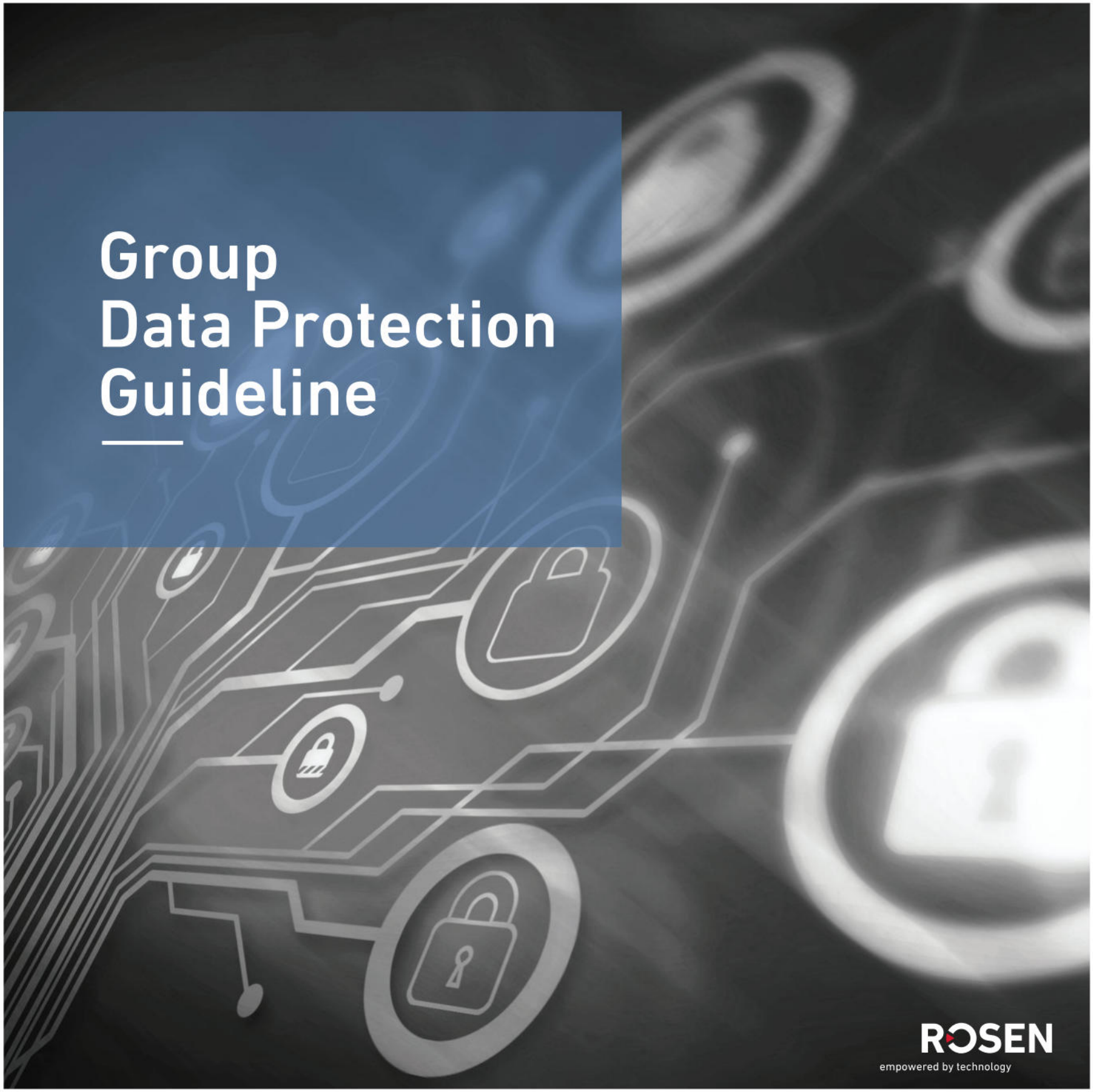
Group Data Protection Guideline



ROSEN
empowered by technology

CONTENTS

1. OBJECTIVE OF THE GROUP DATA PROTECTION GUIDELINE

In the context of its social responsibility, the ROSEN Group is committed to observing international data protection rights.

