ce canal.
- Si la loi l'exige, l'identité du lanceur d'alerte peut être divulguée aux autorités judiciaires.
- Les éléments de nature à identifier la personne mise en cause par un signalement ne peuvent pas être divulgués, sauf à l'autorité judiciaire, qu'une fois établi le caractère fondé de l'alerte.
- Au sein des entités du groupe Rexel, les directions généralement impliquées dans le traitement d'une alerte sont sensibilisées sur le caractère confidentiel de l'identité de l'auteur et des personnes mises en cause.

6. Protection des données à caractère personnel

Dans le cadre du dispositif d'alerte, le groupe Rexel peut être amené à collecter et traiter des données à caractère personnel, notamment celles relatives à l'auteur d'un signalement et à la ou les personne(s) mise(s) en cause. Une notice d'information précise en annexe 4 les conditions dans lesquelles les données sont collectées, traitées, conservées et archivées.

V. Reporting

La Direction Conformité groupe reporte une fois par an le nombre d'alertes, leur type, et les actions prises suite à leur réception, en se limitant aux données strictement nécessaires et proportionnées au regard de la justification de la communication.

VI. Mise à jour de la procédure

Le groupe Rexel se réserve le droit de modifier, compléter ou actualiser la présente procédure à tout moment afin de l'adapter aux évolutions législatives, réglementaires, jurisprudentielles, ou aux besoins internes du groupe. Toute mise à jour sera effectuée dans le respect des lois et règles locales applicables.

Les collaborateurs, fournisseurs et autres parties prenantes concernés seront informés des changements selon des modalités adaptées (communication interne, courrier électronique, publication intranet, information directe aux fournisseurs, etc.), conformément aux exigences légales locales.

La version à jour et faisant foi de la présente procédure sera publiée et accessible sur les sites internet du groupe Rexel, sur l'intranet du groupe et sur la plateforme de signalement en ligne.

Contact

Société : Rexel Développement

Adresse : 13 boulevard Fort de Vaux 75017 Paris (France) – *A l'attention de la Direction Conformité groupe.*

Adresse email : compliance@rexel.com

Lancer l'alerte

Si vous suspectez ou avez connaissance d'un fait contraire à la loi, au Guide d'Éthique, ou au Code de conduite anti-corruption, signalez-le !



Qui peut lancer une alerte ?

Tous les collaborateurs et les tiers du groupe peuvent utiliser la ligne d'alerte.



Quand lancer l'alerte ?

Quand vous avez connaissance ou suspectez une **violation des lois ou de nos principes éthiques**.

Ce peut être :

- des faits de corruption ;
- une violation des droits humains ;
- des faits de harcèlement ou de discrimination ;
- une fraude, etc.



Est-ce confidentiel ?

Oui et vous pouvez également lancer une alerte de manière **anonyme**



Suis-je protégé.e ?

Vous devez lancer l'alerte de bonne foi et sans contrepartie financière directe.
Dans ce cas, vous êtes protégé.e.



Comment lancer une alerte

1. Utilisez la **ligne d'alerte éthique** en ligne (voir *le lien ci-après*)
 - accessible 24h/24 et 7j/7 ;
 - disponible dans toutes les langues principales du groupe.
2. Utilisez le **dispositif d'alerte mis en place localement**.
3. Contactez la **Direction Juridique ou Conformité** ou la **Direction des Ressources humaines** (groupe ou local)



Qui traite cette alerte ?

Pour le groupe : le Comité Éthique.
Pour le dispositif local : voir procédure locale.

Aller plus loin

Rendez-vous sur :
<https://www.rexel.com/fr/alerte-ethique/>

Annexe 2 : Liste des pays avec une procédure d'alerte locale

Cette procédure est complétée dans certains pays par des procédures locales, qui définissent les exigences légales applicables et, le cas échéant, les canaux disponibles localement.

Les informations relatives aux canaux locaux sont répertoriées ci-dessous. Veuillez consulter la procédure locale pour obtenir les informations les plus récentes.

- Australie :

o Service de divulgation Rexel STOPline (géré par un prestataire de services externe indépendant) :

Téléphone : 1300 30 45 50

Fax : Rexel Holdings Australia (C/- the STOPline) 03 9882 4480

E-mail : rexel@stopline.com.au

En ligne : <https://rexel.stoplينereport.com/>

Courrier : Rexel Holdings Australia

C/- the STOPline

Locked Bag 8

HAWTHORN VIC 3122

- Canada : vous pouvez contacter le Comité éthique.

- Allemagne :

o E-mail : whistleblowing@rexel.de

o Courrier :

Rexel Germany GmbH & Co.

KG - z. Hd. Frau Nicole Steuer | General Counsel

Ridlerstr.5780339 München

- Irlande

o Vous pouvez contacter le service des ressources humaines, le responsable des signalements, le directeur général ou notre hotline externe dédiée aux signalements, gérée par Safecall.

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- Italie :

o <https://report.whistleb.com/rexel>

- Pays-Bas : vous pouvez contacter le correspondant éthique.

- Suède :

o <https://whistleblow.vismadraftit.se/rexel-sverige-ab>

o Téléphone : 08-556 214 14.

- Royaume-Uni

o Vous pouvez contacter le service des ressources humaines, le responsable des signalements, le directeur général ou notre service d'assistance téléphonique externe géré par Safecall.

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- États-Unis

o E-mail dédié à la conformité : ethics@rexelusa.com

o Ligne d'assistance dédiée à la conformité : 1-800-714-8774

Annexe 3 : Exemples de comportements ou manquements visés par la procédure d'alerte

Catégories	Périmètre
Corruption	Dans le cadre des lois et réglementations locales applicables et des politiques du groupe relatives à la lutte contre la corruption : la corruption désigne le fait d'échanger, directement ou par l'intermédiaire de tiers, des avantages (argent, cadeaux, invitations, services, relations, etc.) contre l'accomplissement ou l'abstention d'un acte lié à une fonction ou à un mandat. Elle peut prendre la forme d'une personne qui propose ou offre un avantage pour obtenir une faveur (corruption active) ou d'une personne qui sollicite ou accepte un avantage en retour d'un service (corruption passive). La corruption peut concerner tant des acteurs publics que privés, fausse la concurrence, nuit à la transparence des décisions et expose les personnes et organisations impliquées à des sanctions et à des poursuites.
Harcèlement	Le harcèlement désigne des comportements répétés ou un acte isolé grave qui portent atteinte à la dignité, à la sécurité ou aux conditions de travail d'une personne. Il se manifeste par des propos, des gestes, des attitudes ou des actions visant à intimider, humilier, isoler, menacer ou dégrader la situation d'un collaborateur ou d'un tiers en lien avec l'activité professionnelle. Le harcèlement peut prendre une forme morale : par exemple des remarques dénigrantes, l'isolement volontaire, la surcharge ou la privation de moyens de travail, la mise à l'écart, la diffusion de rumeurs ou la dévalorisation systématique. Il peut également revêtir une forme à connotation sexuelle. Le harcèlement sexuel se caractérise par des comportements ou des propos à connotation sexuelle non désirés, répétés ou constituant un acte isolé grave, qui portent atteinte à la dignité de la personne ou créent un environnement de travail intimidant, hostile, dégradant ou humiliant. Cela comprend, entre autres, des avances insistantes, des commentaires sur le corps, des demandes de faveurs sexuelles, des gestes ou contacts physiques non consentis, ou la diffusion d'images à caractère sexuel sans consentement. Le harcèlement, qu'il soit moral ou sexuel, est inacceptable et engage la responsabilité des auteurs conformément aux lois locales applicables.

Discrimination	La discrimination au travail vise à traiter défavorablement une personne en se fondant sur un critère interdit par la loi. Il existe plusieurs critères de discrimination prohibés par la loi tels que l'origine, le sexe, la situation de famille (...) ou toute autre caractéristique protégée par la loi locale. La discrimination peut par exemple avoir pour conséquences une inégalité de traitement dans l'accès à l'emploi, aux conditions de travail, à la formation, à la mobilité ou à toute autre situation liée à l'activité professionnelle. Elle peut se traduire par des décisions de recrutement, d'évaluation, de promotion, d'affectation ou de licenciement qui désavantagent une personne sans justification objective fondée sur les exigences du poste. Au sein d'une entreprise, la discrimination peut prendre 2 formes : Discrimination directe. Dans ce cas, l'auteur des faits prend volontairement une décision en fonction d'un critère discriminatoire interdit par la loi. Discrimination indirecte. Dans cette hypothèse, l'auteur prend une décision qui paraît neutre mais qui, finalement, désavantage certaines personnes par rapport à d'autres. Par exemple, un règlement intérieur autorise uniquement les hommes à rester dans l'entreprise après 50 ans. Il y a donc une discrimination indirecte basée sur le sexe et sur l'âge.
Santé/Sécurité	Toute atteinte ou risque sérieux portés à la santé et la sécurité au travail. La santé et la sécurité au travail désignent l'ensemble des mesures et pratiques visant à protéger l'intégrité physique et mentale des personnes sur leur lieu de travail, en réduisant les risques d'accidents, de blessures et de maladies professionnelles. Cela comprend l'identification et l'évaluation des risques, la mise en place de protections techniques et organisationnelles, la formation et l'information des collaborateurs, ainsi que les dispositifs de prévention, d'intervention et de secours. Le respect de ces obligations contribue à un environnement de travail sûr et conforme aux exigences locales.
Droits Humains (autres que discrimination et harcèlement)	Toute atteinte ou risque sérieux portés aux droits humains et libertés fondamentales reconnus au niveau national et international, ainsi que toute violation des exigences locales applicables en la matière. Il s'agit notamment, de façon non exhaustive, de situations mettant en cause des principes tels que le respect des libertés d'association et d'expression, l'accès à des conditions de travail décentes et sûres, et la possibilité pour les personnes concernées d'accéder à des voies de recours.

Conflits d'intérêts	Un conflit d'intérêts est une situation dans laquelle les intérêts personnels d'une personne, financiers, familiaux, amicaux, politiques ou liés à d'autres avantages, sont susceptibles d'influencer, ou de donner l'apparence d'influencer, son jugement ou ses décisions dans le cadre de ses missions au sein du groupe Rexel. Il ne s'agit pas nécessairement d'une faute ou d'un acte illégal, mais d'un risque de biais qui compromet l'impartialité attendue. Ce risque peut suffire à affaiblir la confiance des personnes concernées, altérer la qualité des décisions et nuire à la réputation de l'organisation. Un conflit d'intérêts peut être actuel (déjà présent), potentiel (susceptible de survenir) ou apparent (perçu par des tiers). Le dispositif d'alerte n'a pas vocation à se substituer à la procédure de déclaration des conflits d'intérêts définie par le groupe Rexel.
Pratiques anticoncurrentielles	Les pratiques anticoncurrentielles désignent des comportements d'entreprises qui altèrent la libre concurrence et nuisent aux autres acteurs du marché (clients, fournisseurs, concurrents). Elles couvrent notamment les accords entre concurrents, formels ou informels, visant à coordonner les prix, les conditions commerciales, la répartition de marchés, de territoires ou de produits, ou encore à limiter l'offre ou à boycotter certains partenaires. Elles incluent aussi les situations d'abus de position dominante (par exemple évincer un rival, imposer des prix prédateurs ou des ventes liées injustifiées), l'influence sur le prix de revente pratiqué par des distributeurs, ainsi que l'échange d'informations stratégiques non publiques susceptibles d'orienter le comportement de marché (telles que plans, données marketing ou capacités). Ces pratiques sont interdites par les règles de concurrence et exposent à des sanctions importantes.
Environnement	Toute situation où les exigences environnementales applicables ne sont pas respectées, un risque ou un dommage significatif à l'environnement est identifié, que ce soit au sein de l'entreprise ou chez ses partenaires de la chaîne de valeur. Cela vise la prévention de la pollution, l'usage responsable des ressources et la gestion sûre des substances et déchets, conformément aux obligations réglementaires et aux standards internes.
Fraude	Toute situation impliquant la dissimulation, la tromperie ou la manipulation destinée à obtenir un avantage indu ou à éluder des obligations, qu'elle soit fiscale, financière ou comptable. Cela inclut, par exemple, la falsification de documents ou d'écritures, la présentation inexacte d'informations financières, la dissimulation de revenus ou d'actifs, ou tout schéma visant à contourner les règles applicables, au sein de l'entreprise ou dans sa chaîne de valeur.

Délit d'initié	Le délit d'initié est le fait d'acheter, vendre ou recommander des instruments financiers en utilisant, ou en se fondant sur, une information privilégiée non publique concernant un émetteur ou ses titres. Il inclut aussi la communication illégale de cette information à des tiers. Ces comportements confèrent un avantage indu sur les marchés et sont strictement interdits et sanctionnés.
Emplois fictifs	Un emploi fictif est une situation où une personne est rémunérée pour un poste ou des missions qui ne sont pas réellement exercés, ou qui n'existent pas, afin d'obtenir un avantage indu. Cela peut impliquer l'absence totale de travail effectif, des fonctions factices, ou l'affectation nominale à un service sans contribution réelle, au sein de l'entreprise ou via des tiers.
Protection des données à caractère personnel / Sécurité informatique	Toute situation où des données à caractère personnel ou des systèmes informatiques ne sont pas protégés conformément aux lois et aux règles internes, exposant des personnes ou l'entreprise à un risque d'accès, d'usage, de divulgation, de modification ou de destruction non autorisés. Cela couvre la collecte et le traitement licites et minimisés des données, la sécurité des systèmes (contrôles d'accès, chiffrement, sauvegardes), la gestion des incidents et des violations, ainsi que la confidentialité et l'intégrité des informations tout au long de leur cycle de vie, y compris chez les prestataires. Une donnée personnelle correspond à toute information permettant d'identifier directement ou indirectement une personne physique (par exemple nom, coordonnées, identifiants, photo, données de localisation ou d'autres éléments relatifs à son identité ou sa vie personnelle).

POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES

DISPOSITIF D'ALERTE

Version 12/2025

Le groupe Rexel a mis en œuvre un dispositif d'alerte professionnelle permettant à ses collaborateurs ainsi qu'aux tiers avec lesquels le groupe Rexel est en relation de signaler des faits ou des comportements contraires à la loi. Les domaines couverts par le dispositif sont détaillés dans la Procédure de recueil et de traitement de l'alerte éthique disponible sur le site internet rexel.com.

 Dans le cadre de ce dispositif, le groupe Rexel peut être amené à collecter et traiter des données qui vous concernent. La confidentialité des données est le fondement de notre relation de confiance. Par conséquent, nous prenons la protection de vos données personnelles au sérieux lorsque nous exerçons nos activités.

La présente politique vous est communiquée afin que vous puissiez prendre connaissance des engagements du groupe Rexel, en matière de protection des données personnelles. Les informations suivantes vous permettent également de connaître les droits dont vous disposez, ainsi que les conditions dans lesquelles vos données à caractère personnel sont collectées, traitées, conservées et archivées.

Qui sommes-nous ?

La société REXEL DEVELOPPEMENT SAS, société par actions simplifiée de droit français, dont le siège social est sis 13, Boulevard du Fort de Vaux, Paris, immatriculée auprès du Registre du commerce et des sociétés de Paris sous le numéro 480 172 840 est responsable de traitement.

L'entité du Groupe qui a un contrat de travail ou collabore avec l'auteur du signalement est également responsable de traitement.

Ils déterminent les finalités et les moyens du traitement de vos données.

Ils sont désignés dans la présente politique par « Rexel », « nous », ou « Responsables de traitement ».

EY Poland agit en qualité de sous-traitant des traitements réalisés sur la plateforme d'alerte en ligne.

Comment traitons-nous vos données dans le cadre du dispositif d’alerte ?

Le tableau ci-dessous détaille :

- (i) pourquoi nous traitons vos données personnelles,
- (ii) quels types de données nous traitons et,
- (iii) quelle est la base légale du traitement de vos données.

Finalités poursuivie 1	Type de données
Recueillir et traiter les alertes visant à signaler des faits contraires à la loi ou au Code de conduite anti-corruption couverts par le dispositif d’alerte (voir la Procédure de recueil et de traitement de l’alerte éthique) <u>Sous-finalités :</u> - Gestion centralisée des signalements professionnels (réception et traitements des alertes, mise en place d’un canal sécurisé, stockage et conservation des informations, sécurisation) - Instruction des signalements professionnels (réalisation d’enquêtes internes, évaluation des faits concernés) - Prise de décision et mise en œuvre de mesures appropriées à la clôture du signalement (information et mise en œuvre des mesures) - Suivi statistiques et amélioration du dispositif d’alerte - Exercer ou défendre des droits en justice.	Dans le cadre du dispositif, les catégories de données ci-dessous peuvent être traitées : - Données identifiantes (nom et prénom, coordonnées), données professionnelles (fonction, employeur, lieu de travail) de l’auteur du signalement (sauf si alerte anonyme) et toute autre information transmise volontairement par lui - Données identifiantes (nom et prénom, coordonnées), données professionnelles (fonction, employeur, lieu de travail) des personnes mises en cause - Données identifiantes (nom et prénom, adresse mail), données professionnelles (fonction, employeur, lieu de travail) des personnes intervenant ou consultées dans le recueil ou le traitement de l’alerte et des facilitateurs et personnes en lien avec l’auteur du signalement - Données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données de santé, vie sexuelle ou orientation sexuelle) en cas de stricte nécessité afin d’exercer ou défendre des droits en justice (article 9.2.f du RGPD) ou pour des motifs d’intérêts public important (article 9.2.g du RGPD) - Données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexe en cas de stricte nécessité et dans le respect de l’article 10 du RGPD - Eléments recueillis dans le cadre de la vérification des faits - Comptes-rendus des opérations de vérification - Données relatives aux suites données au signalement

Base légale du traitement de vos données

Obligation légale de mettre en œuvre un dispositif d’alerte : notamment articles 8.I.B et 17 II de la loi dite Sapin II et l'article L. 225-102-4 du code de commerce ainsi que toute loi équivalente en matière de protection des lanceurs d’alerte, de lutte contre la corruption ou répondant au devoir de vigilance.

Finalité poursuivie 2	Type de données
Recueillir et traiter les alertes visant à signaler des faits contraires au Guide d’Ethique <u>Sous-finalités :</u> - Gestion centralisée des signalements professionnels (réception et traitements des alertes, mise en place d’un canal sécurisé, stockage et conservation des informations, sécurisation) - Instruction des signalements professionnels (réalisation d’enquêtes internes, évaluation des faits concernés) - Prise de décision et mise en œuvre de mesures appropriées à la clôture du signalement (information et mise en œuvre des mesures) - Suivi statistiques et amélioration du dispositif d’alerte. - Exercer ou défendre des droits en justice	Dans le cadre du dispositif, les catégories de données ci-dessous peuvent être traitées : - Données identifiantes (nom et prénom, coordonnées), données professionnelles (fonction, employeur, lieu de travail) de l’auteur du signalement (sauf si alerte anonyme) et toute autre information transmise volontairement par lui - Données identifiantes (nom et prénom, coordonnées), données professionnelles (fonction, employeur, lieu de travail) des personnes mises en cause - Données identifiantes (nom et prénom, adresse mail), données professionnelles (fonction, employeur, lieu de travail) des personnes intervenant ou consultées dans le recueil ou le traitement de l’alerte et des facilitateurs et personnes en lien avec l’auteur du signalement - Données sensibles (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données de santé, vie sexuelle ou orientation sexuelle) en cas de stricte nécessité afin d’exercer ou défendre des droits en justice (article 9.2.f du RGPD) ou pour des motifs d’intérêts public important (article 9.2.g du RGPD) - Données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexe en cas de stricte nécessité et dans le respect de l’article 10 du RGPD - Eléments recueillis dans le cadre de la vérification des faits - Comptes-rendus des opérations de vérification - Données relatives aux suites données au signalement
Base légale du traitement de vos données Intérêt légitime à traiter les alertes éthiques non couvertes par une obligation légale	

Qui sont les destinataires de vos données ?



Les données à caractère personnel que nous collectons, de même que celles qui sont recueillies ultérieurement, nous sont destinées en notre qualité de responsable de traitement.



Nous veillons à ce que seules les personnes habilitées puissent avoir accès à ces données.

En interne :

- Les personnes en charge du recueil et du traitement des alertes, à savoir :
 - Les membres du Comité Ethique du groupe Rexel
 - Les membres habilités de la Direction juridique ou conformité au niveau Groupe et local
 - Les membres habilités de la Direction des Ressources Humaines au niveau Groupe et local
- Les personnes habilitées de la Direction de l’audit et du contrôle interne au niveau Groupe et local afin de garantir l’efficacité des contrôles internes et de la gouvernance
- Lorsque la situation le justifie, d’autres personnes internes peuvent avoir accès aux données, notamment en cas de besoin d’expertise comptable, financière, juridique, technique ou informatique.

En externe :

- Nos conseils
- Nos courtiers et assureurs
- Nos commissaires aux comptes
- Les autorités compétentes (judiciaires, administratives et organismes de réglementation), conformément à la réglementation applicable
- Nos prestataires de services, et plus particulièrement EY Poland qui met à notre disposition la plateforme de signalement en ligne.

Ces destinataires sont situés dans l’Union Européenne.

Combien de temps conservons-nous vos données ?

Situations	Durée de conservation
Alertes non recevable (n’entrant pas dans le champ d’application, n’ayant pas de caractère sérieux, manquant d’informations, faite de mauvaise foi, etc.)	Suppression ou archivage et anonymisation dans les meilleurs délais
Alerte recevable mais classée sans suite (non suivie d’une procédure disciplinaire ou judiciaire)	Suppression ou anonymisation et archivage dans le délai de deux (2) mois
Alerte donnant lieu à une procédure disciplinaire ou judiciaire	Conservation des données jusqu’au terme de la procédure et des voies de recours. Passé ce délai, suppression ou anonymisation et archivage.

Quels sont vos droits ?



Conformément à la réglementation sur la protection des données à caractère personnel, vous disposez des droits suivants :

- droit d'accès : vous pouvez accéder aux informations que l'on détient sur vous et en obtenir une copie ;
- droit de rectification : vous pouvez faire modifier, compléter, actualiser, effacer une donnée vous concernant qui serait inexacte ;
- droit d'opposition : vous pouvez vous opposer à ce que nous traitons vos données, sauf s'il existe des motifs légitimes et impérieux pour nous de les traiter ;
- droit à l'effacement : vous pouvez demander à ce que nous effacions les données qui vous concernent dans la limite des conditions de l'article 17 du RGPD ;
- droit à la portabilité de vos données : vous pouvez récupérer les données vous concernant pour les transférer à un autre organisme ou pour un usage personnel ;
- droit à la limitation du traitement ;
- droit de formuler des directives spécifiques et générales concernant la conservation, l'effacement et la communication de vos données post-mortem.

Toute personne faisant l'objet d'un signalement en sera informée dans les meilleurs délais (au plus tard dans un délai d'un mois) suivant l'enregistrement, informatisé ou non, des données la concernant afin de lui permettre d'exercer ses droits. Toutefois, si une telle information est susceptible de compromettre gravement les objectifs du traitement et notamment le déroulement de l'enquête (par exemple en présence d'un risque de destruction de preuves), alors cette information pourra être différée et n'interviendra qu'une fois que tout risque aura été écarté.

La personne qui fait l'objet d'un signalement ne peut en aucun cas obtenir communication du responsable du traitement, sur le fondement de son droit d'accès, des informations concernant l'identité de l'Auteur du Signalement ou de toute autre personne impliquée dans l'enquête

En cas d'absence de réponse ou de réponse que vous estimez insatisfaisante ou si vous estimez que les traitements de vos données ne sont pas conformes aux dispositions légales et réglementaires, vous avez la faculté de saisir la Commission Nationale de l'Informatique et des Libertés (CNIL) : <https://www.cnil.fr/fr/plaintes>

Comment exercer vos droits ?



Par demande écrite auprès de notre Délégué à la Protection des Données :

Pays	Entités	Adresse
Allemagne	REXEL GERMANY BETEILIGUNGS GMBH	Datenschutzbeauftragter@rexel.de
	Rexel Germany GmbH & Co KG	Datenschutzbeauftragter@rexel.de
	REXEL GERMANY VERWALTUNGS GMBH	Datenschutzbeauftragter@rexel.de
Autriche	COMTECH IT-SOLUTIONS GMBH	datenschutz@rexel.at
	Rexel Austria GmbH	datenschutz@rexel.at
Belgique	Rexel Belgique SA	gdpr@rexel.be
France	Cordia	donnees.personnelles@francofa-eurodis.fr
	Rexel Développement SAS / Rexel Group	data.protection@rexel.com
	Rexel France SAS	donnees.personnelles@rexel.fr
	Bizline	data.protection@rexel.com
	Gigamedia	data.protection@rexel.com
	Sofinther SAS	donnees.personnelles@sofinther.fr
	Espace Elec SAS	donnees.personnelles@espace-elec.fr
	Esabora Digital Services SAS	dataprotection-rda@rexel.fr
	Francofa Eurodis	donnees.personnelles@francofa-eurodis.fr
	Freshmile Services SAS	donnees.personnelles@rexel.fr
Italie	ITESA	donnees.personnelles@rexel.fr
	Rexel Italia S.p.A	dataprotection@rexel.it
	Tecno-Bi S.r.l.	dataprotection@rexel.it
Irlande	Comm-Tech S.r.l.	dataprotection@rexel.it
	M. Kelliher 1998	data.protection@rexel.ie
Luxembourg	Rexel Industrial Solutions	data.protection@rexel.ie
Pays-Bas	Rexel Luxembourg SA	gdpr@rexel.be
	Rexel Nederland B.V	AVG@rexel.nl
	Wasco Group B.V.	AVG@rexel.nl
	Wasco Holding B.V.	AVG@rexel.nl
	Wasco Groothandels Greop B.V.	AVG@rexel.nl
	Wasco Distributlecentrum B.V.	AVG@rexel.nl
Royaume-Uni	Rexel (UK) Ltd.	data.protection@rexel.co.uk
Slovenie	Rexel d.o.o.	dpc@rexel.si
Suède	Rexel Sverige AB	dataskydd@rexel.se
Suisse	ELEKTRO-MATERIAL AG	datenschutz@e-m.ch
	Rexel 3S	data.protection@rexel.com



Whistleblowing-Verfahren Dezember 2025_V1

Zusammenfassung

I.	<u>Einleitung</u>	3
1.	<u>Zweck des internen Whistleblowing-Systems</u>	3
2.	<u>Hinweis auf den rechtlichen Rahmen</u>	3
3.	<u>Geltungsbereich</u>	3
II.	<u>Erfassung ethischer Meldungen</u>	4
1.	<u>Voraussetzungen für die Zulässigkeit einer ethischen Meldung</u>	4
	<u>Wer kann eine Meldung einreichen?</u>	4
	<u>Wie können Sie vom Whistleblower-Status und dem damit verbundenen Rechtsschutz profitieren?</u>	4
	<u>Welche Sachverhalte können gemeldet werden?</u>	5
2.	<u>Wie reicht man eine Meldung ein?</u>	6
3.	<u>Inhalt der Meldung</u>	7
4.	<u>Anonyme Meldungen</u>	7
5.	<u>Externe Kanäle</u>	7
III.	<u>Behandlung interner ethischer Meldungen</u>	7
1.	<u>Bestätigung des Eingangs der Meldung</u>	7
2.	<u>Prüfung der Zulässigkeit der Meldung</u>	7
3.	<u>Durchführung der internen Untersuchung</u>	8
4.	<u>Entscheidungsfindung und Abschluss der Untersuchung</u>	9
IV.	<u>Gewährte Schutzmaßnahmen und Garantien</u>	10
1.	<u>Allgemeine Grundsätze</u>	10
2.	<u>Informationen</u>	10
3.	<u>Schutz in Straf-, Zivil- und Sozialangelegenheiten</u>	10
4.	<u>Begrenzte Aufbewahrungsfrist für Daten</u>	11
5.	<u>Vertraulichkeit und Sicherheit</u>	11
6.	<u>Schutz personenbezogener Daten</u>	12
V.	<u>Berichterstattung</u>	12
VI.	<u>Aktualisierung des Verfahrens</u>	12
	<u>Anhang 1: Zusammenfassung</u>	13
	<u>Anhang 2: Liste der Länder mit lokalen Whistleblowing-Verfahren</u>	14
	<u>Anhang 3: Beispiele für Verhaltensweisen oder Fehlverhalten, die unter das Whistleblowing-Verfahren fallen</u>	15

I. Einleitung

1. Zweck des internen Whistleblowing-Systems

Im Rahmen der Ethik- und Compliance-Richtlinien der Rexel-Gruppe, die insbesondere in ihrem Ethikleitfaden, ihrer Charta für verantwortungsbewusste Lieferanten und ihrem Verhaltenskodex zur Korruptionsbekämpfung beschrieben sind, hat die Rexel-Gruppe ein internes Whistleblowing-System eingerichtet.

Das interne Whistleblowing-System der Rexel-Gruppe ermöglicht es allen Mitarbeitern sowie Dritten, mit denen die Rexel-Gruppe in Beziehung steht, Situationen zu melden, die gegen das Gesetz, den Ethikleitfaden der Rexel-Gruppe oder ihren Verhaltenskodex zur Korruptionsbekämpfung verstoßen.

Der Zweck dieses Verfahrens besteht darin, den Prozess zur Erfassung und Bearbeitung von ethischen Meldungen innerhalb der Rexel-Gruppe zu beschreiben.

Eine Zusammenfassung des Verfahrens ist in **Anhang 1** beigefügt.

2. Hinweis zum rechtlichen Rahmen

Da die Holdinggesellschaft der Rexel-Gruppe in Frankreich eingetragen ist, wurde das Verfahren in Übereinstimmung mit den folgenden französischen Gesetzen festgelegt:

- Das Sapin-II-Gesetz vom 9. Dezember 2016 über Transparenz, Korruptionsbekämpfung und wirtschaftliche Modernisierung;
- Das Gesetz vom 27. März 2017 über die Sorgfaltspflicht von Muttergesellschaften und Auftragnehmern;
- Das Gesetz „Waserman“ vom 21. März 2022 zur Verbesserung des Schutzes von Whistleblowern und dessen Durchführungsdekret vom 3. Oktober 2022.

Das Verfahren basiert auch auf einer Reihe von Veröffentlichungen der französischen Antikorruptionsbehörde (AFA) und der französischen Datenschutzbehörde (CNIL):

- Die Empfehlungen der AFA;
- Der praktische Leitfaden „Interne Korruptionsbekämpfungsuntersuchungen“, der im März 2023 von der AFA und der französischen Finanzstaatsanwaltschaft veröffentlicht wurde;
- Das Referenzdokument „Professionelle Warnmeldungen“ der CNIL, das ursprünglich 2019 veröffentlicht und 2023 aktualisiert wurde.

Generell erfolgt die Erfassung und Bearbeitung von Meldungen in Übereinstimmung mit den geltenden Gesetzen und Vorschriften, und dieses Verfahren kann bei Bedarf aktualisiert werden, um gesetzlichen Entwicklungen und bewährten Verfahren Rechnung zu tragen.

Wenn ein lokales Gesetz oder eine lokale Vorschrift strengere Schutzvorschriften für Hinweisgeber vorsieht als dieses Verfahren, haben die lokalen Bestimmungen Vorrang. Wenn dieses Verfahren jedoch strengere Schutzgarantien vorsieht, wird die Rexel-Gruppe diese freiwillig anwenden, soweit dies nach geltendem Recht zulässig ist.

3. Geltungsbereich

Dieses Verfahren soll in allen Unternehmen der Rexel-Gruppe umgesetzt werden. Es wird bei Bedarf geändert, um Änderungen der Gesetze und Vorschriften Rechnung zu tragen.

Dieses Verfahren wird in bestimmten Ländern innerhalb der Rexel-Gruppe durch lokale Verfahren ergänzt. Diese legen die geltenden gesetzlichen Anforderungen und gegebenenfalls die lokal verfügbaren Kanäle fest (siehe **Anhang 2**).

Der Verfasser einer Meldung kann daher den Meldeweg seiner Wahl (konzernweit oder lokal) wählen. Es gilt dann das für den gewählten Meldeweg geltende Verfahren. Je nach Art und Schwere des gemeldeten Verhaltens oder Fehlverhaltens kann eine über den lokalen Meldeweg erfolgte Meldung an den Konzern weitergeleitet werden und umgekehrt.

Dieses Verfahren gilt für alle Mitarbeiter der Rexel-Gruppe (unabhängig von ihrer Funktion, Position oder Abteilung) und für Dritte, mit denen die Rexel-Gruppe in Beziehung steht. Es umfasst die Erfassung und Bearbeitung interner Meldungen durch die Rexel-Gruppe und insbesondere:

- die Einreichung;
- ihren Eingang;
- die Beurteilung ihrer Zulässigkeit;
- die wichtigsten Schritte der internen Untersuchung
- den Abschluss des Falls.

II. Die Sammlung ethischer Warnmeldungen

1. Voraussetzungen für die Zulässigkeit einer ethischen Meldung

Wer kann eine Meldung einreichen?

Das interne Meldesystem der Rexel-Gruppe steht folgenden Personen offen:

- Mitarbeiter der Rexel-Gruppe (Festangestellte, befristet Beschäftigte, Auszubildende, Praktikanten)
- Externe oder befristete Mitarbeiter (Zeitarbeitskräfte, Berater usw.)
- Bewerber
- Ehemalige Mitarbeiter
- Aktionäre, Partner und Stimmrechtsinhaber der Hauptversammlung
- Mitglieder der Verwaltungs-, Exekutiv- oder Aufsichtsorgane
- Alle Mitarbeiter von Drittunternehmen, mit denen die Rexel-Gruppe in Beziehung steht (z. B. Kunden, Lieferanten, Dienstleister usw.).

Das interne Meldesystem steht allen Unternehmen der Rexel-Gruppe offen und ist in den Hauptsprachen der Gruppe verfügbar: Englisch, Deutsch, Chinesisch, Französisch, Italienisch, Niederländisch, Schwedisch und Slowenisch.

Wie können Sie vom Status eines Whistleblowers und dem damit verbundenen Rechtsschutz profitieren?

Um als Whistleblower zu gelten und den gesetzlich vorgesehenen Schutz zu genießen, müssen Sie die gesetzliche Definition eines Whistleblowers erfüllen, d. h. alle folgenden Kriterien erfüllen, sofern das geltende lokale Recht nichts anderes vorsieht:

- Sie müssen eine natürliche Person sein.
- Sie dürfen keine direkte finanzielle Vergütung für die Meldung erhalten.
- Sie müssen in gutem Glauben handeln.
- Wenn die gemeldeten Tatsachen außerhalb eines beruflichen Kontexts erlangt wurden, müssen Sie über persönliche Kenntnis der gemeldeten Tatsachen verfügen.

Welche Tatsachen können gemeldet werden?

Das interne Meldesystem der Rexel-Gruppe ermöglicht die Meldung von Sachverhalten, die unter die folgenden Kategorien von Verhaltensweisen oder Fehlverhalten fallen können:

- Eine Straftat oder ein Vergehen
- Eine Bedrohung oder Schädigung des öffentlichen Interesses
- Verstoß gegen nationale, europäische oder internationale Gesetze und Vorschriften oder versuchte Verschleierung eines solchen Verstoßes
- Verstoß gegen den Ethikleitfaden oder den Verhaltenskodex zur Korruptionsbekämpfung der Rexel-Gruppe oder Situation, die diesen widerspricht
- Erhebliche Risiken im Zusammenhang mit den Aktivitäten der Rexel-Gruppe, die die Menschenrechte, Grundfreiheiten, die Gesundheit und Sicherheit von Menschen oder die Umwelt beeinträchtigen könnten

Beispiele für zu meldende Verhaltensweisen oder Fehlverhalten können sein:

- Korruption, einschließlich Verstößen gegen den Verhaltenskodex zur Korruptionsbekämpfung
- Belästigung (psychisch oder sexuell)
- Diskriminierung
- Gesundheit, Hygiene oder Sicherheit (z. B. Gefährdung der körperlichen oder geistigen Unversehrtheit)
- Menschenrechte (außer Diskriminierung, Verletzung der Privatsphäre und Belästigung)
- Interessenkonflikte
- Wettbewerbswidrige Praktiken
- Umwelt (z. B. Umweltverschmutzung, Abfallwirtschaft)
- Steuerbetrug
- Finanz- oder Bilanzbetrug
- Insiderhandel
- Fiktive Arbeitsplätze
- Personenbezogene Daten/IT-Sicherheit

Anhang 3 veranschaulicht einige dieser Verhaltensweisen oder Verfehlungen.

Meldungen, die sich auf nicht oben aufgeführte Kategorien beziehen, fallen nicht in den Anwendungsbereich dieses Verfahrens. Ebenso sind Tatsachen, Informationen oder Dokumente,

unabhängig von ihrer Form oder ihrem Medium, deren Offenlegung durch die Bestimmungen des Gesetzes über die Geheimhaltung von Informationen () in Bezug auf Staatsgeheimnisse, ärztliche Schweigepflicht, Geheimhaltung von Gerichtsverhandlungen, Geheimhaltung von gerichtlichen Ermittlungen oder Untersuchungen oder Anwaltsgeheimnis (attorney-client privilege) verboten ist, von diesem Verfahren ausgeschlossen. Gegebenenfalls wird der Verfasser der Meldung informiert und an die Personen weitergeleitet, die für die Bearbeitung der gemeldeten Tatsachen zuständig sind.

2. Wie man eine Meldung einreicht

Der Verfasser einer Meldung hat mehrere Möglichkeiten, um Hinweise einzureichen:

- Die Online-Meldeplattform unter: <https://www.rexel.com/en/rexel-group-ethics-alert>;
- Zusätzliche Meldekanäle, die auf Gruppen- oder Länderebene bestehen können.

Es gibt keine Hierarchie zwischen den Kanälen. Der Verfasser einer Meldung kann jeden ihm zur Verfügung stehenden Kanal nutzen.

Unabhängig vom verwendeten Kanal werden die für die Entgegennahme von Meldungen zuständigen Personen im Folgenden als „interne Manager“ bezeichnet.

Die Online-Meldeplattform

Der Verfasser einer Meldung kann über die Online-Meldeplattform unter <https://www.rexel.com/en/rexel-group-ethics-alert> eine Meldung abgeben, auch anonym.

Es handelt sich um eine spezielle, kostenlose Plattform, die rund um die Uhr verfügbar ist.

Sie wird in der Europäischen Union von einem externen Dienstleister (EY) gehostet, der strenge Maßnahmen zur Gewährleistung der Datensicherheit und Vertraulichkeit umsetzt. Es ist zu beachten, dass die Mitarbeiter dieses Dienstleisters nicht an der Bearbeitung von Meldungen beteiligt sind und keinen Zugriff auf die ausgetauschten Informationen haben.

Diese Plattform ermöglicht die direkte Kommunikation mit dem Empfänger der Meldung per Chat. Außerdem kann der Verfasser der Meldung Dokumente zur Untermauerung der Fakten übermitteln.

Der Link zu dieser Plattform ist auf den Websites der Gruppe verfügbar: , <https://www.rexel.com/en/rexel-group-ethics-alert>, und <https://ethique.rexel.com/en/> sowie auf den Intranetseiten der Unternehmen der Rexel-Gruppe.

Zusätzliche Meldewege

Interne Mitarbeiter der Rexel-Gruppe können eine Meldung schriftlich oder mündlich an einen der folgenden internen Manager richten: (i) den lokalen Compliance-Manager (Rechts- oder Compliance-Abteilung), (ii) die lokale Personalabteilung, (iii) die Compliance-Abteilung der Gruppe oder (iv) die Personalabteilung der Gruppe.

Die Personalabteilung (lokal oder Konzern) sammelt in der Regel Meldungen über Verstöße gegen das Arbeitsrecht oder unangemessenes Verhalten am Arbeitsplatz (Belästigung, Diskriminierung, Gesundheit, Hygiene oder Sicherheit usw.).

Der lokale Compliance-Beauftragte oder die Compliance-Abteilung der Gruppe sammelt in der Regel Meldungen über Verstöße gegen das Gesetz, den Ethik-Leitfaden, den Verhaltenskodex zur Korruptionsbekämpfung und die Compliance-Verfahren der Rexel-Gruppe usw.

Wenn eine Meldung mündlich erfolgt, kann sie telefonisch entgegengenommen werden und auf Wunsch der meldenden Person und nach deren Wahl im Rahmen einer Videokonferenz oder eines persönlichen Treffens, das spätestens zwanzig (20) Werktage nach Eingang des Antrags organisiert wird. Mündliche Meldungen werden schriftlich festgehalten.

Die Mitarbeiter können in jedem Fall den Rat ihres direkten oder indirekten Vorgesetzten einholen und ihm ihre Bedenken mitteilen, es sei denn, der Vorgesetzte selbst ist der mutmaßliche Urheber des fraglichen Verhaltens. Wenn sich nach einem solchen Gespräch herausstellt, dass diese Bedenken in den Anwendungsbereich dieses Verfahrens fallen, muss der Vorgesetzte den Mitarbeiter ermutigen, eine Meldung über die oben genannten Kanäle oder durch Kontaktaufnahme mit der lokalen Rechts- oder Compliance-Abteilung oder der lokalen Personalabteilung zu machen.

3. Inhalt der Meldung

Der Verfasser einer Meldung muss die Fakten und Informationen, die Gegenstand seiner Meldung sind, präzise und objektiv darlegen, damit die Meldung bearbeitet werden kann.

Wenn möglich, sollte er seine Meldung durch folgende Angaben untermauern:

- Angabe des Datums/der Daten und des Ortes/der Orte, an dem/denen sich die gemeldeten Tatsachen ereignet haben, der betroffenen Einheit sowie der Identität und Position der beteiligten Person(en);
- eine detaillierte Beschreibung der Fakten mit spezifischen und sachlichen Informationen, die in direktem Zusammenhang mit dem Gegenstand der Meldung stehen, unabhängig von deren Form oder Medium.

4. Anonyme Meldungen

Es ist vorzuziehen, dass der Verfasser einer Meldung sich identifiziert, insbesondere um die Durchführung der Untersuchung zu vereinfachen. Der Verfasser einer Meldung kann sich jedoch dafür entscheiden, eine anonyme Meldung zu machen, wie in der Online-Meldeplattform vorgesehen, vorausgesetzt, dass (i) die Schwere der Tatsachen festgestellt ist und (ii) die Sachverhalte ausreichend detailliert sind.

5. Externe Kanäle

Vorbehaltlich der Einhaltung der geltenden lokalen Vorschriften ist zu beachten, dass der Verfasser einer Meldung auch die Möglichkeit hat, eine externe Meldung an (i) die zuständige Behörde, (ii) den Ombudsmann, (iii) die Justizbehörde oder (iv) jede relevante lokale oder internationale Institution, Stelle oder Behörde zu richten, die für die Entgegennahme solcher Meldungen zuständig ist. Meldende können externe Meldungen entweder direkt bei einer Behörde oder nach Einreichung einer Meldung bei der Rexel-Gruppe einreichen.

III. Behandlung interner ethischer Meldungen

1. Bestätigung des Eingangs der Meldung

Wenn die Meldung über die Online-Meldeplattform oder über herkömmliche Kanäle eingeht, bestätigt der interne Manager (die für die Entgegennahme von Meldungen zuständige Person, wie oben definiert) den Eingang der Meldung innerhalb von sieben (7) Werktagen nach Erhalt.

Die Empfangsbestätigung stellt keine Annahme der Meldung dar.

