



Privacy Policy for the Whistleblowing System

Language versions

SUMMARY OF THE VERSIONS

English Version	2
French Version	8
Deutsche Version	14
Versione Italiana	20
Nederlandse Versie	26
Slovenska Verzija	32
Svensk Version	38
中文版	44



English Version

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



French Version

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



Deutsche Version

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 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



Versione Italiana

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



Nederlandse Versie

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 gearchiveerd.



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



Slovenska Verzija

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.

 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 pooblaščne 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



Svensk Version

INTEGRITETSPOLICY

—

VISSELBLÅSARSYSTEM

Version 12/2025

Rexel-koncernen har inrättat ett professionellt visselblåsarssystem 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 visselblåsningsförfarandet, 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



中文版

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。

i

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？

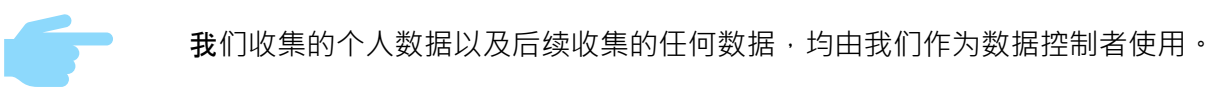
下表详细说明：

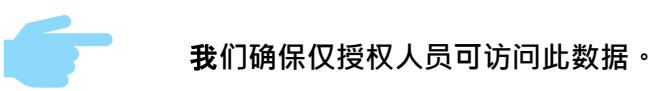
- (i) 我们处理您个人数据的目的，
- (ii) 我们处理的数据类型，以及
- (iii) 处理您数据的法律依据。

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