CHROMOS Group AG
Privacy Policy

Contents

Introduction

This policy governs the protection of personal data within the framework of the CHROMOS Group's business activities.

Protecting personal data is an important issue to the CHROMOS Group. That is why companies in the CHROMOS Group process the personal data belonging to their employees, clients and business partners in compliance with the applicable regulations on the protection of personal data and data security.

The CHROMOS Group is reliant upon data and information and the resulting electronic business processes. The accuracy, integrity and availability of data and information is of great importance to the CHROMOS Group.

1. Area of application

This policy will apply to all processing (see point 13 m)) of personal data (see point 13 k)) within the CHROMOS Group, regardless of the location of said processing.

2. Target audience for this policy / responsibilities / sanctions

To effectively ensure the processing of information and data security that is compliant with data protection regulations and reasonable responses to the concerns of data subjects (see point 13 d)), this policy is aimed at every employee within the CHROMOS Group.

The **management boards** of the CHROMOS Group companies will bear overall responsibility for data protection and for implementing the data protection requirements within each respective company. They are therefore obliged to ensure proper data processing in compliance with the statutory data protection requirements, and those contained in this Privacy Policy, through organisational, personnel and technical measures. The relevant employees will be responsible for implementing these instructions. In the event of data protection checks by the authorities, the relevant responsible Data Protection Officer must be notified immediately. Unless otherwise agreed, all members of the respective management board will be joint controllers (Art. 26(1) of the General Data Protection Regulation (GDPR)).

Each employee will be responsible for compliance with the data protection rules within the framework of the company guidelines in his or her area of responsibility, in particular for the ongoing implementation of this policy. All employees of the CHROMOS Group will also receive ongoing training regarding the data protection rules.

With regard to the monitoring of their own areas of responsibility, the **department managers** must also ensure that their staff (including temporary staff where applicable) and/or individuals involved in the processes are informed about this policy. In relation to data collection/processing within their division, they will also be responsible for

- providing the necessary material and human resources for compliance with the requirements laid down in the policy,
- ensuring proper monitoring of compliance with the requirements laid down in the policy,
- ensuring that obligations to inform data subjects are met,
- ensuring that the specified procedure descriptions are followed,
- ensuring that the specified data protection impact assessments are performed, and
- Informing the relevant responsible Data Protection Officers (see point 13 j)) regularly about the collection and processing of personal data within their department.

The **relevant responsible Data Protection Officers** (see point 13 j) of the CHROMOS Group companies will advise the management boards and other company employees regarding implementation of this policy and will check their compliance with it. They will keep a record of the processing activities undertaken by each CHROMOS Group company pursuant to Art. 30 of the GDPR and will process requests for information/rectification and any objections in relation to data protection from data subjects. At least once a year, they will review (see point 9) the technical and organisational data protection measures (see point 11) in collaboration with the IT security officer.

The **IT security officer** will organise and support the Data Protection Officers when creating the procedure logs. The IT security officer will propose technical and organisational measures to safeguard this policy for the CHROMOS Group. The measures will be documented in section 11. All measures pursuant to this policy will be reviewed regularly by the IT security officer and the review will be documented.

The **HR department** will satisfy employees' rights to information and inspection.

Any improper processing of personal data or other breaches of data protection law will also be prosecuted in many countries and can lead to claims for compensation. Infringements attributable to individual employees may result in employment law sanctions.

3. Basic principles for the processing of personal data

3.1. Fairness and legality

When personal data is processed within the CHROMOS Group, the data subject's (see point 13 d)) individual rights are safeguarded. Personal data will be collected and processed lawfully and fairly.

3.2. Purpose limitation

Personal data may only be processed for the purposes specified prior to collection of said data. Subsequent changes to the purpose are only possible to a limited extent and must be justified.

3.3. Transparency

The data subject (see point 13 d)) must be informed about the use of his or her data. Personal data must generally be collected from the data subjects themselves. Upon collection of the data, the data subject must be able to determine, or have been informed about, the following at a minimum:

- the identity of the data controller (see point 13 n))
- the purpose of the data processing
- third parties (see point 13 f)) or categories of third parties to whom the data may be transmitted.