2. Prüfung der Zulässigkeit der Meldung

Jede eingegangene Meldung wird vom internen Manager einer vorläufigen Analyse unterzogen, um sicherzustellen, dass sie in den Anwendungsbereich des Verfahrens fällt und zulässig ist.

Diese Überprüfung, die eine Kommunikation mit dem Verfasser oder dem Hinweisgeber erforderlich machen kann, konzentriert sich insbesondere auf folgende Punkte:

- **Der Status des Verfassers als „Whistleblower“:** insbesondere, dass er in gutem Glauben und ohne direkte finanzielle Entschädigung zu verlangen handelt;
- **Die Art der Meldung:** dass sie tatsächlich unter eine der Kategorien von Meldungen fällt, die unter das Verfahren fallen;
- **Der Inhalt des Berichts:** Die darin enthaltenen Informationen und Fakten sind objektiv und ausreichend detailliert, um die Einleitung einer Untersuchung zu ermöglichen.
- **Das Vorliegen geschützter Geheimnisse:** Der Bericht darf keine Tatsachen offenlegen, die unter das Verteidigungsgeheimnis, das Arztgeheimnis, das Beratungsgeheimnis, das Ermittlungs- oder Untersuchungsgeheimnis oder das Anwaltsgeheimnis fallen.

Die Entscheidung über die Zulässigkeit trifft der interne Manager. Der Verfasser eines Berichts wird gegebenenfalls über die Unzulässigkeit seines Berichts und die Gründe für diese Entscheidung informiert.

In jedem Fall muss der interne Manager innerhalb von drei (3) Monaten eine erste Antwort geben. Die Rexel-Gruppe ist nicht verpflichtet, die Meldung innerhalb dieser Frist zu bearbeiten, muss jedoch den Verfasser der Meldung über die geplanten oder bereits ergriffenen Maßnahmen zur Bewertung der Gültigkeit der Meldung und zur Behebung der gemeldeten Situation informieren.

Die Meldung wird streng vertraulich behandelt.

Je nach Art und Schwere der gemeldeten Sachverhalte kann die Meldung vom Ethikausschuss der Rexel-Gruppe behandelt werden. Der Ethikausschuss der Rexel-Gruppe ist ein Ad-hoc-Ausschuss, der innerhalb von Rexel Développement eingerichtet wurde und dessen Aufgabe es ist, die schwerwiegendsten Meldungen von Rexel-Mitarbeitern oder Dritten, mit denen Rexel in Beziehung steht, zu bearbeiten.

Der Ethikausschuss der Rexel-Gruppe besteht aus drei ständigen Mitgliedern:

- dem Generalsekretär,
- dem Personalvorstand der Gruppe und
- dem Direktor für Ethik und Compliance

3. Durchführung der internen Untersuchung

Ziele und Verwaltung der internen Untersuchung

Die für die Bearbeitung einer Meldung erforderliche Zeit variiert und hängt von der Komplexität der gemeldeten Sachverhalte und der Art der bereitgestellten Informationen ab.

Das Ziel der internen Untersuchung ist es, die Richtigkeit und Wesentlichkeit der gemeldeten Sachverhalte zu überprüfen. Die Meldung wird mit Methoden (Befragungen, Datensuchen usw.) untersucht, die je nach Kontext und Art des Themas variieren können.

Diese Untersuchung kann durchgeführt werden von:

- (xi) die lokale Personalabteilung;
- (xii) die lokale Compliance- oder Rechtsabteilung;
- (xiii) die Compliance-Abteilung der Gruppe;
- (xiv) die Personalabteilung der Gruppe;
- (xv) dem Ethikausschuss der Rexel-Gruppe, je nach Art und Schwere der gemeldeten Sachverhalte

(im Folgenden als „**Untersuchungsleiter**“ bezeichnet).

In jedem Fall leitet der Untersuchungsleiter die interne Untersuchung der Meldung. Informationen über das Vorliegen und den Inhalt der Meldung werden nur den für die Untersuchung zuständigen Personen in dem unbedingt erforderlichen Umfang mitgeteilt.

Bei einer Meldung garantiert die Rexel-Gruppe die Unabhängigkeit des Untersuchungsprozesses. Vor Einleitung einer internen Untersuchung wird überprüft, dass keine der an der Untersuchung der Meldung beteiligten Personen direkt oder indirekt von den gemeldeten Sachverhalten betroffen ist oder in irgendeiner Weise mit den beteiligten Personen in Verbindung steht. Wird ein Risiko eines Interessenkonflikts festgestellt, wird der betreffende Mitarbeiter unverzüglich aus dem Verfahren entfernt und ersetzt. Dieser Grundsatz der Unabhängigkeit ist integraler Bestandteil des Ethik- und Compliance-Systems von Rexel und soll eine strenge, unparteiische und glaubwürdige Bearbeitung aller eingegangenen Meldungen gewährleisten.

Beschlagnahme von E-Mails, Dokumenten oder Computermedien

Die interne Untersuchung kann die Überprüfung und Verarbeitung von E-Mails oder Computerdaten von einem oder mehreren Mitarbeitern erfordern. Vor der Beschlagnahme oder Sperrung von E-Mail-Konten oder Computerdaten muss der Untersuchungsleiter gemäß den lokalen Verfahren (z. B. beim Ethikausschuss der Gruppe, beim lokalen General Counsel oder beim lokalen Datenschutzbeauftragten) die Genehmigung zur Beschlagnahme und Aufbewahrung dieser E-Mails für Untersuchungszwecke einholen.

Gast-Experte

Wenn es die Situation erfordert, kann der Untersuchungsleiter beschließen, eine oder mehrere Personen einzuladen, ihn im Rahmen der Bearbeitung einer bestimmten Meldung zu unterstützen, insbesondere wenn Fachkenntnisse in den Bereichen Buchhaltung, Finanzen, Technik oder IT erforderlich sind.

Der Untersuchungsleiter kann daher beschließen, sich bei seiner Aufgabe von einem fachkundigen Mitarbeiter von Rexel unterstützen zu lassen, z. B. von der Innenrevision, der Finanzabteilung, der Einkaufsabteilung, einem Länder- oder Zonenmanagementteam oder einer anderen Person innerhalb der Rexel-Gruppe, die der Untersuchungsleiter für kompetent und notwendig hält (), oder von einem entsprechend qualifizierten externen Dienstleister.

Der Auftrag des Experten endet automatisch mit dem Abschluss aller Überprüfungs- oder Bearbeitungsvorgänge im Zusammenhang mit der Meldung, für die der Untersuchungsleiter seine Unterstützung angefordert hat, oder auf einfache Anfrage des Untersuchungsleiters.

Der hinzugezogene Sachverständige unterliegt denselben Vertraulichkeitsverpflichtungen wie der interne Manager und der Untersuchungsleiter.

4. Entscheidungsfindung und Abschluss der Untersuchung

Wenn sich die Tatsachen nicht bestätigen, wird die Meldung geschlossen und der Verfasser der Meldung informiert.

Wenn sich die Tatsachen bestätigen, entscheidet der Untersuchungsleiter auf der Grundlage der Untersuchungsergebnisse, ob Verstöße gegen das Gesetz, den Ethikleitfaden oder den Verhaltenskodex zur Korruptionsbekämpfung vorliegen, und empfiehlt gegebenenfalls Korrekturmaßnahmen und/oder angemessene Sanktionen.

Der Meldende wird schriftlich über den Abschluss der Untersuchung informiert.

Auch die betroffene Person wird über den Abschluss der Untersuchung informiert. Wenn sich nach der Untersuchung herausstellt, dass der Verstoß schwerwiegend und nachgewiesen ist, kann die zuständige Geschäftsleitung je nach Art und Schwere der mutmaßlichen Tatsachen Disziplinarmaßnahmen bis hin zur Entlassung gegen die betroffene Person ergreifen.

IV. Bieteter Schutz und Garantien

1. Allgemeine Grundsätze

Alle Untersuchungen werden fair und unter vollständiger Einhaltung der geltenden lokalen Gesetze und Vorschriften durchgeführt. In allen Fällen stellt die Rexel-Gruppe sicher, dass der Grundsatz der Unschuldsvermutung für die betroffenen Personen gewahrt bleibt.

Das Whistleblowing-System kann nur auf der Grundlage von Informationen funktionieren, die in gutem Glauben bereitgestellt werden. Jede Meldung, die in böser Absicht erfolgt, d. h. mit der alleinigen Absicht, Schaden zu verursachen, kann zu Disziplinarmaßnahmen bis hin zur Entlassung führen.

2. Informationen

Der Hinweisgeber wird innerhalb von sieben (7) Werktagen nach Eingang seiner Meldung informiert.

Innerhalb einer angemessenen Frist von höchstens drei (3) Monaten nach Bestätigung des Eingangs der Meldung wird der Verfasser der Meldung schriftlich über die geplanten oder getroffenen

Maßnahmen zur Überprüfung der Richtigkeit der Vorwürfe und gegebenenfalls zur Behebung des Gegenstands der Meldung sowie über die Gründe für diese Maßnahmen informiert. Sind die Vorwürfe unzutreffend oder unbegründet oder ist die Meldung gegenstandslos geworden, wird der Verfasser der Meldung schriftlich über die Einstellung des Verfahrens informiert.

Jede Person, die von einer zulässigen Meldung betroffen ist, wird über die Art der sie betreffenden Vorwürfe informiert. Sind jedoch Vorsichtsmaßnahmen erforderlich, um die Vernichtung von Beweismitteln im Zusammenhang mit der Meldung zu verhindern, wird die von der Meldung betroffene Person erst nach Ergreifen dieser Maßnahmen gemäß den geltenden Gesetzen informiert.

Die von einer Meldung betroffene Person kann unter keinen Umständen auf der Grundlage ihres Auskunftsrechts von der Rexel-Gruppe die Identität der Person erfahren, die die Meldung gemacht hat.

Es wird darauf hingewiesen, dass der Umfang der bereitgestellten Informationen je nach den geltenden lokalen Gesetzen variieren kann.

3. Schutz in strafrechtlichen, zivilrechtlichen und sozialen Angelegenheiten

Whistleblower werden darauf hingewiesen, dass vorbehaltlich der lokal geltenden Vorschriften

- Sie haften nicht zivilrechtlich für Schäden, die durch ihre Meldung oder Offenlegung verursacht wurden, vorausgesetzt, dass ihre Meldung in Übereinstimmung mit den geltenden Bestimmungen erfolgte und dass der Verfasser der Meldung zum Zeitpunkt der Meldung berechnete Gründe zu der Annahme hatte, dass die Meldung oder die öffentliche Offenlegung aller dieser Informationen zum Schutz der betroffenen Interessen erforderlich war.
- Sie sind nicht strafrechtlich haftbar für den Erhalt oder den Zugriff auf Informationen, die öffentlich gemeldet oder offengelegt werden, sofern dieser Erhalt oder Zugriff nach den vor Ort geltenden Vorschriften keine separate Straftat darstellt. Wenn dieser Erhalt oder Zugriff eine separate Straftat darstellt, gelten die vor Ort geltenden Vorschriften zur strafrechtlichen Haftung.
- Sie dürfen nicht bestraft, entlassen, diskriminiert (insbesondere in Bezug auf Vergütung, Fortbildung, Beförderung) oder Repressalien oder der Androhung oder dem Versuch der Anwendung solcher Maßnahmen ausgesetzt werden, weil sie Informationen gemäß den Vorschriften gemeldet oder offengelegt haben, sofern die Meldung in gutem Glauben erfolgte.

Unter denselben Bedingungen dürfen Personen, die die Meldung eines Whistleblowers unterstützt haben oder mit ihm in Verbindung stehen, keinen Vergeltungsmaßnahmen, Drohungen oder Versuchen, solche Maßnahmen zu ergreifen, ausgesetzt werden.

Die Rexel-Gruppe toleriert keinerlei Form von Vergeltungsmaßnahmen, Drohungen oder Versuchen, solche Maßnahmen gegen Whistleblower und ihre Angehörigen, wie z. B. Belästigungen, zu ergreifen.

4. Begrenzte Aufbewahrungsfrist für Daten

Meldungen dürfen nur so lange aufbewahrt werden, wie dies für ihre Bearbeitung und den Schutz ihrer Verfasser, der betroffenen Personen und der von ihnen genannten Dritten unter Berücksichtigung der für zusätzliche Untersuchungen erforderlichen Zeit unbedingt erforderlich und verhältnismäßig ist. Daten im Zusammenhang mit Meldungen können jedoch über diesen Zeitraum hinaus aufbewahrt werden, sofern die betroffenen Personen weder identifiziert noch identifizierbar sind.

Es gibt mehrere Systeme zur Archivierung von ethischen Meldungen:

- **Unzulässige Meldungen** (Meldungen, die nicht in den Anwendungsbereich fallen, nicht schwerwiegend sind, unbegründet sind, in böser Absicht gemacht wurden usw.): Diese werden so schnell wie möglich gelöscht oder archiviert und anonymisiert.
- **Für zulässige Meldungen:**
 - Wenn auf die Meldung keine Disziplinar- oder Gerichtsverfahren folgen, stellt die Rexel-Gruppe sicher, dass alle Elemente der Meldungsakte, die Rückschlüsse auf die Identität des Meldenden sowie der betroffenen Personen zulassen, innerhalb einer Frist von maximal zwei (2) Monaten nach Abschluss der Überprüfungs- oder Ermittlungsmaßnahmen vernichtet werden.
 - Führt die Untersuchung zu einem Gerichtsverfahren oder zu Disziplinarmaßnahmen, werden die Elemente der Akte für den erforderlichen Zeitraum bis zum Ablauf der Verjährungsfrist (sechs (6) Jahre) oder bis zum Ausschöpfung aller Rechtsmittel ordnungsgemäß aufbewahrt. Nach Ablauf der vorgeschriebenen Frist werden diese Daten vernichtet oder archiviert und anonymisiert.

5. Vertraulichkeits- und Sicherheits

Die Rexel-Gruppe trifft alle erforderlichen Vorkehrungen, um die Vertraulichkeit und Sicherheit der Daten während ihrer Erhebung, Verarbeitung, Übermittlung oder Speicherung zu gewährleisten.

Vorbehaltlich lokal geltender Vorschriften gewährleisten die zur Erfassung und Bearbeitung von Meldungen implementierten Verfahren strenge Vertraulichkeit hinsichtlich der Identität der Verfasser der Meldung, der Personen, auf die sich die Meldung bezieht, und der von den für die Erfassung und Bearbeitung der Meldung zuständigen Personen gesammelten Informationen.

In diesem Zusammenhang gilt Folgendes:

- Die weitergegebenen Informationen sind auf diejenigen Personen beschränkt, die ein berechtigtes Interesse an der Kenntnis dieser Informationen haben, um die Meldung bearbeiten zu können.
- Alle an der Bearbeitung von Meldungen beteiligten Personen sind geschult und unterliegen der Geheimhaltungspflicht. Insbesondere verpflichten sie sich, die Daten nicht für unzulässige Zwecke zu verwenden und die begrenzte Aufbewahrungsfrist für Daten gemäß geltendem Recht einzuhalten.
- Die Online-Meldeplattform ist sicher und die dort eingereichten Meldungen können nur von autorisierten Personen eingesehen werden. Dieses System ermöglicht es auch Mitarbeitern, die anonym bleiben möchten, diesen Kanal zu nutzen.
- Die Identität von Hinweisgebern kann den Justizbehörden offengelegt werden, wenn dies gesetzlich vorgeschrieben ist.

- Informationen, die Rückschlüsse auf die Identität der in einer Meldung genannten Person zulassen, dürfen nicht weitergegeben werden, außer an die Justizbehörden, sobald die Gültigkeit der Meldung festgestellt wurde.
- Innerhalb der Unternehmen der Rexel-Gruppe sind sich die Abteilungen, die in der Regel mit der Bearbeitung von Meldungen befasst sind, der Vertraulichkeit der Identität des Verfassers und der betroffenen Personen bewusst.

6. Schutz personenbezogener Daten

Im Rahmen des Whistleblowing-Systems kann die Rexel-Gruppe personenbezogene Daten erheben und verarbeiten, insbesondere Daten, die sich auf den Verfasser einer Meldung und die betroffene(n) Person(en) beziehen. Eine detaillierte Informationsmitteilung in **Anhang 4** legt die Bedingungen fest, unter denen Daten erhoben, verarbeitet, gespeichert und archiviert werden.

V. Berichterstattung

Die Compliance-Abteilung der Gruppe berichtet einmal jährlich über die Anzahl der Meldungen, deren Art und die nach ihrem Eingang ergriffenen Maßnahmen, wobei sie sich auf Daten beschränkt, die für die Begründung der Mitteilung unbedingt erforderlich und verhältnismäßig sind.

VI. Aktualisierung des Verfahrens

Die Rexel-Gruppe behält sich das Recht vor, dieses Verfahren jederzeit zu ändern, zu ergänzen oder zu aktualisieren, um es an Änderungen der Gesetzgebung, der Vorschriften, der Rechtsprechung oder der internen Anforderungen der Gruppe anzupassen. Alle Aktualisierungen erfolgen in Übereinstimmung mit den geltenden lokalen Gesetzen und Vorschriften.

Die betroffenen Mitarbeiter, Lieferanten und anderen Interessengruppen werden über die Änderungen in geeigneter Weise (interne Kommunikation, E-Mail, Veröffentlichung im Intranet, direkte Information der Lieferanten usw.) gemäß den lokalen gesetzlichen Bestimmungen informiert.

Die aktuelle und verbindliche Fassung dieses Verfahrens wird auf den Websites der Rexel-Gruppe, im Intranet der Gruppe und auf der Online-Berichtsplattform veröffentlicht und zur Verfügung gestellt.

Kontakt

Unternehmen: Rexel Développement

Adresse: 13 boulevard Fort de Vaux 75017 Paris (Frankreich) – *Zu Händen der Compliance-Abteilung der Gruppe.*

E-Mail-Adresse: compliance@rexel.com

Eine Situation melden

Wenn Sie einen Verdacht haben oder Kenntnis von einem Verstoß gegen das Gesetz, den Ethik-Leitfaden oder des Verhaltenskodexes zur Korruptionsbekämpfung, melden Sie dies!



01. Wer kann einen Alarm auslösen?

Alle Mitarbeiter der Gruppe und Dritte können die Ethik-Hotline nutzen.



02. Wann sollte eine Meldung erfolgen?

oder einen Verdacht auf einen **Verstoß gegen das Gesetz oder unserer ethischen Grundsätze.**

- Dazu können gehören:
- Korruptionshandlungen;
 - Menschenrechtsverletzungen;
 - Belästigung oder Diskriminierung;
 - Betrug usw.



03. Ist es vertraulich?

Ja, und Sie können auch eine **anonyme** Meldung senden



04. Bin ich geschützt?

Sie müssen die Warnung in gutem Glauben und ohne direkte finanzielle Entschädigung. In diesem Fall sind Sie geschützt.



05. Wer bearbeitet diese Warnmeldung?

Für die Gruppe: den Ethikausschuss.
Für das lokale System: siehe lokales Verfahren.



Weitere

Besuchen Sie :
<https://www.rexel.com/en/ethical-alert/>

Anhang 2: Liste der Länder mit lokalen Whistleblowing-Verfahren

Dieses Verfahren wird in bestimmten Ländern durch lokale Verfahren ergänzt, in denen die geltenden gesetzlichen Anforderungen und gegebenenfalls die lokal verfügbaren Kanäle festgelegt sind.

Informationen zu den lokalen Kanälen finden Sie unten. Die aktuellsten Details entnehmen Sie bitte dem lokalen Verfahren.

- Australien:

o Rexel STOPline-Offenlegungsdienst (betrieben von einem unabhängigen externen Dienstleister):

Telefon: 1300 30 45 50

Fax: Rexel Holdings Australia (C/- the STOPline) 03 9882 4480

E-Mail: rexel@stopline.com.au

Online: <https://rexel.stoplينereport.com/>

Post: Rexel Holdings Australia

C/- the STOPline

Locked Bag 8

HAWTHORN VIC 3122

- Kanada: Sie können sich an den Ethikausschuss wenden.

- Deutschland:

o E-Mail: whistleblowing@rexel.de

o Post:

Rexel Germany GmbH & Co.

KG - z. Hd. Frau Nicole Steuer | General Counsel

Ridlerstr. 5780339 München

- Irland

o Sie können sich an die Personalabteilung, den Whistleblowing Officer, den Chief Executive Officer oder unsere externe Whistleblower-Hotline wenden, die von Safecall betrieben wird.

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- Italien:

o <https://report.whistleb.com/rexel>

- Niederlande: Sie können sich an den Ethikbeauftragten.

- Schweden:

o <https://whistleblow.vismadraftit.se/rexel-sverige-ab>

o Telefon: 08-556 214 14.

- Vereinigtes Königreich

o Sie können sich an die Personalabteilung, den Whistleblowing Officer, den Chief Executive Officer oder unsere externe Whistleblower-Hotline wenden, die von Safecall betrieben wird.

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- USA

o Compliance-E-Mail: ethics@rexelusa.com

o Compliance-Helpline: 1-800-714-8774

Anhang 3: Beispiele für Verhaltensweisen oder Fehlverhalten, die unter das Whistleblowing-Verfahren fallen

Kategorien	Geltungsbereich
Korruption	Im Rahmen der geltenden lokalen Gesetze und Vorschriften sowie der Antikorruptionsrichtlinien der Gruppe: Korruption bezeichnet den direkten oder über einen Dritten erfolgenden Austausch von Vorteilen (Geld, Geschenke, Einladungen, Dienstleistungen, Beziehungen usw.) als Gegenleistung für die Vornahme oder Unterlassung einer Handlung im Zusammenhang mit einer Funktion oder einem Auftrag. Dies kann in Form eines Vorteils geschehen, den eine Person anbietet oder verspricht, um eine Gegenleistung zu erhalten (aktive Korruption), oder in Form eines Vorteils, den eine Person als Gegenleistung für eine Dienstleistung fordert oder annimmt (passive Korruption). Korruption kann sowohl öffentliche als auch private Akteure betreffen, verzerrt den Wettbewerb, untergräbt die Transparenz von Entscheidungen und setzt die beteiligten Personen und Organisationen Sanktionen und Strafverfolgung aus.
Belästigung	Belästigung bezeichnet wiederholtes Verhalten oder eine einzelne schwerwiegende Handlung, die die Würde, Sicherheit oder Arbeitsbedingungen einer Person beeinträchtigt. Sie äußert sich in Worten, Gesten, Einstellungen oder Handlungen, die darauf abzielen, einen Mitarbeiter oder einen Dritten im Zusammenhang mit seiner beruflichen Tätigkeit einzuschüchtern, zu demütigen, zu isolieren, zu bedrohen oder herabzuwürdigen. Belästigung kann psychischer Natur sein, z. B. in Form von abfälligen Bemerkungen, absichtlicher Isolierung, Überlastung oder Entzug von Arbeitsmitteln, Ausgrenzung, Verbreitung von Gerüchten oder systematischer Herabwürdigung. Sie kann auch sexueller Natur sein. Sexuelle Belästigung ist gekennzeichnet durch unerwünschtes sexuelles Verhalten oder Kommentare, die wiederholt auftreten oder einen einzelnen schwerwiegenden Vorfall darstellen und die Würde einer Person untergraben oder ein einschüchterndes, feindseliges, erniedrigendes oder demütigendes Arbeitsumfeld schaffen. Dazu gehören unter anderem beharrliche Annäherungsversuche, Kommentare über den Körper, Aufforderungen zu sexuellen Gefälligkeiten,

	nicht einvernehmliche körperliche Gesten oder Berührungen oder die Verbreitung sexueller Bilder ohne Zustimmung. Belästigung, sei sie moralischer oder sexueller Natur, ist inakzeptabel und die Täter sind nach den geltenden lokalen Gesetzen haftbar.
Diskriminierung	Diskriminierung am Arbeitsplatz bedeutet, jemanden aufgrund von gesetzlich verbotenen Kriterien wie Herkunft, Geschlecht, Familienstand usw. oder anderen durch lokale Gesetze geschützten Merkmalen benachteiligt zu behandeln. Diskriminierung kann beispielsweise zu einer Ungleichbehandlung beim Zugang zu Beschäftigung, bei den Arbeitsbedingungen, bei der Ausbildung, bei der Mobilität oder in jeder anderen Situation im Zusammenhang mit der beruflichen Tätigkeit führen. Sie kann in Form von Entscheidungen über Einstellung, Bewertung, Beförderung, Zuweisung oder Entlassung erfolgen, die eine Person ohne objektive Rechtfertigung aufgrund der Anforderungen der Position benachteiligen. Am Arbeitsplatz kann Diskriminierung zwei Formen annehmen: - Direkte Diskriminierung. In diesem Fall trifft der Täter bewusst eine Entscheidung auf der Grundlage eines gesetzlich verbotenen diskriminierenden Kriteriums. Indirekte Diskriminierung. In diesem Fall trifft der Täter eine Entscheidung, die neutral erscheint, aber letztendlich bestimmte Personen gegenüber anderen benachteiligt. Beispielsweise erlauben interne Vorschriften nur Männern, nach dem 50. Lebensjahr im Unternehmen zu bleiben. Dies stellt somit eine indirekte Diskriminierung aufgrund des Geschlechts und des Alters dar.
Gesundheit/Sicherheit	Jeder schwerwiegende Verstoß gegen oder jedes Risiko für die Gesundheit und Sicherheit am Arbeitsplatz. Sicherheit am Arbeitsplatz bezieht sich auf alle Maßnahmen und Praktiken, die darauf abzielen, die körperliche und geistige Unversehrtheit von Menschen an ihrem Arbeitsplatz zu schützen, indem das Risiko von Unfällen, Verletzungen und Berufskrankheiten verringert wird. Dazu gehören die Ermittlung und Bewertung von Risiken, die Umsetzung technischer und organisatorischer Sicherheitsvorkehrungen, die Schulung und Unterrichtung der Mitarbeiter sowie die Einführung von Präventions-, Interventions- und Notfallmaßnahmen. Die Einhaltung dieser Verpflichtungen trägt zu einer sicheren Arbeitsumgebung bei, die den lokalen Anforderungen entspricht.
	Jede schwerwiegende Verletzung oder Gefährdung der auf nationaler und internationaler Ebene anerkannten Menschenrechte und Grundfreiheiten sowie jede Verletzung

Menschenrechte (außer Diskriminierung und Belästigung)	der geltenden lokalen Anforderungen in diesem Bereich. Dazu gehören unter anderem Situationen, die Grundsätze wie die Achtung der Vereinigungs- und Meinungsfreiheit, den Zugang zu angemessenen und sicheren Arbeitsbedingungen und die Möglichkeit für die Betroffenen, Rechtsbehelfe in Anspruch zu nehmen, betreffen.
Interessenkonflikte	Ein Interessenkonflikt liegt vor, wenn die persönlichen Interessen einer Person, sei es finanzieller, familiärer, freundschaftlicher, politischer oder sonstiger Art, ihr Urteilsvermögen oder ihre Entscheidungen im Rahmen ihrer Tätigkeit innerhalb der Rexel-Gruppe beeinflussen oder zu beeinflussen scheinen. Dabei handelt es sich nicht unbedingt um ein Fehlverhalten oder eine rechtswidrige Handlung, sondern um das Risiko einer Voreingenommenheit, die die erwartete Unparteilichkeit beeinträchtigt. Dieses Risiko einer Voreingenommenheit kann ausreichen, um das Vertrauen der Betroffenen zu untergraben, die Qualität von Entscheidungen zu beeinträchtigen und den Ruf der Organisation zu schädigen. Ein Interessenkonflikt kann tatsächlich (bereits vorhanden), potenziell (wahrscheinlich) oder scheinbar (von Dritten wahrgenommen) sein. Das Whistleblowing-System soll nicht das von der Rexel-Gruppe festgelegte Verfahren zur Meldung von Interessenkonflikten ersetzen.
Wettbewerbswidrige Praktiken	Wettbewerbswidrige Praktiken beziehen sich auf Unternehmensverhalten, das den freien Wettbewerb beeinträchtigt und anderen Marktteilnehmern (Kunden, Lieferanten, Wettbewerbern) schadet. Dazu gehören formelle oder informelle Vereinbarungen zwischen Wettbewerbern zur Koordinierung von Preisen, Geschäftsbedingungen, der Aufteilung von Märkten, Gebieten oder Produkten oder zur Begrenzung des Angebots oder zum Boykott bestimmter Partner. Dazu gehören auch Situationen des Missbrauchs einer marktbeherrschenden Stellung (z. B. Verdrängung eines Konkurrenten, Durchsetzung von Verdrängungspreisen oder ungerechtfertigten Kopplungsgeschäften), die Beeinflussung der von Händlern verlangten Wiederverkaufspreise und der Austausch nicht öffentlicher strategischer Informationen, die das Marktverhalten beeinflussen könnten (z. B. Pläne, Marketingdaten oder Kapazitäten). Diese Praktiken sind nach den Wettbewerbsregeln verboten und unterliegen erheblichen Strafen.
Umwelt	Jede Situation, in der geltende Umwelanforderungen nicht erfüllt werden oder in der ein erhebliches Risiko oder eine erhebliche Schädigung der Umwelt festgestellt wird, sei es innerhalb des Unternehmens oder bei seinen Partnern in der Wertschöpfungskette. Dies umfasst die Vermeidung von Umweltverschmutzung, den verantwortungsvollen Umgang

	mit Ressourcen und die sichere Handhabung von Stoffen und Abfällen in Übereinstimmung mit den gesetzlichen Verpflichtungen und internen Standards.
Betrug	Jede Situation, in der Verschleierung, Täuschung oder Manipulation zum Einsatz kommen, um sich einen ungerechtfertigten Vorteil zu verschaffen oder Verpflichtungen zu umgehen, sei es in steuerlicher, finanzieller oder buchhalterischer Hinsicht. Dazu gehören beispielsweise die Fälschung von Dokumenten oder Aufzeichnungen, die falsche Darstellung von Finanzinformationen, die Verschleierung von Einkünften oder Vermögenswerten sowie alle Maßnahmen, die darauf abzielen, geltende Vorschriften innerhalb des Unternehmens oder in seiner Wertschöpfungskette zu umgehen.
Insiderhandel	Insiderhandel ist der Kauf, Verkauf oder die Empfehlung von Finanzinstrumenten unter Verwendung oder unter Berufung auf nicht öffentliche privilegierte Informationen über einen Emittenten oder dessen Wertpapiere. Dazu gehört auch die illegale Weitergabe solcher Informationen an Dritte. Ein solches Verhalten verschafft einen unfairen Vorteil auf den Märkten und ist strengstens verboten und strafbar.
Fiktive Arbeitsplätze	Ein fiktiver Arbeitsplatz ist eine Situation, in der eine Person für eine Position oder Aufgaben bezahlt wird, die sie nicht tatsächlich ausübt oder die nicht existieren, um sich einen unfairen Vorteil zu verschaffen. Dies kann das völlige Fehlen tatsächlicher Arbeit, fiktive Aufgaben oder die nominelle Zuweisung zu einer Abteilung ohne wirklichen Beitrag innerhalb des Unternehmens oder über Dritte umfassen.
Schutz personenbezogener Daten / IT-Sicherheit	Jede Situation, in der personenbezogene Daten oder IT-Systeme nicht gemäß den Gesetzen und internen Vorschriften geschützt sind und Personen oder das Unternehmen dem Risiko eines unbefugten Zugriffs, einer unbefugten Nutzung, Offenlegung, Änderung oder Zerstörung ausgesetzt sind. Dies umfasst die rechtmäßige und minimierte Erhebung und Verarbeitung von Daten, die Systemsicherheit (Zugriffskontrollen, Verschlüsselung, Backups), das Management von Vorfällen und Verstößen sowie die Vertraulichkeit und Integrität von Informationen während ihres gesamten Lebenszyklus, auch bei Dienstleistern. Personenbezogene Daten sind alle Informationen, die eine natürliche Person direkt oder indirekt identifizieren (z. B. Name, Kontaktdaten, Identifikatoren, Foto, Standortdaten oder andere Elemente, die sich auf ihre Identität oder ihr Privatleben beziehen).

DATENSCHUTZERKLÄRUNG

–

WHISTLEBLOWING-SYSTEM

Version 12/2025

Die Rexel-Gruppe hat ein professionelles Whistleblowing-System eingerichtet, über das ihre Mitarbeiter und Dritte, mit denen die Rexel-Gruppe in Beziehung steht, rechtswidrige Handlungen oder Fehlverhalten melden können. Der Umfang des Systems ist in der Whistleblowing-Verfahrensbeschreibung beschrieben, die auf der Website [rexel.com](https://www.rexel.com) verfügbar ist.



Im Rahmen dieses Systems kann ein Unternehmen der Rexel-Gruppe Daten über Sie erheben und verarbeiten. Die Vertraulichkeit von Daten ist die Grundlage unserer Vertrauensbeziehung. Daher nehmen wir den Schutz Ihrer personenbezogenen Daten im Rahmen unserer Geschäftstätigkeit sehr ernst.

Diese Richtlinie beschreibt die Verpflichtungen der Rexel-Gruppe zum Schutz personenbezogener Daten. In der folgenden Mitteilung erfahren Sie außerdem mehr über Ihre Rechte und die Bedingungen, unter denen Ihre personenbezogenen Daten erfasst, verarbeitet, gespeichert und archiviert werden.

Wer sind wir?

REXEL DEVELOPPEMENT SAS, eine vereinfachte Aktiengesellschaft nach französischem Recht mit Sitz in 13, Boulevard du Fort de Vaux, Paris, eingetragen im Handels- und Gesellschaftsregister von Paris unter der Nummer 480 172 840, ist der Datenverantwortliche.

Das Unternehmen innerhalb der Gruppe, das einen Arbeitsvertrag mit dem Verfasser des Berichts hat oder mit ihm zusammenarbeitet, ist ebenfalls für die Datenverarbeitung verantwortlich.

Sie legen die Zwecke und Mittel der Verarbeitung Ihrer Daten fest.

Sie werden in dieser Richtlinie als „Rexel“, „wir“ oder „Datenverantwortliche“ bezeichnet.

EY Polen fungiert als Auftragsverarbeiter für die Verarbeitung auf der Online-Meldeplattform.

Wie verarbeiten wir Ihre Daten im Rahmen des Meldesystems?

Die folgende Tabelle enthält detaillierte Informationen zu folgenden Punkten:

- (i) warum wir Ihre personenbezogenen Daten verarbeiten,
- (ii) welche Arten von Daten wir verarbeiten und
- (iii) die Rechtsgrundlage für die Verarbeitung Ihrer Daten.

Zweck 1	Art der Daten
Sammeln und Bearbeiten von Meldungen über Handlungen, die gegen das Gesetz oder den im Whistleblowing-System (siehe Whistleblowing-Verfahren) geregelten Verhaltenskodex zur Korruptionsbekämpfung verstoßen <u>Unterzwecke:</u> - Zentrale Verwaltung von beruflichen Meldungen (Entgegennahme und Bearbeitung von Meldungen, Einrichtung eines sicheren Kanals, Speicherung und Aufbewahrung von Informationen, Gewährleistung der Sicherheit) - Bearbeitung von professionellen Meldungen (Durchführung interner Untersuchungen, Bewertung der relevanten Fakten) - Entscheidungsfindung und Umsetzung geeigneter Maßnahmen nach Abschluss der Meldung (Benachrichtigung und Umsetzung von Maßnahmen) - Statistische Überwachung und Verbesserung des Whistleblowing-Systems - Ausübung oder Verteidigung von Rechten in Gerichtsverfahren	Im Rahmen des Systems können folgende Datenkategorien verarbeitet werden: - Identitätsdaten (Vor- und Nachname, Kontaktdaten), berufliche Daten (Position, Arbeitgeber, Arbeitsort) der meldenden Person (sofern die Meldung nicht anonym erfolgt) und alle anderen von ihr freiwillig zur Verfügung gestellten Informationen - Identitätsdaten (Vor- und Nachname, Kontaktdaten), berufliche Daten (Position, Arbeitgeber, Arbeitsort) der betroffenen Personen - Identitätsdaten (Vor- und Nachname, E-Mail-Adresse), berufliche Daten (Position, Arbeitgeber, Arbeitsort) von Personen, die an der Erfassung oder Bearbeitung der Meldung beteiligt oder dazu konsultiert wurden, sowie von Vermittlern und Personen, die mit dem Hinweisgeber in Kontakt stehen - Sensible Daten (rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten, Sexualleben oder sexuelle Orientierung), sofern dies zur Ausübung oder Verteidigung von Rechtsansprüchen (Artikel 9.2.f der DSGVO) oder aus Gründen eines erheblichen öffentlichen Interesses (Artikel 9.2.g der DSGVO) unbedingt erforderlich ist - Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherheitsmaßnahmen, sofern dies unbedingt erforderlich ist und im Einklang mit Artikel 10 der DSGVO steht - Im Rahmen der Faktenprüfung erhobene Informationen - Berichte über Überprüfungsmaßnahmen - Daten im Zusammenhang mit der Weiterverfolgung des Berichts
Rechtsgrundlage für die Verarbeitung Ihrer Daten Gesetzliche Verpflichtung zur Einrichtung eines Meldesystems: insbesondere Artikel 8.I.B und 17 II des Sapin-II-Gesetzes und Artikel L. 225-102-4 des Handelsgesetzbuches sowie alle gleichwertigen Gesetze zum Schutz von Hinweisgebern, zur Korruptionsbekämpfung oder zur Sorgfaltspflicht.	

Zweck 2	Art der Daten
Erfassung und Verarbeitung von Meldungen über Verstöße gegen den Ethik-Leitfaden <u>Unterzwecke:</u> - Zentrale Verwaltung von beruflichen Meldungen (Entgegennahme und Bearbeitung von Meldungen, Einrichtung eines sicheren Kanals, Speicherung und Aufbewahrung von Informationen, Gewährleistung der Sicherheit) - Bearbeitung von professionellen Meldungen (Durchführung interner Untersuchungen, Bewertung der relevanten Fakten) - Entscheidungsfindung und Umsetzung geeigneter Maßnahmen nach Abschluss der Meldung (Benachrichtigung und Umsetzung von Maßnahmen) - Statistische Überwachung und Verbesserung des Whistleblowing-Systems - Ausübung oder Verteidigung von Rechten in Gerichtsverfahren	Im Rahmen des Systems können folgende Datenkategorien verarbeitet werden: - Identitätsdaten (Vor- und Nachname, Kontaktdaten), berufliche Daten (Position, Arbeitgeber, Arbeitsort) der meldenden Person (sofern die Meldung nicht anonym erfolgt) und alle anderen von ihr freiwillig zur Verfügung gestellten Informationen - Identitätsdaten (Vor- und Nachname, Kontaktdaten), berufliche Daten (Position, Arbeitgeber, Arbeitsort) der betroffenen Personen - Identitätsdaten (Vor- und Nachname, E-Mail-Adresse), berufliche Daten (Position, Arbeitgeber, Arbeitsort) von Personen, die an der Erfassung oder Bearbeitung der Meldung beteiligt oder dazu konsultiert wurden, sowie von Vermittlern und Personen, die mit dem Hinweisgeber in Kontakt stehen - Sensible Daten (rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten, Sexualleben oder sexuelle Orientierung), sofern dies zur Ausübung oder Verteidigung von Rechtsansprüchen (Artikel 9.2.f der DSGVO) oder aus Gründen eines erheblichen öffentlichen Interesses (Artikel 9.2.g der DSGVO) unbedingt erforderlich ist - Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherheitsmaßnahmen, sofern dies unbedingt erforderlich ist und im Einklang mit Artikel 10 der DSGVO steht - Im Rahmen der Faktenprüfung erhobene Informationen - Berichte über Überprüfungsmaßnahmen - Daten im Zusammenhang mit der Weiterverfolgung des Berichts
Rechtsgrundlage für die Verarbeitung Ihrer Daten	
Rechtsgrundlage: Berechtigtes Interesse an der Bearbeitung von ethischen Meldungen, die nicht unter eine gesetzliche Verpflichtung fallen.	

Wer sind die Empfänger Ihrer Daten?



Die von uns erhobenen personenbezogenen Daten sowie alle später erhobenen Daten sind für uns in unserer Eigenschaft als Datenverantwortlicher bestimmt.



Wir stellen sicher, dass nur befugte Personen Zugriff auf diese Daten haben.

Intern:

- Die für die Erfassung und Verarbeitung von Meldungen Verantwortlichen, nämlich:
 - Mitglieder des Ethikausschusses der Rexel-Gruppe
 - Autorisierte Mitglieder der Rechts- oder Compliance-Abteilung auf Gruppen- und lokaler Ebene
 - Autorisierte Mitglieder der Personalabteilung auf Gruppen- und lokaler Ebene
- Befugte Mitglieder der Abteilung für Revision und interne Kontrolle auf Gruppen- und lokaler Ebene, um die Wirksamkeit der internen Kontrollen und der Unternehmensführung sicherzustellen
- Wenn es die Situation rechtfertigt, können auch andere interne Mitarbeiter Zugriff auf die Daten erhalten, insbesondere wenn Fachwissen in den Bereichen Buchhaltung, Finanzen, Recht, Technik oder IT erforderlich ist.

Extern:

- Unsere Berater
- Unsere Makler und Versicherer
- Unsere Wirtschaftsprüfer
- Die zuständigen Behörden (Justiz-, Verwaltungs- und Aufsichtsbehörden) gemäß den geltenden Vorschriften
- Unsere Dienstleister, insbesondere EY Poland, die uns die Online-Berichtsplattform zur Verfügung stellt.

Diese Empfänger befinden sich in der Europäischen Union.

Wie lange speichern wir Ihre Daten auf?

Situationen	Aufbewahrungsfrist
Unzulässige Meldungen (die nicht in den Anwendungsbereich fallen, nicht schwerwiegend sind, unvollständig sind, in böser Absicht gemacht wurden usw.)	Löschung oder Archivierung und Anonymisierung so schnell wie möglich
Zulässige Meldung, aber abgewiesen (keine disziplinarischen oder rechtlichen Schritte)	Löschung oder Anonymisierung und Archivierung innerhalb von zwei (2) Monaten
Meldungen, die zu Disziplinar- oder Gerichtsverfahren führen	Aufbewahrung der Daten bis zum Ende des Verfahrens und der Rechtsmittel. Nach Ablauf dieser Frist Löschung oder Anonymisierung und Archivierung.

Welche Rechte haben Sie?



Gemäß den Datenschutzgesetzen haben Sie folgende Rechte:

- Recht auf Zugang: Sie können auf die Informationen, die wir über Sie gespeichert haben, zugreifen und eine Kopie davon erhalten.
- Recht auf Berichtigung: Sie können unrichtige Daten, die Sie betreffen, ändern, vervollständigen, aktualisieren oder löschen lassen;
- Widerspruchsrecht: Sie können der Verarbeitung Ihrer Daten widersprechen, es sei denn, es liegen berechtigte und zwingende Gründe für die Verarbeitung vor.
- Recht auf Löschung: Sie können verlangen, dass wir Daten, die Sie betreffen, innerhalb der in Artikel 17 der DSGVO festgelegten Bedingungen löschen;
- Recht auf Datenübertragbarkeit: Sie können Ihre Daten abrufen, um sie an eine andere Organisation zu übertragen oder für persönliche Zwecke zu verwenden.
- Recht auf Einschränkung der Verarbeitung;
- Recht auf Festlegung spezifischer und allgemeiner Richtlinien für die Speicherung, Löschung und Weitergabe Ihrer Daten nach Ihrem Tod.