It is our claim that ROSEN not only stands for innovative, leading and tailored solutions for our customers everywhere in the world but also sets standards regarding data protection. As a globally active organization, we therefore consider it our duty to conform to the various statutory requirements throughout the world that are associated with the collection and processing of personal data. Our top priority is to ensure a uniform and globally valid standard when handling personal data. Ultimately, the safeguarding of the personal rights and privacy of every single individual is for us the basis for trustworthy business relationships.

This data protection guideline is valid throughout the world for the entire ROSEN Group and is based on globally accepted basic data protection principles.

Ensuring that data protection is a basis for trustworthy business relationships and the reputation of the ROSEN Group as an attractive employer.

The data protection guideline creates one of the necessary framework conditions for worldwide data transfers between the companies of the ROSEN Group. It guarantees the appropriate level of data protection demanded by the European Data Protection Directive and national laws for cross-border data traffic, including in those countries in which no legally appropriate level of data protection exists.

The executive management and employees of the ROSEN Group are committed to observing this data protection guideline and to upholding the respective data protection laws.

2. SCOPE

This data protection guideline is valid for all companies of the ROSEN Group, i.e. for ROSEN Swiss AG and all group companies dependent on it, as well as associated companies and their employees. The data protection guideline encompasses all processing of personal data. In countries in which the data of legal persons are protected in the same way as personal data, this data protection guideline also applies in the same manner for the data of legal persons. Anonymous data, e.g. for statistical analyses or investigations, are not subject to this data protection guideline.

The individual group companies are not authorized to formulate regulations deviating from this data protection guideline. Other guidelines for the protection of data may only be created in consultation with the Group Data Protection Officer when this is necessary according to the respective national law. Alterations of this data protection guideline take place in consultation with the Group Data Protection Officer pursuant to the procedure specified for the alteration of guidelines. The alterations are reported immediately to the companies of the ROSEN Group. Alterations that have significant implications on compliance with the data protection guideline must be reported annually to the data protection authorities issuing the approval of this data protection guideline as binding intra-corporate data protection regulations.

The latest version of the data protection guideline can be downloaded in the data protection notices area on the ROSEN Group's Internet site: www.rosen-group.com.

3. NATIONAL LAW TAKES PRECEDENCE

Insofar as this data protection guideline includes globally accepted data protection principles, it supplements the respective national data protection law, without replacing it. The respective national law takes precedence if it requires deviations from this data protection guideline or imposes farther-reaching requirements. In particular, the contents of this data protection guideline must be observed when there is no corresponding national law. Existing reporting obligations for data processing based on national law must be observed. Every company of the ROSEN Group is responsible for complying with this data protection guideline and all statutory obligations. If there is reason to assume that statutory obligations conflict with the obligations in this data protection guideline, the group company affected must immediately inform the Group Data Protection Officer. In the event of a collision between national legislation and the data protection guideline, ROSEN Swiss AG will, together with the group company affected, search for a practicable solution in accordance with the objectives of this data protection guideline.

4. PROCESSING PERSONAL DATA

4.1. Legality / Purpose-related / Transparency

When processing personal data, the personal rights of the concerned person must be safeguarded. Personal data must be collected and processed in a lawful manner.
The processing of personal data may only pursue the purposes that were defined before the collection of the data. Only limited subsequent changes to the purposes are possible, and they require justification.
The person concerned must be informed about how his/her data is being handled. Basically, personal data must be collected from the person concerned himself/herself. When collecting the data, the person concerned must at least be able to identify, or be informed accordingly about, the following:

- The identity of the responsible body
- The purpose of the data processing
- The third party or categories of third parties to which the data will be conveyed, if applicable

4.2. Principle of Data Avoidance and Data Economy

Before processing personal data, it must be checked whether and to what extent these data are necessary in order to achieve the purpose pursued with the processing. If it is possible to achieve the purpose, and if the effort is proportionate to the pursued purpose, then anonymous or statistical data must be used. Personal data must not be stored in reserve for potential future purposes, unless this is prescribed or permitted by applicable law.

4.3. Deletion of Data

Personal data that are no longer required after the expiration of statutory or business process-related retention periods must be deleted. If in individual cases there are indications for protection-worthy interests or for a historical significance of these data, the data must be retained stored until the protection-worthy interest has been legally clarified or it has been assessed whether the data stock serves any historical purposes.