3.4. Data avoidance and data economy

Prior to processing personal data, checks must be carried out to determine whether and to what extent this is necessary to achieve the desired purpose behind the processing. Wherever possible to achieve the purpose, and where the expense and effort involved is proportionate to the desired purpose, anonymised (see point 13 b)) or statistical data should be used. Personal data may not be stored for potential future purposes, except where this is required or permitted by national law.

3.5. Erasure

Personal data that is no longer required following expiry of the statutory retention period or that required by the relevant business process (see point 13 h)) must be erased. Where, in the individual case, there are indications of legitimate interests, the data must continue to be stored until the legitimate interest has been legally clarified.

3.6. Factual accuracy and data currency

Stored personal data must be accurate, complete and, where applicable, up to date. Appropriate measures must be taken to ensure that data that is inaccurate, incomplete or out of date is erased, corrected, supplemented or updated.

3.7. Confidentiality and data security

Data secrecy will be safeguarded with regard to personal data. In face-to-face dealings therefore, personal data will be treated as confidential and will be protected against unauthorised access, unlawful processing or disclosure and inadvertent loss, modification or destruction through appropriate technical and organisational measures.

4. Legitimacy of the processing of personal data

4.1. Data processing principles

Personal data may only be processed within the CHROMOS Group to the extent permitted by law. Such information should only ever be collected and processed where necessary to do so in order to fulfil an operational task (see point 13 h)) and in direct connection with the purpose of the processing.

Personal data may only be processed with one of the permissions described in more detail below, namely

- with the data subject's consent (see point 4.2),
- to meet customer requests or where consent has been given to advertising (see point 4.3),
- where necessary to conclude/fulfil a contract (see point 4.4)
- where permitted by law (see point 4.5) or

- where there is a legitimate interest without this being overridden by the interests or fundamental rights and freedoms of the data subject (see point 4.6).

The respective purpose for the data must be documented in writing before any new type of processing is introduced by the controller of the data usage. A change of purpose will then only be permitted where the processing is compatible with the purposes for which the data was originally collected. The evaluation criteria used during a change of purpose must be checked individually. For proper proof, this check must also be documented.

Prior to introducing any new form of processing of personal data, checks must also be carried out to determine whether or not the purpose of the processing could be achieved just as well with anonymisation (see paragraph 13 b)) or pseudonymisation of the data and, if so, preference must be given to processing in this way.

If other bodies request information about data subjects, such information may only be provided without the data subject's consent where there is a legal obligation or where the collecting/processing company has a legitimate interest that justifies the disclosure and the requesting party's identity has been clearly established. In cases of doubt, the relevant responsible Data Protection Officer should be consulted.

The provisions in section 4.8 will apply to personal data processed via the internet.

Employee data will be processed in accordance with the provisions in section 4.9.

4.2. Consent

Data may be processed based on the data subject's consent.

Consent will always be accepted in the knowledge that the data subject's consent to the processing of personal data is voluntary. Before consent is provided, the data subject must be informed in accordance with point 3.3. An unmistakeable statement of will is required from the data subject in the form of a declaration or other clear confirmatory act by which the data subject grants his or her consent to the processing of data about him or her.

The consent must be demonstrable (Art. 7(1) of the GDPR). With this in mind, declarations of consent must be obtained and stored, and/or retained, in writing or electronic text form. Where consent is obtained verbally, e.g. by telephone, in cases agreed upon with the relevant responsible Data Protection Officer, this must be properly documented and the documentation must be saved and/or retained.

Consent granted prior to 25 May 2018 will continue to be effective providing it meets the basic requirements of the GDPR.

4.3. Data processing for advertising purposes

Customer retention or promotional measures require additional legal requirements. Data may be processed for advertising or market and opinion research purposes where this is compatible with the purpose behind collecting the data originally. If data is collected solely for advertising purposes then provision thereof by the data subject will be optional. The data subject must be informed about the option to provide information for this purpose or not. Consent (see point 4.2) must be obtained from the data subject for the processing of his or her data for advertising purposes. As part of the consent, the data subject should be able to choose between the available contact channels, such as by post, email and telephone.

If a data subject contacts a CHROMOS Group company with an information-related request (e.g. request for information to be sent about a product or service) then data may be processed in order to fulfil that request.

If the data subject objects to the use of his or her data for advertising purposes, any further use of his or her data for that purpose will not be permitted and it must be locked for said purpose.