Jede Person, die Gegenstand einer Meldung ist, wird so schnell wie möglich (spätestens innerhalb eines Monats) nach der computergestützten oder nicht computergestützten Erfassung der sie betreffenden Daten informiert, damit sie ihre Rechte ausüben kann. Wenn diese Information jedoch die Ziele der Verarbeitung und insbesondere die Durchführung der Untersuchung ernsthaft gefährden könnte (z. B. wenn die Gefahr der Vernichtung von Beweismitteln besteht), kann diese Information zurückgestellt werden und wird erst dann bereitgestellt, wenn jegliches Risiko beseitigt ist.

Die Person, die Gegenstand einer Meldung ist, kann unter keinen Umständen vom für die Verarbeitung Verantwortlichen auf der Grundlage ihres Auskunftsrechts Informationen über die Identität des Verfassers der Meldung oder einer anderen an der Untersuchung beteiligten Person erhalten.

Wenn Sie keine Antwort erhalten, die Antwort für unbefriedigend halten oder der Meinung sind, dass die Verarbeitung Ihrer Daten nicht den gesetzlichen und behördlichen Bestimmungen entspricht, können Sie sich an die zuständige Aufsichtsbehörde wenden.

Wie können Sie Ihre Rechte ausüben?



Durch schriftliche Anfrage an unseren Datenschutzbeauftragten:

Länder	Unternehmen	Adresse
Österreich	COMTECH IT-SOLUTIONS GMBH	datenschutz@rexel.at
	Rexel Austria GmbH	datenschutz@rexel.at
Belgien	Rexel Belgique SA	gdpr@rexel.be
Frankreich	Cordia	donnees.personnelles@francofa-eurodis.fr
	Rexel Développement SAS / Rexel-Gruppe	data.protection@rexel.com
	Rexel France SAS	donnees.personnelles@rexel.fr
	Bizline	data.protection@rexel.com
	Gigamedia	data.protection@rexel.com
	Sofinther SAS	donnees.personnelles@sofinther.fr
	Espace Elec SAS	donnees.personnelles@espace-elec.fr
	Esabora Digital Services SAS	dataprotection-rda@rexel.fr
	Francofa Eurodis	donnees.personnelles@francofa-eurodis.fr
	Freshmile Services SAS	donnees.personnelles@rexel.fr
	ITESA	donnees.personnelles@rexel.fr
Deutschland	REXEL GERMANY BETEILIGUNGS GMBH	Datenschutzbeauftragter@rexel.de
	Rexel Germany GmbH & Co KG	Datenschutzbeauftragter@rexel.de
	REXEL GERMANY VERWALTUNGS GMBH	Datenschutzbeauftragter@rexel.de
Italien	Rexel Italia S.p.A	dataprotection@rexel.it
	Tecno-Bi S.r.l.	dataprotection@rexel.it
	Comm-Tech S.r.l.	dataprotection@rexel.it
Irland	M. Kelliher 1998	data.protection@rexel.ie
	Rexel Industrial Solutions	data.protection@rexel.ie
Luxemburg	Rexel Luxembourg SA	gdpr@rexel.be
Niederlande	Rexel Nederland B.V	AVG@rexel.nl
	Wasco Group B.V.	AVG@rexel.nl
	Wasco Holding B.V.	AVG@rexel.nl
	Wasco Groothandels Greop B.V.	AVG@rexel.nl
	Wasco Distributlecentrum B.V.	AVG@rexel.nl
Slowenien	Rexel d.o.o.	dpc@rexel.si
Schweden	Rexel Sverige AB	dataskydd@rexel.se
Schweiz	ELEKTRO-MATERIAL AG	datenschutz@e-m.ch
	Rexel 3S	data.protection@rexel.com
Großbritannien	Rexel (UK) Ltd.	data.protection@rexel.co.uk



Procedura di segnalazione di irregolarità Dicembre 2025_V1

Sommario

I.	<u>Introduzione</u>	3
1.	<u>Finalità del sistema interno di segnalazione di irregolarità</u>	3
2.	<u>Promemoria del quadro giuridico</u>	3
3.	<u>Ambito di applicazione</u>	3
II.	<u>La raccolta delle segnalazioni etiche</u>	4
1.	<u>Condizioni di ammissibilità di un'allerta etica</u>	4
	<u>Chi può presentare una segnalazione?</u>	4
	<u>Come si può beneficiare dello status di whistleblower e della relativa protezione giuridica?</u>	4
	<u>Quali fatti possono essere segnalati?</u>	5
2.	<u>Come presentare una segnalazione</u>	6
3.	<u>Contenuto della segnalazione</u>	7
4.	<u>Denunce anonime</u>	7
5.	<u>Canali esterni</u>	7
III.	<u>Gestione delle segnalazioni etiche interne</u>	7
1.	<u>Conferma di ricezione della segnalazione</u>	7
2.	<u>Esame dell'ammissibilità della segnalazione</u>	7
3.	<u>Conduzione dell'indagine interna</u>	8
4.	<u>Processo decisionale e chiusura dell'indagine</u>	9
IV.	<u>Protezione e garanzie offerte</u>	10
1.	<u>Principi generali</u>	10
2.	<u>Informazioni</u>	10
3.	<u>Protezione in materia penale, civile e sociale</u>	10
4.	<u>Periodo di conservazione dei dati limitato</u>	11
5.	<u>Riservatezza e sicurezza</u>	11
6.	<u>Protezione dei dati personali</u>	12
V.	<u>Segnalazione</u>	12
VI.	<u>Aggiornamento della procedura</u>	12
	<u>Appendice 1: Sintesi</u>	13
	<u>Appendice 2: Elenco dei paesi con procedura locale di segnalazione di irregolarità</u>	14
	<u>Appendice 3: Esempi di comportamenti o condotte scorrette contemplati dalla procedura di segnalazione</u>	15
	<u>Appendice 4: Informativa sulla privacy</u>	19

I. Introduzione

1. Scopo del sistema interno di segnalazione

Nell'ambito della politica di Rexel Group in materia di etica e conformità, descritta in particolare nella sua Guida all'etica, nella sua Carta dei fornitori responsabili e nel suo Codice di condotta anticorruzione, Rexel Group ha istituito un sistema di segnalazione interno.

Il sistema di segnalazione interno del Gruppo Rexel consente a qualsiasi dipendente, nonché a terzi con cui il Gruppo Rexel intrattiene rapporti, di segnalare situazioni che violano la legge, la Guida Etica del Gruppo Rexel o il suo Codice di Condotta Anticorruzione.

Lo scopo di questa procedura è descrivere il processo di raccolta e gestione delle segnalazioni etiche all'interno del Gruppo Rexel.

Una sintesi della procedura è allegata all'**Appendice 1**.

2. Promemoria del quadro giuridico

Poiché la holding del Gruppo Rexel è costituita in Francia, la procedura è stata stabilita in conformità con le seguenti leggi francesi:

- La legge Sapin II del 9 dicembre 2016 sulla trasparenza, la lotta alla corruzione e la modernizzazione economica;
- La legge sul "dovere di vigilanza" del 27 marzo 2017, relativa al dovere di vigilanza delle società madri e delle società appaltatrici;
- La legge "Waserman" del 21 marzo 2022, volta a migliorare la protezione degli informatori, e il relativo decreto attuativo del 3 ottobre 2022.

La procedura si basa anche su una serie di pubblicazioni dell'Agenzia francese anticorruzione (AFA) e dell'Autorità francese per la protezione dei dati (CNIL):

- Le raccomandazioni dell'AFA;
- La guida pratica "Indagini interne anticorruzione" pubblicata nel marzo 2023 dall'AFA e dalla Procura finanziaria francese;
- Il documento di riferimento "allarmi professionali" della CNIL, pubblicato inizialmente nel 2019 e aggiornato nel 2023.

Più in generale, la raccolta e il trattamento delle segnalazioni sono effettuati in conformità con le leggi e i regolamenti applicabili e la presente procedura può essere aggiornata, se necessario, per riflettere gli sviluppi legislativi e le migliori pratiche.

Se una legge o un regolamento locale offre norme di protezione per gli informatori più rigorose rispetto alla presente procedura, prevarranno le disposizioni locali. Tuttavia, laddove la presente procedura fornisca maggiori garanzie di protezione, il Gruppo Rexel le applicherà volontariamente nella misura consentita dalla legge applicabile.

3. Ambito di applicazione

La presente procedura è destinata ad essere implementata in tutte le entità del Gruppo Rexel. Sarà modificata, se necessario, per riflettere eventuali cambiamenti nelle leggi e nei regolamenti.

In alcuni paesi del gruppo Rexel, la presente procedura è integrata da procedure locali. Queste ultime specificano i requisiti legali applicabili e, a seconda dei casi, i canali disponibili a livello locale (vedi **Appendice 2**).

L'autore di una segnalazione può quindi scegliere il canale di segnalazione che preferisce (di gruppo o locale). La procedura applicabile sarà quindi quella corrispondente al canale scelto. A seconda della natura e della gravità dei comportamenti o delle condotte scorrette segnalati, una segnalazione effettuata tramite il canale locale può essere inoltrata al gruppo e viceversa.

Questa procedura si applica a tutti i dipendenti del gruppo Rexel (indipendentemente dal loro ruolo, posizione o reparto) e ai terzi con cui il gruppo Rexel intrattiene rapporti. Essa riguarda la raccolta e il trattamento delle segnalazioni interne da parte del gruppo Rexel e, più specificamente:

- La loro presentazione;
- La loro ricezione;
- La valutazione della loro ammissibilità;
- Le principali fasi dell'indagine interna
- La chiusura del caso.

II. La raccolta di segnalazioni di natura etica

1. Condizioni per l'ammissibilità di un allarme etico

Chi può presentare una segnalazione?

Il sistema di segnalazione interno del Gruppo Rexel è aperto alle seguenti persone:

- Dipendenti del Gruppo Rexel (a tempo indeterminato, a tempo determinato, apprendisti, stagisti)
- Dipendenti esterni o temporanei (lavoratori temporanei, consulenti, ecc.)
- Candidati
- Ex dipendenti
- Azionisti, soci e titolari di diritti di voto nell'assemblea generale
- Membri degli organi amministrativi, esecutivi o di controllo
- Qualsiasi dipendente di terzi con cui il Gruppo Rexel intrattiene rapporti (ad esempio, clienti, fornitori, prestatori di servizi, ecc.).

Il sistema di segnalazione interno è aperto a tutte le entità del Gruppo Rexel ed è disponibile nelle principali lingue del Gruppo: inglese, tedesco, cinese, francese, italiano, olandese, svedese e sloveno.

Come si può beneficiare dello status di segnalante e della relativa protezione legale?

Per essere considerato un whistleblower e beneficiare della protezione prevista dalla legge, è necessario soddisfare la definizione legale di whistleblower, ovvero soddisfare tutti i seguenti criteri, salvo diversamente previsto dalla legge locale applicabile:

- Essere una persona fisica;
- Non ricevere alcun compenso finanziario diretto per la segnalazione;
- Agire in buona fede;
- Se i fatti segnalati sono stati ottenuti al di fuori di un contesto professionale, avere conoscenza personale dei fatti segnalati.

Quali fatti possono essere segnalati?

Il sistema di segnalazione interno del Gruppo Rexel consente di segnalare fatti che possono costituire le seguenti categorie di comportamenti o condotte scorrette:

- Un reato o un'infrazione
- Una minaccia o un danno all'interesse pubblico
- Una violazione, o un tentativo di occultamento di una violazione, delle leggi e dei regolamenti nazionali, europei o internazionali
- Una violazione o una situazione contraria alla Guida etica o al Codice di condotta anticorruzione del Gruppo Rexel
- Rischi gravi legati alle attività del Gruppo Rexel che potrebbero ledere i diritti umani, le libertà fondamentali, la salute e la sicurezza delle persone o l'ambiente

Esempi di comportamenti o condotte scorrette da segnalare possono includere:

- Corruzione, compresa qualsiasi violazione del Codice di condotta anticorruzione
- Molestie (psicologiche o sessuali)
- Discriminazione
- Salute, igiene o sicurezza (ad esempio, rischio per l'integrità fisica o mentale)
- Diritti umani (diversi da discriminazione, privacy e molestie)
- Conflitto di interessi
- Pratiche anticoncorrenziali
- Ambiente (ad esempio inquinamento, gestione dei rifiuti)
- Frode fiscale
- Frode finanziaria o contabile
- Insider trading
- Lavori fittizi
- Sicurezza dei dati personali/informatica

L'appendice 3 illustra alcuni di questi tipi di comportamenti o condotte scorrette.

Le segnalazioni relative a categorie non elencate sopra non rientrano nell'ambito di applicazione della presente procedura. Allo stesso modo, sono esclusi dalla presente procedura fatti, informazioni o documenti, indipendentemente dalla loro forma o dal loro supporto, la cui divulgazione è vietata da disposizioni dell' relative al segreto di difesa nazionale, al segreto medico, al segreto delle deliberazioni giudiziarie, al segreto delle indagini o inchieste giudiziarie o al segreto professionale dell'avvocato . Se

del caso, l'autore della segnalazione sarà informato e indirizzato alle persone competenti per trattare i fatti segnalati.

2. Come presentare una segnalazione

L'autore di una segnalazione ha a disposizione diversi canali per inviare le segnalazioni:

- La piattaforma di segnalazione online accessibile all'indirizzo: <https://www.rexel.com/en/rexel-group-ethics-alert>;
- Ulteriori canali di segnalazione che possono esistere a livello di gruppo o di paese locale.

Non esiste una gerarchia tra i canali. L'autore di una segnalazione può utilizzare qualsiasi canale a sua disposizione.

Indipendentemente dal canale utilizzato, le persone responsabili della raccolta delle segnalazioni sono di seguito denominate **"Responsabili interni"**.

La piattaforma di segnalazione online

L'autore di una segnalazione può inviare un avviso, anche in forma anonima, sulla piattaforma di segnalazione online accessibile all'indirizzo: <https://www.rexel.com/en/rexel-group-ethics-alert>

Si tratta di una piattaforma dedicata e gratuita, disponibile 24 ore su 24, 7 giorni su 7.

È ospitata nell'Unione Europea da un fornitore di servizi esterno (EY) che attua misure rigorose per garantire la sicurezza e la riservatezza dei dati. Va notato che i dipendenti di questo fornitore di servizi non sono coinvolti nel trattamento delle segnalazioni e non hanno accesso alle informazioni scambiate.

Questa piattaforma consente la comunicazione diretta con il destinatario della segnalazione tramite chat. Consente inoltre all'autore della segnalazione di inviare documenti a sostegno dei fatti.

Il link a questa piattaforma è disponibile sui siti web del Gruppo: <https://www.rexel.com/en/rexel-group-ethics-alert> e <https://ethique.rexel.com/en/>, nonché sui siti intranet delle entità del Gruppo Rexel.

Ulteriori canali di segnalazione

I dipendenti interni del Gruppo Rexel possono presentare una segnalazione per iscritto o verbalmente a uno dei seguenti responsabili interni: (i) il responsabile locale della conformità (ufficio legale o ufficio conformità), (ii) l'ufficio risorse umane locale, (iii) l'ufficio conformità del Gruppo o (iv) l'ufficio risorse umane del Gruppo.

Il reparto Risorse umane (locale o del Gruppo) raccoglie solitamente le segnalazioni di violazioni del diritto del lavoro o di comportamenti inappropriati sul posto di lavoro (molestie, discriminazioni, salute, igiene o sicurezza, ecc.).

Il responsabile della conformità locale o il dipartimento di conformità del Gruppo raccoglie solitamente le segnalazioni di violazioni della legge, della Guida etica, del Codice di condotta anticorruzione e delle procedure di conformità del Gruppo Rexel, ecc.

Quando una segnalazione viene effettuata verbalmente, può essere ricevuta per telefono e, su richiesta della persona che effettua la segnalazione e a sua discrezione, durante una videoconferenza o un incontro fisico organizzato entro venti (20) giorni lavorativi dal ricevimento della richiesta. Le segnalazioni verbali vengono trascritte per iscritto.

I dipendenti possono, in ogni caso, chiedere consiglio al proprio responsabile diretto o indiretto e condividere eventuali preoccupazioni, tranne nel caso in cui il responsabile stesso sia il presunto autore della condotta in questione. Se, a seguito di tale discussione, risulta che tali preoccupazioni rientrano nell'ambito di applicazione della presente procedura, il responsabile deve incoraggiare il dipendente a presentare una segnalazione tramite i canali sopra indicati o contattando l'Ufficio Legale o l'Ufficio Compliance locale o l'Ufficio Risorse Umane locale.

3. Contenuto della segnalazione

L'autore di una segnalazione deve presentare i fatti e le informazioni oggetto della stessa in modo preciso e obiettivo, al fine di consentire la gestione della segnalazione.

Ove possibile, deve supportare la sua segnalazione:

- indicando la data o le date e il luogo o i luoghi in cui si sono verificati i fatti segnalati, l'entità interessata e l'identità e la posizione della persona o delle persone coinvolte;
- fornendo una descrizione dettagliata dei fatti con informazioni specifiche e concrete direttamente correlate all'oggetto della segnalazione, indipendentemente dalla sua forma o dal mezzo utilizzato.

4. Segnalazioni anonime

È preferibile che l'autore di una segnalazione si identifichi, in particolare per semplificare lo svolgimento dell'indagine. Tuttavia, l'autore di una segnalazione può scegliere di effettuare una segnalazione anonima, come previsto dalla piattaforma di segnalazione online, a condizione che (i) sia accertata la gravità dei fatti e (ii) gli elementi fattuali siano sufficientemente dettagliati.

5. Canali esterni

Fatta salva la conformità alle normative locali applicabili, si precisa che l'autore di una segnalazione ha anche la possibilità di effettuare una segnalazione esterna (i) all'autorità competente, (ii) al difensore civico, (iii) all'autorità giudiziaria o (iv) a qualsiasi istituzione, organismo o agenzia locale o internazionale competente a ricevere tali segnalazioni. Gli autori delle segnalazioni possono presentare segnalazioni esterne direttamente a un'autorità o dopo aver presentato una segnalazione al Gruppo Rexel.

III. Gestione delle segnalazioni etiche interne

1. Conferma di ricezione della segnalazione

Quando la segnalazione viene ricevuta sulla piattaforma di segnalazione online o attraverso i canali tradizionali, il Responsabile interno (la persona incaricata di raccogliere le segnalazioni come definito sopra) conferma la ricezione della segnalazione entro sette (7) giorni lavorativi dalla sua ricezione.

La conferma di ricezione non costituisce accettazione della segnalazione.

2. Esame dell'ammissibilità della segnalazione

Ogni segnalazione ricevuta è soggetta a un'analisi preliminare da parte del Responsabile interno per garantire che rientri nell'ambito di applicazione della procedura e assicurarne l'ammissibilità.

Tale verifica, che può richiedere una comunicazione con l'autore della segnalazione, si concentra in particolare sui seguenti punti:

- **Lo status dell'autore come "informatore"**: in particolare, che agisca in buona fede e senza cercare un compenso finanziario diretto;
- **La natura della segnalazione**: che rientri effettivamente in una delle categorie di segnalazioni contemplate dalla procedura;
- **Il contenuto della relazione**: che le informazioni e i fatti riportati siano oggettivi e sufficientemente dettagliati da consentire l'avvio di un'indagine;
- **Esistenza di segreti protetti**: la segnalazione non rivela fatti coperti dal segreto di difesa nazionale, dal segreto medico, dal segreto delle deliberazioni giudiziarie, dal segreto delle indagini o inchieste giudiziarie o dal segreto professionale dell'avvocato.

La decisione sull'ammissibilità è presa dal Responsabile interno. L'autore di una segnalazione viene informato dell'inammissibilità della stessa, se del caso, e dei motivi di tale decisione.

In ogni caso, il Responsabile interno deve fornire una risposta iniziale entro tre (3) mesi. Il Gruppo Rexel non è tenuto a trattare la segnalazione entro tale termine, ma deve informare l'autore della segnalazione delle azioni previste o già intraprese per valutare la validità della segnalazione e porre rimedio alla situazione segnalata.

La segnalazione sarà trattata in modo assolutamente riservato.

A seconda della natura e della gravità dei fatti segnalati, la segnalazione potrà essere gestita dal Comitato Etico del Gruppo Rexel. Il Comitato Etico del Gruppo Rexel è un comitato ad hoc istituito all'interno di Rexel Développement il cui ruolo è quello di gestire le segnalazioni più gravi effettuate dai dipendenti Rexel o da terzi con cui Rexel intrattiene rapporti.

Il Comitato Etico del Gruppo Rexel è composto da tre membri permanenti:

- il Segretario Generale,
- il Direttore delle Risorse Umane del Gruppo e
- il Direttore Etica e Conformità

3. Conduzione dell'indagine interna

Obiettivi e gestione dell'indagine interna

Il tempo necessario per elaborare una segnalazione varia e dipende dalla complessità dei fatti segnalati e dalla natura delle informazioni fornite.

L'obiettivo dell'indagine interna è verificare l'accuratezza e la rilevanza dei fatti segnalati. La segnalazione viene esaminata utilizzando metodi (interviste, ricerche di dati, ecc.) che possono variare a seconda del contesto e della natura dell'argomento.

L'indagine può essere condotta da:

- (xvi) il Dipartimento Risorse Umane locale;
- (xvii) il reparto locale di conformità o legale;

- (xviii) il Dipartimento Compliance del Gruppo;
- (xix) il Dipartimento Risorse Umane del Gruppo;
- (xx) il Comitato Etico del Gruppo Rexel, a seconda della natura e della gravità dei fatti segnalati (di seguito denominato "**Responsabile dell'indagine**").

In ogni caso, il Responsabile delle indagini condurrà l'indagine interna relativa alla segnalazione. Le informazioni relative all'esistenza e al contenuto della segnalazione saranno comunicate ai responsabili dell'indagine solo nella misura strettamente necessaria.

Quando viene presentata una segnalazione, il Gruppo Rexel garantisce l'indipendenza del processo di indagine. Prima di avviare un'indagine interna, viene verificato che nessuna delle persone coinvolte nell'indagine sulla segnalazione sia direttamente o indirettamente interessata dai fatti segnalati o abbia alcun legame di interesse con le persone coinvolte. Se viene individuato un rischio di conflitto di interessi, il dipendente interessato viene immediatamente allontanato dal processo e sostituito. Questo principio di indipendenza è parte integrante del sistema etico e di conformità di Rexel e mira a garantire una gestione rigorosa, imparziale e credibile di tutte le segnalazioni ricevute.

Sequestro di e-mail, documenti o supporti informatici

L'indagine interna può richiedere la revisione e l'elaborazione di e-mail o qualsiasi supporto informatico appartenente a uno o più dipendenti. Prima di sequestrare o congelare qualsiasi account di posta elettronica o supporto informatico, il responsabile dell'indagine deve richiedere l'autorizzazione, come definito dalla procedura locale (ad esempio, il Comitato Etico del Gruppo, il Consulente Legale locale o il Corrispondente locale per la protezione dei dati), per sequestrare e conservare tali e-mail a fini di indagine.

Esperto ospite

Quando la situazione lo richiede, il responsabile delle indagini può decidere di invitare una o più persone a collaborare con lui nell'ambito specifico della gestione di una segnalazione specifica, in particolare se sono necessarie competenze contabili, finanziarie, tecniche o informatiche.

Il responsabile delle indagini può quindi decidere di chiedere assistenza nella sua missione a un dipendente esperto di Rexel, come il reparto di revisione interna, il reparto finanziario, il reparto acquisti, un team di gestione nazionale o di zona, o qualsiasi altra persona all'interno del Gruppo Rexel che il responsabile delle indagini ritenga competente e necessaria, o a un fornitore di servizi esterno debitamente qualificato.

L'incarico dell'esperto terminerà automaticamente al completamento di tutte le operazioni di verifica o elaborazione relative alla segnalazione per la quale il responsabile delle indagini ha richiesto la sua assistenza, o su semplice richiesta del responsabile delle indagini.

L'esperto invitato è soggetto agli stessi obblighi di riservatezza del Responsabile interno e del Responsabile delle indagini.

4. Processo decisionale e chiusura dell'indagine

Se i fatti non sono provati, la segnalazione viene chiusa e l'autore della segnalazione ne viene informato.

Se i fatti sono provati, sulla base dei risultati dell'indagine, il Responsabile delle indagini determinerà se si sono verificate violazioni della legge, della Guida etica o del Codice di condotta anticorruzione e, in tal caso, raccomanderà azioni correttive e/o sanzioni appropriate.

La persona che ha effettuato la segnalazione viene informata per iscritto della chiusura dell'indagine.

Anche la persona interessata viene informata della chiusura dell'indagine. Quando, dopo l'indagine, la violazione risulta grave e provata, la direzione competente può adottare provvedimenti disciplinari, fino al licenziamento, nei confronti della persona interessata, a seconda della natura e della gravità dei fatti contestati.

IV. Protezione e garanzie offerte

1. Principi generali

Tutte le indagini saranno condotte in modo equo e nel pieno rispetto delle leggi e dei regolamenti locali applicabili. In tutti i casi, il Gruppo Rexel garantirà il rispetto del principio della presunzione di innocenza per le persone interessate.

Il sistema di segnalazione può funzionare solo sulla base di informazioni fornite in buona fede. Qualsiasi segnalazione effettuata in malafede, ovvero con l'unico intento di causare un danno, potrà essere soggetta a provvedimenti disciplinari, fino al licenziamento.

2. Informazioni

Il segnalante sarà informato entro sette (7) giorni lavorativi dal ricevimento della segnalazione.

Entro un termine ragionevole non superiore a tre (3) mesi dalla conferma di ricezione della segnalazione, l'autore della segnalazione viene informato per iscritto delle misure previste o adottate per valutare l'accuratezza delle accuse e, se del caso, per porre rimedio all'oggetto della segnalazione, nonché delle ragioni di tali misure. Qualora le accuse siano inesatte o infondate, o qualora la segnalazione sia diventata irrilevante, l'autore della segnalazione sarà informato per iscritto della chiusura del caso.

Qualsiasi persona coinvolta in una segnalazione ammissibile sarà informata della natura delle accuse che la riguardano. Tuttavia, nel caso di misure cautelari necessarie per impedire la distruzione di prove relative alla segnalazione, la persona interessata dalla segnalazione sarà informata solo dopo che tali misure saranno state adottate, in conformità con le leggi applicabili.

La persona oggetto di una segnalazione non potrà in alcun caso ottenere dal Gruppo Rexel, sulla base del proprio diritto di accesso, la divulgazione dell'identità della persona che ha effettuato la segnalazione.

Si precisa che il livello di informazione fornito può variare a seconda delle leggi locali applicabili.

3. Protezione in materia penale, civile e sociale

Si ricorda agli informatori che, fatte salve le normative locali applicabili:

- Essi non sono civilmente responsabili per i danni causati dalla loro segnalazione o divulgazione, a condizione che la segnalazione sia stata effettuata in conformità con le disposizioni applicabili e che l'autore della segnalazione avesse motivi ragionevoli per ritenere, al momento della segnalazione, che la segnalazione o la divulgazione pubblica di tutte queste informazioni fosse necessaria per salvaguardare gli interessi in gioco.
- Non sono penalmente responsabili per aver ottenuto o consultato informazioni riportate o divulgate pubblicamente, a condizione che tale ottenimento o consultazione non costituisca un reato penale separato ai sensi delle normative locali applicabili. Qualora tale ottenimento o consultazione costituisca un reato penale separato, si applicano le norme locali applicabili in materia di responsabilità penale.
- Non possono essere puniti, licenziati, discriminati (in particolare in termini di retribuzione, formazione, promozione) o sottoposti a ritorsioni o minacce o tentativi di applicare tali misure per aver segnalato o divulgato informazioni in conformità con le normative, a condizione che la segnalazione sia stata effettuata in buona fede.

Alle stesse condizioni, le persone che hanno facilitato la segnalazione di un informatore o che sono associate a quest'ultimo non possono essere oggetto di misure di ritorsione, minacce o tentativi di ricorrere a tali misure.

Il Gruppo Rexel non tollera alcuna forma di ritorsione, minaccia o tentativo di ricorrere a tali misure nei confronti degli informatori e dei loro familiari, come ad esempio le molestie.

4. Periodo di conservazione dei dati limitato

Le segnalazioni possono essere conservate solo per il tempo strettamente necessario e proporzionato al loro trattamento e alla protezione dei loro autori, delle persone che riguardano e di eventuali terzi citati, tenendo conto del tempo necessario per eventuali indagini supplementari. Tuttavia, i dati relativi alle segnalazioni possono essere conservati oltre tale periodo, a condizione che le persone interessate non siano identificate né identificabili.

Esistono diversi sistemi di archiviazione delle segnalazioni etiche:

- **Segnalazioni inammissibili** (segnalazioni che non rientrano nel campo di applicazione, non sono gravi, sono infondate, sono fatte in malafede, ecc.): queste vengono cancellate il prima possibile o archiviate e rese anonime.
- **Per le segnalazioni ammissibili:**
 - quando la segnalazione non è seguita da procedimenti disciplinari o legali, il Gruppo Rexel provvede affinché tutti gli elementi del fascicolo che potrebbero identificare l'autore della segnalazione, nonché quelli delle persone interessate, siano distrutti entro un termine massimo di due (2) mesi dalla fine delle operazioni di verifica o di indagine;
 - nei casi in cui l'indagine dia luogo a procedimenti legali o sanzioni disciplinari, gli elementi del

fascicolo vengono debitamente conservati per il periodo necessario, fino alla scadenza dei termini di prescrizione (sei (6) anni) o all'esaurimento di tutti i mezzi di ricorso. Quindi, una volta scaduto il termine prescritto, questi dati vengono distrutti o archiviati e resi anonimi.

5. Riservatezza e sicurezza

Il Gruppo Rexel adotta tutte le precauzioni necessarie per preservare la riservatezza e la sicurezza dei dati durante la loro raccolta, elaborazione, comunicazione o conservazione.

Fatte salve le normative locali applicabili, le procedure implementate per la raccolta e l'elaborazione delle segnalazioni garantiscono la massima riservatezza in merito all'identità degli autori della segnalazione, alle persone oggetto della segnalazione e alle informazioni raccolte dai responsabili della raccolta e dell'elaborazione della segnalazione.

A questo proposito:

- Le informazioni comunicate sono limitate alle persone che hanno una legittima necessità di conoscerle per trattare la segnalazione.
- Tutte le persone coinvolte nella gestione delle segnalazioni sono formate e soggette all'obbligo di riservatezza. In particolare, si impegnano a non utilizzare i dati per scopi impropri e a rispettare il periodo di conservazione dei dati limitato in conformità con la legge applicabile.
- La piattaforma di segnalazione online è sicura e le segnalazioni inviate possono essere visualizzate solo da persone autorizzate. Questo sistema consente anche ai dipendenti che desiderano rimanere anonimi di utilizzare questo canale.
- L'identità dell'informatore può essere rivelata alle autorità giudiziarie se richiesto dalla legge.
- Le informazioni che potrebbero identificare la persona coinvolta in una segnalazione non possono essere divulgate, se non alle autorità giudiziarie, una volta stabilita la validità della segnalazione.
- All'interno delle entità del Gruppo Rexel, i dipartimenti generalmente coinvolti nella gestione delle segnalazioni sono consapevoli della natura riservata dell'identità dell'autore e delle persone coinvolte.

6. Protezione dei dati personali

Nell'ambito del sistema di segnalazione, il Gruppo Rexel può raccogliere e trattare dati personali, in particolare quelli relativi all'autore di una segnalazione e alla persona o alle persone coinvolte. Una nota informativa dettagliata **nell'Appendice 4** illustra le condizioni in base alle quali i dati vengono raccolti, trattati, conservati e archiviati.

V. Segnalazione

Il Dipartimento Compliance del Gruppo riferisce una volta all'anno sul numero di segnalazioni, sulla loro tipologia e sulle azioni intraprese a seguito della loro ricezione, limitandosi ai dati strettamente necessari e proporzionati alla giustificazione della comunicazione.

VI. Aggiornamento della procedura

Il Gruppo Rexel si riserva il diritto di modificare, integrare o aggiornare la presente procedura in qualsiasi momento al fine di adattarla alle modifiche della legislazione, della normativa, della giurisprudenza o alle esigenze interne del Gruppo. Eventuali aggiornamenti saranno effettuati in conformità con le leggi e i regolamenti locali applicabili.

I dipendenti, i fornitori e gli altri soggetti interessati saranno informati delle modifiche con mezzi adeguati (comunicazione interna, e-mail, pubblicazione sulla intranet, informazione diretta ai fornitori, ecc.), in conformità con i requisiti legali locali.

La versione attuale e autorevole della presente procedura sarà pubblicata e resa disponibile sui siti web del Gruppo Rexel, sulla intranet del Gruppo e sulla piattaforma di segnalazione online.

Contatto

Società: Rexel Développement

Indirizzo: 13 boulevard Fort de Vaux 75017 Parigi (Francia) – *All'attenzione del Dipartimento Compliance del Gruppo.*

Indirizzo e-mail: compliance@rexel.com

Segnalare una situazione

Se sospetti o sei a conoscenza di una violazione della legge, della Guida etica o del Codice di condotta anticorruzione, segnalala!



Chi può segnalare un'irregolarità?

e i terzi possono utilizzare la linea etica.



Quando segnalare un caso?

Quando si viene a conoscenza o si sospetta una **violazione della legge**

o dei nostri principi etici.

Ciò può includere:

- atti di corruzione;
- violazioni dei diritti umani;
 - molestie
- o discriminazione;
- frodi, ecc.



È riservato?

Sì, ed è anche possibile inviare una segnalazione **anonima**



Sono protetto?

È necessario segnalare l'allerta in buona fede e senza alcun compenso economico diretto. In questo caso, sei protetto.



Come segnalare un problema?

1. Utilizza la **linea etica online di Rexel**
(link web sotto)
 - disponibile 24 ore su 24, 7 giorni su 7;
 - disponibile in tutte le lingue principali del Gruppo.
2. Utilizza il sistema di segnalazione istituito a livello locale.
3. Contattare l'Ufficio Legale o l'Ufficio Compliance o l'Ufficio Risorse Umane (di gruppo o locale)



Chi elabora questo avviso?

Per il Gruppo: il Comitato Etico.
Per il sistema locale: consultare la procedura locale.

Ulteriori

Visita : <https://www.rexel.com/en/ethical-alert/>

85

Appendice 2: Elenco dei paesi con procedure locali di segnalazione di irregolarità

In alcuni paesi questa procedura è integrata da procedure locali che stabiliscono i requisiti legali applicabili e, a seconda dei casi, i canali disponibili a livello locale.

Le informazioni sui canali locali sono elencate di seguito. Si prega di consultare la procedura locale per i dettagli più aggiornati.

- Australia:

o Servizio di segnalazione Rexel STOPline (gestito da un fornitore di servizi esterno indipendente):

Telefono: 1300 30 45 50

Fax: Rexel Holdings Australia (C/- the STOPline) 03 9882 4480

E-mail: rexel@stopline.com.au

Online: <https://rexel.stoplinereport.com/>

Posta: Rexel Holdings Australia

C/- the STOPline

Locked Bag 8

HAWTHORN VIC 3122

- Canada: è possibile contattare il Comitato Etico.

- Germania:

o E-mail: whistleblowing@rexel.de

o Posta:

Rexel Germany GmbH & Co.

KG - z. Hd. Frau Nicole Steuer | General Counsel

Ridlerstr.5780339 München

- Irlanda

o È possibile contattare il reparto Risorse umane, il responsabile delle segnalazioni, l'amministratore delegato o la nostra hotline esterna per le segnalazioni gestita da Safecall

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- Italia:

o <https://report.whistleb.com/rexel>

- Paesi Bassi: è possibile contattare il responsabile dell'etica.

- Svezia:

o <https://whistleblow.vismadraftit.se/rexel-sverige-ab>

o Telefono: 08-556 214 14.

- Regno Unito

o È possibile contattare il reparto Risorse umane, il responsabile delle segnalazioni, l'amministratore delegato o la nostra hotline esterna per le segnalazioni gestita da Safecall.

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- Stati Uniti

o E-mail per la conformità: ethics@rexelusa.com

o Helpline per la conformità: 1-800-714-8774

Appendice 3: Esempi di comportamenti o condotte scorrette contemplati dalla procedura di segnalazione di irregolarità

Categorie	Ambito
Corruzione	Nel quadro delle leggi e dei regolamenti locali applicabili e delle politiche anticorruzione del Gruppo: per corruzione si intende lo scambio, diretto o tramite terzi, di vantaggi (denaro, regali, inviti, servizi, contatti, ecc.) in cambio dell'esecuzione o dell'astensione dall'esecuzione di un atto correlato a una funzione o a un mandato. Può assumere la forma di una persona che propone o offre un vantaggio al fine di ottenere un favore (corruzione attiva) o di una persona che sollecita o accetta un vantaggio in cambio di un servizio (corruzione passiva). La corruzione può coinvolgere sia attori pubblici che privati, distorce la concorrenza, compromette la trasparenza delle decisioni ed espone le persone e le organizzazioni coinvolte a sanzioni e procedimenti penali.
Molestie	Le molestie si riferiscono a comportamenti ripetuti o a un singolo atto grave che compromette la dignità, la sicurezza o le condizioni di lavoro di una persona. Si manifestano con parole, gesti, atteggiamenti o azioni intesi a intimidire, umiliare, isolare, minacciare o degradare la situazione di un dipendente o di terzi in relazione all'attività professionale. Le molestie possono assumere una forma psicologica, come commenti denigratori, isolamento deliberato, sovraccarico o privazione delle risorse lavorative, ostracismo, diffusione di voci o sistematica svalutazione. Possono anche assumere una forma sessuale. Le molestie sessuali sono caratterizzate da comportamenti o commenti sessuali indesiderati che si ripetono o costituiscono un singolo episodio grave, che minano la dignità di una persona o creano un ambiente di lavoro intimidatorio, ostile, degradante o umiliante. Ciò include, tra le altre cose, avance persistenti, commenti sul corpo, richieste di favori sessuali, gesti o contatti fisici non consensuali o la diffusione di immagini sessuali senza consenso. Le molestie, sia morali che sessuali, sono inaccettabili e i responsabili sono perseguibili ai sensi delle leggi locali applicabili.

Discriminazione	La discriminazione sul posto di lavoro consiste nel trattare qualcuno in modo sfavorevole sulla base di criteri vietati dalla legge, quali l'origine, il sesso, lo stato civile, ecc. o qualsiasi altra caratteristica protetta dalla legge locale. La discriminazione può, ad esempio, tradursi in un trattamento iniquo nell'accesso al lavoro, nelle condizioni di lavoro, nella formazione, nella mobilità o in qualsiasi altra situazione legata all'attività professionale. Può assumere la forma di decisioni di assunzione, valutazione, promozione, assegnazione o licenziamento che svantaggiano una persona senza una giustificazione oggettiva basata sui requisiti della posizione. Sul posto di lavoro, la discriminazione può assumere due forme: - Discriminazione diretta. In questo caso, l'autore prende deliberatamente una decisione basata su un criterio discriminatorio vietato dalla legge. Discriminazione indiretta. In questo caso, l'autore prende una decisione che appare neutra ma che alla fine svantaggia alcune persone rispetto ad altre. Ad esempio, un regolamento interno consente solo agli uomini di rimanere in azienda dopo i 50 anni. Ciò costituisce quindi una discriminazione indiretta basata sul sesso e sull'età.
Salute/Sicurezza	Qualsiasi grave violazione o rischio per la salute e la sicurezza sul lavoro. La sicurezza sul lavoro si riferisce a tutte le misure e le pratiche volte a proteggere l'integrità fisica e mentale delle persone sul posto di lavoro, riducendo il rischio di incidenti, infortuni e malattie professionali. Ciò include l'identificazione e la valutazione dei rischi, l'attuazione di misure di sicurezza tecniche e organizzative, la formazione e l'informazione dei dipendenti e l'adozione di misure di prevenzione, intervento e risposta alle emergenze. Il rispetto di questi obblighi contribuisce a creare un ambiente di lavoro sicuro e conforme ai requisiti locali.
Diritti umani (diversi da discriminazione e molestie)	Qualsiasi grave violazione o rischio per i diritti umani e le libertà fondamentali riconosciuti a livello nazionale e internazionale, nonché qualsiasi violazione dei requisiti locali applicabili in questo settore. Ciò include, ma non si limita a, situazioni che coinvolgono principi quali il rispetto della libertà di associazione e di espressione, l'accesso a condizioni di lavoro dignitose e sicure e la possibilità per le persone interessate di avere accesso a mezzi di ricorso legali.
Conflitti di interesse	Un conflitto di interessi è una situazione in cui gli interessi personali di una persona, siano essi finanziari, familiari, di amicizia, politici o relativi ad altri benefici, possono influenzare, o sembrare influenzare, il suo giudizio o le sue decisioni nell'esercizio delle sue funzioni all'interno del Gruppo Rexel. Non si tratta necessariamente di una colpa o di un atto illegale, ma di un rischio di parzialità che compromette l'imparzialità prevista. Questo rischio di

	parzialità può essere sufficiente a minare la fiducia delle persone interessate, alterare la qualità delle decisioni e danneggiare la reputazione dell'organizzazione. Un conflitto di interessi può essere effettivo (già presente), potenziale (che potrebbe verificarsi) o apparente (percepito da terzi). Il sistema di segnalazione non è destinato a sostituire la procedura di segnalazione dei conflitti di interessi definita dal Gruppo Rexel.
Pratiche anticoncorrenziali	Le pratiche anticoncorrenziali si riferiscono a comportamenti aziendali che compromettono la libera concorrenza e danneggiano altri attori del mercato (clienti, fornitori, concorrenti). Esse comprendono accordi formali o informali tra concorrenti per coordinare i prezzi, le condizioni commerciali, la ripartizione dei mercati, dei territori o dei prodotti, o per limitare l'offerta o boicottare determinati partner. Includono anche situazioni di abuso di posizione dominante (ad esempio, l'eliminazione di un concorrente, l'imposizione di prezzi predatori o vendite abbinate ingiustificate), l'influenza sul prezzo di rivendita praticato dai distributori e lo scambio di informazioni strategiche non pubbliche che potrebbero influenzare il comportamento del mercato (come piani, dati di marketing o capacità). Queste pratiche sono vietate dalle norme sulla concorrenza e sono soggette a sanzioni significative.
Ambiente	Qualsiasi situazione in cui non siano rispettati i requisiti ambientali applicabili o in cui sia identificato un rischio o un danno significativo per l'ambiente, sia all'interno dell'azienda che tra i suoi partner nella catena del valore. Ciò comprende la prevenzione dell'inquinamento, l'uso responsabile delle risorse e la gestione sicura delle sostanze e dei rifiuti, in conformità con gli obblighi normativi e gli standard interni.
Frode	Qualsiasi situazione che comporti occultamento, inganno o manipolazione finalizzati a ottenere un vantaggio indebito o a eludere obblighi fiscali, finanziari o contabili. Ciò include, ad esempio, la falsificazione di documenti o registri, la presentazione di informazioni finanziarie non veritiere, l'occultamento di redditi o beni, o qualsiasi schema volto ad aggirare le norme applicabili, sia all'interno dell'azienda che nella sua catena del valore.
Insider trading	L'insider trading è l'atto di acquistare, vendere o raccomandare strumenti finanziari utilizzando o basandosi su informazioni privilegiate non di dominio pubblico relative a un emittente o ai suoi titoli. Comprende anche la divulgazione illegale di tali informazioni a terzi. Tale condotta conferisce un vantaggio sleale sui mercati ed è severamente vietata e punibile dalla legge.