4.4. Completeness and Data Topicality

Personal data must be stored correct, complete and, if necessary, at the current status. Suitable measures must be taken to ensure that inapplicable, incomplete or outdated data are deleted, corrected, supplemented or updated.

4.5. Confidentiality and Data Security

Data secrecy applies to personal data. It must be handled confidentially when handled personally and secured by means of appropriate organizational and technical measures against unauthorized access, illegal processing and passing on, as well as accidental loss, modification and destruction.

5. ADMISSIBILITY OF THE DATA PROCESSING

The collection, processing and use of personal data is only permitted if one of the following permissions exists. Such a permission is also required if the purpose for the collection, processing and use of the personal data is to be changed vis-à-vis the original intended purpose.

5.1. Customer and Partner Data

5.1.1. Contractual Relations

Personal data of the interested parties, customers or partners concerned may be processed to justify, implement and terminate a contract. This also includes the support of the contractual partner, insofar as it is in connection with the contractual purpose. At the preliminary stage of a contract – in other words, during the initiation of contract negotiations – the processing of personal data is permitted for the preparation of offers, the preparation of purchase applications or the fulfilment of other requests of the interested parties leading up to the conclusion of a contract. Interested parties may be contacted during the contract negotiations by using the data they have provided. Possible limitations expressed by the interested parties must be observed. Section 5.1.2 applies to advertising measures that go beyond this purpose.

5.1.2. Data Processing for Advertising Purposes

The processing of data to fulfil a concern for information originating from the parties involved is principally permitted.

The processing of personal data for advertising purposes or for market and opinion research is permitted, insofar as this is compatible with the purpose for which the data were originally collected. The person concerned is to be informed about the use of his/her data for advertising purposes. If data are collected exclusively for advertising purposes, their specification by those concerned is voluntary. The person concerned should be informed about the voluntary nature of the specification of data for such purposes. In the context of the communication with the parties concerned, the consent of the person concerned is to be obtained for the processing of his/her data for advertising purposes. In the context of the consent, the person concerned should be able to choose between the available contact channels such as mail, electronic mail and telephone. If the person concerned objects to the use of his/her data for advertising purposes, then any further use of his/her data for this purpose is not permitted and must be blocked for such purposes. Restrictions going beyond this, which exist in some countries regarding the use of data for advertising purposes, must be observed.

5.1.3. Consent

Data processing can take place based on the consent of the party concerned. Before consenting, the party concerned must be informed in accordance with 4.1 of this guideline. The declaration of consent is to be obtained in writing or electronically and must be documented for the purpose of evidence.

5.1.4. Legal Permission

The processing of personal data is also permitted when national legislation demands, requires or permits the processing of data. The type and extent of data processing must be necessary for the legally authorized data processing and must comply with this legislation.

5.1.5. Legitimate Interest

The processing of personal data may also take place if it is required for the realization of a legitimate interest of the ROSEN Group. As a rule, legitimate interests are of a legal or economic nature. A processing of personal data based on a legitimate interest must not take place as long as there are indications that protection-worthy interests of the party concerned outweigh the interest served by the processing. The protection-worthy interests must be checked for every processing.

5.1.6. Particularly Protection-worthy Data

The processing of particularly protection-worthy personal data may only take place when it is required by law or the party concerned has given his/her explicit consent. Particularly protection-worthy are data about, e.g., ethnic origin, political opinions, religious or philosophical beliefs, trades union memberships, the health or sexual orientation of the party concerned, and any crimes he/she may have committed. The processing of these data are also permitted when it is absolutely necessary in order to assert, exercise of defend legal claims against the party concerned. If the processing of particularly protection-worthy data is planned, the Group Data Protection Officer is to be informed beforehand.

5.1.7. Automated Individual Decisions

Automated processing of personal data through which individual personality traits (e.g. creditworthiness) are assessed must not be the only basis for decisions with negative legal consequences or significant impairments for the parties concerned. The person concerned must be notified of the fact and the result of an automated individual decision and given the opportunity to make a statement. To avoid incorrect decisions, a control and a plausibility check by an employee must be ensured.