Lavori fittizi	Un lavoro fittizio è una situazione in cui una persona viene retribuita per una posizione o mansioni che non vengono effettivamente svolte o che non esistono, al fine di ottenere un vantaggio sleale. Ciò può comportare la totale assenza di lavoro effettivo, mansioni fittizie o l'assegnazione nominale a un reparto senza alcun contributo reale, all'interno dell'azienda o tramite terzi.
Protezione dei dati personali / Sicurezza informatica	Qualsiasi situazione in cui i dati personali o i sistemi informatici non siano protetti in conformità con le leggi e le norme interne, esponendo le persone o l'azienda al rischio di accesso, utilizzo, divulgazione, modifica o distruzione non autorizzati. Ciò comprende la raccolta e il trattamento legittimi e ridotti al minimo dei dati, la sicurezza dei sistemi (controlli di accesso, crittografia, backup), la gestione degli incidenti e delle violazioni, nonché la riservatezza e l'integrità delle informazioni durante tutto il loro ciclo di vita, anche presso i fornitori di servizi. I dati personali sono tutte le informazioni che identificano direttamente o indirettamente una persona fisica (ad esempio, nome, recapiti, identificativi, foto, dati di localizzazione o altri elementi relativi alla sua identità o alla sua vita privata).

INFORMATIVA SULLA PRIVACY

—

SISTEMA DI SEGNALAZIONE

Versione 12/2025

Il Gruppo Rexel ha istituito un sistema professionale di segnalazione che consente ai propri dipendenti e ai terzi con cui il Gruppo Rexel intrattiene rapporti di segnalare atti illeciti o comportamenti scorretti. L'ambito di applicazione del sistema è descritto nella Procedura di segnalazione, disponibile sul sito web rexel.com.

 Nell'ambito di tale sistema, un'entità Rexel può raccogliere e trattare dati che vi riguardano. La riservatezza dei dati è alla base del nostro rapporto di fiducia. Pertanto, nel corso delle nostre attività commerciali prendiamo molto sul serio la protezione dei vostri dati personali.

La presente informativa illustra gli impegni del Gruppo Rexel in materia di protezione dei dati personali. La seguente informativa consente inoltre di conoscere i propri diritti e le condizioni alle quali i dati personali vengono raccolti, trattati, conservati e archiviati.

Chi siamo?

REXEL DEVELOPPEMENT SAS, società per azioni semplificata di diritto francese, con sede legale in 13, Boulevard du Fort de Vaux, Parigi, iscritta al Registro del Commercio e delle Imprese di Parigi con il numero 480 172 840, è il titolare del trattamento dei dati.

Anche l'entità del Gruppo che ha un contratto di lavoro con l'autore della segnalazione o che collabora con esso è titolare del trattamento.

Essi determinano le finalità e i mezzi del trattamento dei vostri dati.

Nella presente informativa sono indicati come "Rexel", "noi" o "Titolare del trattamento".

EY Polonia agisce in qualità di responsabile del trattamento per il trattamento effettuato sulla piattaforma di segnalazione online.

Come trattiamo i dati dell'utente nel contesto del sistema di segnalazione?

La tabella seguente illustra in dettaglio:

- (i) perché trattiamo i vostri dati personali,
- (ii) quali tipi di dati trattiamo e
- (iii) la base giuridica del trattamento dei dati.

Finalità 1	Tipo di dati
Raccogliere ed elaborare segnalazioni relative ad atti che violano la legge o il Codice di condotta anticorruzione contemplati dal sistema di segnalazione (vedere la Procedura di segnalazione). <u>Finalità secondarie:</u> - Gestione centralizzata delle segnalazioni professionali (ricezione e trattamento delle segnalazioni, creazione di un canale sicuro, archiviazione e conservazione delle informazioni, garanzia della sicurezza) - Trattamento delle segnalazioni professionali (condurre indagini interne, valutare i fatti rilevanti) - Processo decisionale e attuazione di misure appropriate al termine della segnalazione (notifica e attuazione delle misure) - Monitoraggio statistico e miglioramento del sistema di segnalazione - Esercizio o difesa dei diritti in procedimenti legali	Nell'ambito del sistema possono essere trattate le seguenti categorie di dati: - Dati identificativi (nome e cognome, recapiti), dati professionali (posizione, datore di lavoro, luogo di lavoro) della persona che effettua la segnalazione (a meno che la segnalazione non sia anonima) e qualsiasi altra informazione fornita volontariamente dalla stessa - Dati identificativi (nome e cognome, recapiti), dati professionali (posizione, datore di lavoro, luogo di lavoro) delle persone coinvolte - Dati identificativi (nome e cognome, indirizzo e-mail), dati professionali (posizione, datore di lavoro, luogo di lavoro) delle persone coinvolte o consultate nella raccolta o nel trattamento della segnalazione, nonché dei facilitatori e delle persone in contatto con l'informatore - Dati sensibili (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati relativi alla salute, vita sessuale o orientamento sessuale) ove strettamente necessario per l'esercizio o la difesa di un diritto in sede giudiziaria (articolo 9, paragrafo 2, lettera f), del GDPR) o per motivi di interesse pubblico rilevante (articolo 9, paragrafo 2, lettera g), del GDPR) - Dati relativi a condanne penali e reati o misure di sicurezza correlate, ove strettamente necessario e in conformità con l'articolo 10 del GDPR - Informazioni raccolte nel corso della verifica dei fatti - Relazioni sulle operazioni di verifica - Dati relativi al seguito dato alla relazione
Base giuridica per il trattamento dei vostri dati Obbligo legale di attuare un sistema di segnalazione di irregolarità: in particolare gli articoli 8.I.B e 17 II della legge Sapin II e l'articolo L. 225-102-4 del Codice di commercio, nonché qualsiasi legge equivalente relativa alla protezione degli informatori, alla lotta contro la corruzione o al dovere di vigilanza.	

Finalità 2	Tipo di dati
Raccogliere ed elaborare le segnalazioni relative ad atti che violano la Guida etica <u>Finalità secondarie:</u> - Gestione centralizzata delle segnalazioni professionali (ricezione e trattamento delle segnalazioni, creazione di un canale sicuro, archiviazione e conservazione delle informazioni, garanzia della sicurezza) - Trattamento delle segnalazioni professionali (condurre indagini interne, valutare i fatti rilevanti) - Processo decisionale e attuazione di misure appropriate al termine della segnalazione (notifica e attuazione delle misure) - Monitoraggio statistico e miglioramento del sistema di segnalazione - Esercizio o difesa dei diritti in procedimenti legali	Nell'ambito del sistema possono essere trattate le seguenti categorie di dati: - Dati identificativi (nome e cognome, recapiti), dati professionali (posizione, datore di lavoro, luogo di lavoro) della persona che effettua la segnalazione (a meno che la segnalazione non sia anonima) e qualsiasi altra informazione fornita volontariamente dalla stessa - Dati identificativi (nome e cognome, recapiti), dati professionali (posizione, datore di lavoro, luogo di lavoro) delle persone coinvolte - Dati identificativi (nome e cognome, indirizzo e-mail), dati professionali (posizione, datore di lavoro, luogo di lavoro) delle persone coinvolte o consultate nella raccolta o nel trattamento della segnalazione, nonché dei facilitatori e delle persone in contatto con l'informatore - Dati sensibili (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati relativi alla salute, vita sessuale o orientamento sessuale) ove strettamente necessario per l'esercizio o la difesa di un diritto in sede giudiziaria (articolo 9, paragrafo 2, lettera f) del GDPR) o per motivi di interesse pubblico rilevante (articolo 9, paragrafo 2, lettera g) del GDPR) - Dati relativi a condanne penali e reati o misure di sicurezza correlate, ove strettamente necessario e in conformità con l'articolo 10 del GDPR - Informazioni raccolte nel corso della verifica dei fatti - Relazioni sulle operazioni di verifica - Dati relativi al seguito dato alla relazione
Base giuridica per il trattamento dei tuoi dati	
Base giuridica: interesse legittimo al trattamento delle segnalazioni di natura etica non contemplate da un obbligo giuridico.	

Chi sono i destinatari dei tuoi dati?



I dati personali che raccogliamo, così come eventuali dati raccolti successivamente, sono destinati a noi in qualità di titolari del trattamento.



Garantiamo che solo le persone autorizzate abbiano accesso a questi dati.

Internamente:

- I responsabili della raccolta e del trattamento delle segnalazioni, ovvero:
 - I membri del Comitato Etico del Gruppo Rexel
 - I membri autorizzati dell'Ufficio Legale o dell'Ufficio Compliance a livello di Gruppo e locale
 - I membri autorizzati del dipartimento Risorse umane a livello di Gruppo e locale
- Membri autorizzati del dipartimento di revisione e controllo interno a livello di gruppo e locale per garantire l'efficacia dei controlli interni e della governance
- Quando la situazione lo giustifica, altri membri del personale interno possono avere accesso ai dati, in particolare quando sono richieste competenze contabili, finanziarie, legali, tecniche o informatiche.

Esternamente:

- I nostri consulenti
- I nostri broker e assicuratori
- I nostri revisori
- Le autorità competenti (organi giudiziari, amministrativi e normativi), in conformità con le normative applicabili
- I nostri fornitori di servizi, e più specificatamente EY Polonia, che ci fornisce la piattaforma di segnalazione online.

Questi destinatari hanno sede nell'Unione Europea.

Per quanto tempo conserviamo i vostri dati?

Situazioni	Periodo di conservazione
Segnalazioni inammissibili (non rientranti nell'ambito di applicazione, non gravi, prive di informazioni, effettuate in malafede, ecc.)	Cancellazione o archiviazione e anonimizzazione il prima possibile
Segnalazione ammissibile ma respinta (non seguita da procedimenti disciplinari o legali)	Cancellazione o anonimizzazione e archiviazione entro due (2) mesi
Segnalazioni che danno luogo a procedimenti disciplinari o legali	Conservazione dei dati fino alla conclusione del procedimento e dei ricorsi. Dopo tale periodo, cancellazione o anonimizzazione e archiviazione.

Quali sono i tuoi diritti?



In conformità con le leggi sulla protezione dei dati personali, hai i seguenti diritti:

- diritto di accesso: puoi accedere alle informazioni che deteniamo su di te e ottenerne una copia;
- diritto di rettifica: puoi far modificare, completare, aggiornare o cancellare qualsiasi dato inesatto che ti riguarda;
- diritto di opposizione: puoi opporsi al trattamento dei tuoi dati, a meno che non sussistano motivi legittimi e convincenti che ci consentano di trattarli;
- diritto alla cancellazione: puoi richiederci di cancellare i dati che ti riguardano nei limiti delle condizioni stabilite dall'articolo 17 del GDPR;
- diritto alla portabilità dei dati: potete recuperare i vostri dati per trasferirli a un'altra organizzazione o per uso personale;
- diritto alla limitazione del trattamento;
- diritto di formulare linee guida specifiche e generali relative alla conservazione, alla cancellazione e alla comunicazione dei propri dati dopo la propria morte.

Qualsiasi persona oggetto di una segnalazione sarà informata il prima possibile (entro un mese al massimo) a seguito della registrazione, informatizzata o meno, dei dati che la riguardano, al fine di consentirle di esercitare i propri diritti. Tuttavia, se tale informazione è suscettibile di compromettere gravemente gli obiettivi del trattamento e, in particolare, lo svolgimento dell'indagine (ad esempio, se sussiste il rischio di distruzione delle prove), tale informazione potrà essere differita e sarà fornita solo una volta eliminato qualsiasi rischio.

La persona oggetto di una segnalazione non può in alcun caso ottenere dal responsabile del trattamento, in base al proprio diritto di accesso, informazioni relative all'identità dell'autore della segnalazione o di qualsiasi altra persona coinvolta nell'indagine.

Se non ricevi una risposta, se ritieni che la risposta non sia soddisfacente o se ritieni che il trattamento dei tuoi dati non sia conforme alle disposizioni di legge e regolamentari, puoi contattare l'autorità di controllo competente.

Come esercitare i propri diritti?



Mediante richiesta scritta al nostro responsabile della protezione dei dati:

Paesi	Entità	Indirizzo
Austria	COMTECH IT-SOLUTIONS GMBH	datenschutz@rexel.at
	Rexel Austria GmbH	datenschutz@rexel.at
Belgio	Rexel Belgique SA	gdpr@rexel.be
Francia	Cordia	donnees.personnelles@francofa-eurodis.fr
	Rexel Développement SAS / Gruppo Rexel	data.protection@rexel.com
	Rexel France SAS	donnees.personnelles@rexel.fr
	Bizline	data.protection@rexel.com
	Gigamedia	data.protection@rexel.com
	Sofinther SAS	donnees.personnelles@sofinther.fr
	Espace Elec SAS	donnees.personnelles@espace-elec.fr
	Esabora Digital Services SAS	dataprotection-rda@rexel.fr
	Francofa Eurodis	donnees.personnelles@francofa-eurodis.fr
	Freshmile Services SAS	donnees.personnelles@rexel.fr
	ITESA	donnees.personnelles@rexel.fr
Germania	REXEL GERMANY BETEILIGUNGS GMBH	Datenschutzbeauftragter@rexel.de
	Rexel Germany GmbH & Co KG	Datenschutzbeauftragter@rexel.de
	REXEL GERMANY VERWALTUNGS GMBH	Datenschutzbeauftragter@rexel.de
Italia	Rexel Italia S.p.A	dataprotection@rexel.it
	Tecno-Bi S.r.l.	dataprotection@rexel.it
	Comm-Tech S.r.l.	dataprotection@rexel.it
Irlanda	M. Kelliher 1998	data.protection@rexel.ie
	Rexel Industrial Solutions	data.protection@rexel.ie
Lussemburgo	Rexel Luxembourg SA	gdpr@rexel.be
Paesi Bassi	Rexel Nederland B.V	AVG@rexel.nl
	Wasco Group B.V.	AVG@rexel.nl
	Wasco Holding B.V.	AVG@rexel.nl
	Wasco Groothandels Greop B.V.	AVG@rexel.nl
	Wasco Distributlecentrum B.V.	AVG@rexel.nl
Slovenia	Rexel d.o.o.	dpc@rexel.si
Svezia	Rexel Sverige AB	dataskydd@rexel.se
Svizzera	ELEKTRO-MATERIAL AG	datenschutz@e-m.ch
	Rexel 3S	data.protection@rexel.com
Regno Unito	Rexel (UK) Ltd.	data.protection@rexel.co.uk



Klokkenluidersprocedure December 2025_V1

Samenvatting

I.	<u>Inleiding</u>	3
1.	<u>Doel van het interne klokkenluiderssysteem</u>	3
2.	<u>Herinnering aan het wettelijk kader</u>	3
3.	<u>Toepassingsgebied</u>	3
II.	<u>Het verzamelen van ethische meldingen</u>	4
1.	<u>Voorwaarden voor de ontvankelijkheid van een ethische melding</u>	4
	<u>Wie kan een melding doen?</u>	4
	<u>Hoe kunt u profiteren van de status van klokkenluider en de bijbehorende wettelijke bescherming?</u>	4
	<u>Welke feiten kunnen worden gemeld?</u>	5
2.	<u>Hoe dient u een melding in?</u>	6
3.	<u>Inhoud van de melding</u>	7
4.	<u>Anonieme meldingen</u>	7
5.	<u>Externe kanalen</u>	7
III.	<u>Behandeling van interne ethische meldingen</u>	7
1.	<u>Bevestiging van ontvangst van de melding</u>	7
2.	<u>Beoordeling van de ontvankelijkheid van de melding</u>	7
3.	<u>Uitvoering van het interne onderzoek</u>	8
4.	<u>Besluitvorming en afsluiting van het onderzoek</u>	9
IV.	<u>Boden Schutz und Garantien</u>	10
1.	<u>Algemene beginselen</u>	10
2.	<u>Informatie</u>	10
3.	<u>Bescherming in strafrechtelijke, civielrechtelijke en sociale aangelegenheden</u>	10
4.	<u>Bepaalde bewaartermijn voor gegevens</u>	11
5.	<u>Vertrouwelijkheid en veiligheid</u>	11
6.	<u>Bescherming van persoonsgegevens</u>	12
V.	<u>Rapportage</u>	12
VI.	<u>Actualisering van de procedure</u>	12
	<u>Bijlage 1: Samenvatting</u>	13
	<u>Bijlage 2: Lijst van landen met lokale klokkenluidersprocedures</u>	14
	<u>Bijlage 3: Voorbeelden van gedragingen of wangedragingen die onder de klokkenluidersprocedure vallen</u>	15
	<u>Bijlage 4: Privacybeleid</u>	19

I. Inleiding

1. Doel van het interne klokkenluiderssysteem

Als onderdeel van het ethiek- en nalevingsbeleid van de Rexel Groep, zoals met name beschreven in de Ethische Gids, het Handvest voor Verantwoordelijke Leveranciers en de Gedragscode tegen Corruptie, heeft de Rexel Groep een intern klokkenluiderssysteem opgezet.

Het interne klokkenluiderssysteem van de Rexel Groep stelt elke werknemer, evenals derden met wie de Rexel Groep een relatie heeft, in staat om situaties te melden die in strijd zijn met de wet, de Ethische Gids van de Rexel Groep of haar Gedragscode tegen corruptie.

Het doel van deze procedure is het beschrijven van het proces voor het verzamelen en behandelen van ethische meldingen binnen de Rexel Groep.

Een samenvatting van de procedure is opgenomen in **bijlage 1**.

2. Herinnering aan het wettelijk kader

Aangezien de holdingmaatschappij van de Rexel Groep in Frankrijk is gevestigd, is de procedure opgesteld in overeenstemming met de volgende Franse wetten:

- De Sapin II-wet van 9 december 2016 inzake transparantie, corruptiebestrijding en economische modernisering;
- De wet van 27 maart 2017 inzake de "waakzaamheidsplicht" van moedermaatschappijen en contracterende bedrijven;
- De wet "Waserman" van 21 maart 2022, gericht op het verbeteren van de bescherming van klokkenluiders, en het uitvoeringsbesluit daarvan van 3 oktober 2022.

De procedure is ook gebaseerd op een aantal publicaties van het Franse Agentschap voor Corruptiebestrijding (AFA) en de Franse Autoriteit voor Gegevensbescherming (CNIL):

- De aanbevelingen van het AFA;
- De praktische gids "Interne anticorruptieonderzoeken", gepubliceerd in maart 2023 door het AFA en het Franse Openbaar Ministerie voor Financiën;
- Het referentiedocument "professionele waarschuwingen" van de CNIL, dat oorspronkelijk in 2019 werd gepubliceerd en in 2023 werd bijgewerkt.

Meer in het algemeen worden meldingen verzameld en verwerkt in overeenstemming met de toepasselijke wet- en regelgeving, en deze procedure kan indien nodig worden bijgewerkt om rekening te houden met ontwikkelingen in de wetgeving en beste praktijken.

Als een lokale wet of regelgeving meer beschermende regels voor klokkenluiders biedt dan deze procedure, prevaleren de lokale bepalingen. Wanneer deze procedure echter meer beschermende garanties biedt, zal de Rexel Group deze vrijwillig toepassen voor zover dit door de toepasselijke wetgeving is toegestaan.

3. Toepassingsgebied

Deze procedure is bedoeld om te worden geïmplementeerd in alle entiteiten van de Rexel Groep. Zij zal indien nodig worden aangepast om rekening te houden met wijzigingen in wet- en regelgeving.

Deze procedure wordt in bepaalde landen binnen de Rexel-groep aangevuld met lokale procedures. Deze specificeren de toepasselijke wettelijke vereisten en, in voorkomend geval, de lokaal beschikbare kanalen (zie **bijlage 2**).

De auteur van een melding kan dus het meldingskanaal van zijn keuze kiezen (groeps- of lokaal). De toepasselijke procedure is dan die welke overeenkomt met het gekozen kanaal. Afhankelijk van de aard en de ernst van het gemelde gedrag of de gemelde misstanden, kan een melding via het lokale kanaal worden doorgestuurd naar de groep en omgekeerd.

Deze procedure is van toepassing op alle werknemers van de Rexel-groep (ongeacht hun functie, positie of afdeling) en op derden waarmee de Rexel-groep een relatie heeft. Ze heeft betrekking op het verzamelen en verwerken van interne meldingen door de Rexel-groep en meer bepaald op:

- Het indienen ervan;
- De ontvangst ervan;
- De beoordeling van hun ontvankelijkheid;
- De belangrijkste stappen van het interne onderzoek
- De afsluiting van de zaak.

II. Het verzamelen van ethische waarschuwingen

1. Voorwaarden voor de ontvankelijkheid van een ethische melding

Wie kan een melding doen?

Het interne waarschuwingssysteem van de Rexel Group staat open voor de volgende personen:

- Werknemers van de Rexel Groep (vaste werknemers, werknemers met een tijdelijk contract, stagiaires, stagiairs)
- Externe of tijdelijke werknemers (uitzendkrachten, consultants, enz.)
- Sollicitanten
- Voormalige werknemers
- Aandeelhouders, partners en houders van stemrechten op de algemene vergadering
- Leden van het bestuurs-, uitvoerend comité of toezichthoudende organen
- Alle externe medewerkers waarmee de Rexel Groep een relatie heeft (bijv. klanten, leveranciers, dienstverleners, enz.).

Het interne klokkenluiderssysteem staat open voor alle entiteiten van de Rexel Groep en is beschikbaar in de belangrijkste talen van de Groep: Engels, Duits, Chinees, Frans, Italiaans, Nederlands, Zweeds en Sloveens.

Hoe kunt u profiteren van de status van klokkenluider en de bijbehorende wettelijke bescherming?

Om als klokkenluider te worden beschouwd en te profiteren van de bescherming die de wet biedt, moet u voldoen aan de wettelijke definitie van klokkenluider, namelijk door aan alle volgende criteria te voldoen, tenzij anders bepaald door de toepasselijke lokale wetgeving:

- Een natuurlijke persoon zijn;
- U ontvangt geen directe financiële vergoeding voor de melding;
- Te goeder trouw handelen;
- Als de gemelde feiten buiten een professionele context zijn verkregen, moet u persoonlijke kennis hebben van de gemelde feiten.

Welke feiten kunnen worden gemeld?

Het interne klokkenluiderssysteem van de Rexel Group maakt het mogelijk om meldingen te doen over feiten die kunnen vallen onder de volgende categorieën van gedrag of wangedrag:

- Een misdrijf of overtreding
- Een bedreiging voor of schade aan het algemeen belang
- Een overtreding of poging tot het verbergen van een overtreding van nationale, Europese of internationale wet- en regelgeving
- Een inbreuk op of situatie die in strijd is met de Ethische Gids of de Gedragscode tegen corruptie van de Rexel Groep
- Ernstige risico's in verband met de activiteiten van de Rexel Groep die schade kunnen toebrengen aan de mensenrechten, fundamentele vrijheden, de gezondheid en veiligheid van mensen of het milieu

Voorbeelden van gedragingen of wangedragingen die moeten worden gemeld, zijn onder meer:

- Corruptie, met inbegrip van elke schending van de gedragscode inzake corruptiebestrijding
- Intimidatie (psychologisch of seksueel)
- Discriminatie
- Gezondheid, hygiëne of veiligheid (bijv. risico voor lichamelijke of geestelijke integriteit)
- Mensenrechten (anders dan discriminatie, privacy en intimidatie)
- Belangenconflict
- Concurrentieverstorende praktijken
- Milieu (bijv. vervuiling, afvalbeheer)
- Belastingfraude
- Financiële of boekhoudkundige fraude
- Handel met voorkennis
- Fictieve banen
- Persoonsgegevens/IT-beveiliging

Bijlage 3 illustreert enkele van deze soorten gedragingen of wangedragingen.

Meldingen die betrekking hebben op categorieën die hierboven niet zijn vermeld, vallen niet onder het toepassingsgebied van deze procedure. Evenzo zijn feiten, informatie of documenten, ongeacht hun vorm of medium, waarvan de openbaarmaking verboden is door bepalingen van met betrekking

tot staatsgeheimen, medisch geheim, geheimhouding van gerechtelijke beraadslagingen, geheimhouding van gerechtelijke onderzoeken of verhoren, of het beroepsgeheim van advocaten, uitgesloten van deze procedure. Indien van toepassing wordt de auteur van de melding hiervan op de hoogte gesteld en doorverwezen naar de personen die bevoegd zijn om de gemelde feiten te behandelen.

2. Hoe een melding indienen

De auteur van een melding heeft verschillende kanalen om een melding in te dienen:

- Het online meldingsplatform dat toegankelijk is via: <https://www.rexel.com/en/rexel-group-ethics-alert>;
- Aanvullende meldingskanalen die op groeps- of lokaal niveau kunnen bestaan.

Er is geen hiërarchie tussen de kanalen. De auteur van een melding kan elk kanaal gebruiken dat hem ter beschikking staat.

Ongeacht het gebruikte kanaal worden de personen die verantwoordelijk zijn voor het verzamelen van meldingen hierna aangeduid als "**interne manager(s)**".

Het online meldingsplatform

De auteur van een melding kan, ook anoniem, een waarschuwing geven op het online meldingsplatform dat toegankelijk is via: <https://www.rexel.com/en/rexel-group-ethics-alert>

Dit is een speciaal, gratis platform dat 24 uur per dag en 7 dagen per week beschikbaar is.

Het wordt in de Europese Unie gehost door een externe dienstverlener (EY) die strenge maatregelen neemt om de veiligheid en vertrouwelijkheid van de gegevens te waarborgen. Opgemerkt moet worden dat de medewerkers van deze dienstverlener niet betrokken zijn bij de verwerking van meldingen en geen toegang hebben tot de uitgewisselde informatie.

Dit platform maakt directe communicatie met de ontvanger van de melding via chat mogelijk. Het stelt de auteur van de melding ook in staat om documenten te versturen ter ondersteuning van de feiten.

De link naar dit platform is beschikbaar op de websites van de Groep: <https://www.rexel.com/en/rexel-group-ethics-alert> en <https://ethique.rexel.com/en/>, evenals op de intranetsites van de entiteiten van de Rexel Groep.

Aanvullende meldingskanalen

Interne medewerkers van de Rexel Group kunnen een melding schriftelijk of mondeling indienen bij een van de volgende interne managers: (i) de lokale compliance manager (juridische of compliance-afdeling), (ii) de lokale personeelsafdeling, (iii) de compliance-afdeling van de groep, of (iv) de personeelsafdeling van de groep.

De afdeling Human Resources (lokaal of van de Groep) verzamelt doorgaans meldingen van overtredingen van de arbeidswetgeving of ongepast gedrag op het werk (intimidatie, discriminatie, gezondheid, hygiëne of veiligheid, enz.).

De lokale compliance officer of de complianceafdeling van de groep verzamelt doorgaans meldingen van overtredingen van de wet, de ethische gids, de anticorruptiegedragscode en de complianceprocedures van de Rexel Groep, enz.

Wanneer een melding mondeling wordt gedaan, kan deze telefonisch worden ontvangen en, op verzoek van de persoon die de melding doet en naar zijn/haar keuze, tijdens een videoconferentie of een fysieke vergadering die uiterlijk twintig (20) werkdagen na ontvangst van het verzoek wordt georganiseerd. Mondelinge meldingen worden schriftelijk vastgelegd.

Werknemers kunnen in ieder geval advies inwinnen bij hun directe of indirecte lijnmanager en hun bezorgdheid kenbaar maken, behalve wanneer de lijnmanager zelf de vermeende dader van het betreffende gedrag is. Als na een dergelijk gesprek blijkt dat deze bezorgdheid binnen het toepassingsgebied van deze procedure valt, moet de lijnmanager de werknemer aanmoedigen om een melding te doen via de hierboven aangegeven kanalen of door contact op te nemen met de lokale juridische of compliance-afdeling of de lokale personeelsafdeling.

3. Inhoud van de melding

De auteur van een melding moet de feiten en informatie die het onderwerp van zijn melding vormen op een nauwkeurige en objectieve manier presenteren, zodat de melding kan worden behandeld.

Waar mogelijk moet hij zijn melding onderbouwen door:

- de datum(s) en plaats(en) waarop de gemelde feiten zich hebben voorgedaan, de betrokken entiteit en de identiteit en functie van de betrokken persoon (personen) te vermelden;
- een gedetailleerde beschrijving van de feiten geven met specifieke en feitelijke informatie die rechtstreeks verband houdt met het onderwerp van de waarschuwing, ongeacht de vorm of het medium ervan.

4. Anonieme meldingen

Het verdient de voorkeur dat de auteur van een melding zich identificeert, met name om het onderzoek te vereenvoudigen. De auteur van een melding kan er echter voor kiezen om een anonieme melding te doen, zoals voorzien in het online meldingsplatform, op voorwaarde dat (i) de ernst van de feiten is vastgesteld en (ii) de feitelijke elementen voldoende gedetailleerd zijn.

5. Externe kanalen

Onder voorbehoud van de naleving van de toepasselijke lokale regelgeving, moet worden opgemerkt dat de auteur van een melding ook de mogelijkheid heeft om een externe melding te doen bij (i) de bevoegde autoriteit, (ii) de ombudsman, (iii) de gerechtelijke autoriteit, of (iv) elke relevante lokale of internationale instelling, instantie of agentschap die bevoegd is om dergelijke meldingen in ontvangst te nemen. Melders kunnen externe meldingen rechtstreeks bij een autoriteit indienen of nadat zij een melding bij de Rexel Group hebben ingediend.

III. Behandeling van interne ethische meldingen

1. Bevestiging van ontvangst van de melding

Wanneer de melding wordt ontvangen op het online meldingsplatform of via traditionele kanalen, bevestigt de interne manager (de persoon die verantwoordelijk is voor het verzamelen van meldingen zoals hierboven gedefinieerd) de ontvangst van de melding binnen zeven (7) werkdagen na ontvangst.

Bevestiging van ontvangst houdt geen aanvaarding van de melding in.

2. Beoordeling van de ontvankelijkheid van de melding

Elke ontvangen melding wordt door de interne manager voorlopig geanalyseerd om na te gaan of deze binnen het toepassingsgebied van de procedure valt en om de ontvankelijkheid ervan te garanderen.

Deze verificatie, waarvoor mogelijk contact moet worden opgenomen met de auteur of de melding, richt zich met name op de volgende punten:

- **De status van de auteur als "klokkenluider"**: in het bijzonder dat hij te goeder trouw handelt en geen directe financiële compensatie nastreeft;
- **De aard van de melding**: dat deze inderdaad valt onder een van de categorieën meldingen die onder de procedure vallen;
- **De inhoud van het rapport**: dat de gerapporteerde informatie en feiten objectief en voldoende gedetailleerd zijn om een onderzoek te kunnen starten;
- **Het bestaan van beschermde geheimen**: dat de melding geen feiten onthult die onder het staatsgeheim, het medisch beroepsgeheim, het geheim van de beraadslaging, het geheim van het gerechtelijk onderzoek of het geheim van de advocaat-cliëntrelatie vallen.

De beslissing over de ontvankelijkheid wordt genomen door de interne manager. De auteur van een melding wordt in kennis gesteld van de niet-ontvankelijkheid van zijn melding, indien van toepassing, en van de redenen voor deze beslissing.

In ieder geval moet de interne manager binnen drie (3) maanden een eerste reactie geven. De Rexel Group is niet verplicht om de melding binnen deze termijn te behandelen, maar moet de auteur van de melding informeren over de geplande of reeds genomen maatregelen om de geldigheid van de melding te beoordelen en de gemelde situatie te verhelpen.

De melding wordt volledig vertrouwelijk behandeld.

Afhankelijk van de aard en de ernst van de gemelde feiten kan de melding worden behandeld door de Ethische Commissie van de Rexel Groep. De Ethische Commissie van de Rexel Groep is een ad-hoccommissie die is opgericht binnen Rexel Développement en die tot taak heeft de ernstigste meldingen te behandelen die zijn gedaan door werknemers van Rexel of door derden waarmee Rexel een relatie heeft.

De Ethische Commissie van de Rexel Groep bestaat uit drie permanente leden:

- de secretaris-generaal,
- de directeur Human Resources van de groep en
- de directeur Ethiek & Compliance

3. Het interne onderzoek uitvoeren

Doelstellingen en beheer van het interne onderzoek

De tijd die nodig is om een melding te verwerken, varieert en is afhankelijk van de complexiteit van de gemelde feiten en de aard van de verstrekte informatie.

Het doel van het interne onderzoek is om de juistheid en relevantie van de gemelde feiten te verifiëren. De melding wordt onderzocht met behulp van methoden (interviews, gegevensonderzoek, enz.) die kunnen variëren afhankelijk van de context en de aard van het onderwerp.

Dit onderzoek kan worden uitgevoerd door:

- (xxi) de lokale afdeling Human Resources;
- (xxii) de lokale compliance- of juridische afdeling;
- (xxiii) de complianceafdeling van de groep;
- (xxiv) de personeelsafdeling van de groep;
- (xxv) de Ethische Commissie van de Rexel Groep, afhankelijk van de aard en ernst van de gemelde feiten

(hierna de "**onderzoeksmanager**" genoemd).

In elk geval zal de onderzoeksmanager het interne onderzoek naar de melding leiden. Informatie over het bestaan en de inhoud van de melding wordt alleen bekendgemaakt aan de personen die verantwoordelijk zijn voor het onderzoek, voor zover dat strikt noodzakelijk is.

Wanneer een melding wordt ingediend, garandeert de Rexel Groep de onafhankelijkheid van het onderzoeksproces. Alvorens een intern onderzoek te starten, wordt gecontroleerd of geen van de personen die bij het onderzoek naar de melding betrokken zijn, direct of indirect betrokken is bij de gemelde feiten of een belangenverband heeft met de betrokken personen. Als er een risico op belangenverstrengeling wordt vastgesteld, wordt de betrokken werknemer onmiddellijk uit het proces verwijderd en vervangen. Dit principe van onafhankelijkheid maakt integraal deel uit van het ethiek- en nalevingssysteem van Rexel en heeft tot doel een rigoureuze, onpartijdig en geloofwaardig beheer van alle ontvangen meldingen te waarborgen.

Inbeslagname van e-mails, documenten of computermedia

Het interne onderzoek kan het nodig maken om e-mails of computermedia van een of meer werknemers te bekijken en te verwerken. Alvorens e-mailaccounts of computermedia in beslag te nemen of te bevriezen, moet de onderzoeksmanager toestemming vragen, zoals bepaald in de lokale procedure (bijvoorbeeld aan de Ethische Commissie van de Groep, de lokale General Counsel of de lokale Data Protection Correspondent), om deze e-mails in beslag te nemen en te bewaren voor onderzoeksdoeleinden.

Gastdeskundige

Wanneer de situatie dit rechtvaardigt, kan de onderzoeksmanager besluiten om een of meer personen uit te nodigen om hem of haar bij te staan in het specifieke kader van de behandeling van een specifieke melding, met name als er boekhoudkundige, financiële, technische of IT-expertise vereist is.

De onderzoeksmanager kan dus besluiten om voor zijn of haar taak hulp in te roepen van een deskundige medewerker van Rexel, zoals de interne auditafdeling, de financiële afdeling, de inkoopafdeling, een managementteam van een land of zone, of een andere persoon binnen de Rexel-groep die de onderzoeksmanager competent en noodzakelijk acht (), of van een gekwalificeerde externe dienstverlener.

De opdracht van de deskundige eindigt automatisch bij voltooiing van alle verificatie- of verwerkingshandelingen met betrekking tot de melding waarvoor de onderzoeksmanager om hun hulp heeft gevraagd, of op eenvoudig verzoek van de onderzoeksmanager.

De uitgenodigde deskundige is onderworpen aan dezelfde geheimhoudingsverplichtingen als de interne manager en de onderzoeksmanager.

4. Besluitvorming en afsluiting van het onderzoek

Als de feiten niet worden bewezen, wordt de melding gesloten en wordt de auteur van de melding hiervan op de hoogte gesteld.

Als de feiten worden bewezen, bepaalt de onderzoeksmanager op basis van de bevindingen van het onderzoek of er sprake is van schendingen van de wet, de ethische gids of de anticorruptiegedragscode en, zo ja, beveelt hij corrigerende maatregelen en/of passende sancties aan.

De persoon die de melding heeft gedaan, wordt schriftelijk op de hoogte gebracht van de afsluiting van het onderzoek.

Ook de betrokken persoon wordt op de hoogte gebracht van de afsluiting van het onderzoek. Wanneer na onderzoek blijkt dat de overtreding ernstig en bewezen is, kan het betreffende management, afhankelijk van de aard en ernst van de vermeende feiten, disciplinaire maatregelen nemen tegen de betrokken persoon, tot en met ontslag.

IV. Bodem bescherming en garanties

1. Algemene beginselen

Alle onderzoeken worden eerlijk en in volledige overeenstemming met de toepasselijke lokale wet- en regelgeving uitgevoerd. In alle gevallen zorgt de Rexel Group ervoor dat het beginsel van het vermoeden van onschuld voor de betrokken personen wordt gerespecteerd.

Het klokkenluiderssysteem kan alleen functioneren op basis van informatie die te goeder trouw wordt verstrekt. Elke melding die te kwader trouw wordt gedaan, d.w.z. met als enig doel schade te berokkenen, kan worden onderworpen aan disciplinaire maatregelen, tot en met ontslag.

2. Informatie

De klokkenluider wordt binnen zeven (7) werkdagen na ontvangst van zijn melding op de hoogte gebracht.

Binnen een redelijke termijn van maximaal drie (3) maanden na ontvangstbevestiging van de melding wordt de auteur van de melding schriftelijk in kennis gesteld van de maatregelen die worden overwogen of genomen om de juistheid van de beschuldigingen te beoordelen en, indien nodig, de inhoud van de melding te verhelpen, alsmede van de redenen voor deze maatregelen. Wanneer de beschuldigingen onjuist of ongegrond zijn, of wanneer de melding irrelevant is geworden, wordt de auteur van de melding schriftelijk op de hoogte gebracht van de afsluiting van de zaak.

Elke persoon die betrokken is bij een ontvankelijke melding wordt in kennis gesteld van de aard van de beschuldigingen die op hem betrekking hebben. Indien echter voorzorgsmaatregelen nodig zijn om te voorkomen dat bewijsmateriaal met betrekking tot de melding wordt vernietigd, wordt de persoon op wie de melding betrekking heeft pas in kennis gesteld nadat deze maatregelen zijn genomen, overeenkomstig de toepasselijke wetgeving.

De persoon op wie een melding betrekking heeft, kan in geen geval op grond van zijn recht op toegang van de Rexel Group de identiteit van de persoon die de melding heeft gedaan, vernemen.

Er wordt opgemerkt dat het niveau van de verstrekte informatie kan variëren afhankelijk van de toepasselijke lokale wetgeving.

3. Bescherming in strafrechtelijke, civielrechtelijke en sociale aangelegenheden

Klokkenluiders worden eraan herinnerd dat, onder voorbehoud van de lokaal geldende regelgeving:

- zij niet civielrechtelijk aansprakelijk zijn voor schade die voortvloeit uit hun melding of openbaarmaking, op voorwaarde dat hun melding in overeenstemming met de toepasselijke bepalingen is gedaan en dat de auteur van een melding op het moment van de melding redelijke gronden had om aan te nemen dat de melding of openbaarmaking van al deze informatie noodzakelijk was om de belangen die op het spel stonden te beschermen.
- Zij zijn niet strafrechtelijk aansprakelijk voor het verkrijgen van of toegang krijgen tot informatie die openbaar is gemeld of bekendgemaakt, op voorwaarde dat het verkrijgen van of toegang krijgen tot deze informatie geen afzonderlijk strafbaar feit vormt volgens de lokaal geldende regelgeving. Wanneer het verkrijgen van of toegang krijgen tot deze informatie een afzonderlijk strafbaar feit vormt, zijn de lokaal geldende regels inzake strafrechtelijke aansprakelijkheid van toepassing.
- Zij mogen niet worden gestraft, ontslagen, gediscrimineerd (met name wat betreft beloning, opleiding, promotie) of onderworpen aan represailles of een dreiging of poging om dergelijke maatregelen toe te passen voor het melden of openbaar maken van informatie in overeenstemming met de regelgeving, op voorwaarde dat de melding te goeder trouw is gedaan.

Onder dezelfde voorwaarden mogen personen die de melding van een klokkenluider hebben gefaciliteerd of die met hen in verband staan, niet worden onderworpen aan vergeldingsmaatregelen, bedreigingen of pogingen om dergelijke maatregelen te nemen.

De Rexel Group tolereert geen enkele vorm van vergelding, bedreiging of poging tot vergelding tegen klokkenluiders en hun familieleden, zoals intimidatie.

4. Beperkte bewaartermijn voor gegevens

Meldingen mogen alleen worden bewaard zolang dit strikt noodzakelijk en evenredig is voor de verwerking ervan en voor de bescherming van de auteurs, de personen op wie zij betrekking hebben en eventuele derden die zij noemen, rekening houdend met de tijd die nodig is voor eventueel aanvullend onderzoek. Gegevens met betrekking tot meldingen mogen echter langer worden bewaard, op voorwaarde dat de betrokken personen niet worden geïdentificeerd of identificeerbaar zijn.

Er bestaan verschillende systemen voor het archiveren van ethische meldingen:

- **Ongeldige meldingen** (meldingen die niet binnen het toepassingsgebied vallen, niet ernstig zijn, niet onderbouwd zijn, te kwader trouw zijn gedaan, enz.): deze worden zo snel mogelijk verwijderd of gearchiveerd en geanonimiseerd.
- **Voor ontvankelijke meldingen:**
 - wanneer het rapport niet wordt gevolgd door disciplinaire of gerechtelijke procedures, zorgt de Rexel Groep ervoor dat alle elementen van het rapportdossier die de auteur van het

rapport of de betrokken personen zouden kunnen identificeren, binnen een termijn van maximaal twee (2) maanden na afloop van de verificatie- of onderzoeksoperaties worden vernietigd;

- in gevallen waarin het onderzoek leidt tot gerechtelijke procedures of disciplinaire sancties, worden de elementen van het dossier naar behoren bewaard gedurende de vereiste periode, totdat de verjaringstermijn is verstreken (zes (6) jaar) of alle beroepsmogelijkheden zijn uitgeput. Zodra de voorgeschreven termijn is verstreken, worden deze gegevens vernietigd of gearhiveerd en geanonimiseerd.

5. Vertrouwelijkheid en beveiligings

De Rexel Groep neemt alle nodige voorzorgsmaatregelen om de vertrouwelijkheid en veiligheid van gegevens te waarborgen tijdens het verzamelen, verwerken, communiceren of opslaan ervan.

Afhankelijk van de lokaal geldende regelgeving garanderen de procedures die worden toegepast voor het verzamelen en verwerken van meldingen strikte vertrouwelijkheid met betrekking tot de identiteit van de auteurs van de melding, de personen op wie de melding betrekking heeft en de informatie die wordt verzameld door de personen die verantwoordelijk zijn voor het verzamelen en verwerken van de melding.

In dit verband:

- De meegedeelde informatie is beperkt tot die personen die een legitieme behoefte hebben om deze te kennen om de melding te kunnen verwerken.
- Alle personen die betrokken zijn bij het beheer van meldingen zijn opgeleid en onderworpen aan een geheimhoudingsplicht. Zij verbinden zich er met name toe de gegevens niet voor oneigenlijke doeleinden te gebruiken en zich te houden aan de beperkte bewaartermijn voor gegevens in overeenstemming met de toepasselijke wetgeving.
- Het online meldingsplatform is beveiligd en meldingen die daarop worden ingediend, kunnen alleen worden bekeken door bevoegde personen. Dit systeem maakt het ook mogelijk dat werknemers die anoniem willen blijven, van dit kanaal gebruikmaken.
- De identiteit van klokkenluiders kan aan gerechtelijke autoriteiten worden bekendgemaakt indien dit wettelijk vereist is.
- Informatie die de in een melding betrokken persoon zou kunnen identificeren, mag niet worden bekendgemaakt, behalve aan de gerechtelijke autoriteiten, zodra de geldigheid van de melding is vastgesteld.
- Binnen de entiteiten van de Rexel Group zijn de afdelingen die doorgaans betrokken zijn bij de behandeling van meldingen zich bewust van het vertrouwelijke karakter van de identiteit van de auteur en de betrokken personen.

6. Bescherming van persoonsgegevens

In het kader van het klokkenluiderssysteem kan de Rexel Group persoonsgegevens verzamelen en verwerken, met name gegevens met betrekking tot de auteur van een melding en de betrokken persoon of personen. In **bijlage 4** wordt in een gedetailleerde informatieverklaring uiteengezet onder welke voorwaarden gegevens worden verzameld, verwerkt, opgeslagen en gearhiveerd.

V. Rapportage

De complianceafdeling van de Groep brengt eenmaal per jaar verslag uit over het aantal meldingen, het type meldingen en de maatregelen die naar aanleiding daarvan zijn genomen, waarbij zij zich beperkt tot gegevens die strikt noodzakelijk en evenredig zijn aan de rechtvaardiging van de mededeling.

VI. van de procedure bijwerken

De Rexel Groep behoudt zich het recht voor om deze procedure te allen tijde te wijzigen, aan te vullen of bij te werken om deze aan te passen aan wijzigingen in de wetgeving, regelgeving, jurisprudentie of de interne behoeften van de Groep. Eventuele updates zullen worden uitgevoerd in overeenstemming met de toepasselijke lokale wet- en regelgeving.

Medewerkers, leveranciers en andere betrokken partijen worden op passende wijze (interne communicatie, e-mail, publicatie op het intranet, directe informatie aan leveranciers, enz.) op de hoogte gebracht van de wijzigingen, in overeenstemming met de lokale wettelijke vereisten.

De huidige en gezaghebbende versie van deze procedure wordt gepubliceerd en beschikbaar gesteld op de websites van de Rexel Group, op het intranet van de groep en op het online rapportageplatform.

Contact

Bedrijf: Rexel Développement

Adres: 13 boulevard Fort de Vaux 75017 Parijs (Frankrijk) – *Ter attentie van de afdeling Compliance van de Groep.*

E-mailadres: compliance@rexel.com

Een situatie melden

Als u vermoedt of weet dat een overtreding van de wet, de Ethische Gids, of de Gedragscode tegen corruptie, meld dit dan!



02. Wanneer moet u een melding doen?

of vermoedt **dat de wet of onze ethische principes.**

Dit kan onder meer zijn:

- corruptie;
- schending van mensenrechten;
 - intimidatie
 - of discriminatie;
 - fraude, enz.



04. Is het vertrouwelijk?

Ja, en u kunt ook een **anonieme** melding doen



06. Ben ik beschermd?

U moet de waarschuwing geven te goeder trouw en zonder directe financiële compensatie.
In dat geval bent u beschermd.



01. Wie kan een melding doen?

Alle medewerkers van de Groep en derden kunnen gebruikmaken van de ethische hotline.



03. Hoe een melding doen?

1. Gebruik de **online Rexel-ethische hotline**

(weblink hieronder)

- 24/7 beschikbaar;
- beschikbaar in alle de belangrijkste talen van de Groep.

2. **Gebruik het klokkenluidersysteem dat lokaal is opgezet.**

3. **Neem contact op met de juridische of complianceafdeling of de personeelsafdeling (van de groep of lokaal)**



05. Wie verwerkt deze waarschuwing?

Voor de groep: de ethische commissie.

Voor het lokale systeem: zie lokale procedure.



Meer informatie

Bezoek : **109**
<https://www.rexel.com/en/ethical-alert/>

Bijlage 2: Lijst van landen met lokale klokkenluidersprocedures

Deze procedure wordt in bepaalde landen aangevuld met lokale procedures, waarin de toepasselijke wettelijke vereisten en, in voorkomend geval, de lokaal beschikbare kanalen worden uiteengezet.

Hieronder vindt u informatie over de lokale kanalen. Raadpleeg de lokale procedure voor de meest actuele informatie.

- Australië:

o Rexel STOPline-meldingsdienst (beheerd door een onafhankelijke externe dienstverlener):

Telefoon: 1300 30 45 50

Fax: Rexel Holdings Australia (C/- the STOPline) 03 9882 4480

E-mail: rexel@stopline.com.au

Online: <https://rexel.stoplinereport.com/>

Post: Rexel Holdings Australia

C/- the STOPline

Locked Bag 8

HAWTHORN VIC 3122

- Canada: u kunt contact opnemen met de Ethische Commissie.

- Duitsland:

o E-mail: whistleblowing@rexel.de

o Post:

Rexel Germany GmbH & Co.

KG - z. Hd. Frau Nicole Steuer | General Counsel

Ridlerstr.5780339 München

- Ierland

o U kunt contact opnemen met de HR-afdeling, de klokkenluidersfunctionaris, de Chief Executive Officer of onze externe klokkenluidershotline die wordt beheerd door Safecall

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- Italië:

o <https://report.whistleb.com/rexel>

- Nederland: u kunt contact opnemen met de Ethics Correspondent.

- Zweden:

o <https://whistleblow.vismadraftit.se/rexel-sverige-ab>

o Telefoon: 08-556 214 14.

- Verenigd Koninkrijk

o U kunt contact opnemen met de HR-afdeling, de klokkenluidersfunctionaris, de Chief Executive Officer of onze externe klokkenluidershotline die wordt beheerd door Safecall.

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- Verenigde Staten

o Compliance E-mail: ethics@rexelusa.com

o Compliance-hulplijn: 1-800-714-8774

Bijlage 3: Voorbeelden van gedragingen of wangedragingen die onder de klokkenluidersprocedure vallen

Categorieën	Toepassingsgebied
Corruptie	In het kader van de toepasselijke lokale wet- en regelgeving en het anticorruptiebeleid van de Groep: corruptie verwijst naar het direct of via een derde partij uitwisselen van voordelen (geld, geschenken, uitnodigingen, diensten, connecties, enz.) in ruil voor het uitvoeren of nalaten van een handeling die verband houdt met een functie of mandaat. Dit kan de vorm aannemen van een persoon die een voordeel voorstelt of aanbiedt om een gunst te verkrijgen (actieve corruptie) of een persoon die een voordeel vraagt of aanvaardt in ruil voor een dienst (passieve corruptie). Corruptie kan zowel publieke als private actoren betreffen, verstoort de concurrentie, ondermijnt de transparantie van beslissingen en stelt de betrokken personen en organisaties bloot aan sancties en vervolging.
Intimidatie	Intimidatie verwijst naar herhaaldelijk gedrag of een enkele ernstige handeling die de waardigheid, veiligheid of arbeidsomstandigheden van een persoon ondermijnt. Het uit zich in woorden, gebaren, houdingen of handelingen die bedoeld zijn om een werknemer of derde partij in verband met professionele activiteiten te intimideren, te vernederen, te isoleren, te bedreigen of te kleineren. Intimidatie kan een psychologische vorm aannemen, zoals denigrerende opmerkingen, opzettelijke isolatie, overbelasting of het onthouden van werkmiddelen, uitsluiting, het verspreiden van geruchten of systematische kleinering. Het kan ook een seksuele vorm aannemen. Seksuele intimidatie wordt gekenmerkt door ongewenst seksueel gedrag of opmerkingen die herhaaldelijk voorkomen of een enkel ernstig incident vormen, waardoor de waardigheid van een persoon wordt aangetast of een intimiderende, vijandige, vernederende of beledigende werkomgeving wordt gecreëerd. Dit omvat onder meer aanhoudende avances, opmerkingen over het lichaam, verzoeken om seksuele gunsten, fysieke gebaren of contact zonder toestemming, of het verspreiden van seksuele afbeeldingen zonder toestemming.

	Intimidatie, zowel moreel als seksueel, is onaanvaardbaar en de daders zijn aansprakelijk volgens de toepasselijke lokale wetgeving.
Discriminatie	Discriminatie op de werkplek houdt in dat iemand ongunstig wordt behandeld op basis van criteria die bij wet verboden zijn, zoals afkomst, geslacht, gezinssituatie, enz., of enig ander kenmerk dat door de lokale wetgeving wordt beschermd. Discriminatie kan bijvoorbeeld leiden tot ongelijke behandeling bij de toegang tot werk, arbeidsomstandigheden, opleiding, mobiliteit of elke andere situatie die verband houdt met beroepsactiviteiten. Het kan de vorm aannemen van beslissingen over aanwerving, evaluatie, promotie, toewijzing of ontslag die een persoon benadelen zonder objectieve rechtvaardiging op basis van de vereisten van de functie. Op de werkplek kan discriminatie twee vormen aannemen: - Directe discriminatie. In dit geval neemt de dader opzettelijk een beslissing op basis van een discriminerend criterium dat bij wet verboden is. Indirecte discriminatie. In dit geval neemt de dader een beslissing die neutraal lijkt, maar uiteindelijk bepaalde mensen benadeelt ten opzichte van anderen. Bijvoorbeeld: interne regels staan alleen mannen toe om na hun 50e bij het bedrijf te blijven werken. Dit vormt dus indirecte discriminatie op basis van geslacht en leeftijd.
Gezondheid/veiligheid	Elke ernstige inbreuk op of elk ernstig risico voor de gezondheid en veiligheid op het werk. Veiligheid op het werk verwijst naar alle maatregelen en praktijken die gericht zijn op het beschermen van de fysieke en mentale integriteit van mensen op hun werkplek door het risico op ongevallen, letsel en beroepsziekten te verminderen. Dit omvat het identificeren en beoordelen van risico's, het implementeren van technische en organisatorische veiligheidsmaatregelen, het opleiden en informeren van werknemers en het nemen van preventieve, interventie maatregelen en noodmaatregelen. Het naleven van deze verplichtingen draagt bij aan een veilige werkomgeving die voldoet aan de lokale vereisten.
Mensenrechten (anders dan discriminatie en intimidatie)	Elke ernstige schending of elk ernstig risico voor de mensenrechten en fundamentele vrijheden die op nationaal en internationaal niveau worden erkend, evenals elke schending van de toepasselijke lokale vereisten op dit gebied. Dit omvat, maar is niet beperkt tot, situaties waarbij principes zoals eerbiediging van de vrijheid van vereniging en meningsuiting, toegang tot fatsoenlijke en veilige arbeidsomstandigheden en de mogelijkheid voor de betrokkenen om toegang te hebben tot rechtsmiddelen in het geding zijn.

Belangenconflicten	Een belangenconflict is een situatie waarin de persoonlijke belangen van een persoon, of deze nu financieel, familiaal, vriendschappelijk, politiek of gerelateerd aan andere voordelen zijn, waarschijnlijk zijn oordeel of beslissingen in de uitoefening van zijn taken binnen de Rexel Groep beïnvloeden of lijken te beïnvloeden. Dit is niet noodzakelijkerwijs een fout of een onwettige handeling, maar een risico op vooringenomenheid dat de verwachte onpartijdigheid in gevaar brengt. Dit risico op vooringenomenheid kan voldoende zijn om het vertrouwen van de betrokkenen te ondermijnen, de kwaliteit van beslissingen te beïnvloeden en de reputatie van de organisatie te schaden. Een belangenconflict kan feitelijk (reëel aanwezig), potentieel (waarschijnlijk) of schijnbaar (waargenomen door derden) zijn. Het klokkenluiderssysteem is niet bedoeld ter vervanging van de door de Rexel Groep vastgestelde procedure voor het melden van belangenconflicten.
Concurrentieverstorende praktijken	Concurrentieverstorende praktijken zijn gedragingen van bedrijven die de vrije concurrentie belemmeren en andere marktdeelnemers (klanten, leveranciers, concurrenten) schaden. Het gaat onder meer om formele of informele afspraken tussen concurrenten om prijzen, commerciële voorwaarden, de verdeling van markten, gebieden of producten te coördineren, of om het aanbod te beperken of bepaalde partners te boycotten. Het omvat ook situaties van misbruik van een machtspositie (bijvoorbeeld het verdrijven van een concurrent, het opleggen van roofprijzen of ongerechtvaardigde koppelverkoop), het beïnvloeden van de door distributeurs gehanteerde wederverkoop prijs en het uitwisselen van niet-openbare strategische informatie die het marktgedrag zou kunnen beïnvloeden (zoals plannen, marketinggegevens of capaciteiten). Deze praktijken zijn verboden door de mededingingsregels en kunnen worden bestraft met aanzienlijke boetes.
Milieu	Elke situatie waarin niet wordt voldaan aan de toepasselijke milieueisen, of waarin een aanzienlijk risico of schade voor het milieu wordt vastgesteld, zowel binnen het bedrijf als bij zijn partners in de waardeketen. Dit omvat het voorkomen van vervuiling, verantwoord gebruik van hulpbronnen en veilig beheer van stoffen en afval, in overeenstemming met wettelijke verplichtingen en interne normen.
Fraude	Elke situatie waarbij sprake is van verzwijging, misleiding of manipulatie met het oogmerk om een onrechtmatig voordeel te verkrijgen of verplichtingen te ontduiken, zowel op fiscaal, financieel als boekhoudkundig gebied. Dit omvat bijvoorbeeld het vervalsen van documenten of gegevens, het verkeerd voorstellen van financiële informatie,

	het verbergen van inkomsten of activa , of elke regeling die bedoeld is om de toepasselijke regels te omzeilen, zowel binnen het bedrijf als in zijn waardeketen.
Handel met voorkennis	Handel met voorkennis is het kopen, verkopen of aanbevelen van financiële instrumenten op basis van of met gebruikmaking van niet-openbare bevoorrechte informatie over een emittent of zijn effecten. Het omvat ook het illegaal bekendmaken van dergelijke informatie aan derden. Dergelijk gedrag levert een oneerlijk voordeel op in de markten en is ten strengste verboden en strafbaar.
Fictieve banen	Een fictieve baan is een situatie waarin een persoon wordt betaald voor een functie of taken die niet daadwerkelijk worden uitgevoerd of die niet bestaan, om een oneerlijk voordeel te verkrijgen. Dit kan betrekking hebben op het volledig ontbreken van daadwerkelijk werk, fictieve taken of een nominale toewijzing aan een afdeling zonder enige echte bijdrage, binnen het bedrijf of via derden.
Bescherming van persoonsgegevens / IT-beveiliging	Elke situatie waarin persoonsgegevens of IT-systemen niet worden beschermd in overeenstemming met de wetgeving en interne regels, waardoor personen of het bedrijf worden blootgesteld aan het risico van ongeoorloofde toegang, gebruik, openbaarmaking, wijziging of vernietiging. Dit omvat het rechtmatig en minimaal verzamelen en verwerken van gegevens, systeembeveiliging (toegangscontroles, encryptie, back-ups), incident- en inbreukbeheer, en de vertrouwelijkheid en integriteit van informatie gedurende de hele levenscyclus ervan, ook bij dienstverleners. Persoonsgegevens zijn alle gegevens die direct of indirect een natuurlijke persoon identificeren (bijv. naam, contactgegevens, identificatiegegevens, foto, locatiegegevens of andere elementen die betrekking hebben op hun identiteit of privéleven).

PRIVACYBELEID

—

KLOKKENLUIDERSREGELING

Versie 12/2025

De Rexel Groep heeft een professioneel klokkenluiderssysteem opgezet waarmee haar werknemers en derden met wie de Rexel Groep een relatie heeft, onwettige handelingen of wangedrag kunnen melden. De reikwijdte van het systeem wordt beschreven in de klokkenluidersprocedure, die beschikbaar is op de website [rexel.com](https://www.rexel.com).

 In het kader van dit systeem kan een Rexel-entiteit gegevens over u verzamelen en verwerken. De vertrouwelijkheid van gegevens vormt de basis van onze vertrouwensrelatie. Daarom nemen wij de bescherming van uw persoonsgegevens tijdens onze bedrijfsactiviteiten zeer serieus.

Dit beleid beschrijft de toezeggingen van de Rexel Group op het gebied van de bescherming van persoonsgegevens. In de volgende verklaring kunt u ook lezen wat uw rechten zijn en onder welke voorwaarden uw persoonsgegevens worden verzameld, verwerkt, opgeslagen en gearhiveerd.

Wie zijn wij?

REXEL DEVELOPPEMENT SAS, een vereenvoudigde naamloze vennootschap naar Frans recht, met maatschappelijke zetel te 13, Boulevard du Fort de Vaux, Parijs, ingeschreven in het handels- en vennootschapsregister van Parijs onder nummer 480 172 840, is de verwerkingsverantwoordelijke.

De entiteit binnen de Groep die een arbeidsovereenkomst heeft met of samenwerkt met de auteur van het rapport is ook een verwerkingsverantwoordelijke.

Zij bepalen de doeleinden en middelen voor de verwerking van uw gegevens.

In dit beleid worden zij aangeduid als "Rexel", "wij" of "verantwoordelijken voor de verwerking".

EY Polen treedt op als verwerker voor de verwerking die wordt uitgevoerd op het online meldingsplatform.

Hoe verwerken wij uw gegevens in het kader van het waarschuwingssysteem?

In de onderstaande tabel wordt het volgende uiteengezet:

- (i) waarom wij uw persoonsgegevens verwerken,
- (ii) welke soorten gegevens we verwerken, en
- (iii) de rechtsgrondslag voor de verwerking van uw gegevens.

Doel 1	Soort gegevens
Verzamelen en verwerken van meldingen van handelingen die in strijd zijn met de wet of de anticorruptiegedragscode die onder het klokkenluiderssysteem vallen (zie de klokkenluidersprocedure). <u>Subdoeleinden:</u> - Gecentraliseerd beheer van professionele meldingen (ontvangen en behandelen van meldingen, opzetten van een beveiligd kanaal, opslaan en bewaren van informatie, waarborgen van de veiligheid) - Verwerking van professionele meldingen (uitvoeren van interne onderzoeken, beoordelen van de relevante feiten) - Besluitvorming en uitvoering van passende maatregelen na afsluiting van de melding (kennisgeving en uitvoering van maatregelen) - Statistische monitoring en verbetering van het klokkenluiderssysteem - Uitoefening of verdediging van rechten in gerechtelijke procedures	Als onderdeel van het systeem kunnen de volgende categorieën gegevens worden verwerkt: - Identiteitsgegevens (voor- en achternaam, contactgegevens), beroepsgegevens (functie, werkgever, werkplek) van de persoon die de melding doet (tenzij de melding anoniem is) en alle andere informatie die vrijwillig door hem/haar wordt verstrekt - Identiteitsgegevens (voor- en achternaam, contactgegevens), professionele gegevens (functie, werkgever, werkplek) van de betrokken personen - Identiteitsgegevens (voor- en achternaam, e-mailadres), professionele gegevens (functie, werkgever, werkplek) van personen die betrokken zijn bij of geraadpleegd worden in het kader van het verzamelen of verwerken van de melding, en tussenpersonen en personen die in contact staan met de klokkenluider - Gevoelige gegevens (ras of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen, lidmaatschap van een vakbond, gezondheidsgegevens, seksleven of seksuele geaardheid) wanneer dit strikt noodzakelijk is voor de uitoefening of verdediging van wettelijke rechten (artikel 9, lid 2, onder f), van de AVG) of om redenen van zwaarwegend algemeen belang (artikel 9, lid 2, onder g), van de AVG) - Gegevens met betrekking tot strafrechtelijke veroordelingen en overtredingen of daarmee verband houdende veiligheidsmaatregelen, indien strikt noodzakelijk en in overeenstemming met artikel 10 van de AVG - Informatie verzameld in het kader van feitencontrole - Verslagen over verificatieactiviteiten - Gegevens met betrekking tot de follow-up van het rapport
Rechtsgrondslag voor de verwerking van uw gegevens Wettelijke verplichting om een klokkenluidersregeling in te voeren: met name de artikelen 8.I.B en 17 II van de Sapin II-wet en artikel L. 225-102-4 van het Wetboek van Koophandel, evenals elke gelijkwaardige wet met betrekking tot de bescherming van klokkenluiders, de bestrijding van corruptie of de zorgplicht.	

Doel 2	Soort gegevens
Verzamelen en verwerken van meldingen van handelingen die in strijd zijn met de ethische gids <u>Subdoeleinden:</u> - Gecentraliseerd beheer van professionele meldingen (ontvangen en behandelen van meldingen, opzetten van een beveiligd kanaal, opslaan en bewaren van informatie, waarborgen van de veiligheid) - Verwerking van professionele meldingen (uitvoeren van interne onderzoeken, beoordelen van de relevante feiten) - Besluitvorming en uitvoering van passende maatregelen na afsluiting van de melding (kennisgeving en uitvoering van maatregelen) - Statistische monitoring en verbetering van het klokkenluiderssysteem - Uitoefening of verdediging van rechten in gerechtelijke procedures	Als onderdeel van het systeem kunnen de volgende categorieën gegevens worden verwerkt: - Identiteitsgegevens (voor- en achternaam, contactgegevens), professionele gegevens (functie, werkgever, werkplek) van de persoon die de melding doet (tenzij de melding anoniem is) en alle andere informatie die vrijwillig door hem/haar wordt verstrekt - Identiteitsgegevens (voor- en achternaam, contactgegevens), professionele gegevens (functie, werkgever, werkplek) van de betrokken personen - Identiteitsgegevens (voor- en achternaam, e-mailadres), professionele gegevens (functie, werkgever, werkplek) van personen die betrokken zijn bij of geraadpleegd worden in het kader van het verzamelen of verwerken van de melding, en bemiddelaars en personen die in contact staan met de klokkenluider - Gevoelige gegevens (ras of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen, lidmaatschap van een vakbond, gezondheidsgegevens, seksleven of seksuele geaardheid) wanneer dit strikt noodzakelijk is voor de uitoefening of verdediging van wettelijke rechten (artikel 9, lid 2, onder f), van de AVG) of om redenen van zwaarwegend algemeen belang (artikel 9, lid 2, onder g), van de AVG) - Gegevens met betrekking tot strafrechtelijke veroordelingen en overtredingen of daarmee verband houdende veiligheidsmaatregelen, indien strikt noodzakelijk en in overeenstemming met artikel 10 van de AVG - Informatie verzameld in het kader van feitencontrole - Verslagen over verificatieactiviteiten. - Gegevens met betrekking tot de follow-up van het rapport
Rechtsgrondslag voor de verwerking van uw gegevens	
Rechtsgrondslag: gerechtvaardigd belang bij de verwerking van ethische meldingen die niet onder een wettelijke verplichting vallen.	

Wie zijn de ontvangers van uw gegevens?



De persoonsgegevens die wij verzamelen, evenals alle gegevens die later worden verzameld, zijn bestemd voor ons in onze hoedanigheid van verwerkingsverantwoordelijke.



Wij zorgen ervoor dat alleen bevoegde personen toegang hebben tot deze gegevens.

Intern:

- Degenen die verantwoordelijk zijn voor het verzamelen en verwerken van meldingen, namelijk:
 - Leden van de Ethische Commissie van de Rexel Groep
 - Bevoegde leden van de juridische of compliance-afdeling op groeps- en lokaal niveau
 - Bevoegde leden van de afdeling Human Resources op groeps- en lokaal niveau
- Bevoegde leden van de afdeling Audit en Interne Controle op groeps- en lokaal niveau om de effectiviteit van interne controles en governance te waarborgen
- Wanneer de situatie dit rechtvaardigt, kunnen andere interne medewerkers toegang krijgen tot de gegevens, met name wanneer boekhoudkundige, financiële, juridische, technische of IT-expertise vereist is.

Extern:

- Onze adviseurs
- Onze makelaars en verzekeraars
- Onze auditors
- De bevoegde autoriteiten (gerechtelijke, administratieve en regelgevende instanties), in overeenstemming met de toepasselijke regelgeving
- Onze dienstverleners, en meer specifiek EY Polen, die ons het online rapportageplatform ter beschikking stelt.

Deze ontvangers zijn gevestigd in de Europese Unie.

Hoe lang bewaren we uw gegevens?

Situaties	Bewaartermijn
Ongeldige meldingen (vallen niet onder het toepassingsgebied, zijn niet ernstig van aard, bevatten onvolledige informatie, zijn te kwader trouw gedaan, enz.)	Verwijdering of archivering en anonimisering zo snel mogelijk
Toelaatbare melding maar afgewezen (niet gevolgd door disciplinaire of gerechtelijke procedures)	Verwijdering of anonimisering en archivering binnen twee (2) maanden
Meldingen die aanleiding geven tot disciplinaire of gerechtelijke procedures	Bewaring van gegevens tot het einde van de procedure en beroepsprocedures. Na deze periode verwijdering of anonimisering en archivering.

Wat zijn uw rechten?



In overeenstemming met de wetgeving inzake de bescherming van persoonsgegevens hebt u de volgende rechten:

- recht op inzage: u kunt de informatie die wij over u hebben inzien en een kopie ervan verkrijgen;
- recht op rectificatie: u kunt onjuiste gegevens over uzelf laten wijzigen, aanvullen, bijwerken of verwijderen;
- recht van bezwaar: u kunt bezwaar maken tegen de verwerking van uw gegevens, tenzij er legitieme en dwingende redenen zijn om deze te verwerken;
- recht op verwijdering: u kunt ons verzoeken om gegevens over u te verwijderen binnen de grenzen van de voorwaarden die zijn vastgelegd in artikel 17 van de AVG;
- recht op gegevensoverdraagbaarheid: u kunt uw gegevens opvragen om deze over te dragen aan een andere organisatie of voor persoonlijk gebruik;
- recht op beperking van de verwerking;
- recht om specifieke en algemene richtlijnen te formuleren met betrekking tot de opslag, verwijdering en communicatie van uw gegevens na uw overlijden.

Elke persoon die het onderwerp is van een rapportage, wordt zo snel mogelijk (uiterlijk binnen een maand) na de registratie, al dan niet geautomatiseerd, van gegevens over hem of haar op de hoogte gesteld, zodat hij of zij zijn of haar rechten kan uitoefenen. Indien deze informatie echter de doelstellingen van de verwerking en met name het verloop van het onderzoek ernstig in gevaar kan brengen (bijvoorbeeld als het risico bestaat dat bewijsmateriaal wordt vernietigd), kan deze informatie worden uitgesteld en zal zij pas worden verstrekt nadat elk risico is weggenomen.

De persoon op wie de melding betrekking heeft, kan in geen geval op grond van zijn recht op toegang van de voor de verwerking verantwoordelijke informatie verkrijgen over de identiteit van de auteur van de melding of enige andere persoon die bij het onderzoek betrokken is.

Als u geen antwoord ontvangt, als u het antwoord onbevredigend vindt of als u van mening bent dat de verwerking van uw gegevens niet in overeenstemming is met de wettelijke en reglementaire bepalingen, kunt u contact opnemen met de bevoegde toezichthoudende autoriteit.

Hoe kunt u uw rechten uitoefenen?



Door een schriftelijk verzoek te richten aan onze functionaris voor gegevensbescherming:

Landen	Entiteiten	Adres
Oostenrijk	COMTECH IT-SOLUTIONS GMBH	datenschutz@rexel.at
	Rexel Austria GmbH	datenschutz@rexel.at
België	Rexel Belgique SA	gdpr@rexel.be
Frankrijk	Cordia	donnees.personnelles@francofa-eurodis.fr
	Rexel Développement SAS / Rexel Group	data.protection@rexel.com
	Rexel France SAS	donnees.personnelles@rexel.fr
	Bizline	data.protection@rexel.com
	Gigamedia	data.protection@rexel.com
	Sofinther SAS	donnees.personnelles@sofinther.fr
	Espace Elec SAS	donnees.personnelles@espace-elec.fr
	Esabora Digital Services SAS	dataprotection-rda@rexel.fr
	Francofa Eurodis	donnees.personnelles@francofa-eurodis.fr
	Freshmile Services SAS	donnees.personnelles@rexel.fr
	ITESA	donnees.personnelles@rexel.fr
Duitsland	REXEL DUITSLAND BETEILIGUNGS GMBH	Datenschutzbeauftragter@rexel.de
	Rexel Germany GmbH & Co KG	Datenschutzbeauftragter@rexel.de
	REXEL DUITSLAND VERWALTUNGS GMBH	Datenschutzbeauftragter@rexel.de
Italië	Rexel Italia S.p.A	dataprotection@rexel.it
	Tecno-Bi S.r.l.	dataprotection@rexel.it
	Comm-Tech S.r.l.	dataprotection@rexel.it
Ierland	M. Kelliher 1998	data.protection@rexel.ie
	Rexel Industrial Solutions	data.protection@rexel.ie
Luxemburg	Rexel Luxembourg SA	gdpr@rexel.be
Nederland	Rexel Nederland B.V	AVG@rexel.nl
	Wasco Group B.V.	AVG@rexel.nl
	Wasco Holding B.V.	AVG@rexel.nl
	Wasco Groothandels Groep B.V.	AVG@rexel.nl
	Wasco Distributielecentrum B.V.	AVG@rexel.nl
Slovenië	Rexel d.o.o.	dpc@rexel.si
Zweden	Rexel Sverige AB	dataskydd@rexel.se
Zwitserland	ELEKTRO-MATERIAL AG	datenschutz@e-m.ch
	Rexel 3S	data.protection@rexel.com
Verenigd Koninkrijk	Rexel (UK) Ltd.	data.protection@rexel.co.uk



Postopek za prijavo nepravilnosti

December 2025_V1

Povzetek

I.	<u>Uvod</u>	3
1.	<u>Namen notranjega sistema za prijavo nepravilnosti</u>	3
2.	<u>Opomnik o pravnem okviru</u>	3
3.	<u>Področje</u>	3
II.	<u>Zbiranje etičnih opozoril</u>	4
1.	<u>Pogoji za sprejemljivost etičnega opozorila</u>	4
	<u>Kdo lahko vloži prijavo?</u>	4
	<u>Kako lahko izkoristite status prijavitelja in s tem povezano pravno zaščito?</u>	4
	<u>Katera dejstva se lahko prijavijo?</u>	5
2.	<u>Kako vložiti prijavo</u>	6
3.	<u>Vsebina prijave</u>	7
4.	<u>Anonimna prijava</u>	7
5.	<u>Zunanji kanali</u>	7
III.	<u>Obravnavanje notranjih etičnih opozoril</u>	7
1.	<u>Potrditev prejema poročila</u>	7
2.	<u>Pregled dopustnosti poročila</u>	7
3.	<u>Izvedba notranje preiskave</u>	8
4.	<u>Sprejemanje odločitev in zaključek preiskave</u>	9
IV.	<u>Zaščita in zagotovila</u>	10
1.	<u>Splošna načela</u>	10
2.	<u>Informacije</u>	10
3.	<u>Zaščita v kazenskih, civilnih in socialnih zadevah</u>	10
4.	<u>Omejeno obdobje hrambe podatkov</u>	11
5.	<u>Zaupnost in varnost</u>	11
6.	<u>Varstvo osebnih podatkov</u>	12
V.	<u>Poročanje</u>	12
VI.	<u>Posodobitev postopka</u>	12
	<u>Priloga 1: Povzetek</u>	13
	<u>Priloga 2: Seznam držav z lokalnim postopkom za prijavo nepravilnosti</u>	14
	<u>Priloga 3: Primeri ravnanj ali kršitev, ki jih zajema postopek za prijavo nepravilnosti</u>	15
	<u>Priloga 4: Politika zasebnosti</u>	19

I. Uvod

1. Namen notranjega sistema za prijavo nepravilnosti

V okviru politike etike in skladnosti skupine Rexel, ki je opisana zlasti v njenem Etičnem vodniku, Listini odgovornih dobaviteljev in Kodeksu ravnanja proti korupciji, je skupina Rexel vzpostavila notranji sistem za prijavo nepravilnosti.

Notranji sistem za prijavo nepravilnosti skupine Rexel omogoča vsem zaposlenim in tretjim osebam, s katerimi skupina Rexel sodeluje, da prijavijo primere kršitve zakona, Etičnega priročnika skupine Rexel ali Kodeksa ravnanja proti korupciji.

Namen tega postopka je opisati proces zbiranja in obravnavanja etičnih opozoril znotraj skupine Rexel.

Povzetek postopka je priložen v **Prilogi 1.**

2. Opomnik pravnega okvira

Ker je holding Skupine Rexel registriran v Franciji, je bil postopek vzpostavljen v skladu z naslednjimi francoskimi zakoni:

- Zakon Sapin II z dne 9. decembra 2016 o preglednosti, boju proti korupciji in gospodarski modernizaciji;
- Zakon o »dolžnosti pazljivosti« z dne 27. marca 2017, ki se nanaša na dolžnost pazljivosti matičnih družb in pogodbenih družb;
- Zakon „Waserman“ z dne 21. marca 2022 o izboljšanju zaščite prijaviteljev nepravilnosti in njegov izvedbeni odlok z dne 3. oktobra 2022.

Postopek temelji tudi na številnih publikacijah francoske agencije za boj proti korupciji (AFA) in francoskega organa za varstvo podatkov (CNIL):

- Priporočila AFA;
- Praktični vodnik „Notranje protikorupcijske preiskave“, ki sta ga marca 2023 objavila AFA in francosko finančno tožilstvo;
- Referenčni dokument CNIL „strokovna opozorila“, prvotno objavljen leta 2019 in posodobljen leta 2023.

Na splošno se zbiranje in obdelava poročil izvaja v skladu z veljavnimi zakoni in predpisi, ta postopek pa se lahko po potrebi posodobi, da odraža zakonodajne spremembe in najboljše prakse.

Če lokalni zakoni ali predpisi zagotavljajo večjo zaščito prijaviteljev kot ta postopek, prevladajo lokalne določbe. Vendar, če ta postopek zagotavlja večje zaščitne garancije, bo skupina Rexel te prostovoljno uporabila v obsegu, ki ga dovoljuje veljavna zakonodaja.

3. Področje uporabe

Ta postopek je namenjen izvajanju v vseh subjektih skupine Rexel. Po potrebi bo spremenjen, da bo odražal morebitne spremembe zakonov in predpisov.

Ta postopek je v nekaterih državah znotraj skupine Rexel dopolnjen z lokalnimi postopki. Ti določajo veljavne zakonske zahteve in, odvisno od primera, lokalno razpoložljive kanale (glej Prilogo 2).

Avtor poročila lahko zato izbere kanal za poročanje po lastni izbiri (skupinski ali lokalni). Veljaven postopek bo nato tisti, ki ustreza izbranemu kanalu. Glede na naravo in resnost prijavljenega ravnanja ali kršitev se lahko opozorilo, posredovano prek lokalnega kanala, posreduje skupini in obratno.

Ta postopek velja za vse zaposlene v skupini Rexel (ne glede na njihovo vlogo, položaj ali oddelek) in tretje osebe, s katerimi ima skupina Rexel poslovne odnose. Zajema zbiranje in obdelavo notranjih opozoril s strani skupine Rexel, natančneje:

- njihovo predložitev;
- njihov sprejem;
- oceno njihove dopustnosti;
- glavne stopnje notranje preiskave
- zaključek primera.

II. Zbiranje etičnih opozoril

1. Pogoji za sprejemljivost etičnega opozorila

Kdo lahko vloži prijavo?

Notranji sistem opozoril skupine Rexel je na voljo naslednjim osebam:

- zaposlenim v skupini Rexel (stalnim, za določen čas, vajencem, pripravnikom)
- Zunanji ali začasni zaposleni (začasni delavci, svetovalci itd.)
- Kandidati za zaposlitev
- Nekdanji zaposleni
- Delničarji, partnerji in imetniki glasovalnih pravic na skupščini
- Člani upravnega, izvršnega odbora ali nadzornega organa
- Vsi zunanji zaposleni, s katerimi ima skupina Rexel poslovne odnose (npr. stranke, dobavitelji, ponudniki storitev itd.).

Notranji sistem za prijavo nepravilnosti je odprt za vse subjekte skupine Rexel in je na voljo v glavnih jezikih skupine: angleščini, nemščini, kitajščini, francoščini, italijanščini, nizozemščini, švedščini in slovenščini.

Kako lahko izkoristite status prijavitelja nepravilnosti in s tem povezano pravno zaščito?

Da bi bili obravnavani kot prijavitelj in izkoristili zaščito, ki jo zagotavlja zakon, morate ustrezati zakonski opredelitvi prijavitelja, in sicer izpolniti vsa naslednja merila, razen če veljavna lokalna zakonodaja ne določa drugače:

- Biti fizična oseba;
- za prijavo ne smete prejeti nobenega neposrednega finančnega nadomestila;
- delovati v dobri veri;
- Če so bila prijavljena dejstva pridobljena zunaj poklicnega konteksta, imeti osebno znanje o prijavljenih dejstvih.

Katera dejstva se lahko prijavijo?

Notranji sistem za prijavo nepravilnosti skupine Rexel omogoča prijavo dejstev, ki lahko sodijo v naslednje kategorije ravnanja ali kršitev:

- Kaznivo dejanje ali prekršek
- Grožnja ali škoda javnemu interesu
- Kršitev ali poskus prikrivanja kršitve nacionalnih, evropskih ali mednarodnih zakonov in predpisov
- Kršitev ali ravnanje, ki je v nasprotju z Etičnim kodeksom ali Kodeksom ravnanja proti korupciji skupine Rexel
- Resna tveganja v zvezi z dejavnostmi skupine Rexel, ki bi lahko škodovala človekovim pravicam, temeljnim svoboščinam, zdravju in varnosti ljudi ali okolju

Primeri ravnanj ali kršitev, ki jih je treba prijaviti, lahko vključujejo:

- Korupcija, vključno z vsako kršitvijo Kodeksa ravnanja proti korupciji
- Nadlegovanje (psihološko ali spolno)
- Diskriminacija
- Zdravje, higiena ali varnost (npr. tveganje za fizično ali duševno integriteto)
- Človekove pravice (razen diskriminacije, zasebnosti in nadlegovanja)
- Navzkrižje interesov
- Protekcionistične prakse
- Okolje (npr. onesnaževanje, ravnanje z odpadki)
- Davčna goljufija
- Finančne ali računovodske goljufije
- Trgovanje z notranjimi informacijami
- Fiktivna delovna mesta
- Osebni podatki/varnost IT

V prilogi 3 so navedeni nekateri primeri takšnega ravnanja ali kršitev.

Prijave, ki se nanašajo na kategorije, ki niso navedene zgoraj, ne sodijo v obseg tega postopka. Podobno so iz tega postopka izključena dejstva, informacije ali dokumenti, ne glede na njihovo obliko ali medij, katerih razkritje je prepovedano z določbami zakona o tajnosti nacionalne obrambe () v zvezi z nacionalno obrambno tajnostjo, zdravniško tajnostjo, tajnostjo sodnih razprav, tajnostjo sodnih preiskav ali poizvedb ali odvetniško tajnostjo (). Kadar je to primerno, bo avtor poročila obveščen in preusmerjen na osebe, pristojne za obravnavo prijavljenih dejstev.

2. Kako oddati poročilo

Avtor poročila ima na voljo več kanalov za oddajo opozoril:

- Spletna platforma za poročanje, dostopna na: <https://www.rexel.com/en/rexel-group-ethics-alert>;
- Dodatni kanali za poročanje, ki lahko obstajajo na ravni skupine ali lokalne države.

Med kanali ni hierarhije. Avtor poročila lahko uporabi kateri koli kanal, ki je na voljo.

Ne glede na uporabljeni kanal se oseba(-e), odgovorna(-e) za zbiranje poročil, v nadaljevanju imenuje(-jo) »**notranji vodja(-ji)**«.

Spletna platforma za poročanje

Avtor poročila lahko pošlje opozorilo, tudi anonimno, na spletni platformi za poročanje, dostopni na naslovu: <https://www.rexel.com/en/rexel-group-ethics-alert>

To je namenska, brezplačna platforma, ki je na voljo 24 ur na dan, 7 dni v tednu.

V Evropski uniji jo gosti zunanji ponudnik storitev (EY), ki izvaja stroge ukrepe za zagotavljanje varnosti in zaupnosti podatkov. Treba je opozoriti, da zaposleni tega ponudnika storitev niso vključeni v obdelavo poročil in nimajo dostopa do izmenjanih informacij.

Ta platforma omogoča neposredno komunikacijo s prejemnikom opozorila prek klepeta. Avtorju poročila omogoča tudi pošiljanje dokumentov, ki podpirajo dejstva.

Povezava do te platforme je na voljo na spletnih straneh Skupine: <https://www.rexel.com/en/rexel-group-ethics-alert> in <https://ethique.rexel.com/en/>, pa tudi na intranetnih straneh podjetij Skupine Rexel.

Dodatni kanali za poročanje

Notranji zaposleni v skupini Rexel lahko poročilo predložijo v pisni ali ustni obliki enemu od naslednjih notranjih vodij: (i) lokalnemu vodji za skladnost (pravni ali oddelek za skladnost), (ii) lokalnemu oddelku za človeške vire, (iii) oddelku za skladnost skupine ali (iv) oddelku za človeške vire skupine.

Oddelek za človeške vire (lokalni ali skupine) običajno zbira prijave kršitev delovne zakonodaje ali neprimernega vedenja na delovnem mestu (nadlegovanje, diskriminacija, zdravje, higiena ali varnost itd.).

Lokalni odgovorni za skladnost ali oddelek za skladnost skupine običajno zbirajo poročila o kršitvah zakona, etičnega kodeksa, kodeksa ravnanja proti korupciji, postopkov skladnosti skupine Rexel itd.

Če je prijava podana ustno, se lahko sprejme po telefonu in, na zahtevo osebe, ki podaja prijavo, in po njeni izbiri, med videokonferenco ali fizičnim sestankom, ki se organizira najpozneje dvajset (20) delovnih dni po prejemu zahteve. Ustna prijava se prepiše v pisno obliko.

Zaposleni lahko v vsakem primeru poiščejo nasvet svojega neposrednega ali posrednega nadrejenega in mu zaupajo svoje pomisleke, razen če je nadrejeni sam domnevni avtor zadevnega ravnanja. Če se po takem pogovoru izkaže, da ti pomisleki sodijo v okvir tega postopka, mora nadrejeni zaposlenega spodbuditi, da prijavo vloži prek zgoraj navedenih kanalov ali pa se obrne na lokalni oddelek za pravne zadeve ali skladnost ali lokalni oddelek za človeške vire.

3. Vsebina prijave

Avtor poročila mora natančno in objektivno predstaviti dejstva in informacije, ki so predmet njegovega poročila, da se lahko opozorilo obravnava.

Kadar je mogoče, mora poročilo podpreti z:

- navajanjem datuma(-ov) in kraja(-ev), kjer so se prijavljena dejstva zgodila, zadevnega subjekta ter identitete in položaja vpletenih oseb;

- podrobno opisati dejstva s konkretnimi in dejanskimi informacijami, ki so neposredno povezane s predmetom opozorila, ne glede na njegovo obliko ali medij.

4. Anonimna poročila

Zaželeno je, da se avtor poročila identificira, zlasti da se poenostavi izvedba preiskave. Vendar pa se avtor poročila lahko odloči za anonimno poročilo, kot je določeno v spletni platformi za poročanje, pod pogojem, da (i) je resnost dejstev ugotovljena in (ii) so dejanski elementi dovolj podrobni.

5. Zunanji kanali

Ob upoštevanju veljavnih lokalnih predpisov je treba opozoriti, da ima avtor poročila tudi možnost, da zunanje poročilo predloži (i) pristojnemu organu, (ii) varuhu človekovih pravic, (iii) sodnemu organu ali (iv) kateri koli ustrezni lokalni ali mednarodni instituciji, organu ali agenciji, ki je pristojna za prejemanje takih poročil. Prijavitelji lahko zunanja poročila predložijo neposredno organu ali po predložitvi poročila skupini Rexel.