5.1.8. User Data and Internet

If personal data are collected, processed and used on websites or in apps, the persons concerned must be informed about this in appropriate data protection notices and, if applicable, references to cookies. The data protection notices, and, if applicable, cookie references must be integrated, so that they are easily recognizable for the persons concerned, directly accessible and constantly available.
If usage profiles are created for the evaluation of the usage behavior of websites and apps (tracking), then the persons concerned must be informed about this in all cases in the data protection notices. Person-related

tracking may only take place if the national law permits it or the person concerned has consented. If the tracking takes place under a pseudonym, then the person concerned should be given the opportunity to object in the data protection notices (opt-out).
If access to personal data is enabled in an area subject to registration on websites or apps, then the identification and authentication of the person concerned must be designed such that adequate protection is achieved for the respective access.

5.2. Employee Data

5.2.1. Data Processing for the Employment Relationship

For the employment relationship, those personal data may be processed that are required for the justification, implementation and termination of the employment contract.
During the initiation of an employment relationship, personal data of applicants may be processed. Following rejection, the applicant's data must be deleted, taking into consideration the periods required for legal proof, unless the applicant has consented in a further storing to a subsequent selection process. Consent is also required for use of the data for other application procedures or before the application is passed on to other companies of the ROSEN Group.
In an existing employment relationship, the data processing must always be related to the purpose of the employment contract, insofar as one of the following permissions for the data processing does not take precedence.
If during the initiation of the employment relationship or in an existing employment relationship the collection of further information by a third party is required from the applicant, the respective national statutory requirements must be taken into consideration. In case of doubt, consent of the person concerned is to be obtained.
For processing personal data that are closely related to the employment relationship but originally do not serve the fulfilment of the employment contract, a legal legitimation must exist in each case. That can be statutory requirements, collective agreements with employee representatives, employee consent or the legitimate interests of the company.

5.2.2. Legal Permission

The processing of personal employee data is also permitted when national legislation demands, requires or permits the processing of data. The type and extent of data processing must be necessary for the legally authorized data processing and must comply with this legislation. If there is legal room for maneuvering, the protection-worthy interests of the employee must be taken into consideration.

5.2.3. Consent

A processing of employee data can take place based on the consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consents are invalid. The declaration of consent is generally to be obtained in writing or electronically and properly documented in all cases. With an informed voluntary specification of data by the person concerned, consent can be assumed if national law does not prescribe any explicit consent. Before consenting, the person concerned must be informed in accordance with this guideline.

5.2.4. Legitimate Interest

The processing of personal employee data can also take place if this is required for the realization of a legitimate interest of the ROSEN Group. As a rule, legitimate interests are justified legally (e.g. the assertion, exercise or defense of legal claims) or economically (e.g. evaluation of companies).
A processing of personal data based on a legitimate interest must not take place if in an individual case there is an indication that protection-worthy interests of the employee outweigh the interest served by the processing. The existence of protection-worthy interests is to be checked for each processing.
Control measures that require a processing of employee data may only be implemented if there is a legal obligation to do so or a justified reason exists. Even with the existence of a justified reason, the proportionality of the control measure must be checked. The legitimate interests of the company in the implementation of the control measure (e.g. observance of legal provisions and internal company rules) must be weighed against a possible protection-worthy interest of the employee affected by the measure in the exclusion of the measure. Measures may only be implemented when they are appropriate. The legitimate interest of the company and the possible protection-worthy interests of the employee must be determined and documented before each measure. In addition, other requirements that exist pursuant to national law (e.g. co-determination rights of the employee representative and information rights of the person concerned) must be taken into consideration, if necessary.

5.2.5. Particularly Protection-worthy Data

Particularly protection-worthy personal data may only be processed under certain conditions. Particularly protection-worthy data are data concerning racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, and the health or sexual orientation of the person concerned. Based on national law, further data categories can be classified as particularly protection-worthy, or the content of the data categories can be filled out differently. Likewise, data concerning crimes may frequently only be processed under special conditions established by national law.
The processing must be explicitly permitted or prescribed based on national law. In addition, a processing can be permitted if it is necessary to enable the responsible body to fulfil its rights and obligations in the field of labor law. The employee can also explicitly consent to the processing voluntarily.
If the processing of particularly protection-worthy data is planned, the Group Data Protection Officer is to be informed beforehand.

5.2.6. Automated Decisions

If, during the employment relationship, personal data through which individual personality traits are assessed (e.g. in the framework of personnel selection, for performance evaluations etc.) are processed in an automated way, such an automated processing must not be the only basis for decisions with negative consequences or significant impairments for the employees concerned. To avoid incorrect decisions in automated processes, it must be ensured that a content-related verification of the facts is carried out by a natural person and that this verification is the basis for the decision. In addition, the employee concerned must be notified of the fact and the result of an automated individual decision and given the opportunity to make a statement.

5.2.7. Telecommunication and Internet

Telephone systems, e-mail addresses, Intranet and Internet are primarily provided by the company in the framework of operational tasking. They are regarded as work equipment and resource of the company. They may only be used in the framework of the respective valid legislation and internal company guidelines. In the case of permitted use for private purposes, the secrecy of telecommunications and the respective nationally applicable telecommunications law must be observed if they are used. General monitoring of telephone or e-mail communications or Intranet and Internet use does not take place. To defend against attacks on the IT infrastructure or on individual users, protective measures can be implemented at the transitions to the ROSEN network, which block technically damaging content or analyze the patterns of attacks. For reasons of security, the use of telephone systems, e-mail addresses, Intranet and Internet can be temporarily logged. Person-related analyses of this data may only take place with a concrete justified suspicion of a violation of laws or guidelines of the ROSEN Group. These controls may only be carried out by investigating departments, safeguarding the principle of proportionality. The respective national laws are also to be observed, as are the group-wide regulations existing at ROSEN for this purpose.

6. TRANSMISSION OF PERSONAL DATA

Transmission of personal data to recipients outside the ROSEN Group or to recipients inside the ROSEN Group is subject to the admissibility requirements for the processing of personal data according to this guideline. The recipient of the data must be obliged to only use these data for the defined purposes.

In the case of a transmission of data to a recipient outside the ROSEN Group in a third country, that country must ensure a level of data protection equivalent to this data protection guideline. This does not apply if the transmission takes place based on a statutory obligation. Such a statutory obligation can result from the law of the country where the respective ROSEN company that transmits the data has its head office or the law of the country where the respective ROSEN company has its head office recognizes the aim of the data transmission pursued with the statutory obligation of a third country.

In the case of a transmission of data from third parties to companies of the ROSEN Group, it must be ensured that the data may be used for the intended purposes.

If personal data are transmitted from a ROSEN company with head office in the European Economic Area to a ROSEN company with head office outside the European Economic Area (third country), then the data-importing company shall be obliged to cooperate with the supervisory authority responsible for it with all inquiries and requests and to observe the findings of the supervisory authority with regard to the transmitted data. The same applies for data transmissions by ROSEN companies from other countries. If you participate in an international certification system for binding group data protection regulations, you must ensure the cooperation provided there with the relevant auditing agencies and authorities. The participation in such certification systems is to be coordinated with the Group Data Protection Officer beforehand.

In the case of a violation of this data protection guideline by a data-importing company of the ROSEN Group with head office in a third country alledeg by an interested party, the data-exporting ROSEN company with head office in the European Economic Area undertakes to support the interested party whose data have been collected in the European Economic Area, both with the clarification of the facts as well as by ensuring the enforcement of its rights vis-à-vis the data-importing company of the ROSEN Group in accordance with this data protection guideline. Furthermore, the affected party is also entitled to assert its rights vis-à-vis the data-exporting company of the ROSEN Group. With an alleged violation, the data-exporting company must produce the evidence vis-à-vis the interested party that with a further processing of the data received, a violation of this data protection guideline is not attributable to the data-importing ROSEN company in a third country.

In the case of a transmission of personal data from a company of the ROSEN Group with head office in the European Economic Area to a ROSEN company with head office in a third country, the data-transmitting party shall be held liable vis-à-vis the interested party whose personal data was collected in the European Economic Area for any violations of this data protection guideline committed by the ROSEN company with head office in a third country, as if the violation had been committed by the data-transmitting party. Place of jurisdiction is the competent court at the domicile of the data-exporting party.