III. Obravnavanje notranjih etičnih opozoril

1. Potrditev prejema poročila

Ko je poročilo prejeto na spletni platformi za poročanje ali prek tradicionalnih kanalov, notranji vodja (oseba, odgovorna za zbiranje poročil, kot je opredeljeno zgoraj) potrdi prejem opozorila v sedmih (7) delovnih dneh od prejema.

Potrditev prejema ne pomeni sprejetja opozorila.

2. Pregled dopustnosti poročila

Vsako prejeto opozorilo je predmet predhodne analize notranjega upravitelja, da se zagotovi, da sodi v obseg postopka in da je sprejemljivo.

Ta preverjanje, ki lahko zahteva komunikacijo z avtorjem ali poročevalcem, se osredotoča zlasti na naslednje točke:

- **Status avtorja kot „prijavitelja nepravilnosti“:** zlasti, da deluje v dobri veri in ne išče neposrednega finančnega nadomestila;
- **narava poročila:** da dejansko sodi v eno od kategorij poročil, ki jih zajema postopek;
- **Vsebina poročila:** da so navedene informacije in dejstva objektivni in dovolj podrobni, da omogočajo začetek preiskave;
- **Obstoj zaščitene tajnosti:** da poročilo ne razkriva dejstev, ki so zajeta v tajnosti nacionalne obrambe, zdravniške tajnosti, tajnosti sodnih razprav, tajnosti sodnih preiskav ali poizvedb ali odvetniške tajnosti.

Odločitev o dopustnosti sprejme notranji vodja. Avtor poročila je obveščen o nedopustnosti svojega poročila, če je to primerno, in o razlogih za to odločitev.

V vsakem primeru mora notranji vodja dati prvi odgovor v treh (3) mesecih. Skupina Rexel ni dolžna obravnavati opozorila v tem roku, vendar mora avtorja poročila obvestiti o ukrepih, ki so načrtovani ali že sprejeti za oceno veljavnosti opozorila in odpravo prijavljene situacije.

Prijava bo obravnavana popolnoma zaupno.

Glede na naravo in resnost prijavljenih dejstev lahko opozorilo obravnava etični odbor skupine Rexel. Etični odbor skupine Rexel je ad hoc odbor, ustanovljen v okviru Rexel Développement, katerega vloga je obravnavati najresnejša opozorila, ki jih prijavijo zaposleni v Rexel ali tretje osebe, s katerimi Rexel sodeluje.

Etika komisija skupine Rexel je sestavljena iz treh stalnih članov:

- generalni sekretar,
- direktorja kadrovske službe skupine in
- direktorja za etiko in skladnost

3. Izvedba notranje preiskave

Cilji in vodenje notranje preiskave

Čas, potreben za obravnavo prijave, je različen in je odvisen od zapletenosti prijavljenih dejstev in narave posredovanih informacij.

Cilj notranje preiskave je preveriti točnost in pomembnost prijavljenih dejstev. Prijava se preiskuje z uporabo metod (intervjuji, iskanje podatkov itd.), ki se lahko razlikujejo glede na kontekst in naravo zadeve.

Preiskavo lahko izvedejo:

- (xxvi) lokalni oddelek za človeške vire;
- (xxvii) lokalni oddelek za skladnost ali pravni oddelek;
- (xxviii) oddelek za skladnost skupine;
- (xxix) oddelek za človeške vire skupine;
- (xxx) odbor za etiko skupine Rexel, odvisno od narave in resnosti prijavljenih dejstev

(v nadaljnjem besedilu: **»vodja preiskave«**).

V vsakem primeru bo vodja preiskave vodil notranjo preiskavo opozorila. Informacije v zvezi z obstojem in vsebino opozorila bodo razkrite le osebam, odgovornim za preiskavo, v obsegu, ki je nujno potreben.

Ko je prijava vložena, skupina Rexel zagotavlja neodvisnost preiskovalnega postopka. Pred začetkom notranje preiskave se preveri, da nobena od oseb, vključenih v preiskavo prijave, ni neposredno ali posredno prizadeta zaradi prijavljenih dejstev ali da nima nobene povezave z interesom vpletenih oseb. Če se ugotovi tveganje za navzkrižje interesov, se zadevni zaposleni takoj odstrani iz postopka in nadomesti. To načelo neodvisnosti je sestavni del Rexelovega sistema etike in skladnosti ter ima za cilj zagotoviti strogo, nepristransko in verodostojno obravnavanje vseh prejetih opozoril.

Zasežba elektronske pošte, dokumentov ali računalniških medijev

Notranja preiskava lahko zahteva pregled in obdelavo e-pošte ali računalniških medijev, ki pripadajo enemu ali več zaposlenim. Pred zasegom ali zamrznitvijo e-poštne račune ali računalniških medijev mora vodja preiskave zaprositi za pooblastilo, kot je določeno v lokalnem postopku (npr. pri skupinskem odboru za etiko, lokalnem generalnem svetovalcu ali lokalnem pooblaščenцу za varstvo podatkov), da lahko zasega in zadrži te e-pošte za namene preiskave.

Gostujoči strokovnjak

Kadar to zahteva situacija, lahko vodja preiskave odloči, da povabi eno ali več oseb, da se mu pridružijo v okviru obravnavanja konkretnega opozorila, zlasti če je potrebno računovodsko, finančno, tehnično ali informacijsko-tehnološko strokovno znanje.

Vodja preiskave se tako lahko odloči, da bo pri svojem delu zaprosil za pomoč strokovnjaka iz podjetja Rexel, npr. iz oddelka za notranjo revizijo, finančnega oddelka, oddelka za nabavo, vodstvene ekipe države ali območja ali katere koli druge osebe znotraj skupine Rexel, ki jo vodja preiskave šteje za kompetentno in potrebno (), ali pa za pomoč zaprosi ustrezno usposobljenega zunanjega izvajalca storitev.

Naloga strokovnjaka se samodejno konča po zaključku vseh preverjanj ali postopkov obdelave v zvezi z opozorilom, za katerega je vodja preiskave zaprosil za pomoč, ali na preprosto zahtevo vodje preiskave.

Povabljeni strokovnjak je zavezan k enakim obveznostim glede zaupnosti kot notranji vodja in vodja preiskave.

4. Sprejemanje odločitev in zaključek preiskave

Če dejstva niso dokazana, se opozorilo zaključi in o tem se obvesti avtor poročila.

Če se dejstva dokažejo, bo vodja preiskave na podlagi ugotovitev preiskave ugotovil, ali je prišlo do kršitve zakona, Etičnega kodeksa ali Kodeksa ravnanja proti korupciji, in če je tako, bo priporočil popravne ukrepe in/ali ustrezne sankcije.

Oseba, ki je podala poročilo, je pisno obveščena o zaključku preiskave.

O zaključku preiskave se obvesti tudi zadevno osebo. Če se po preiskavi ugotovi, da je kršitev resna in dokazana, lahko pristojno vodstvo proti zadevni osebi sprejme disciplinske ukrepe, vključno z odpustom, odvisno od narave in resnosti domnevnih dejstev.

IV. Zaščita in zagotovila

1. Splošna načela

Vse preiskave se bodo izvajale pošteno in v popolni skladnosti z veljavnimi lokalnimi zakoni in predpisi. V vseh primerih bo skupina Rexel zagotovila, da se za zadevne osebe spoštuje načelo domneve nedolžnosti.

Sistem za prijavo nepravilnosti lahko deluje le na podlagi informacij, posredovanih v dobri veri. Vsaka prijava, posredovana v slabi veri, tj. z edini namenom povzročiti škodo, je lahko predmet disciplinskih ukrepov, vključno z odpustom.

2. Informacije

Prijavitelj bo obveščen v sedmih (7) delovnih dneh od prejema njegove prijave.

V razumnem roku, ki ne presega treh (3) mesecev od potrditve prejema prijave, je avtor prijave pisno obveščen o ukrepih, ki so predvideni ali sprejeti za oceno točnosti trditev in, kadar je to primerno, za odpravo predmeta prijave, ter o razlogih za te ukrepe. Če so obtožbe netočne ali neutemeljene ali če je poročilo postalo nepomembno, se avtor poročila pisno obvesti o zaključku primera.

Vsaka oseba, vpletena v dopustno opozorilo, bo obveščena o naravi obtožb, ki se nanašajo nanjo. Vendar pa bo v primeru previdnostnih ukrepov, potrebnih za preprečitev uničenja dokazov v zvezi z opozorilom, oseba, na katero se opozorilo nanaša, obveščena šele po sprejetju teh ukrepov, v skladu z veljavnimi zakoni.

Oseba, na katero se nanaša poročilo, v nobenem primeru ne sme od skupine Rexel na podlagi svoje pravice do dostopa zahtevati razkritja identitete osebe, ki je podala poročilo.

Določeno je, da se raven posredovanih informacij lahko razlikuje glede na veljavno lokalno zakonodajo.

3. Zaščita v kazenskih, civilnih in socialnih zadevah

Prijavitelji morajo upoštevati, da v skladu z lokalno veljavnimi predpisi:

- niso civilno odgovorni za škodo, ki je nastala zaradi njihovega poročila ali razkritja, pod pogojem, da je bilo njihovo poročilo podano v skladu z veljavnimi določbami in da je imel avtor poročila v času podaje poročila utemeljene razloge za domnevo, da je bilo poročilo ali javno razkritje vseh teh informacij potrebno za zaščito ogroženih interesov.
- niso kazensko odgovorni za pridobivanje ali dostop do informacij, ki so javno prijavljene ali razkrite, pod pogojem, da takšno pridobivanje ali dostop ne predstavlja ločenega kaznivega dejanja v skladu z lokalno veljavnimi predpisi. Kadar takšno pridobivanje ali dostop predstavlja ločeno kaznivo dejanje, se uporabljajo lokalno veljavna pravila o kazenski odgovornosti.
- Ne smejo biti kaznovani, odpuščeni, diskriminirani (zlasti v smislu plačila, usposabljanja, napredovanja) ali izpostavljeni povračilnim ukrepom ali grožnjam ali poskusom uporabe takih ukrepov zaradi poročanja ali razkritja informacij v skladu s predpisi, če je bilo poročilo podano v dobri veri.

Pod istimi pogoji posamezniki, ki so olajšali prijavo prijavitelja ali so z njim povezani, ne smejo biti izpostavljeni povračilnim ukrepom, grožnjam ali poskusom uporabe takih ukrepov.

Skupina Rexel ne dopušča nobene oblike povračilnih ukrepov, groženj ali poskusov uporabe takih ukrepov proti prijaviteljem in njihovim sorodnikom, kot je nadlegovanje.

4. Omejeno obdobje hrambe podatkov

Prijave se lahko hranijo le toliko časa, kolikor je nujno potrebno in sorazmerno z njihovo obdelavo ter zaščito njihovih avtorjev, oseb, na katere se nanašajo, in morebitnih tretjih oseb, ki so v njih omenjene, ob upoštevanju časa, potrebnega za morebitne dodatne preiskave. Podatki v zvezi s prijavo se lahko hranijo tudi po tem obdobju, če zadevne osebe niso identificirane ali identificirane.

Obstaja več sistemov za arhiviranje etičnih opozoril:

- **Nedopustna opozorila** (opozorila, ki ne sodijo v področje uporabe, niso resna, so neutemeljena, so podana v slabi veri itd.): ta se čim prej izbrišejo ali arhivirajo in anonimizirajo.
- **Za dopustna opozorila:**
 - če poročilu ne sledijo disciplinski ali pravni postopki, skupina Rexel zagotovi, da se vsi elementi poročila, ki bi lahko identificirali avtorja poročila, kot tudi elemente oseb, ki jih poročilo zadeva, uničijo v največ dveh (2) mesecih od konca preverjanja ali preiskave;
 - v primerih, ko preiskava vodi do pravnih postopkov ali disciplinskih sankcij, se elementi datoteke ustrezno hranijo za potrebno obdobje, dokler ne poteče zastaralni rok (šest (6) let) ali dokler niso izčrpane vse možnosti pritožbe. Po poteku predpisanega roka se ti podatki uničijo ali arhivirajo in anonimizirajo.

5. Zaupnost in varnost

Skupina Rexel sprejme vse potrebne ukrepe za ohranitev zaupnosti in varnosti podatkov med njihovim zbiranjem, obdelavo, posredovanjem ali shranjevanjem.

v skladu z lokalno veljavnimi predpisi postopki za zbiranje in obdelavo poročil zagotavljajo strogo zaupnost glede identitete avtorjev poročila, oseb, na katere se poročilo nanaša, in informacij, ki jih zbirajo osebe, odgovorne za zbiranje in obdelavo poročila.

V zvezi s tem:

- Posredovane informacije so omejene na osebe, ki jih morajo vedeti zaradi obdelave opozorila.
- Vse osebe, vključene v upravljanje opozoril, so usposobljene in zavezane k zaupnosti. Zlasti se zavezujejo, da podatkov ne bodo uporabljale za neprimerne namene in da bodo upoštevale omejeno obdobje hrambe podatkov v skladu z veljavno zakonodajo.
- Spletna platforma za poročanje je varna in opozorila, ki so na njej vložena, lahko pregledujejo le pooblaščen osebe. Ta sistem omogoča tudi zaposlenim, ki želijo ostati anonimni, da uporabijo ta kanal.
- Identiteta prijavitelja se lahko razkrije sodnim organom, če to zahteva zakon.
- Informacije, ki bi lahko identificirale osebo, vpleteno v prijavo, se ne smejo razkriti, razen sodnim organom, ko je bila ugotovljena veljavnost prijave.
- Znotraj subjektov skupine Rexel so oddelki, ki se običajno ukvarjajo z obravnavanjem opozoril, seznanjeni z zaupno naravo identitete avtorja in vpletenih oseb.

6. Varstvo osebnih podatkov

V okviru sistema za prijavo nepravilnosti lahko skupina Rexel zbira in obdeluje osebne podatke, zlasti podatke v zvezi z avtorjem prijave in osebo(-ami), vpleteno(-imi) v prijavo. Podrobno obvestilo v **Prilogi 4** določa pogoje, pod katerimi se podatki zbirajo, obdelujejo, shranjujejo in arhivirajo.

V. Poročanje

Oddelek za skladnost skupine enkrat letno poroča o številu opozoril, njihovi vrsti in ukrepih, sprejetih po njihovem prejemu, pri čemer se omeji na podatke, ki so nujno potrebni in sorazmerni z utemeljitvijo sporočila.

VI. Posodobitev postopka

Skupina Rexel si pridržuje pravico, da kadarkoli spremeni, dopolni ali posodobi ta postopek, da ga prilagodi spremembam zakonodaje, predpisov, sodne prakse ali notranjih potreb skupine. Vse posodobitve bodo izvedene v skladu z veljavnimi lokalnimi zakoni in predpisi.

Zaposleni, dobavitelji in druge zainteresirane strani bodo o spremembah obveščeni na ustrezen način (notranja komunikacija, e-pošta, objava na intranetu, neposredno obveščanje dobaviteljev itd.), v skladu z lokalnimi zakonskimi zahtevami.

Veljavna in uradna različica tega postopka bo objavljena in dostopna na spletnih straneh skupine Rexel, v intranetu skupine in na spletni platformi za poročanje.

Kontakt

Podjetje: Rexel Développement

Naslov: 13 boulevard Fort de Vaux 75017 Pariz (Francija) – *V vednost oddelku za skladnost skupine.*

E-poštni naslov: compliance@rexel.com

Prijavi situacijo

Če sumite ali veste za
kršitvi zakona, Etičnega kodeksa
ali Kodeksa ravnanja proti korupciji, to prijavite!



Kdo lahko sproži opozorilo?

**Vsi zaposleni v skupini
in tretje osebe** lahko uporabijo
etično linijo.



Kdaj je treba sprožiti alarm?

ali sumite **kršitev zakona
ali naših etičnih načel.**

To lahko vključuje:

- dejanja korupcije;
- kršitve človekovih pravic;
 - nadlegovanje
 - ali diskriminacijo;
 - goljufije itd.



Ali je to zaupno?

Da, lahko pa pošljete tudi
anonimno poročilo



Ali sem zaščiten?

Opozorilo morate podati
v dobri veri in brez kakršnega koli
neposrednega finančnega
nadomestila.

V tem primeru ste zaščiteni.



Kako sprožiti opozorilo?

1. Uporabite **spletno etično linijo
Rexel**

(povezava na spletu spodaj)

- na voljo 24 ur na dan, 7 dni v
tednu;

- na voljo v vseh
glavnih jezikih skupine.

2. **Uporabite sistem za prijavo
nepravilnosti**

, vzpostavljenega na lokalni ravni.

3. **Obrnite se na pravno ali oddelek
za skladnost ali oddelek za človeške
vire (skupine ali lokalni)**



Kdo obdeluje to opozorilo?

Za skupino: etični odbor.

Za lokalni sistem: glej lokalni
postopek.



Dodatne

Obiščite :

[https://www.rexel.com/en/
ethical-alert/](https://www.rexel.com/en/ethical-alert/)

Priloga 2: Seznam držav z lokalnim postopkom za prijavo nepravilnosti

Ta postopek je v nekaterih državah dopolnjen z lokalnimi postopki, ki določajo veljavne zakonske zahteve in, odvisno od primera, lokalno dostopne kanale.

Informacije o lokalnih kanalih so navedene spodaj. Za najnovejše podrobnosti se posvetujte z lokalnim postopkom.

- Avstralija:

o Storitev za razkritje Rexel STOPlne (ki jo upravlja neodvisni zunanji ponudnik storitev):

Telefon: 1300 30 45 50

Faks: Rexel Holdings Australia (C/- the STOPlne) 03 9882 4480

E-pošta: rexel@stopline.com.au

Spletna stran: <https://rexel.stoplinereport.com/>

Pošta: Rexel Holdings Australia

C/- the STOPlne

Locked Bag 8

HAWTHORN VIC 3122

- **Kanada:** lahko se obrnete na etični odbor.

- Nemčija:

o E-pošta: whistleblowing@rexel.de

o Pošta:

Rexel Germany GmbH & Co.

KG - z. Hd. Frau Nicole Steuer | General Counsel

Ridlerstr.5780339 München

- Irska

o Lahko se obrnete na oddelek za človeške vire, pooblaščenca za prijavo nepravilnosti, izvršnega direktorja ali našo zunanjo telefonsko linijo za prijavo nepravilnosti, ki jo upravlja Safecall.

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- Italija:

o <https://report.whistleb.com/rexel>

- **Nizozemska:** lahko se obrnete na odgovornega za etiko.

- Švedska:

o <https://whistleblow.vismadraftit.se/rexel-sverige-ab>

o Telefon: 08-556 214 14.

- Združeno kraljestvo

o Lahko se obrnete na oddelek za človeške vire, uradnika za prijavo nepravilnosti, izvršnega direktorja ali našo zunanjo telefonsko linijo za prijavo nepravilnosti, ki jo upravlja Safecall.

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- ZDA

o E-pošta za skladnost: ethics@rexelusa.com

o Telefonska linija za skladnost: 1-800-714-8774

Priloga 3: Primeri ravnanj ali kršitev, ki jih zajema postopek za prijavo nepravilnosti

Kategorije	Obseg
Korupcija	V okviru veljavnih lokalnih zakonov in predpisov ter protikorupcijskih politik Skupine: korupcija se nanaša na izmenjavo, neposredno ali prek tretje osebe, koristi (denar, darila, povabila, storitve, povezave itd.) v zameno za izvedbo ali opustitev dejanja, povezanega z delom ali mandatom. Lahko gre za osebo, ki predlaga ali ponuja korist, da bi pridobila uslugo (aktivna korupcija), ali za osebo, ki prosi za korist ali jo sprejme v zameno za storitev (pasivna korupcija). Korupcija lahko vključuje javne in zasebne akterje, izkrivlja konkurenco, ogroža preglednost odločitev in izpostavlja vpletene posameznike in organizacije sankcijam in kazenskemu pregonu.
Nadlegovanje	Nadlegovanje se nanaša na ponavljajoče se vedenje ali eno samo resno dejanje, ki ogroža dostojanstvo, varnost ali delovne pogoje osebe. Izraža se v besedah, gestah, odnosih ali dejanjih, ki so namenjeni ustrahovanju, poniževanju, izolaciji, grožnjam ali poslabšanju položaja zaposlenega ali tretje osebe v zvezi s poklicno dejavnostjo. Nadlegovanje je lahko psihološke narave, na primer v obliki ponižujočih pripomb, namernega izoliranja, preobremenjevanja ali odvzemanja delovnih sredstev, izključevanja, širjenja govoric ali sistematičnega poniževanja. Lahko je tudi spolne narave. Spolno nadlegovanje je značilno za neželjeno spolno vedenje ali komentarje, ki se ponavljajo ali predstavljajo en sam resen incident, ki spodbija dostojanstvo osebe ali ustvarja zastrašujoče, sovražno, ponižujoče ali sramotilno delovno okolje. To med drugim vključuje vztrajno spogledovanje, komentarje o telesu, zahteve po spolnih uslugah, nezaželene fizične geste ali dotike ali širjenje spolnih podob brez soglasja. Nadlegovanje, bodisi moralno ali spolno, je nesprejemljivo, storilci pa so odgovorni v skladu z veljavnimi lokalnimi zakoni.
	Diskriminacija na delovnem mestu vključuje neugodno obravnavanje osebe na podlagi meril, ki jih prepoveduje zakon, kot so poreklo, spol, družinski status itd. ali katerakoli druga značilnost, ki jo ščiti lokalna zakonodaja. Diskriminacija lahko na primer povzroči neenako obravnavanje pri dostopu

Diskriminacija	do zaposlitve, delovnih pogojih, usposabljanju, mobilnosti ali kateri koli drugi situaciji, povezani s poklicno dejavnostjo. Lahko se kaže v obliki odločitev o zaposlovanju, ocenjevanju, napredovanju, dodelitvi nalog ali odpustitvi, ki osebo postavljajo v neugoden položaj brez objektivne utemeljitve, ki bi temeljila na zahtevah delovnega mesta. Na delovnem mestu lahko diskriminacija poteka v dveh oblikah: - Neposredna diskriminacija. V tem primeru storilec namerno sprejme odločitev na podlagi diskriminatornih meril, ki so prepovedana z zakonom. Posredna diskriminacija. V tem primeru storilec sprejme odločitev, ki se zdi nevtralna, vendar na koncu postavlja nekatere osebe v neugoden položaj v primerjavi z drugimi. Na primer, notranji predpisi dovoljujejo, da v podjetju po 50. letu starosti ostanejo samo moški. To zato predstavlja posredno diskriminacijo na podlagi spola in starosti.
Zdravje/varnost	Vsaka resna kršitev ali tveganje za zdravje in varnost pri delu. Varnost pri delu se nanaša na vse ukrepe in prakse, namenjene zaščiti fizične in duševne integritete ljudi na delovnem mestu z zmanjšanjem tveganja za nesreče, poškodbe in poklicne bolezni. To vključuje prepoznavanje in ocenjevanje tveganj, izvajanje tehničnih in organizacijskih varnostnih ukrepov, usposabljanje in obveščanje zaposlenih ter uvedbo ukrepov za preprečevanje, posredovanje in odzivanje v nujnih primerih. Izpolnjevanje teh obveznosti prispeva k varnemu delovnemu okolju, ki je v skladu z lokalnimi zahtevami.
Človekove pravice (razen diskriminacije in nadlegovanja)	Vsaka resna kršitev ali tveganje za človekove pravice in temeljne svoboščine, priznane na nacionalni in mednarodni ravni (), ter vsaka kršitev veljavnih lokalnih zahtev na tem področju. To vključuje, vendar ni omejeno na, situacije, ki vključujejo načela, kot so spoštovanje svobode združevanja in izražanja, dostop do dostojnih in varnih delovnih pogojev ter možnost, da imajo zadevne osebe dostop do pravnih sredstev.
Navzkrižje interesov	Navzkrižje interesov je situacija, v kateri osebni interesi posameznika, bodisi finančni, družinski, prijateljski, politični ali povezani z drugimi koristmi, lahko vplivajo ali se zdi, da vplivajo na njegovo presojo ali odločitve pri opravljanju njegovih dolžnosti v skupini Rexel. To ni nujno krivda ali nezakonito dejanje, ampak tveganje pristranskosti, ki ogroža pričakovano nepristranskost. To tveganje pristranskosti je lahko dovolj veliko, da omaje zaupanje vpletenih, spremeni kakovost odločitev in škodi ugledu organizacije. Navzkrižje interesov je lahko dejansko (že prisotno), potencialno (verjetno bo nastalo) ali navidezno (tako ga dojemajo tretje osebe). Sistem za prijavo nepravilnosti ni namenjen

	nadomestitvi postopka za prijavo navzkrižja interesov, ki ga je opredelila skupina Rexel.
Protekcioniistične prakse	Proti-konkurenčne prakse se nanašajo na ravnanje podjetij, ki ovira prosto konkurenco in škoduje drugim akterjem na trgu (strankam, dobaviteljem, konkurentom). Vključujejo formalne ali neformalne dogovore med konkurenti o usklajevanju cen, poslovnih pogojev, razdelitvi trgov, ozemelj ali proizvodov ali omejevanju ponudbe ali bojkotu določenih partnerjev. Vključujejo tudi primere zlorabe prevladujočega položaja (npr. izrinjanje konkurenta, vsiljevanje plenilskih cen ali neupravičenih vezanih prodaj), vplivanje na ceno nadaljnje prodaje, ki jo zaračunavajo distributerji, in izmenjavo nezaupnih strateških informacij, ki bi lahko vplivale na tržno ravnanje (kot so načrti, tržni podatki ali zmogljivosti). Te prakse so prepovedane s pravili o konkurenci in se kaznujejo z visokimi globami.
Okolje	Vsak primer, ko niso izpolnjene veljavne okoljske zahteve ali ko je ugotovljeno znatno tveganje ali škoda za okolje, bodisi znotraj podjetja bodisi med njegovimi partnerji v vrednostni verigi. To vključuje preprečevanje onesnaževanja, odgovorno rabo virov in varno ravnanje s snovmi in odpadki v skladu z zakonskimi obveznostmi in notranjimi standardi.
Goljufija	Vsaka situacija, ki vključuje prikrivanje, zavajanje ali manipulacijo z namenom pridobiti neupravičeno prednost ali se izogniti obveznostim, bodisi davčnim, finančnim ali računovodskim. To vključuje na primer ponarejanje dokumentov ali evidenc, napačno predstavljanje finančnih podatkov, prikrivanje dohodkov ali premoženj a ali kakršno koli shemo, namenjeno zaobiti veljavna pravila, bodisi znotraj podjetja bodisi v njegovi vrednostni verigi.
Trgovanje z notranjimi informacijami	Trgovanje z notranjimi informacijami je dejanje nakupa, prodaje ali priporočanja finančnih instrumentov z uporabo ali zanašanjem na nezaupne informacije o izdajatelju ali njegovih vrednostnih papirjih. Vključuje tudi nezakonito razkritje takih informacij tretjim osebam. Takšno ravnanje daje nepošteno prednost na trgih in je strogo prepovedano ter kaznivo po zakonu.
Fiktivna delovna mesta	Fiktivno delovno mesto je situacija, v kateri je oseba plačana za delovno mesto ali naloge, ki se dejansko ne opravljajo ali ne obstajajo, da bi pridobila nepošteno prednost. To lahko vključuje popolno odsotnost dejanskega dela, fiktivne naloge ali nominalno dodelitev oddelku brez dejanskega prispevka, znotraj podjetja ali prek tretjih oseb.
	Vsak primer, ko osebni podatki ali IT-sistemi niso zaščiteni v skladu z zakoni in notranjimi pravili, kar izpostavlja

Varstvo osebnih podatkov / varnost IT	posameznike ali podjetje tveganju nepooblaščenega dostopa, uporabe, razkritja, spremembe ali uničenja. To zajema zakonito in minimalno zbiranje in obdelavo podatkov, varnost sistema (nadzor dostopa, šifriranje, varnostne kopije), upravljanje incidentov in kršitev ter zaupnost in celovitost informacij skozi njihov življenjski cikel, vključno pri ponudnikih storitev. Osební podatki so vse informacije, ki neposredno ali posredno identificirajo fizično osebo (npr. ime, kontaktni podatki, identifikatorji, fotografija, podatki o lokaciji ali drugi elementi, povezani z njeno identiteto ali osebnim življenjem).
---	--

POLITIKA ZASEBNOSTI

—

SISTEM ZA PRIJAVLJANJE KRŠITEV

Različica 12/2025

Skupina Rexel je vzpostavila profesionalni sistem za prijavo nepravilnosti, ki omogoča njenim zaposlenim in tretjim osebam, s katerimi skupina Rexel sodeluje, da prijavijo nezakonita dejanja ali neprimerno ravnanje. Obseg sistema je opisan v postopku za prijavo nepravilnosti, ki je na voljo na spletni strani [rexel.com](https://www.rexel.com).

 V okviru tega sistema lahko podjetje Rexel zbira in obdeluje podatke o vas. Zaupnost podatkov je temelj našega odnosa zaupanja. Zato v okviru naših poslovnih dejavnosti resno jemljemo zaščito vaših osebnih podatkov.

Ta politika opisuje zaveze skupine Rexel na področju varstva osebnih podatkov. V nadaljevanju boste izvedeli več o svojih pravicah in pogojih, pod katerimi se vaši osebni podatki zbirajo, obdelujejo, shranjujejo in arhivirajo.

Kdo smo?

REXEL DEVELOPPEMENT SAS, poenostavljena delniška družba po francoskem pravu, s sedežem na naslovu 13, Boulevard du Fort de Vaux, Pariz, vpisana v pariški register trgovskih družb pod številko 480 172 840, je upravljavec podatkov.

Subjekt znotraj skupine, ki ima pogodbo o zaposlitvi z avtorjem poročila ali z njim sodeluje, je prav tako upravljavec podatkov.

Ti določajo namene in načine obdelave vaših podatkov.

V tej politiki se nanje sklicujemo kot na »Rexel«, »mi« ali »upravljavci podatkov«.

EY Poljska deluje kot obdelovalec za obdelavo, ki se izvaja na spletni platformi za opozarjanje.

Kako obdelujemo vaše podatke v okviru sistema za opozarjanje?

V spodnji tabeli je podrobno navedeno:

- (i) zakaj obdelujemo vaše osebne podatke,
- (ii) katere vrste podatkov obdelujemo in
- (iii) pravno podlago za obdelavo vaših podatkov.

Namen 1	Vrsta podatkov
Zbiranje in obdelava opozoril o dejanjih, ki kršijo zakon ali protikorupcijski kodeks ravnanja, ki ga zajema sistem za prijavo nepravilnosti (glej Postopek za prijavo nepravilnosti) <u>Podcilji:</u> - Centralizirano upravljanje strokovnih poročil (sprejemanje in obravnavanje opozoril, vzpostavitev varnega kanala, shranjevanje in hranjenje informacij, zagotavljanje varnosti) - Obdelava strokovnih poročil (izvajanje notranjih preiskav, ocena relevantnih dejstev) - Sprejemanje odločitev in izvajanje ustreznih ukrepov po zaključku poročila (obveščanje in izvajanje ukrepov) - Statistično spremljanje in izboljšanje sistema za prijavo nepravilnosti - Uveljavljanje ali zagovarjanje pravic v sodnih postopkih	V okviru sistema se lahko obdelujejo naslednje kategorije podatkov: - Osebni podatki (ime in priimek, kontaktni podatki), poklicni podatki (delovno mesto, delodajalec, kraj dela) osebe, ki je podala poročilo (razen če je poročilo anonimno), in vse druge informacije, ki jih je ta oseba prostovoljno posredovala - Osebni podatki (ime in priimek, kontaktni podatki), poklicni podatki (delovno mesto, delodajalec, kraj dela) vpletenih oseb - Identitetni podatki (ime in priimek, e-poštni naslov), poklicni podatki (delovno mesto, delodajalec, kraj dela) oseb, vpletenih ali posvetovanih pri zbiranju ali obdelavi prijave, ter posrednikov in oseb, ki so v stiku s prijaviteljem - Občutljivi podatki (rasna ali etnična pripadnost, politična prepričanja, verska ali filozofska prepričanja, članstvo v sindikatu, podatki o zdravju, spolno življenje ali spolna usmerjenost), kadar je to nujno potrebno za uveljavljanje ali zaščito pravnih pravic (člen 9.2.f GDPR) ali iz razlogov pomembnega javnega interesa (člen 9.2.g GDPR) - Podatki v zvezi s kazenskimi obsodbami in kaznivimi dejanji ali s tem povezanimi varnostnimi ukrepi, kadar je to nujno potrebno in v skladu s členom 10 GDPR - Informacije, zbrane med preverjanjem dejstev - Poročila o preverjanju - Podatki v zvezi z nadaljnjim ukrepanjem na podlagi poročila
Pravna podlaga za obdelavo vaših podatkov Zakonska obveznost vzpostavitve sistema za prijavo nepravilnosti: zlasti členi 8.I.B in 17 II zakona Sapin II ter člen L. 225-102-4 Trgovinskega zakonika, kakor tudi vsi enakovredni zakoni v zvezi z zaščito prijaviteljev nepravilnosti, bojem proti korupciji ali dolžnostjo pazljivosti.	

Namen 2	Vrsta podatkov
Zbiranje in obdelava opozoril o dejanjih, ki kršijo Etični kodeks <u>Podnamene:</u> - Centralizirano upravljanje strokovnih poročil (sprejemanje in obravnavanje opozoril, vzpostavitev varnega kanala, shranjevanje in hranjenje informacij, zagotavljanje varnosti) - Obdelava strokovnih poročil (izvajanje notranjih preiskav, ocena relevantnih dejstev) - Sprejemanje odločitev in izvajanje ustreznih ukrepov po zaključku poročila (obveščanje in izvajanje ukrepov) - Statistično spremljanje in izboljšanje sistema za prijavo nepravilnosti - Uveljavljanje ali zagovarjanje pravic v sodnih postopkih	V okviru sistema se lahko obdelujejo naslednje kategorije podatkov: - Identitetni podatki (ime in priimek, kontaktni podatki), poklicni podatki (delovno mesto, delodajalec, kraj dela) osebe, ki prijavlja (razen če je prijava anonimna), in vse druge informacije, ki jih ta oseba prostovoljno posreduje - Identitetni podatki (ime in priimek, kontaktni podatki), poklicni podatki (delovno mesto, delodajalec, kraj dela) oseb, vpletenih v zadevo - Identitetni podatki (ime in priimek, e-poštni naslov), poklicni podatki (delovno mesto, delodajalec, kraj dela) oseb, vpletenih ali posvetovanih pri zbiranju ali obdelavi prijave, ter posrednikov in oseb, ki so v stiku s prijaviteljem - Občutljivi podatki (rasna ali etnična pripadnost, politična prepričanja, verska ali filozofska prepričanja, članstvo v sindikatu, podatki o zdravju, spolno življenje ali spolna usmerjenost), kadar je to nujno potrebno za uveljavljanje ali zaščito pravnih pravic (člen 9.2.f GDPR) ali iz razlogov pomembnega javnega interesa (člen 9.2.g GDPR) - Podatki v zvezi s kazenskimi obsodbami in kaznivimi dejanji ali s tem povezanimi varnostnimi ukrepi, kadar je to nujno potrebno in v skladu s členom 10 GDPR - Informacije, zbrane med preverjanjem dejstev - Poročila o preverjanju - Podatki v zvezi z nadaljnjim ukrepanjem na podlagi poročila
Pravna podlaga za obdelavo vaših podatkov	
Pravna podlaga: legitimni interes za obdelavo etičnih opozoril, ki niso zajeta v zakonski obveznosti.	

Kdo so prejemniki vaših podatkov?



Osebni podatki, ki jih zbiramo, ter vsi podatki, ki se zbirajo naknadno, so namenjeni nam v naši vlogi upravljavca podatkov.



Zagotavljamo, da imajo dostop do teh podatkov le pooblaščene osebe.

Notranje:

- Osebe, odgovorne za zbiranje in obdelavo opozoril, in sicer:
 - Člani etičnega odbora skupine Rexel
 - Pooblaščeni člani pravne službe ali službe za skladnost na ravni skupine in lokalni ravni
 - Pooblaščeni člani oddelka za človeške vire na ravni skupine in lokalni ravni
- Pooblaščeni člani oddelka za revizijo in notranjo kontrolo na ravni skupine in lokalni ravni, ki zagotavljajo učinkovitost notranjih kontrol in upravljanja
- Če to upravičuje situacija, lahko do podatkov dostopajo tudi drugi notranji zaposleni, zlasti kadar je potrebno računovodsko, finančno, pravno, tehnično ali informacijsko-tehnološko strokovno znanje.

Zunanji:

- Naši svetovalci
- Naši posredniki in zavarovalci
- Naši revizorji
- Pristojni organi (sodni, upravni in regulativni organi) v skladu z veljavnimi predpisi
- Naši ponudniki storitev, natančneje EY Poland, ki nam zagotavlja spletno platformo za poročanje.

Ti prejemniki se nahajajo v Evropski uniji.

Kako dolgo hranimo vaše podatke?

Situacije	Obdobje hrambe
Nedopustna opozorila (ki ne sodijo v področje uporabe, niso resna, nimajo zadostnih informacij, so v nasprotju z dobrim verom itd.)	Čimprejšnje izbrisanje ali arhiviranje in anonimiziranje
Dopustno opozorilo, vendar zavrnjeno (ni sledil disciplinski ali pravni postopek)	Izbris ali anonimiziranje in arhiviranje v roku dveh (2) mesecev
Opozorila, ki so povzročila disciplinske ali pravne postopke	Hranjenje podatkov do konca postopkov in pritožb. Po tem obdobju izbris ali anonimiziranje in arhiviranje.

Kakšne so vaše pravice?



V skladu z zakoni o varstvu osebnih podatkov imate naslednje pravice:

- pravico do dostopa: lahko dostopate do informacij, ki jih hranimo o vas, in pridobite njihovo kopijo;
- pravica do popravka: lahko zahtevate, da se netočni podatki, ki se nanašajo na vas, spremenijo, dopolnijo, posodobijo ali izbrišejo;
- pravica do ugovora: lahko ugovarjate obdelavi vaših podatkov, razen če obstajajo legitimni in nujni razlogi za njihovo obdelavo;
- pravica do izbrisa: lahko zahtevate, da izbrišemo podatke o vas v okviru pogojev, določenih v členu 17 GDPR;
- pravica do prenosljivosti podatkov: lahko pridobite svoje podatke, da jih prenesete v drugo organizacijo ali za osebno uporabo;
- pravica do omejitve obdelave;
- pravica do oblikovanja posebnih in splošnih smernic v zvezi s shranjevanjem, izbrisom in posredovanjem vaših podatkov po vaši smrti.

Vsaka oseba, ki je predmet poročila, bo čim prej (najpozneje v enem mesecu) po računalniški ali drugi obliki evidentiranja podatkov, ki se nanašajo nanjo, obveščena, da bo lahko uveljavila svoje pravice. Vendar če bi takšne informacije lahko resno ogrozile cilje obdelave in zlasti potek preiskave (na primer, če obstaja tveganje uničenja dokazov), se lahko te informacije odložijo in se posredujejo šele, ko je tveganje odpravljeno.

Oseba, ki je predmet poročila, v nobenem primeru ne sme od upravljavca podatkov na podlagi svoje pravice do dostopa pridobiti informacij o identiteti avtorja poročila ali katere koli druge osebe, vključene v preiskavo.

Če ne prejmete odgovora ali če menite, da je odgovor nezadovoljiv, ali če menite, da obdelava vaših podatkov ni v skladu z zakonskimi in regulativnimi določbami, se lahko obrnete na pristojni nadzorni organ.

Kako uveljaviti svoje pravice?



S pisno prošnjo našemu pooblaščenču za varstvo podatkov:

Države	Subjekti	Naslov
Avstrija	COMTECH IT-SOLUTIONS GMBH	datenschutz@rexel.at
	Rexel Austria GmbH	datenschutz@rexel.at
Belgija	Rexel Belgique SA	gdpr@rexel.be
Francija	Cordia	donnees.personnelles@francofa-eurodis.fr
	Rexel Développement SAS / Rexel Group	data.protection@rexel.com
	Rexel France SAS	donnees.personnelles@rexel.fr
	Bizline	data.protection@rexel.com
	Gigamedia	data.protection@rexel.com
	Sofinther SAS	donnees.personnelles@sofinther.fr
	Espace Elec SAS	donnees.personnelles@espace-elec.fr
	Esabora Digital Services SAS	dataprotection-rda@rexel.fr
	Francofa Eurodis	donnees.personnelles@francofa-eurodis.fr
	Freshmile Services SAS	donnees.personnelles@rexel.fr
	ITESA	donnees.personnelles@rexel.fr
Nemčija	REXEL GERMANY BETEILIGUNGS GMBH	Datenschutzbeauftragter@rexel.de
	Rexel Germany GmbH & Co KG	Datenschutzbeauftragter@rexel.de
	REXEL GERMANY VERWALTUNGS GMBH	Datenschutzbeauftragter@rexel.de
Italija	Rexel Italia S.p.A	dataprotection@rexel.it
	Tecno-Bi S.r.l.	dataprotection@rexel.it
	Comm-Tech S.r.l.	dataprotection@rexel.it
Irska	M. Kelliher 1998	data.protection@rexel.ie
	Rexel Industrial Solutions	data.protection@rexel.ie
Luksemburg	Rexel Luxembourg SA	gdpr@rexel.be
Nizozemska	Rexel Nederland B.V	AVG@rexel.nl
	Wasco Group B.V.	AVG@rexel.nl
	Wasco Holding B.V.	AVG@rexel.nl
	Wasco Groothandels Greop B.V.	AVG@rexel.nl
	Wasco Distributlecentrum B.V.	AVG@rexel.nl
Slovenija	Rexel d.o.o.	dpc@rexel.si
Švedska	Rexel Sverige AB	dataskydd@rexel.se
Švica	ELEKTRO-MATERIAL AG	datenschutz@e-m.ch
	Rexel 3S	data.protection@rexel.com
Velika Britanija	Rexel (UK) Ltd.	data.protection@rexel.co.uk



Anmälningförfarande December 2025_V1

Sammanfattning

I.	<u>Inledning</u>	3
1.	<u>Syftet med det interna visseblåsningssystemet</u>	3
2.	<u>Påminnelse om den rättsliga ramen</u>	3
3.	<u>Tillämpningsområde</u>	3
II.	<u>Insamling av etiska varningar</u>	4
1.	<u>Villkor för att en etisk varning ska vara tillåtlig</u>	4
	<u>Vem kan lämna in en anmälan?</u>	4
	<u>Hur kan du dra nytta av visseblåsartillstånd och det därmed förknippade rättsliga skyddet?</u>	4
	<u>Vilka fakta kan rapporteras?</u>	5
2.	<u>Hur man lämnar in en anmälan</u>	6
3.	<u>Anmälanens innehåll</u>	7
4.	<u>Anonyma anmälningar</u>	7
5.	<u>Externa kanaler</u>	7
III.	<u>Hantering av interna etiska varningar</u>	7
1.	<u>Bekräftelse av mottagandet av rapporten</u>	7
2.	<u>Granskning av rapportens tillåtlighet</u>	7
3.	<u>Genomförande av den interna utredningen</u>	8
4.	<u>Beslutsfattande och avslutande av utredningen</u>	9
IV.	<u>Skydd och garantier</u>	10
1.	<u>Allmänna principer</u>	10
2.	<u>Information</u>	10
3.	<u>Skydd i brottmål, civilrättsliga mål och sociala ärenden</u>	10
4.	<u>Begränsad lagringstid för uppgifter</u>	11
5.	<u>Sekretess och säkerhet</u>	11
6.	<u>Skydd av personuppgifter</u>	12
V.	<u>Rapportering</u>	12
VI	<u>Uppdatering av förfarandet</u>	12
	<u>Bilaga 1: Sammanfattning</u>	13
	<u>Bilaga 2: Förteckning över länder med lokala visseblåsningförfaranden</u>	14
	<u>Bilaga 3: Exempel på beteenden eller förseelser som omfattas av visseblåsningförfarandet</u>	15
	<u>Bilaga 4: Integritetspolicy</u>	19

I. Inledning

1. Syftet med det interna visseblåsningssystemet

Som en del av Rexel-koncernens policy för etik och regelefterlevnad, som beskrivs särskilt i dess Etikguide, dess hållbara uppförandekod för leverantörer och dess uppförandekod mot korruption, har Rexel-koncernen inrättat ett internt visseblåsarsystem.