7. CONTRACT DATA PROCESSING

Contract data processing exists when a contractor is commissioned with the processing of personal data, without the responsibility for the associated business process being transferred to him. In these cases, a contract data processing agreement is to be concluded both with external contractors as well as between companies within the ROSEN Group. The commissioning company thereby retains the full responsibility for the correct implementation of the data processing. The contractor may only process personal data in the framework of the instructions of the customer. When the order is placed, the following specifications must be observed; the commissioning department must ensure their implementation.

a) The contractor is to be selected according to his/her suitability to guarantee the required technical and organizational protective measures.
b) The order is to be issued in written form, thereby documenting the instructions for the data processing and the responsibilities of the ordering party and the contractor.
c) The contract standards provided by the Group Data Protection Officer must be observed.
d) Before beginning the data processing, the ordering party must assure itself of the observance of the obligations by the contractor. In particular, a contractor can prove observance of the data processing requirements through presentation of appropriate certification. Depending on the risk of the data processing, the inspection is to be repeated regularly during the term of the contract, if necessary.

For a cross-border contract data processing, the respective national requirements for a transfer of personal data abroad must be fulfilled. In particular, the processing of personal data from the European Economic Area in a third country may only take place if the contractor proves a level of data protection equivalent to this data protection guideline.

8. RIGHTS OF PERSONS CONCERNED

Every person concerned can exercise the following rights. Their assertion is to be processed immediately by the departments determined for this within the ROSEN Group and must not lead to any disadvantages for the persons concerned.

a) The person concerned can demand information about which personal data of which origin are stored about him/her for what purpose. In an employment relationship, if according to the respective labor law farther-reaching rights of inspection of employer documents (e.g. personal file) are provided, then these remain unaffected.
b) If personal data are transmitted to a third party, information must also be provided about the identity of the recipient or about the categories of recipients.
c) If personal data are incorrect or incomplete, the person concerned can demand their correction or supplementation.

d) The person concerned is entitled to demand the deletion of his/her data if the legal basis for the processing of the data is missing or has been omitted. The same applies in the case that the purpose of the data processing has been omitted due to the expiration of time or due to other reasons. Existing safeguarding obligations and a deletion of conflicting protection-worthy interests must be observed.
e) The person concerned has a basic right of objection to the processing of his/her data, which is always to be taken into consideration when his/her protection-worthy interest based on a particular personal situation outweighs the interest served by the processing. This does not apply if a legal provision mandates the implementation of the processing.

In addition, every person concerned can assert his/her rights as a third-party beneficiary, as determined according to this guideline, if a company that has committed to observing the data protection guideline does not observe its requirements and, as a result, his/her rights have been violated.

9. CONFIDENTIALITY OF THE DATA PROCESSING

Personal data are subject to data secrecy. Any unauthorized collection, processing or use is prohibited for employees. Unauthorized is any processing that an employee undertakes without being entrusted with it and correspondingly authorized in the framework of the fulfilment of his/her tasks. The need-to-know principle applies: employees may only obtain access to personal data when and insofar as this is necessary for their respective tasks. This requires the careful distribution and separation of roles and responsibilities as well as their implementation and management in the framework of authorization concepts.
Employees must not use personal data for their own private or economical purposes, transmit it to unauthorized persons or make it accessible in any other way. Supervisors must instruct their employees at the beginning of the employment relationship about the obligation to ensure data secrecy. This obligation also continues to exist after termination of the employment relationship

10. SECURITY OF THE DATA PROCESSING

Personal data must be protected at all times against unauthorized access, illegal processing and distribution, as well as against loss, falsification and destruction. This applies regardless of whether the data processing is carried out electronically or in paper form. Before introducing new methods of data processing – in particular, new IT systems – technical and organizational measures for the protection of personal data must be defined and implemented. These measures must be guided by the state of technology, the risks emanating from the processing and the protection requirement for the data (determined through the information classification process). For this purpose, the responsible department can call, in particular, on its Information Security Officer and Data Protection Coordinator for advice. The technical-organizational measures for the protection of personal data are part of the group-wide Information Security Management system and must be continuously adapted to technical developments and organizational changes.

11. DATA PROTECTION CONTROL

Observance of the directives for data protection and the applicable data protection laws is regularly verified by means of data protection audits and other inspections. Implementation is the responsibility of the Group Data Protection Officer and the local Data Protection Coordinators. The results of data protection checks must be reported to the Group Data Protection Officer.

In the framework of the respective reporting obligations, the administrative council of ROSEN Swiss AG is to be informed about key results. At the request of the authorities, the results of data protection inspections are made available to the responsible Data Protection Supervisory Authority. In the framework of the powers to which it is entitled according to national law, the responsible Data Protection Supervisory Authority can also carry out its own monitoring of the observance of the regulations of this guideline.