Rxel-koncernens interna visseblåsningssystem gör det möjligt för alla anställda, samt tredje parter som Rexel-koncernen har en relation med, att rapportera situationer som bryter mot lagen, Rexel-koncernens etikguide eller dess uppförandekod mot korruption.

Syftet med denna rutin är att beskriva processen för insamling och hantering av etiska rapporter inom Rexel-koncernen.

En sammanfattning av förfarandet finns i **bilaga 1**.

2. Påminnelse om det rättsliga ramverket

Eftersom Rexel-koncernens holdingbolag är registrerat i Frankrike har förfarandet fastställts i enlighet med följande franska lagar:

- "Sapin II-lagen" av den 9 december 2016 om transparens, antikorrupktion och ekonomisk modernisering.
- "Lagen om vaksamhetsplikt" av den 27 mars 2017, som avser vaksamhetsplikten för moderbolag och entreprenadföretag.
- "Waserman-lagen" av den 21 mars 2022, som syftar till att förbättra skyddet för visseblåsare, och dess förordning om implementering av den 3 oktober 2022.

Förfarandet baseras också på ett antal publikationer från den franska antikorrupktionsbyrå (AFA) och den franska dataskyddsmyndigheten (CNIL):

- AFA:s rekommendationer
- Den praktiska guiden "Interna antikorrupktionsutredningar" som publicerades i mars 2023 av AFA och den franska finansåklagarmyndigheten.
- CNIL:s referensdokument "professionella varningar", som ursprungligen publicerades 2019 och uppdaterades 2023.

Mer generellt sker insamling och behandling av rapporter i enlighet med tillämpliga lagar och förordningar, och denna procedur kan uppdateras vid behov för att återspegla lagstiftningsutvecklingen och bästa praxis.

Om en lokal lag eller förordning erbjuder mer skyddande regler för visseblåsare än detta förfarande, ska de lokala bestämmelserna ha företräde. Om detta förfarande dock ger större skyddsgarantier, kommer Rexel-koncernen att tillämpa dem frivilligt i den utsträckning som tillämplig lag tillåter.

3. Tillämpningsområde

Denna rutin är avsedd att implementeras i alla Rexel-koncernens enheter. Den kommer att ändras efter behov för att återspegla eventuella förändringar i lagar och förordningar.

Denna rutin kompletteras i vissa länder inom Rexel-koncernen med lokala rutiner. Sådana specificerar tillämpliga lagkrav och, i förekommande fall, de kanaler som finns tillgängliga lokalt (se bilaga 2).

Den som lämnar in en rapport kan därför välja vilken rapporteringskanal han eller hon vill använda (koncernens eller den lokala). Det tillämpliga förfarandet är då det som motsvarar den valda kanalen. Beroende på arten och allvarlighetsgraden av det rapporterade beteendet eller missförhållandena kan en rapport som lämnats via den lokala kanalen vidarebefordras till koncernen och vice versa.

Denna rutin gäller alla anställda inom Rexel-koncernen (oavsett roll, position eller avdelning) och tredje parter som Rexel-koncernen har en relation med. Den omfattar insamling och behandling av interna rapporter av Rexel-koncernen och, mer specifikt:

- Inlämning av dessa
- Mottagandet av dem
- Bedömning av deras tillåtlighet
- De viktigaste stegen i den interna utredningen
- Avslutandet av ärendet.

II. Insamling av etiska varningar

1. Villkor för att en etisk varning ska kunna tas upp till prövning

Vem kan lämna in en rapport?

Rxel-koncernens interna varningssystem är öppet för följande personer:

- Rexel-koncernens anställda (fast anställda, visstidsanställda, lärlingar, praktikanter)
- Externa eller tillfälliga anställda (tillfälligt anställda, konsulter etc.)
- Arbetssökande
- Tidigare anställda
- Aktieägare, partners och innehavare av rösträtt vid bolagsstämman
- Medlemmar i administrativa organ, ledningsgrupp eller tillsynsorgan
- Alla anställda vid tredje parter som Rexel-koncernen har en relation till (t.ex. kunder, leverantörer, tjänsteleverantörer etc.).

Det interna visseblåarsystemet är öppet för alla enheter inom Rexel-koncernen och finns tillgängligt på koncernens huvudspråk: engelska, tyska, kinesiska, franska, italienska, nederländska, svenska och slovenska.

Hur kan du dra nytta av visseblåarsstatus och det därmed sammanhängande rättsliga skyddet?

För att betraktas som visseblåare och få ta av det skydd som lagen ger måste du uppfylla den juridiska definitionen av visseblåare, dvs. uppfylla alla följande kriterier, om inte annat föreskrivs i tillämplig lokal lagstiftning:

- Vara en fysisk person.
- Inte erhålla någon direkt ekonomisk ersättning för anmälan.

- Agera i god tro.
- Om de fakta som rapporterats har erhållits utanför ett professionellt sammanhang, ha personlig kännedom om de fakta som har rapporterats.

Vilka fakta kan rapporteras?

Rexel-koncernens interna visselblåsarsystem tillåter rapporter om fakta som kan utgöra följande kategorier av beteende eller tjänstefel:

- Brott eller förseelse
- Ett hot mot eller skada på allmänintresset
- En överträdelse eller försök att dölja en överträdelse av nationella, europeiska eller internationella lagar och förordningar
- Brott mot eller en situation som strider mot Rexel-koncernens etiska riktlinjer eller uppförandekod mot korruption
- Allvarliga risker relaterade till Rexel-koncernens verksamhet som kan skada mänskliga rättigheter, grundläggande friheter, människors hälsa och säkerhet eller miljön

Exempel på beteenden eller förseelser som ska rapporteras kan vara:

- Korruption, inklusive alla överträdelser av uppförandekoden mot korruption
- Trakasserier (psykologiska eller sexuella)
- Diskriminering
- Hälsa, hygien eller säkerhet (t.ex. risk för fysisk eller psykisk integritet)
- Mänskliga rättigheter (andra än diskriminering, integritet och trakasserier)
- Intressekonflikt
- Konkurrensbegränsande metoder
- Miljö (t.ex. föroreningar, avfallshantering)
- Skattebedrägeri
- Finansiellt eller redovisningsmässigt bedrägeri
- Insiderhandel
- Fiktiva jobb
- Personuppgifter/IT-säkerhet

Bilaga 3 illustrerar några av dessa typer av beteenden eller förseelser.

Rapporter som avser kategorier som inte anges ovan omfattas inte av detta förfarande. På samma sätt undantas fakta, information eller dokument, oavsett form eller medium, vars offentliggörande är förbjudet enligt bestämmelser om nationell försvarssekretess, läkarsekretess, sekretess för rättsliga överläggningar, sekretess för rättsliga utredningar eller förhör, eller advokatsekretess från detta förfarande. I tillämpliga fall kommer rapportens författare att informeras och hänvisas till de personer som är behöriga att hantera de fakta som har rapporterats.

2. Hur man lämnar in en rapport

Den som lämnar in en rapport har flera kanaler att välja mellan för att lämna in varningar:

- Den webbaserade rapporteringsplattformen som är tillgänglig på:
<https://www.rexel.com/en/rexel-group-ethics-alert>;
- Ytterligare rapporteringskanaler som kan finnas på koncern- eller lokal nivå.

Det finns ingen hierarki mellan kanalerna. Den som lämnar in en rapport kan använda vilken kanal som helst.

Oavsett vilken kanal som används kallas den eller **de** personer som ansvarar för att samla in rapporterna nedan för **"intern chef"**.

Onlineplattformen för rapportering

Den som lämnar in en rapport kan göra en anmälan, även anonymt, på den onlineplattform för rapportering som är tillgänglig på: <https://www.rexel.com/en/rexel-group-ethics-alert>

Detta är en särskild, kostnadsfri plattform som är tillgänglig dygnet runt.

Den drivs inom Europeiska unionen av en extern tjänsteleverantör (EY) som har implementerat strikta åtgärder för att säkerställa datasäkerhet och konfidentialitet. Det bör noteras att denna tjänsteleverantörs anställda inte är involverade i behandlingen av rapporter och inte har tillgång till den information som utbyts.

Plattformen möjliggör direkt kommunikation med mottagaren av en rapporten via chatt. Den gör det också möjligt för den som lämnar in en rapport att skicka dokument som styrker fakta.

Länken till denna plattform finns på koncernens webbplatser: <https://www.rexel.com/en/rexel-group-ethics-alert> och <https://ethique.rexel.com/en/>, samt på intranätssidorna för Rexel-koncernens enheter.

Ytterligare rapporteringskanaler

Interna anställda inom Rexel-koncernen kan lämna in en rapport skriftligen eller muntligen till någon av följande interna chefer: (i) den lokala compliance-chefen (juridiska avdelningen eller compliance-avdelningen), (ii) den lokala personalavdelningen, (iii) koncernens compliance-avdelning eller (iv) koncernens personalavdelning.

Personalavdelningen (lokal eller koncernens) samlar vanligtvis in rapporter om överträdelser av arbetsrätten eller olämpligt beteende på arbetsplatsen (trakasserier, diskriminering, hälsa, hygien eller säkerhet etc.).

Den lokala compliance-chefen eller koncernens compliance-avdelning samlar vanligtvis in rapporter om överträdelser av lagen, etikkoden, uppförandekoden mot korruption och Rexel-koncernens compliance-rutiner etc.

När en anmälan görs muntligt kan den tas emot per telefon och, på begäran av den person som gör anmälan och efter hans/hennes eget val, under en videokonferens eller ett fysiskt möte som anordnas senast tjugo (20) arbetsdagar efter mottagandet av begäran. Muntliga anmälningar transkriberas skriftligt.

Anställda kan i alla fall rådfråga sin direkta eller indirekta linjeförman och dela med sig av eventuella farhågor, utom i de fall då linjeförman själv är den som påstås ha begått det aktuella brottet. Om det efter en sådan diskussion framgår att dessa farhågor faller inom ramen för detta förfarande, måste linjeförman uppmuntra den anställda att göra en anmälan via de kanaler som anges ovan eller genom att kontakta den lokala juridiska avdelningen, complianceavdelningen eller den lokala personalavdelningen.

3. Anmälans innehåll

Den som gör en anmälan måste redogöra för de fakta och uppgifter som är föremål för anmälan på ett precist och objektivt sätt, så att anmälan kan hanteras.

Om möjligt bör anmälaren stödja sin anmälan genom att

- ange datum och plats för de rapporterade fakta, den berörda enheten samt identiteten och befattningen för den eller de personer som är inblandade
- ge en detaljerad beskrivning av fakta med specifik och saklig information som är direkt relaterad till föremålet för varningen, oavsett dess form eller medium.

4. Anonyma rapporter

Det är att föredra att den som lämnar en anmälan identifierar sig, särskilt för att underlätta utredningen. Den som lämnar en anmälan kan dock välja att göra en anonym anmälan, enligt vad som anges i den elektroniska anmälningsplattformen, förutsatt att (i) fakta är allvarliga och (ii) faktauppgifterna är tillräckligt detaljerade.

5. Externa kanaler

Med förbehåll för att tillämpliga lokala bestämmelser följs, bör det noteras att rapportförfattaren också har möjlighet att göra en extern rapport till (i) den behöriga myndigheten, (ii) ombudsmannen, (iii) den rättsliga myndigheten eller (iv) någon relevant lokal eller internationell institution, organ eller myndighet som är behörig att ta emot sådana rapporter. Rapportörer kan lämna in externa rapporter antingen direkt till en myndighet eller efter att ha lämnat in en rapport till Rexel-koncernen.

III. Hantering av interna etiska varningar

1. Bekräftelse av mottagandet av rapporten

När rapporten tas emot på den elektroniska rapporteringsplattformen eller via traditionella kanaler bekräftar den interna chefen (den person som ansvarar för att samla in rapporter enligt definitionen ovan) mottagandet av anmälan inom sju (7) arbetsdagar efter mottagandet.

Bekräftelse av mottagandet innebär inte att anmälan accepteras.

2. Granskning av anmälans tillåtlighet

Varje mottagen anmälan genomgår en preliminär analys av den interna chefen för att säkerställa att den faller inom förfarandets tillämpningsområde och att den är tillåtlig.

Denna kontroll, som kan kräva kommunikation med anmälaren eller rapporten, fokuserar särskilt på följande punkter:

- **Anmälarens status som "visselblåsare":** i synnerhet att denne agerar i god tro och utan att söka direkt ekonomisk ersättning.
- **Anmälans art:** att den verkligen faller inom en av de kategorier av anmälningar som omfattas av förfarandet.
- **Rapportens innehåll:** att den information och de fakta som redovisas är objektiva och

tillräckligt detaljerade för att en utredning ska kunna inledas.

- **Förekomsten av skyddade hemligheter:** att rapporten inte avslöjar fakta som omfattas av nationell försvarssekretess, läkarsekretess, sekretess i rättsliga överläggningar, sekretess i rättsliga utredningar eller förhör, eller advokatsekretess.

Beslutet om tillåtlighet fattas av den interna chefen. Författaren till en rapport informeras om att rapporten inte är tillåtlig, om så är fallet, och om skälen till detta beslut.

Under alla omständigheter måste den interna chefen lämna ett första svar inom tre (3) månader. Rexel-koncernen är inte skyldig att behandla anmälan inom denna tidsram, men måste informera anmälaren om de åtgärder som planeras eller redan vidtagits för att bedöma anmälans giltighet och åtgärda den rapporterade situationen.

Anmälan behandlas med fullständig sekretess.

Beroende på arten och allvarlighetsgraden av de rapporterade fakta kan anmälan hanteras av Rexel-koncernens etikkommitté. Rexel-koncernens etikkommitté är en ad hoc-kommitté som inrättats inom Rexel Développement och vars uppgift är att hantera de allvarligaste anmälningarna som rapporterats av Rexel-anställda eller tredje parter som Rexel har en relation med.

Rxel-koncernens etikkommitté består av tre permanenta medlemmar:

- generalsekreteraren,
- koncernens personalchef och
- direktören för etik och efterlevnad

3. Genomförande av den interna utredningen

Mål och hantering av den interna utredningen

Den tid som krävs för att behandla en anmälan varierar och beror på komplexiteten i de rapporterade fakta och typen av information som lämnats.

Syftet med den interna utredningen är att verifiera riktigheten och väsentligheten i de rapporterade fakta. Anmälan utreds med hjälp av metoder (intervjuer, datasökningar etc.) som kan variera beroende på sammanhanget och ärendets natur.

Denna utredning kan genomföras av:

- (xxxi) den lokala personalavdelningen
- (xxxii) den lokala compliance- eller juridiska avdelningen
- (xxxiii) koncernens complianceavdelning;
- (xxxiv) koncernens personalavdelning
- (xxxv) Rexel-koncernens etikkommitté, beroende på arten och allvarlighetsgraden av de rapporterade fakta

(nedan kallad **"utredningsansvarig"**).

I alla fall kommer utredningschefen att leda den interna utredningen av anmälan. Information om förekomsten och innehållet i anmälan kommer endast att lämnas ut till de personer som ansvarar för utredningen i den utsträckning som är absolut nödvändig.

När en anmälan görs garanterar Rexel-koncernen utredningsprocessens oberoende. Innan en intern utredning inleds kontrolleras att ingen av de personer som deltar i utredningen av anmälan är direkt

eller indirekt berörd av de rapporterade fakta eller har någon intressekonflikt med de inblandade personerna. Om en risk för intressekonflikt identifieras, avlägsnas den berörda medarbetaren omedelbart från processen och ersätts. Denna princip om oberoende är en integrerad del av Rexels etiska och efterlevnadssystem och syftar till att säkerställa en rigorös, opartisk och trovärdig hantering av alla inkomna anmälningar.

Beslagtagande av e-postmeddelanden, dokument eller datormedia

Den interna utredningen kan kräva granskning och behandling av e-postmeddelanden eller datormedia som tillhör en eller flera anställda. Innan e-postkonton eller datormedia beslagtas eller spärras måste utredningschefen begära tillstånd, enligt lokala rutiner (t.ex. från koncernens etikkommitté, lokala chefsjuristen eller lokala dataskyddsombudet), för att beslagta och behålla dessa e-postmeddelanden för utredningsändamål.

Gästexpert

När situationen så kräver kan utredningschefen besluta att bjuda in en eller flera personer att delta i hanteringen av en specifik anmälan, särskilt om det krävs expertis inom redovisning, ekonomi, teknik eller IT.

Utredningschefen kan således besluta att söka hjälp i sitt uppdrag från en expertanställd hos Rexel, t.ex. internrevisionsavdelningen, ekonomiavdelningen, inköpsavdelningen, ett lands- eller zonledningsgrupp eller någon annan person inom Rexel-koncernen som utredningschefen anser vara kompetent och nödvändig, eller från en behörig extern tjänsteleverantör.

Expertens uppdrag upphör automatiskt när alla verifierings- eller behandlingsåtgärder som rör den varning för vilken utredningschefen begärt hjälp har slutförts, eller på enkel begäran av utredningschefen.

Den inbjudna experten är underkastad samma sekretessplikt som den interna chefen och utredningschefen.

4. Beslutsfattande och avslutande av utredningen

Om fakta inte kan bevisas avslutas anmälan och anmälaren informeras.

Om fakta bevisas, kommer utredningschefen, på grundval av utredningens resultat, att avgöra om brott mot lagen, etikkoden eller antikorrupsionskoden har begåtts och, om så är fallet, rekommendera korrigerande åtgärder och/eller lämpliga sanktioner.

Den person som lämnat in rapporten informeras skriftligen om att utredningen avslutats.

Den berörda personen informeras också om att utredningen avslutats. Om överträdelsen efter utredningen befinns vara allvarlig och bevisad kan den berörda personen bli föremål för disciplinära åtgärder, upp till och inklusive avskedande, beroende på arten och allvarlighetsgraden av de påstådda fakta.

IV. Skydd och garantier

1. Allmänna principer

Alla utredningar kommer att genomföras på ett rättvist sätt och i full överensstämmelse med tillämpliga lokala lagar och förordningar. I alla fall kommer Rexel-koncernen att se till att principen om oskuldspresumtion respekteras för de berörda personerna.

Visselblåsarsystemet kan endast fungera på grundval av information som lämnas i god tro. Varje anmälan som görs i ond tro, dvs. med den enda avsikten att orsaka skada, kan bli föremål för disciplinära åtgärder, inklusive uppsägning.

2. Information

Den som slår larm kommer att informeras inom sju (7) arbetsdagar efter mottagandet av rapporten.

Inom en rimlig tidsperiod som inte överstiger tre (3) månader från mottagandet av anmälan informeras anmälaren skriftligen om de åtgärder som planeras eller vidtagits för att bedöma riktigheten i anklagelserna och, i förekommande fall, för att åtgärda det som anmälan avser, samt om skälen till dessa åtgärder. Om anklagelserna är felaktiga eller ogrundade, eller om anmälan har blivit irrelevant, ska anmälaren skriftligen informeras om att ärendet har avslutats.

Alla personer som är inblandade i en godtagbar anmälan ska informeras om arten av de anklagelser som rör dem. Om det är nödvändigt att vidta försiktighetsåtgärder för att förhindra att bevis som rör anmälan förstörs, ska den person som berörs av anmälan dock först informeras efter det att dessa åtgärder har vidtagits, i enlighet med tillämplig lagstiftning.

Den person som är föremål för en anmälan får under inga omständigheter, på grundval av sin rätt till tillgång, få information från Rexel-koncernen om identiteten på den person som gjort anmälan.

Det anges att nivån på den information som lämnas kan variera beroende på tillämplig lokal lagstiftning.

3. Skydd i brottmål, civilrättsliga mål och sociala frågor

Visselblåsare påminns om att, med förbehåll för lokalt tillämpliga bestämmelser:

- De är inte civilrättsligt ansvariga för skador som orsakats till följd av deras anmälan eller avslöjande, förutsatt att anmälan gjorts i enlighet med tillämpliga bestämmelser och att anmälaren hade rimliga skäl att tro, vid tidpunkten för anmälan, att anmälan eller offentliggörandet av all denna information var nödvändig för att skydda de intressen som stod på spel.
- De är inte straffrättsligt ansvariga för att ha erhållit eller fått tillgång till information som är offentligt rapporterad eller offentliggjord, förutsatt att sådan erhållande eller tillgång inte utgör ett separat brott enligt lokalt tillämpliga bestämmelser. Om sådan erhållande eller tillgång utgör ett separat brott, ska de lokalt tillämpliga reglerna om straffrättsligt ansvar tillämpas.
- De får inte straffas, avskedas, diskrimineras (särskilt när det gäller ersättning, utbildning, befordran) eller utsättas för repressalier eller hot eller försök att tillämpa sådana åtgärder för

att ha rapporterat eller offentliggjort information i enlighet med bestämmelserna, förutsatt att rapporten gjordes i god tro.

Under samma förutsättningar får personer som har underlättat en visselblåsares rapportering eller som är associerade med denne inte utsättas för repressalier, hot eller försök att tillgripa sådana åtgärder.

Rexel-koncernen tolererar inte någon form av repressalier, hot eller försök att tillgripa sådana åtgärder mot visselblåsare och deras anhöriga, såsom trakasserier.

4. Begränsad lagringstid för data

Anmälningar får endast lagras så länge som det är absolut nödvändigt och proportionerligt för behandlingen av dem och för att skydda deras upphovsmän, de personer som de avser och eventuella tredje parter som de nämner, med beaktande av den tid som krävs för eventuella ytterligare utredningar. Uppgifter som rör anmälningar får dock lagras längre än denna period, förutsatt att de berörda personerna varken identifieras eller kan identifieras.

Det finns flera system för arkivering av etiska varningar:

- **Ogodtagbara varningar** (varningar som inte omfattas av tillämpningsområdet, inte är allvarliga, är ogrundade, görs i ond tro osv.): dessa raderas så snart som möjligt eller arkiveras och anonymiseras.
- **Godtagbara anmälningar:**
 - Om rapporten inte följs av disciplinära eller rättsliga åtgärder, säkerställer Rexel-koncernen att alla delar av rapporten som kan identifiera rapportens författare, liksom de berörda personerna, förstörs inom högst två (2) månader från slutet av verifierings- eller utredningsåtgärderna.
 - I fall där utredningen leder till rättsliga åtgärder eller disciplinära sanktioner bevaras uppgifterna i akten under den tid som krävs, tills preskriptionstiden löper ut (sex (6) år) eller alla möjligheter till överklagande har uttömts. När den föreskrivna tiden har löpt ut förstörs eller arkiveras och anonymiseras dessa uppgifter.

5. Sekretess och säkerhets

Rexel-koncernen vidtar alla nödvändiga försiktighetsåtgärder för att bevara konfidentialiteten och säkerheten för uppgifterna under insamling, behandling, kommunikation eller lagring.

Med förbehåll för lokalt tillämpliga bestämmelser säkerställer förfarandena för insamling och behandling av rapporter strikt sekretess avseende identiteten på rapportens författare, de personer som rapporten avser och den information som samlas in av de personer som ansvarar för insamlingen och behandlingen av rapporten.

I detta avseende gäller följande:

- Den information som kommuniceras är begränsad till de personer som har ett legitimt behov av att känna till den för att kunna behandla varningen.
- Alla personer som är involverade i hanteringen av varningar är utbildade och omfattas av sekretessplikt. De förbinder sig särskilt att inte använda uppgifterna för olämpliga ändamål och att följa den begränsade lagringstiden för uppgifter i enlighet med tillämplig lagstiftning.

- Den webbaserade rapporteringsplattformen är säker och varningar som lämnas in till den kan endast ses av behöriga personer. Detta system gör det också möjligt för anställda som vill vara anonyma att använda denna kanal.
- Whistleblowners identitet kan avslöjas för rättsliga myndigheter om lagen så kräver.
- Information som kan identifiera den person som är inblandad i en anmälan får inte lämnas ut, utom till rättsliga myndigheter, när larmets giltighet har fastställts.
- Inom Rexel-koncernens enheter är de avdelningar som vanligtvis hanterar rapporter medvetna om att identiteten på rapportören och de personer som är inblandade är konfidentiell.

6. Skydd av personuppgifter

Som en del av visselblåarsystemet kan Rexel Group samla in och behandla personuppgifter, särskilt uppgifter om anmälaren och den eller de personer som är inblandade. En detaljerad informationsnot i **bilaga 4** beskriver villkoren för insamling, behandling, lagring och arkivering av uppgifter.

V. Rapportering

Koncernens complianceavdelning rapporterar en gång om året om antalet varningar, deras typ och de åtgärder som vidtagits efter mottagandet, och begränsar sig till uppgifter som är absolut nödvändiga och proportionerliga i förhållande till skälet för anmälan.

VI. Uppdatering av förfarandet

Rexel-koncernen förbehåller sig rätten att när som helst ändra, komplettera eller uppdatera denna procedur för att anpassa den till förändringar i lagstiftning, regler, rättspraxis eller koncernens interna behov. Alla uppdateringar kommer att göras i enlighet med tillämpliga lokala lagar och regler.

Berörda anställda, leverantörer och andra intressenter kommer att informeras om ändringarna på lämpligt sätt (intern kommunikation, e-post, publicering på intranätet, direkt information till leverantörer etc.), i enlighet med lokala lagkrav.

Den aktuella och giltiga versionen av denna procedur kommer att publiceras och göras tillgänglig på Rexel-koncernens webbplatser, på koncernens intranät och på den elektroniska rapporteringsplattformen.

Kontakt

Företag: Rexel Développement

Adress: 13 boulevard Fort de Vaux 75017 Paris (Frankrike) – *Till koncernens complianceavdelning.*

E-postadress: compliance@rexel.com

Anmäl en situation

Om du misstänker eller har kännedom om en överträdelse av lagen, etikkoden eller uppförandekoden mot korruption, rapportera det!

02.



När ska man slå larm?

När du får kännedom om eller misstänker ett **brott mot lagen eller våra etiska principer**.

Detta kan omfatta:

- korruption;
- brott mot mänskliga rättigheter;
 - trakasserier
 - eller diskriminering
- bedrägeri etc.

04.



Är det konfidentiellt?

Ja, och du kan också skicka en **anonym** rapport

06.



Är jag skyddad?

Du måste slå larm i god tro och utan någon direkt ekonomisk ersättning. I detta fall är du skyddad.

01.



Vem kan slå larm?

Alla anställda inom koncernen och tredje part kan använda etikkontaktlinjen.

03.



Hur gör man en anmälan?

1. Använd **Rexel Ethics Line online** (webblänk nedan)
 - tillgänglig dygnet runt
 - tillgänglig på alla av koncernens huvudspråk.
2. Använd det lokalt inrättade **visselblåsarsystemet** som finns på plats.
3. Kontakta **juridik- eller complianceavdelningen** eller **personalavdelningen** (koncern eller lokal)

05.



Vem hanterar denna varning?

För koncernen: etikkommittén.
För det lokala systemet: se lokala rutiner.

Ytterligare

Besök :
<https://www.rexel.com/en/ethical-alert/>

Bilaga 2: Förteckning över länder med lokala visselblåsningsförfaranden

Denna procedur kompletteras i vissa länder med lokala procedurer, som fastställer tillämpliga rättsliga krav och, i förekommande fall, de kanaler som finns tillgängliga lokalt.

Information om lokala kanaler finns nedan. Vänligen konsultera den lokala proceduren för de senaste uppgifterna.

- Australien:

o Rexel STOPline-tjänst för anmälningar (drivs av en oberoende extern tjänsteleverantör):

Telefon: 1300 30 45 50

Fax: Rexel Holdings Australia (C/- the STOPline) 03 9882 4480

E-post: rexel@stopline.com.au

Online: <https://rexel.stoplinereport.com/>

Post: Rexel Holdings Australia

C/- the STOPline

Locked Bag 8

HAWTHORN VIC 3122

- Kanada: Du kan kontakta etikkommittén.

- Tyskland:

o E-post: whistleblowing@rexel.de

o Post:

Rexel Germany GmbH & Co.

KG - z. Hd. Frau Nicole Steuer | General Counsel

Ridlerstr.5780339 München

- Irland

o Du kan kontakta HR-avdelningen, visselblåsningsansvarig, verkställande direktör eller vår externa visselblåsningsshotline som drivs av Safecall.

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- Italien:

o <https://report.whistleb.com/rexel>

- Nederländerna: Du kan kontakta etikansvarig.

- Sverige:

o <https://whistleblow.vismadraftit.se/rexel-sverige-ab>

o Telefon: 08-556 214 14.

- Storbritannien

o Du kan kontakta HR-avdelningen, visselblåsningsansvarig, verkställande direktör eller vår externa visselblåsningsshotline som drivs av Safecall.

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- USA

o E-post för efterlevnad: ethics@rexelusa.com

o Hjälpelinje för regelefterlevnad: 1-800-714-8774

Bilaga 3: Exempel på beteenden eller förseelser som omfattas av visseblåsningsförfarandet

Kategorier	Tillämpningsområde
Korruption	Inom ramen för tillämpliga lokala lagar och förordningar samt koncernens antikorrupcionspolicyer avses med korruption utbyte, direkt eller via tredje part, av förmåner (pengar, gåvor, inbjudningar, tjänster, kontakter etc.) i utbyte mot att utföra eller avstå från att utföra en handling som är relaterad till en funktion eller ett uppdrag. Det kan ta formen av att en person föreslår eller erbjuder en förmån för att erhålla en tjänst (aktiv korruption) eller att en person begär eller accepterar en förmån i utbyte mot en tjänst (passiv korruption). Korruption kan involvera både offentliga och privata aktörer, snedvrider konkurrensen, undergräver beslutsprocessens transparens och utsätter de inblandade individerna och organisationerna för sanktioner och åtal.
Trakasserier	Trakasserier avser upprepat beteende eller en enskild allvarlig handling som undergräver en persons värdighet, säkerhet eller arbetsförhållanden. Det yttrar sig i ord, gester, attityder eller handlingar som syftar till att skrämja, förnedra, isolera, hota eller försämma situationen för en anställd eller tredje part i samband med yrkesutövningen. Trakasserier kan vara av psykologisk karaktär, till exempel nedsättande kommentarer, avsiktlig isolering, överbelastning eller berövande av arbetsresurser, utfrysning, spridning av rykten eller systematisk nedvärdering. De kan också vara av sexuell karaktär. Sexuella trakasserier kännetecknas av oönskat sexuellt beteende eller kommentarer som upprepas eller utgör en enskild allvarlig incident, som undergräver en persons värdighet eller skapar en hotfull, fientlig, förnedrande eller kränkande arbetsmiljö. Detta inkluderar bland annat ihållande närmanden, kommentarer om kroppen, begäran om sexuella tjänster, fysiska gester eller kontakt utan samtycke, eller spridning av sexuella bilder utan samtycke. Trakasserier, vare sig de är moraliska eller sexuella, är oacceptabla och förövarna är ansvariga enligt tillämpliga lokala lagar.

Diskriminering	Diskriminering på arbetsplatsen innebär att behandla någon ofördelaktigt på grund av kriterier som är förbjudna enligt lag, såsom ursprung, kön, familjestatus etc., eller andra egenskaper som skyddas av lokal lagstiftning. Diskriminering kan till exempel resultera i ojämlik behandling när det gäller tillgång till anställning, arbetsvillkor, utbildning, rörlighet eller andra situationer som rör yrkesverksamhet. Det kan ta sig uttryck i beslut om rekrytering, utvärdering, befordran, tilldelning av arbetsuppgifter eller uppsägning som missgynnar en person utan objektiv motivering baserad på kraven för tjänsten. På arbetsplatsen kan diskriminering ta två former: - Direkt diskriminering. I detta fall fattar förövaren medvetet ett beslut baserat på diskriminerande kriterier som är förbjudna enligt lag. Indirekt diskriminering. I detta fall fattar gärningsmannen ett beslut som verkar neutralt men som i slutändan missgynnar vissa personer framför andra. Till exempel tillåter interna regler endast män att stanna kvar i företaget efter 50 års ålder. Detta utgör därför indirekt diskriminering på grund av kön och ålder.
Hälsa/säkerhet	Alla allvarliga överträdelser eller risker för hälsa och säkerhet på arbetsplatsen. Säkerhet på arbetsplatsen avser alla åtgärder och rutiner som syftar till att skydda människors fysiska och psykiska integritet på arbetsplatsen genom att minska risken för olyckor, skador och yrkessjukdomar. Detta innefattar att identifiera och bedöma risker, införa tekniska och organisatoriska skyddsåtgärder, utbilda och informera anställda samt införa förebyggande åtgärder, interventionsåtgärder och åtgärder för hantering av nödsituationer. Efterlevnad av dessa skyldigheter bidrar till en säker arbetsmiljö som uppfyller lokala krav.
Mänskliga rättigheter (utom diskriminering och trakasserier)	Allvarliga kränkningar eller risker för de mänskliga rättigheterna och grundläggande friheter som erkänns på nationell och internationell nivå, samt alla överträdelser av tillämpliga lokala krav på detta område. Detta inkluderar, men är inte begränsat till, situationer som rör principer som respekt för förenings- och yttrandefrihet, tillgång till anständiga och säkra arbetsförhållanden och möjligheten för berörda personer att få tillgång till rättsliga prövningsmöjligheter.
Intressekonflikter	En intressekonflikt är en situation där en persons personliga intressen, vare sig de är ekonomiska, familjära, vänskapliga, politiska eller relaterade till andra fördelar, sannolikt kommer att påverka eller verkar påverka deras omdöme eller beslut i samband med deras arbetsuppgifter inom Rexel-koncernen. Detta är inte nödvändigtvis ett fel eller en olaglig handling, utan en risk för partiskhet som äventyrar den förväntade opartiskheten. Denna risk för partiskhet kan vara tillräcklig för att undergräva de berördas förtroende, förändra kvaliteten

	på besluten och skada organisationens rykte. En intressekonflikt kan vara faktisk (redan föreliggande), potentiell (sannolikt att uppstå) eller uppenbar (uppfattad av tredje part). Visselblåarsystemet är inte avsett att ersätta det förfarande för rapportering av intressekonflikter som definierats av Rexel-koncernen.
Konkurrensbegränsande metoder	Konkurrensbegränsande metoder avser företagsbeteende som hindrar fri konkurrens och skadar andra marknadsaktörer (kunder, leverantörer, konkurrenter). De omfattar formella eller informella avtal mellan konkurrenter om att samordna priser, kommersiella villkor, fördelning av marknader, territorier eller produkter, eller att begränsa utbudet eller bojkotta vissa partner. De omfattar också situationer där en dominerande ställning missbrukas (t.ex. genom att driva bort en konkurrent, införa rovpriser eller orättfärdiga kopplade försäljningar), påverka återförsäljarnas återförsäljningspriser och utbyta icke-offentlig strategisk information som kan påverka marknadsbeteendet (t.ex. planer, marknadsföringsdata eller kapacitet). Dessa metoder är förbjudna enligt konkurrensreglerna och kan leda till betydanse påföljder.
Miljö	Alla situationer där tillämpliga miljökrav inte uppfylls eller där en betydande risk eller skada för miljön identifieras, vare sig det är inom företaget eller bland dess partners i värdekedjan. Detta omfattar förebyggande av föroreningar, ansvarsfull användning av resurser och säker hantering av ämnen och avfall, i enlighet med lagstadgade skyldigheter och interna standarder.
Bedrägeri	Alla situationer som innefattar döljande, bedrägeri eller manipulation i syfte att erhålla en otillbörlig fördel eller undvika skyldigheter, vare sig dessa är skattemässiga, finansiella eller redovisningsmässiga. Detta inkluderar till exempel förfalskning av dokument eller register, felaktig redovisning av finansiell information, döljande av inkomster eller tillgångar, eller alla former av planer som syftar till att kringgå gällande regler, antingen inom företaget eller i dess värdekedja.
Insiderhandel	Insiderhandel är köp, försäljning eller rekommendation av finansiella instrument med hjälp av eller på grundval av icke-offentlig privilegierad information om en emittent eller dess värdepapper. Det omfattar även olaglig utlämning av sådan information till tredje part. Sådant beteende ger en orättvis fördel på marknaden och är strängt förbjudet och straffbart enligt lag.
	Ett fiktivt jobb är en situation där en person får betalt för en befattning eller uppgifter som inte faktiskt utförs eller som inte existerar, i syfte att uppnå en orättvis fördel. Detta kan

Fiktiva jobb	innebära total frånvaro av faktiskt arbete, fiktiva arbetsuppgifter eller nominell tilldelning till en avdelning utan någon verklig insats, inom företaget eller via tredje part.
Skydd av personuppgifter/IT-säkerhet	Alla situationer där personuppgifter eller IT-system inte skyddas i enlighet med lagar och interna regler, vilket utsätter individer eller företaget för risk för obehörig åtkomst, användning, avslöjande, modifiering eller förstörelse. Detta omfattar laglig och minimerad insamling och behandling av data, systemsäkerhet (åtkomstkontroller, kryptering, säkerhetskopiering), hantering av incidenter och överträdelser samt sekretess och integritet för information under hela dess livscykel, inklusive hos tjänsteleverantörer. Personuppgifter är all information som direkt eller indirekt identifierar en fysisk person (t.ex. namn, kontaktuppgifter, identifierare, foto, platsuppgifter eller andra element som rör deras identitet eller privatliv).

INTEGRITETSPOLICY

—

VISSELBLÅSARSYSTEM

Version 12/2025

Rexel-koncernen har inrättat ett professionellt visseblåarsystem som gör det möjligt för dess anställda och tredje parter som Rexel-koncernen har en relation med att rapportera olagliga handlingar eller tjänstefel. Systemets omfattning beskrivs i visseblåsningsförfarandet, som finns tillgängligt på webbplatsen rexel.com.



Inom ramen för detta system kan ett Rexel-företag samla in och behandla uppgifter om dig. Uppgifters konfidentialitet är grunden för vårt förtroendeförhållande. Därför tar vi skyddet av dina personuppgifter på stort allvar i vår affärsverksamhet.

Denna policy beskriver Rexel-koncernens åtaganden när det gäller skydd av personuppgifter. I följande meddelande kan du också läsa om dina rättigheter och villkoren för insamling, behandling, lagring och arkivering av dina personuppgifter.

Vem är vi?

REXEL DEVELOPPEMENT SAS, ett förenklat aktiebolag enligt fransk lag, med säte på 13, Boulevard du Fort de Vaux, Paris, registrerat i Paris handels- och företagsregister under nummer 480 172 840, är personuppgiftsansvarig.

Den enhet inom koncernen som har ett anställningsavtal med eller samarbetar med rapportförfattaren är också personuppgiftsansvarig.

De bestämmer syftet med och metoderna för behandlingen av dina uppgifter.

De benämns i denna policy som "Rexel", "vi" eller "personuppgiftsansvariga".

EY Polen fungerar som personuppgiftsbiträde för den behandling som utförs på den onlinebaserade varningsplattformen.

Hur behandlar vi dina uppgifter inom ramen för varningssystemet?

I tabellen nedan anges:

- (i) varför vi behandlar dina personuppgifter,
- (ii) vilka typer av uppgifter vi behandlar, och
- (iii) den rättsliga grunden för behandlingen av dina uppgifter.

Syfte 1	Typ av uppgifter
Samla in och behandla varningar om handlingar som bryter mot lagen eller den antikorrupsionskod som omfattas av visselblåsarsystemet (se visselblåsningsförfarandet). <u>Deländamål:</u> - Centraliserad hantering av professionella rapporter (mottagande och hantering av varningar, inrättande av en säker kanal, lagring och bevarande av information, säkerställande av säkerhet) - Behandling av professionella rapporter (genomförande av interna utredningar, bedömning av relevanta fakta) - Beslutsfattande och genomförande av lämpliga åtgärder efter avslutad rapport (meddelande och genomförande av åtgärder) - Statistisk övervakning och förbättring av visselblåsarsystemet - Utövande eller försvar av rättigheter i rättsliga förfaranden	Som en del av systemet kan följande kategorier av uppgifter behandlas: - Identitetsuppgifter (för- och efternamn, kontaktuppgifter), yrkesuppgifter (befattning, arbetsgivare, arbetsplats) för den person som gör anmälan (om inte anmälan är anonym) och all annan information som personen frivilligt lämnar - Identitetsuppgifter (för- och efternamn, kontaktuppgifter), yrkesuppgifter (befattning, arbetsgivare, arbetsplats) för de personer som är inblandade - Identitetsuppgifter (för- och efternamn, e-postadress), yrkesuppgifter (befattning, arbetsgivare, arbetsplats) för personer som är inblandade eller konsulterade i insamlingen eller behandlingen av anmälan, samt förmedlare och personer som har kontakt med visselblåsaren - Känsliga uppgifter (ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, fackföreningstillhörighet, hälsouppgifter, sexliv eller sexuell läggning) när det är absolut nödvändigt för att utöva eller försvara lagliga rättigheter (artikel 9.2.f i GDPR) eller av skäl av betydande allmänintresse (artikel 9.2.g i GDPR) - Uppgifter om fällande domar i brottmål och brott eller därmed sammanhängande säkerhetsåtgärder när det är absolut nödvändigt och i enlighet med artikel 10 i GDPR. - Information som samlas in i samband med faktagranskning. - Rapporter om verifieringsåtgärder. - Uppgifter om uppföljningen av rapporten.
Rättslig grund för behandlingen av dina uppgifter Rättslig skyldighet att införa ett visselblåsarsystem: särskilt artiklarna 8.1.B och 17 II i Sapin II-lagen och artikel L. 225-102-4 i handelslagen, samt alla motsvarande lagar om skydd av visselblåsare, bekämpning av korruption eller vaksamhetsplikt.	