12. RESPONSIBILITIES

Within their scope of responsibility, the senior management teams of the group companies are responsible for data processing. Consequently, they are obliged to ensure that statutory data protection requirements and those contained in the data protection guideline are taken into consideration (e.g. national reporting obligations). It is a management task of executive personnel to ensure proper data processing, while taking data protection into consideration by means of organizational, technical and personnel-related measures. The implementation of these requirements is the responsibility of the competent employee. In the case of data protection monitoring by authorities, the Group Data Protection Officer is to be informed immediately.

The respective management boards and plant management teams must nominate a Data Protection Coordinator for the Group Data Protection Officer. As regards organization, in consultation with the Group Data Protection Officer, this task can also be performed by one Data Protection Coordinator for several companies or plants. The Data Protection Coordinators are on-site contact partners for the protection of data. They can carry out inspections and must familiarize the employees with the contents of the data protection guidelines. The respective management boards are obliged to support the Group Data Protection Officer and the Data Protection Coordinators in their activities. The specialist personnel responsible for business processes and projects must inform the Data Protection Coordinators in a timely manner about new instances of the processing of personal data. In cases where data processing is planned that could entail particular risks to the personal rights of the persons concerned, the Group Data Protection Officer is to be involved from the outset, before the processing starts. In particular, this applies to particularly protection-worthy personal data. Executive management must ensure that their employees are trained to the required extent in data protection. In addition, improper processing of personal data or other violations of data protection laws are prosecuted in many countries and can involve claims for compensation. Violations for which individual employees are responsible can lead to labor law sanctions.

13. GROUP DATA PROTECTION OFFICER

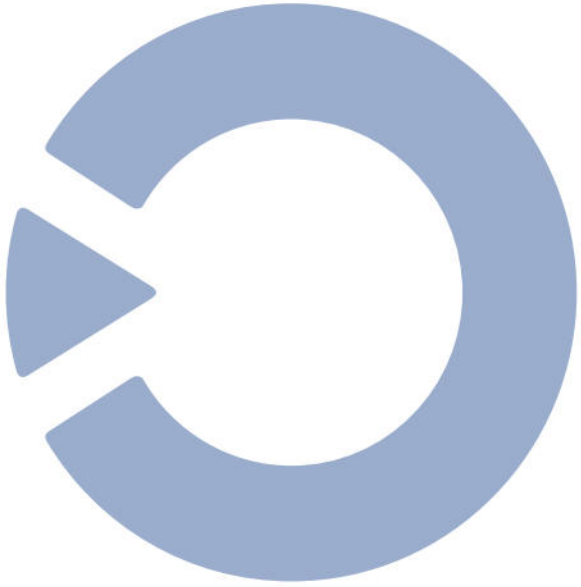
As an internal professional organ independent of instruction, the Group Data Protection Officer works towards compliance with national and international data protection regulations. He/she is responsible for the data protection guidelines and monitors their compliance. The Group Data Protection Officer is appointed by the administrative council of ROSEN Swiss AG. Principally, group companies that are obliged to do so also appoint the group officer as legal data protection officer. Specific exceptions must be coordinated with the Group Data Protection Officer.

The Data Protection Coordinators inform the Group Data Protection Officer in a timely manner about data protection risks. Every person concerned can contact the Group Data Protection Officer or the Data Protection Coordinator responsible for him/her with suggestions, inquiries, requests for information or complaints in connection with questions of data protection or data security. Upon request, inquiries and complaints are handled confidentially.

If the responsible Data Protection Coordinator cannot remedy a complaint or stop a violation of data protection guidelines, he/she must involve the Group Data Protection Officer. The decisions of the Group Data Protection Officer to remedy the data protection violation must be taken into consideration by the respective management boards. Inquiries from supervisory authorities also must always be brought to the attention of the Group Data Protection Officer.

You can contact the Group Data Protection Officer and his staff as follows:

ROSEN Swiss AG
Group Data Protection Officer
Obere Spichermatt 14 | 6370 Stans, Switzerland
E-Mail: cdpo@rosen-group.com



Obere Spichermatt 14 · 6370 Switzerland · Phone: +41-41-618-0300 · Email: rosen-stans@rosen-group.com
Data_Protection_Guideline_EN_18.1.6

cdpo@rosen-group.com