Syfte 2	Typ av uppgifter
Insamling och behandling av varningar om handlingar som strider mot etikoden <u>Deländamål:</u> - Centraliserad hantering av professionella rapporter (mottagande och hantering av varningar, inrättande av en säker kanal, lagring och bevarande av information, säkerställande av säkerhet) - Behandling av professionella rapporter (genomförande av interna utredningar, bedömning av relevanta fakta) - Beslutsfattande och genomförande av lämpliga åtgärder efter avslutad rapport (meddelande och genomförande av åtgärder) - Statistisk övervakning och förbättring av visselblåsarsystemet - Utövande eller försvar av rättigheter i rättsliga förfaranden	Som en del av systemet kan följande kategorier av uppgifter behandlas: - Identitetsuppgifter (för- och efternamn, kontaktuppgifter), yrkesuppgifter (befattning, arbetsgivare, arbetsplats) för den person som gör anmälan (om inte anmälan är anonym) och annan information som personen frivilligt lämnar - Identitetsuppgifter (för- och efternamn, kontaktuppgifter), yrkesuppgifter (befattning, arbetsgivare, arbetsplats) för de personer som är inblandade - Identitetsuppgifter (för- och efternamn, e-postadress), yrkesuppgifter (befattning, arbetsgivare, arbetsplats) för personer som är inblandade eller konsulterade i insamlingen eller behandlingen av anmälan, samt förmedlare och personer som har kontakt med visselblåsaren - Känsliga uppgifter (ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, fackföreningstillhörighet, hälsouppgifter, sexliv eller sexuell läggning) när det är absolut nödvändigt för att utöva eller försvara lagliga rättigheter (artikel 9.2.f i GDPR) eller av skäl som rör ett betydande allmänintresse (artikel 9.2.g i GDPR) - Uppgifter om fällande domar i brottmål och brott eller därmed sammanhängande säkerhetsåtgärder när det är absolut nödvändigt och i enlighet med artikel 10 i GDPR. - Information som samlas in i samband med faktagranskning. - Rapporter om verifieringsåtgärder. - Uppgifter om uppföljningen av rapporten.
Rättslig grund för behandlingen av dina uppgifter	
Rättslig grund: Berättigat intresse av att behandla etiska varningar som inte omfattas av en rättslig skyldighet.	

Vem är mottagare av dina uppgifter?



De personuppgifter vi samlar in, liksom alla uppgifter som samlas in senare, är avsedda för oss i vår egenskap av personuppgiftsansvarig.



Vi säkerställer att endast behöriga personer har tillgång till dessa uppgifter.

Internt:

- De som ansvarar för att samla in och behandla varningar, nämligen:
 - Medlemmar i Rexel Groups etikkommitté
 - Auktoriserade medlemmar av juridik- eller complianceavdelningen på koncern- och lokal nivå
 - Auktoriserade medlemmar av personalavdelningen på koncern- och lokal nivå
- Auktoriserade medlemmar av revisions- och internkontrollavdelningen på koncern- och lokal nivå för att säkerställa effektiviteten i internkontroller och styrning
- När situationen motiverar det kan annan intern personal få tillgång till uppgifterna, särskilt när det krävs expertis inom redovisning, ekonomi, juridik, teknik eller IT.

Externt:

- Våra rådgivare
- Våra mäklare och försäkringsbolag
- Våra revisorer
- De behöriga myndigheterna (rättsliga, administrativa och tillsynsmyndigheter) i enlighet med tillämpliga bestämmelser
- Våra tjänsteleverantörer, och mer specifikt EY Poland, som tillhandahåller vår onlineplattform för rapportering.

Dessa mottagare är belägna i Europeiska unionen.

Hur länge sparar vi dina uppgifter?

Situationer	Lagringstid
Otillåtna varningar (som inte omfattas av tillämpningsområdet, inte är allvarliga till sin natur, saknar information, gjorts i ond tro etc.)	Radering eller arkivering och anonymisering så snart som möjligt
Godtagbar anmälan men avvisad (följs inte av disciplinära eller rättsliga åtgärder)	Radering eller anonymisering och arkivering inom två (2) månader
Varningar som leder till disciplinära eller rättsliga åtgärder	Lagring av uppgifter till dess att förfarandet och överklaganden är avslutade. Efter denna period, radering eller anonymisering och arkivering.

Vilka är dina rättigheter?



I enlighet med lagstiftningen om skydd av personuppgifter har du följande rättigheter:

- rätt till tillgång: du kan få tillgång till den information vi har om dig och få en kopia av den;
- rätt till rättelse: du kan få felaktiga uppgifter om dig ändrade, kompletterade, uppdaterade eller raderade;
- Rätt att invända: Du kan invända mot att vi behandlar dina uppgifter, såvida det inte finns legitima och tvingande skäl för oss att behandla dem.
- Rätt till radering: Du kan begära att vi raderar uppgifter om dig inom ramen för de villkor som anges i artikel 17 i GDPR.
- Rätt till dataportabilitet: du kan hämta dina uppgifter för att överföra dem till en annan organisation eller för personligt bruk.
- rätt till begränsning av behandling;
- rätt att formulera specifika och allmänna riktlinjer för lagring, radering och kommunikation av dina uppgifter efter din död.

Varje person som är föremål för en rapport kommer att informeras så snart som möjligt (senast inom en månad) efter registreringen, vare sig den är datoriserad eller inte, av uppgifter som rör dem för att de ska kunna utöva sina rättigheter. Om sådan information dock kan äventyra målen med behandlingen och i synnerhet utredningens genomförande (till exempel om det finns risk för att bevis förstörs), kan denna information skjutas upp och kommer endast att lämnas ut när risken har eliminerats.

Den person som är föremål för en anmälan får under inga omständigheter, på grundval av sin rätt till tillgång, erhålla information från den registeransvarige om identiteten på den som gjort anmälan eller någon annan person som är inblandad i utredningen.

Om du inte får något svar, om du anser att svaret är otillfredsställande eller om du anser att behandlingen av dina uppgifter inte överensstämmer med lagar och förordningar, kan du kontakta den behöriga tillsynsmyndigheten.

Hur utövar du dina rättigheter?



Genom skriftlig begäran till vår dataskyddsombud:

Länder	Enheter	Adress
Österrike	COMTECH IT-SOLUTIONS GMBH	datenschutz@rexel.at
	Rexel Austria GmbH	datenschutz@rexel.at
Belgien	Rexel Belgique SA	gdpr@rexel.be
Frankrike	Cordia	donnees.personnelles@francofa-eurodis.fr
	Rexel Développement SAS / Rexel Group	data.protection@rexel.com
	Rexel France SAS	donnees.personnelles@rexel.fr
	Bizline	data.protection@rexel.com
	Gigamedia	data.protection@rexel.com
	Sofinther SAS	donnees.personnelles@sofinther.fr
	Espace Elec SAS	donnees.personnelles@espace-elec.fr
	Esabora Digital Services SAS	dataprotection-rda@rexel.fr
	Francofa Eurodis	donnees.personnelles@francofa-eurodis.fr
	Freshmile Services SAS	donnees.personnelles@rexel.fr
	ITESA	donnees.personnelles@rexel.fr
Tyskland	REXEL GERMANY BETEILIGUNGS GMBH	Datenschutzbeauftragter@rexel.de
	Rexel Germany GmbH & Co KG	Datenschutzbeauftragter@rexel.de
	REXEL GERMANY VERWALTUNGS GMBH	Datenschutzbeauftragter@rexel.de
Italien	Rexel Italia S.p.A	dataprotection@rexel.it
	Tecno-Bi S.r.l.	dataprotection@rexel.it
	Comm-Tech S.r.l.	dataprotection@rexel.it
Irland	M. Kelliher 1998	data.protection@rexel.ie
	Rexel Industrial Solutions	data.protection@rexel.ie
Luxemburg	Rexel Luxembourg SA	gdpr@rexel.be
Nederländerna	Rexel Nederland B.V	AVG@rexel.nl
	Wasco Group B.V.	AVG@rexel.nl
	Wasco Holding B.V.	AVG@rexel.nl
	Wasco Groothandels Greop B.V.	AVG@rexel.nl
	Wasco Distributlecentrum B.V.	AVG@rexel.nl
Slovenien	Rexel d.o.o.	dpc@rexel.si
Sverige	Rexel Sverige AB	dataskydd@rexel.se
Schweiz	ELEKTRO-MATERIAL AG	datenschutz@e-m.ch
	Rexel 3S	data.protection@rexel.com
Storbritannien	Rexel (UK) Ltd.	data.protection@rexel.co.uk



举报程序 2025年12月_V1

摘要

举报程序 2025年12月_V1	1
举报程序 2025年12月_V1	1
I. 引言	3
1. 内部举报系统的目的	3
2. 法律框架说明	3
3. 适用范围	4
II. 举报信息收集	4
1. 举报信息受理条件	4
谁可以举报?	4
举报人如何获得相关法律保护?	5
可举报哪些事实?	5
2. 如何提交举报	6
在线举报平台	6
其他举报渠道	6
3. 举报内容	7
4. 匿名举报	7
5. 外部渠道	7
1. 举报收悉确认	7
2. 举报可受理性审查	8
3. 开展内部调查	8
内部调查的目标与管理	8
扣押电子邮件、文件或计算机介质	9
客座专家	9
4. 调查决策与结案	9
IV. 提供的保护与保障	10
1. 一般原则	10
2. 通知	10
3. 刑事、民事及社会事务保护	10
4. 数据保留期限	11
5. 保密与安全	11

6. <u>个人数据保护</u>	12
V. <u>报告机制</u>	12
<u>集团合规部每年就举报数量、类型及后续处理措施提交报告，所披露数据严格限于与举报事由相关的必要信息。</u>	12
VI. <u>程序更新</u>	12
<u>附录1：摘要</u>	14
<u>举情况举报</u>	14
.....	14
<u>附录2：设有本地举报程序的国家列表</u>	15
<u>附录3：举报程序涵盖的行为或不当行为示例</u>	16
<u>附录4：隐私政策</u>	19

1. 引言

1. 内部举报系统的目的

作为蓝格赛集团道德与合规政策的一部分（特别详见其《道德指南》、《可持续供应商章程》及《反腐败行为准则》），蓝格赛集团建立了内部举报系统。

蓝格赛集团的内部举报系统允许任何员工以及与蓝格赛集团存在合作关系的第三方举报违反法律、蓝格赛集团《道德指南》或《反腐败行为准则》的行为。

本程序旨在阐述蓝格赛集团内部收集与处理道德举报信息的流程。

相关程序概要详见附录1。

2. 法律框架说明

鉴于蓝格赛集团控股公司注册于法国，本程序依据下列法国法律制定：

- 2016年12月9日颁布的《萨宾第二法案》（Sapin II Law）（涉及透明度、反腐败及经济现代化）；
- 2017年3月27日颁布的《尽职调查义务法》（关于母公司与签约合作公司的尽职调查义务）；
- 2022年3月21日颁布的《瓦瑟曼法》（旨在加强举报人保护）及2022年10月3日颁布的实施细则。

本程序还基于法国反腐败局（AFA）和法国国家信息和自由委员会（CNIL）的多项出版物：

- 法国反腐败局的建议；
- 法国反腐败局与法国金融检察院于2023年3月联合发布的《内部反腐败调查实务指南》；
- 法国国家信息和自由委员会于2019年首次发布并于2023年修订的《举报专业指南》参考文件。

总体而言，举报信息的收集与处理均遵循现行法律法规的要求，本程序将根据立法进展及最佳实践适时更新。

若当地法律法规对举报人的保护规则优于本程序，则以当地规定为准。但当本程序提供更高保护标准时，蓝格赛集团将在法律允许范围内主动适用更优条款。

3. 适用范围

本程序适用于蓝格赛集团所有实体，并将根据法律法规变化进行必要修订，以确保持续合规。

在蓝格赛集团部分国家/地区，本程序由当地细则进行补充规定。这些细则明确当地法律要求及当地可用的举报渠道（详见附录2）。

举报人可自主选择举报渠道（集团或当地举报渠道），相应程序将根据所选渠道适用。根据所举报行为或不端行为的性质及严重程度，通过当地渠道提交的举报可能转交集团处理，反之亦然。

本程序适用于蓝格赛集团全体员工（无论其职务、职位或部门）及与集团存在业务往来的第三方。蓝格赛集团内部举报信息的收集与处理流程，具体包括：

- 举报信息提交流程；
- 举报信息接收流程；
- 可受理性评估；
- 内部调查主要环节；
- 案件结案流程。

II. 举报信息收集

1. 举报信息受理条件

谁可以举报？

蓝格赛集团内部举报系统向以下人员开放：

- 蓝格赛集团员工（正式员工、定期合同工、学徒、实习生）
- 外部或临时雇员（临时工、顾问等）
- 求职者
- 离职员工
- 股东、合伙人及股东大会表决权持有者
- 董事会或监事会成员
- 与蓝格赛集团有业务往来的任何第三方雇员（例如客户、供应商、服务提供商等）。

本内部举报系统对蓝格赛集团所有实体开放，并提供集团的主要语言版本：英语、德语、中文、法语、意大利语、荷兰语、瑞典语和斯洛文尼亚语。

举报人如何获得相关法律保护？

要被认定为举报人并享受法律保护，您必须符合举报人的法定要件，即同时满足以下标准（除非当地法律另有规定）：

- 为自然人主体；
- **未因举报获得任何直接经济利益；**
- **出于善意行事；**
- **若举报事实系在非工作环境中获取，举报人须对举报事实具有亲身认知。**

可举报哪些事实？

蓝格赛集团内部举报系统受理可能构成以下行为类别的事项举报：

- **涉嫌犯罪或违法行为**
- **危害公共利益的行为**
- 违反或试图隐瞒违反国家、欧盟或国际法律法规的行为
- 违反或违背蓝格赛集团《道德指南》或《反腐败行为准则》的行为
- **与蓝格赛集团业务相关的重大风险（可能损害人权、基本自由、健康安全或环境）**

可举报事项示例包括但不限于：

- **腐败行为，包括违反《反腐败行为准则》的任何行为**
- **骚扰（心理或性骚扰）**
- **歧视行为**
- **健康卫生或安全隐患（例如对身心完整性的威胁）**
- **人权侵害（除歧视、隐私及骚扰外）**
- **利益冲突**
- **反竞争行为**
- **环境违规（例如污染、废弃物处置不当）**
- **税务欺诈**
- **财务或会计欺诈**
- **内幕交易**
- **虚设职位**
- **个人数据/信息技术安全**

附录3列举了部分行为。

未列入上述范畴的举报事项不适用本程序。。同样，根据 国防机密、医疗保密义务、司法评议秘密、司法调查秘密或律师-客户保密特权等相关规定**禁止披露的事实、信息或文件**（无论其形式或载体），**均不适用本程序**。若涉及此类情况，举报人将收到通知并被引导至有权处理所举报事项的职能部门。

2. 如何提交举报

举报人可通过以下渠道提交举报：

- 在线举报平台：<https://www.rexel.com/en/rexel-group-ethics-alert>；
- 集团或国家层面可能存在的其他举报渠道。

各渠道无层级之分，举报人可自由选择任一渠道提交。

无论采用何种渠道，负责收集举报的主体下文统称为“**内部管理部门**”。

在线举报平台

举报人可通过在线举报平台（网址：<https://www.rexel.com/en/rexel-group-ethics-alert>）进行举报，包括匿名举报。

该平台为专属免费平台，全天候开放。

该平台由外部服务提供商（安永）在欧盟境内托管，并采取严格措施确保数据安全与保密性。需特别说明：该服务提供商员工不参与举报处理流程，亦无权限接触相关信息。

该平台支持通过聊天功能与举报受理人直接沟通，并允许举报人上传事实佐证文件。

该平台的链接可在集团网站上找到：[、https://www.rexel.com/en/rexel-group-ethics-alert](#)、以及 <https://ethique.rexel.com/en/>，同时也可通过蓝格赛集团各实体的内网网站访问。

其他举报渠道

蓝格赛集团内部员工可通过书面或口头形式向以下内部管理人员提交报告：(i) 当地合规经理（法务或合规部门），(ii) 当地人力资源部，(iii) 集团合规部，或 (iv) 集团人力资源部。

人力资源部门（地方或集团层面）通常受理违反劳动法的行为或工作场所其他不当行为（如骚扰、歧视、健康卫生或安全问题等）的举报。

当地合规官或集团合规部通常受理违反法律法规、《道德指南》、《反腐败行为准则》及蓝格赛集团合规程序等事项的举报。

口头举报可通过电话受理，根据举报人要求及其选择，也可在收到请求后二十（20）个工作日内安排视频会议或面谈。口头举报内容需以书面形式记录。

在任何情况下，员工均可向其直接或间接直线经理寻求建议并反映相关疑虑，但当该直线经理本人涉嫌相关行为时除外。若经讨论后认定该等疑虑属于本程序处理范围，直线经理须引导员工通过上述渠道进行举报，或联系当地法律合规部门及人力资源部门进行举报。

3. 举报内容

举报人须以精准客观的方式陈述举报事项，以确保举报事项得到有效处理。

在可能情况下，应通过以下方式佐证举报内容：

- 说明所举报事实发生的日期、地点、相关实体以及涉事人员的身份和职位；
- 提供与举报主题直接相关的具体事实细节描述，无论其表现形式或载体。

4. 匿名举报

举报人最好能表明身份，这尤其有助于简化调查程序。但举报人可选择通过在线举报平台匿名举报，前提是：(i) 所述事实严重性已得到确认，且 (ii) 事实要素足够详尽。

5. 外部渠道

在遵守当地适用法规的前提下，需特别说明的是，举报人亦可选择向以下外部机构进行举报：

(i) 主管当局；(ii) 监察专员；(iii) 司法机关；或 (iv) 任何有权受理此类举报的相关地方或国际机构、组织或部门。举报人可直接向上述外部机构提交举报，亦可在向蓝格赛集团内部举报后另行外部举报。

III. 内部举报处理流程

1. 举报收悉确认

当举报通过在线举报平台或传统渠道提交后，内部管理部门（即前文定义的举报受理负责人）应在收到举报后七（7）个工作日内确认收悉。

该收悉确认不构成对举报内容的认可。

2. 举报可受理性审查

内部管理部门将对每份收到的举报进行初步分析，以确保其符合程序适用范围并具备受理资格。

此核查可能需要与举报人沟通，重点关注以下要点：

- 举报人的“举报者”的身份：特别是确认其出于善意且不寻求直接经济利益；
- 举报性质：确认其确实属于本程序涵盖的举报类别之一；
- 举报内容：确保所举报的信息和事实客观且详尽，以便启动调查程序；
- 涉密审查：举报内容未涉及国防保密、医疗隐私、司法审议保密、司法调查或询问保密，以及律师-客户保密特权等受法律保护的保密事项。

受理决定由内部管理部门作出。若举报不被受理，将通知举报人并说明理由。

在任何情况下，**内部**管理部门须在三个月内作出初步回应。蓝格赛集团虽无义务在此期限内处理举报，但必须向举报人说明为评估举报有效性及解决所涉问题已采取或计划采取的措施。

举报将予以完全保密处理。

根据所报告事实的性质和严重程度，举报可能由蓝格赛集团**道德委员会**处理。该委员会是蓝格赛集团公司内部设立的特别委员会，负责处理蓝格赛员工或与蓝格赛有业务往来的第三方提交的最严重举报事项。

蓝格赛集团**道德委员会**由三名常任成员组成：

- 秘书长、
- 集团人力资源总监，以及
- 道德与合规总监

3. 开展内部调查

内部调查的目标与管理

处理举报所需时间因举报事实的复杂程度及所提供信息的性质而异。

内部调查旨在核实所举报事实的准确性与重要性。调查将采用多种方法进行（访谈、数据检索等），具体方式将根据调查对象的背景与性质而定。

此类调查工作可由以下部门开展：

- (xxxvi) 当地人力资源部门；
- (xxxvii) 当地合规或法律部门；
- (xxxviii) 集团合规部；
- (xxxix) 集团人力资源部；
- (xl) 蓝格赛集团**道德委员会**（视举报事项性质及严重程度而定）
（下称“调查负责人”）。

在任何情况下，调查负责人将主导对举报事项的内部调查。**有关**举报本身与其内容的信息仅在严格必要范围内向调查相关人人员披露。

当收到举报时，蓝格赛集团**保证**调查过程的独立性。在启动内部调查前，将核实参与调查人员均未直接或间接受到举报事实影响，亦与**涉事人员无利益关联**。若发现存在利益冲突风险，相关员工将立即退出流程并予以替换。此独立性原则是蓝格赛道德与合规体系的核心组成部分，旨在确保对所有举报进行严谨、公正且可信的管理。

扣押电子邮件、文件或计算机介质

内部调查可能需要审查和处理一名或多名员工的电子邮件或任何计算机介质。在扣押或冻结任何电子邮件账户或计算机介质之前，调查经理**必须按照当地程序规定**（例如集团道德委员会、当地总法律顾问或当地数据保护联络员）**申请授权**，以便为调查目的扣押并保留这些电子邮件。

客座专家

当情况需要时，调查经理可在处理特定举报的框架内决定邀请一名或多名人员协助，尤其当需要会计、财务、技术或IT专业知识时。

调查经理可决定寻求蓝格赛内部专家协助，例如内部审计部、财务部、采购部、国家或区域管理团队，或调查经理认为具备资质且必要的蓝格赛集团内任何人员（），亦可寻求经正式认证的外部服务提供商协助。

专家的任务将在完成调查经理所请求协助的举报相关所有核查或处理操作后自动终止，或在调查经理提出简单要求时终止。

受邀专家须承担与内部经理及调查经理相同的保密义务。

4. 调查决策与结案

若事实未获证实，则关闭举报并通知举报人。

若事实成立，调查经理将依据调查结果判定是否存在违反法律、道德指南或反腐败行为准则的行为，并据此建议整改措施和/或相应处分。

举报人将收到书面通知，告知调查已结案。

相关人员也将收到调查结束通知。若经调查认定违规行为性质严重且事实成立，相关管理层可根据指控事实的性质和严重程度，对当事人采取纪律处分措施，包括但不限于解雇。

IV. 提供的保护与保障

1. 一般原则

所有调查均将秉持公正原则，并严格遵守当地适用法律法规。在任何情况下，蓝格赛集团均确保尊重相关人员的无罪推定原则。

举报制度仅基于善意提供的信息方能有效运作。任何恶意举报——即纯粹意图造成损害的行为——可能面临纪律处分，直至解雇。

2. 通知

举报人将在举报提交后七（7）个工作日内收到通知。

在确认收到举报后的合理期限内（不超过三个月），将以书面形式告知举报提交人拟采取或已采取的措施，以评估指控的准确性，并在适当情况下对举报所述事项进行补救，同时说明采取这些措施的理由。若指控不实或缺乏依据，或举报已失去相关性，应以书面形式通知举报提交人案件已结案。

任何涉及可受理举报的人员将获知针对其个人的指控性质。但若为防止销毁举报相关证据而需采取预防措施，则应依据适用法律在措施实施后方可告知举报涉及人员。

被举报对象在任何情况下均不得依据知情权要求蓝格赛集团披露举报人身份。

需特别说明的是，所提供信息的详细程度可能因当地适用法律而有所不同。

3. 刑事、民事及社会事务保护

提醒举报人注意，在遵守当地适用法规的前提下：

- 若举报行为符合适用规定，且举报人在提交举报时有合理理由相信该举报或披露对维护相关权益确有必要，则其不承担因举报或披露行为造成的损害赔偿责任。
- 获取或查阅公开举报或披露的信息不构成刑事责任，前提是此类获取或查阅行为未违反当地适用法规构成独立刑事犯罪。若构成独立刑事犯罪，则适用当地刑事责任相关规定。
- 只要举报是出于善意，则不得因其依法举报或披露信息而受到惩罚、解雇、歧视（特别是薪酬、培训、晋升方面），也不得遭受报复、威胁或企图采取此类措施。

在相同条件下，协助举报人进行举报或与其有关联的个人，不得遭受报复性措施、威胁或企图采取此类措施的行为。

蓝格赛集团绝不容忍对举报人及其亲属采取任何形式的报复、威胁或企图采取此类措施的行为，例如骚扰。

4. 数据保留期限

举报仅可保留至严格必要且与处理目的及保护举报人、涉事人员及提及第三方权益相称的期限，同时需考虑后续调查所需时间。但若相关数据中涉及人员均无法被识别或追溯，则可延长保留期限。

道德警示存档系统分为以下几类：

- **不予受理的举报**（不属于适用范围、不严重、无事实依据、恶意举报等）：应尽快删除或归档并匿名化处理。
- **可受理举报**：
 - 当举报未引发纪律处分或法律程序时，蓝格赛集团**确保在核查或调查工作结束后两个月内**销毁举报档案中所有可能识别举报人及相关人员身份的材料；
 - 若调查导致法律诉讼或纪律处分，相关文件要素将依法保留至必要期限，直至诉讼时效届满（六年）或所有上诉途径耗尽。此后，在规定期限届满时，该数据将被销毁或归档并匿名化处理。

5. 保密与安全

蓝格赛集团采取一切必要措施，确保数据在收集、处理、传输或存储过程中的保密性与安全性。

在符合当地适用法规的前提下，所实施的报告收集与处理程序确保对报告提交者的身份、报告所涉对象的身份，以及报告收集与处理负责人所收集的信息严格保密。

具体而言：

- 信息仅限于为处理举报而具有合法知情需求的人员。
- 所有参与举报管理的人员均接受过培训并承担保密义务。特别是，他们承诺不将数据用于不当目的，并遵守适用法律规定的有限数据保留期限。
- 在线举报平台具备安全防护措施，提交的举报信息仅限授权人员查阅。该系统同时允许希望保持匿名的员工使用此渠道。
- 根据法律要求，举报人的身份可向司法机关披露。
- 除非向司法机关披露，否则在确认举报有效性之前，不得透露可能识别举报对象身份的信息。
- 在蓝格赛集团各实体内部，通常参与处理举报的部门均知悉举报人及涉事人员身份的保密性质。

6. 个人数据保护

作为举报制度的一部分，蓝格赛集团可能收集并处理个人数据，特别是与举报人及涉事人员相关的数据。附录4中的详细信息公示规定了数据收集、处理、存储及归档的具体条件。

V. 报告机制

集团合规部每年就举报数量、类型及后续处理措施提交报告，所披露数据严格限于与举报事由相关的必要信息。

VI. 程序更新

蓝格赛集团保留随时修改、补充或更新本程序的权利，以适应法律法规、判例法或集团内部需求的变更。所有更新均须符合当地适用法律法规。

相关员工、供应商及其他利益相关方将通过适当渠道（内部通讯、电子邮件、内网公告、供应商直接通知等）获知变更内容，具体方式符合当地法律要求。

本程序的最新权威版本将发布于蓝格赛集团网站、集团内网及在线举报平台。

联系方式

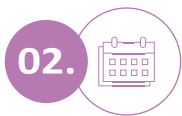
公司：蓝格赛发展公司

地址：法国巴黎17区沃堡大道13号（邮编75017）——收件人：集团合规部

电子邮箱：compliance@rexel.com

举情况举报

若您怀疑或知悉
违反法律、道德指南
或《反腐败行为准则》的行为，请立即举报！



何时应发出警报？

当您知悉
或怀疑存在**违反法律**
或违反我们道德准则的行为时。

这可能包括：

- 腐败行为；
- 侵犯人权行为；
- 骚扰
或歧视；
- 欺诈等行为。



是否涉及机密？

是的，您也可以发送
匿名举报



我受保护吗？

你必须诚信地发出警报
必须出于善意且不寻求任何直接
经济补偿。
在此情况下，您将受到保护。



谁可以发出警报？

集团全体员工
及第三方均可使用道德热线



如何提出警报？

1. 使用**在线蓝格赛道德热线**
(下方网页链接)
- 7天、24小时全天候开放；
- 支持集团所有主要语言
提供服务。
2. 使用当地设立的**举报系统**；
3. 联系**法律/合规部门或人力资源
部门**（集团或当地）



谁处理此警报？

集团层面：道德委员会。
针对本地系统：参见当地程序。

更多信息

访问：
<https://www.rexel.com/en/ethical-alert/>

179

附录2：设有本地举报程序的国家列表

某些国家/地区还设有地方性程序作为补充，这些程序规定了适用的法律要求，并视具体情况说明当地可用的渠道。

地方渠道信息如下所示。请查阅当地程序以获取最新详情。

- 澳大利亚：

o 瑞赛尔举报热线披露服务（由独立外部服务提供商运营）：

电话：1300 30 45 50

传真：瑞赛尔控股澳大利亚公司（转举报热线）03 9882 4480

电子邮件：rexel@stopline.com.au

在线：<https://rexel.stoplinereport.com/>

邮寄：Rexel Holdings Australia

C/- the STOPline

Locked Bag 8

HAWTHORN VIC 3122

- 加拿大：可联系道德委员会。

- 德国：

o 电子邮件：whistleblowing@rexel.de

o 邮寄地址：Rexel Germany GmbH & Co.

KG - 收件人：Nicole Steuer女士 | 法务总监

Ridlerstr.5780339 München

- 爱尔兰

o 可联系人力资源部、举报专员、首席执行官或由Safecall运营的外部举报热线

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- 意大利：

o <https://report.whistleb.com/rexel>

- 荷兰：可联系Rexel荷兰公司道德事务联络人。

- 瑞典：

o <https://whistleblow.vismadraftit.se/rexel-sverige-ab>

o 电话：08-556 214 14。

- 英国

o 您可联系人力资源部、举报专员、首席执行官或由Safecall运营的外部举报热线

Safecall

0800 915 1571

rexel@safecall.co.uk

www.safecall.co.uk/report

- 美国

o 合规邮箱：ethics@rexelusa.com

o 合规热线：1-800-714-8774

附录3：举报程序涵盖的行为或不当行为示例

类别	范围
腐败	在适用当地法律法规及集团反腐败政策框架下：腐败指直接或通过第三方交换利益（金钱、礼品、邀请、服务、人脉等），以换取履行或不履行与职能或职责相关行为的行为。 其表现形式包括：为获取便利而主动提议或提供利益（主动腐败），或为获取服务而索取或接受利益（被动腐败）。 腐败可能涉及公共和私营部门行为者，扭曲竞争，破坏决策透明度，并使相关个人和组织面临制裁和起诉风险。
骚扰	骚扰指通过反复行为或单次严重行为损害个人尊严、安全或工作条件的行为。其表现形式包括言语、手势、态度或行动，旨在恐吓、羞辱、孤立、威胁或贬损雇员或第三方在职业活动中的处境。 骚扰可表现为心理形式，如贬损性言论、蓄意孤立、过度工作或剥夺工作资源、排挤、散布谣言或系统性贬低。亦可表现为性骚扰形式。 性骚扰特征在于反复发生或构成单次严重事件的不当性行为或言论，此类行为损害个人尊严或营造出恐吓性、敌意性、贬损性或羞辱性的工作环境。具体包括但不限于：持续性求爱、涉及身体的言论、索要性好处、未经同意的身体接触或肢体动作、未经许可传播色情图像等。 无论道德骚扰或性骚扰均不可接受，施害者须承担当地法律规定的责任。
	职场歧视是指基于法律禁止的标准（如出身、性别、家庭状况等）或任何其他受当地法律保护的特征，对某人

歧视	给予不利待遇的行为。例如，歧视可能导致在就业机会、工作条件、培训、调动或其他与职业活动相关的情境中受到不平等对待。其表现形式包括：在招聘、评估、晋升、岗位分配或解雇决策中，在缺乏基于岗位要求的客观依据的情况下对个人造成不利影响。 职场歧视主要分为两种形式： - 直接歧视：行为人基于法律明令禁止的歧视性标准蓄意作出决策。 间接歧视。此类情形中，实施者作出的决策看似中立，但最终使特定人群处于不利地位。例如，公司内部规定仅允许男性员工年满50岁后留任，此举即构成基于性别和年龄的间接歧视。
健康/安全	任何严重侵害或危及工作健康安全的行为。工作安全涵盖所有旨在通过降低事故、伤害及职业病风险来保护员工身心完整性的措施与实践，包括风险识别评估、技术与组织保障措施实施、员工培训告知，以及预防干预应急响应机制建立。履行这些义务有助于构建符合当地法规的安全工作环境。
人权（除歧视和骚扰外）	任何严重侵犯或危及国家及国际层面公认的人权与基本自由的行为，以及违反该领域适用当地法规的情况。此类情形包括但不限于涉及以下原则的事件：尊重结社自由与言论自由、保障体面安全的工作条件、确保相关人员获得法律救济途径。
利益冲突	利益冲突是指个人在履行蓝格赛集团职责时，其财务、家庭、友谊、政治或其他利益可能实际或看似影响其判断或决策的情形。此类情形未必构成过失或违法行为，但存在损害预期公正性的偏见风险。这种偏见风险可能足以动摇相关方的信任、降低决策质量并损害组织声誉。利益冲突可分为实际存在（已发生）、潜在可能（可能发生）或表面存在（被第三方感知）三类。举报系统并非旨在替代蓝格赛集团规定的利益冲突报告程序。
	反竞争行为指损害自由竞争、危害其他市场参与者（客户、供应商、竞争对手）的企业行为。

反竞争行为	其表现形式包括：竞争对手通过正式或非正式协议协调价格、商业条款、市场/区域/产品分配，或限制供应、抵制特定合作伙伴。还包括滥用市场支配地位的行为（如排挤竞争对手、实施掠夺性定价或不合理捆绑销售）、干预分销商转售价格，以及交换可能影响市场行为的非公开战略信息（如计划、营销数据或产能）。 这些行为被竞争规则所禁止，并会受到严厉处罚。
环境	无任何未满足适用环境要求或被认定对环境构成重大风险或损害的情况，无论发生在公司内部还是价值链合作伙伴之间。这涵盖污染预防、资源负责任使用以及物质和废物安全管理，均须符合监管义务和内部标准。
欺诈	任何通过隐瞒、欺骗或操纵手段谋取不当利益或逃避义务的行为，包括税务、财务或会计领域的违规操作。 这包括例如伪造文件或记录、虚报财务信息、隐瞒收入或资产，或任何旨在规避适用规则的计划，无论是在公司内部还是其价值链中。
内幕交易	内幕交易是指利用或依赖发行人或其证券的非公开特权信息进行金融工具买卖或推荐的行为。此类行为还包括向第三方非法披露此类信息。此类行为在市场上构成不公平优势，依法严禁并予以惩处。
虚假职位	虚假职位指为获取不正当利益，向未实际履职或根本不存在职位/任务的人员支付薪酬的行为。此类情况可能表现为：公司内部或通过第三方安排完全无实际工作内容、虚构职责，或名义上分配至部门却毫无实质贡献。
个人数据保护/信息安全	任何未按法律及内部规定保护个人数据或信息系统的行为，均可能使个人或公司面临未经授权的访问、使用、披露、修改或破坏风险。此范畴涵盖数据的合法最小化收集处理、系统安全（访问控制、加密、备份）、事件与违规管理，以及信息全生命周期（含服务提供商环节）的保密性与完整性保障。 个人数据指直接或间接识别自然人的任何信息（如姓名、联系方式、标识符、照片、位置数据或其他与身份或个人生活相关的要素）。

附录4：隐私政策

隐私政策

—

举报系统

版本 12/2025

蓝格赛集团已建立专业举报系统，供集团员工及相关第三方举报违法行为或不当行为。该系统适用范围详见rexel.com网站公布的《举报程序》。

 根据该制度，蓝格赛旗下实体可能收集并处理您的相关数据。数据保密性是我们信任关系的基础。因此，我们在业务活动中高度重视个人数据的保护。

本政策阐明蓝格赛集团在个人数据保护方面的承诺。以下声明将使您了解自身权利，以及个人数据被收集、处理、存储和归档的具体条件。

我们是谁？

REXEL DEVELOPPEMENT SAS（法国法律下的简易股份公司），注册地址：巴黎沃堡大道13号，注册于巴黎商业与公司注册处，注册号480 172 840，是数据控制者。

集团内与报告撰写者签订雇佣合同或与其合作的实体同样作为数据控制者。

上述主体决定数据处理的目的和方式。

本政策中以"蓝格赛"、"我们"或"数据控制者"指代上述主体。

安永波兰公司作为数据处理者，负责在线警报平台的数据处理工作。

在举报系统中我们如何处理您的数据？

下表详细说明：

- (i) 我们处理您个人数据的目的，
- (ii) 我们处理的数据类型，以及
- (iii) 处理您数据的法律依据。

目的 1	数据类型
收集并处理举报系统所涵盖的 违法行为或违反反 腐败行为准则的 举报（参见举报程序） <u>次要目的：</u> - 集中管理专业报告（接收与处理举报、建立安全渠道、存储与保留信息、保障安全） - 处理专业报告（开展内部调查、评估相关事实） - 报告结案后的决策与措施实施（通知及措施执行） - 统计监测与改进举报系统 - 在法律程序中行使或维护权利	作为系统组成部分，可能处理以下类别的数据： - 举报人的身份数据（姓名、联系方式）、职业数据（职位、雇主、工作地点）（除非匿名举报）及其自愿提供的其他信息 - 涉事人员的身份数据（姓名、联系方式）、职业数据（职位、雇主、工作地点） - 参与或协助收集/处理举报的个人身份数据（姓名、电子邮箱）、职业数据（职位、雇主、工作地点），以及协助者和与举报人接触者的相关信息 - 敏感数据（种族或民族出身、政治观点、宗教或哲学信仰、工会会员身份、健康数据、性生活或性取向），仅在为行使或捍卫合法权益（《通用数据保护条例》第9.2.f条）或重大公共利益（《通用数据保护条例》第9.2.g条）所必需时收集 - 与刑事定罪、犯罪行为或相关安全措施相关的数据，仅在严格必要且符合《通用数据保护条例》第10条规定时收集 - 事实核查过程中收集的信息 - 核查操作报告 - 报告后续处理相关数据
数据处理的法律依据	
实施举报制度的法律义务：特别是《萨宾二号法案》第8.I.B条和第17 II条、《商法典》第L. 225-102-4条，以及任何关于保护举报人、反腐败或尽职调查义务的等效法律。	

目的 2	数据类型
收集并处理关于违反《道德指南》行为的举报 <u>子目的：</u> - 集中管理专业报告（接收与处理举报、建立安全渠道、存储与保留信息、保障安全） - 处理专业报告（开展内部调查、评估相关事实） - 报告结案后的决策与措施实施（通知及措施执行） - 统计监测与改进举报系统 - 在法律程序中行使或维护权利	作为系统组成部分，可能处理以下类别数据： - 举报人身份数据（姓名、联系方式）、职业数据（职位、雇主、工作地点）（匿名举报除外）及其自愿提供的其他信息 - 涉事人员的身份数据（姓名、联系方式）、职业数据（职位、雇主、工作地点） - 参与或协助收集/处理举报信息者的身份数据（姓名、电子邮箱）、职业数据（职位、雇主、工作地点），以及协助者和与举报人接触者的相关信息 - 敏感数据（种族或民族出身、政治观点、宗教或哲学信仰、工会会员身份、健康数据、性生活或性取向），仅在为行使或捍卫合法权益（《通用数据保护条例》第9.2.f条）或重大公共利益（《通用数据保护条例》第9.2.g条）所必需时收集 - 与刑事定罪、犯罪行为或相关安全措施相关的数据，仅在严格必要且符合《通用数据保护条例》第10条规定时收集 - 事实核查过程中收集的信息 - 核查操作报告 - 报告后续处理相关数据
处理您数据的法律依据	
法律依据：处理非法律义务涵盖的道德举报所具有的合法利益。	

您的数据接收方是谁？

 我们收集的个人信息以及后续收集的任何数据，均由我们作为数据控制者使用。

 我们确保仅授权人员可访问此数据。

内部：

- 负责收集和处理警报的人员，即：
 - 蓝格赛集团道德委员会成员
 - 集团及地方层面法律或合规部门的授权成员
 - 集团及地方层面人力资源部门的授权成员
- 集团及地方层面审计与内部控制部门的授权成员（确保内部控制与治理有效性）
- 在情况需要时，其他内部人员可访问相关数据，尤其当涉及会计、财务、法律、技术或信息技术专业知识时。

外部人员：

- 我们的顾问
- 我们的经纪人和保险公司
- 我们的审计师
- 主管当局（司法、行政及监管机构），依据适用法规
- 我们的服务提供商，特别是为我们提供在线报告平台的安永波兰公司。

上述接收方均位于欧盟境内。

我们保存您的数据多长时间？

情况	保留期限
不被接受的警报（不属于适用范围、性质不严重、信息不全、恶意提交等）	尽快删除或归档并匿名化
可受理但驳回的举报（未引发纪律或法律程序）	须于两（2）个月内完成删除或匿名化处理并归档
引发纪律或法律程序的举报	保留数据直至程序及上诉结束。 此后进行删除或匿名化处理并归档。

您拥有哪些权利？



根据个人数据保护法规，您享有以下权利：

- 访问权：您可查阅我们持有的关于您的信息并获取副本；
- 更正权：您可要求修改、补充、更新或删除任何不准确的个人数据；
- 反对权：您可反对我们处理您的数据，除非我们有正当且充分的理由继续处理；
- 删除权：您可在《通用数据保护条例》第17条规定的条件范围内要求我们删除您的相关数据；
- 数据可携权：您可提取数据以转移至其他机构或用于个人用途；
- 处理限制权；
- 制定特定及通用指引的权利：您有权就身故后个人数据的存储、删除及披露制定具体或通用指引。

任何报告涉及的个人，在相关数据（无论是否通过计算机化方式）被记录后，将尽快（最迟一个月内）获知该情况，以便其行使相关权利。但若此类通知可能严重损害处理目的（特别是妨碍调查进行，例如存在证据灭失风险），则可延迟通知，待风险消除后再行告知。

被举报人不得基于知情权要求数据控制者提供举报人身份信息或任何其他调查相关人员的身份信息。

若您未获回复、认为回复不满意，或认为数据处理不符合法律法规要求，您有权向法国国家信息与自由委员会（CNIL）申诉：<https://www.cnil.fr/fr/plaintes>

如何行使您的权利？



请向我们的数据保护官提交书面请求：

国家	实体	地址
奥地利	COMTECH IT-SOLUTIONS GMBH	datenschutz@rexel.at
	蓝格赛奥地利有限公司	datenschutz@rexel.at
比利时	蓝格赛比利时股份有限公司	gdpr@rexel.be
法国	Cordia	donnees.personnelles@francofa-eurodis.fr
	蓝格赛发展股份有限公司 / 蓝格赛集团	data.protection@rexel.com
	蓝格赛法国有限责任公司	donnees.personnelles@rexel.fr
	Bizline	data.protection@rexel.com
	Gigamedia	data.protection@rexel.com
	Sofinther SAS	donnees.personnelles@sofinther.fr
	Espace Elec SAS	donnees.personnelles@espace-elec.fr
	Esabora数字服务公司	dataprotection-rda@rexel.fr
	Francofa Eurodis	donnees.personnelles@francofa-eurodis.fr
	Freshmile Services SAS	donnees.personnelles@rexel.fr
	ITESA	donnees.personnelles@rexel.fr
德国	REXEL GERMANY BETEILIGUNGS GMBH	Datenschutzbeauftragter@rexel.de
	Rexel Germany GmbH & Co KG	Datenschutzbeauftragter@rexel.de
	REXEL GERMANY VERWALTUNGS GMBH	Datenschutzbeauftragter@rexel.de
意大利	蓝格赛意大利股份有限公司	dataprotection@rexel.it
	Tecno-Bi S.r.l.	dataprotection@rexel.it
	Comm-Tech S.r.l.	dataprotection@rexel.it
爱尔兰	M. Kelliher 1998	data.protection@rexel.ie
	蓝格赛工业解决方案 公司	data.protection@rexel.ie
卢森堡	蓝格赛卢森堡股份有限公司	gdpr@rexel.be
荷兰	Rexel Nederland B.V	AVG@rexel.nl
	瓦斯科集团有限公司	AVG@rexel.nl
	瓦斯科控股有限公司	AVG@rexel.nl
	Wasco 批发集团 B.V.	AVG@rexel.nl
	Wasco Distributlecentrum B.V.	AVG@rexel.nl
斯洛文尼亚	蓝格赛有限责任公司	dpc@rexel.si
瑞典	Rexel Sverige AB	dataskydd@rexel.se
瑞士	ELEKTRO-MATERIAL AG	datenschutz@e-m.ch
	蓝格赛3S	data.protection@rexel.com
英国	蓝格赛（英国）有限公司	data.protection@rexel.co.uk