4.4. Data processing for a contractual relationship

The processing of personal data for the conclusion, fulfilment or termination of a contract is lawful (Art. 6(1)(b) of the GDPR). This includes supporting the contracting partner where this is connected to the purpose of the contract.

For example, within the framework of existing contracts, the contracting partner's contract data, master data and accounting data, such as its name and address, may be processed regularly, for instance to send invoices or deliveries.

During the contract negotiation phase, personal data may be processed to create quotes, prepare contract documentation or to meet other requirements of the interested parties aimed at concluding a contract. This will include data processing activities required to initiate, or within the framework of, employment relationships.

During the contract initiation, interested parties may be contacted using data they have provided. Any limitations expressed by the interested parties must be complied with.

For additional advertising initiatives, the requirements set out in point 4.3 must be met.

4.5. Data processing permitted by law

Data processing will also be lawful where necessary as a result of, or based on, legal requirements. The legal basis for such processing may be provisions of national or union law to which we, or the acting persons in each case, are subject, Art. 6(1)(c) of the GDPR).

The nature and scope of the data processing must be necessary for the legally permitted data processing and must comply with these legal requirements.

Examples of this include commercial law and tax law regulations which sometimes impose extensive documentation and retention obligations on us.

4.6. Overriding legitimate interests

Personal data may also be processed where this is necessary to safeguard our legitimate interest or that of a third party (see point 13 f)). In particular, legal (e.g. enforcement of outstanding claims) and economic (e.g. avoiding default in performance) interests are to be regarded as “legitimate interests”.

Personal data may not be processed on the basis of a legitimate interest however where, in the individual case, there is an indication of the data subject’s legitimate interests overriding the interest in the processing (Art. 6(1)(f) of the GDPR). The data subject’s legitimate interests must be verified in each case however. A comprehensive weighing up of interests must then determine which interests prevail – ours or those of the data subject. In cases of doubt, the relevant responsible Data Protection Officer should be consulted.

4.7. Processing of particularly sensitive information

Particularly sensitive data (see point 13 c)) may only be processed where legally required or where the data subject has expressly consented to the processing. Such data may also be processed where strictly necessary to assert, exercise or defend legal claims in respect of the data subject.

Where the processing of particularly sensitive information is proposed, the relevant responsible Data Protection Officer (see point 13 j)) must be notified.

Credit card information will be processed in compliance with the PCI DSS compliance requirements in accordance with the measures outlined in Appendix 1 to this policy.

4.8. Userdata and internet

If personal data is processed in CHROMOS Group apps or on websites, the data subjects must be informed about this in data protection notices and, where applicable, cookie notices. The data protection notices and, where applicable, cookie notices must be incorporated such that they are easily identifiable, directly accessible and always available to the data subjects.

If usage profiles are created to analyse the behaviour of website and app users (tracking), the data subjects will always be informed of this in the data protection notices. Tracking that is specific to an individual may only take place with the data subject's consent. If tracking is performed using an alias, the data subject should be given the option to object (opt out) in the data protection notices.

If access to personal data is enabled on websites or apps within an area requiring registration, then identification and authentication of the data subjects must be set up such that an adequate level of protection is afforded for the access in question.

4.9. Processing to conclude/within an employment relationship

When initiating and implementing employment relationships, personal data required to establish, implement and terminate the employment contract may be processed.

During the initiation of an employment relationship, the personal data of applicants may be processed. Following rejection, the applicants' data must be erased taking into account retention periods required under legislation on proof, except where the applicant has consented to further storage of his or her data for a subsequent selection process. Consent will also be required to use the data for subsequent application procedures or prior to forwarding the application to other CHROMOS Group companies.

Within existing employment relationships, the data processing must always be related to the purpose of the employment contract in the absence of any of the other grounds for legitimacy specified above in this section 4.

If, during the initiation of the employment relationship, or within an existing employment relationship, the collection of additional information is required via the applicant for a third party (see point 13 f)), the data subject's consent must be obtained in cases of doubt.

There must be a legal basis in each case for processing personal data within the context of the employment relationship but which does not originally serve to fulfil the employment contract. This may be statutory requirements, collective rules to be established with employee representatives within the data protection requirements, employee consent or the existence of an overriding legitimate interest on our part (see point 4.6). Where there is statutory or agreed power to act, consideration must always be given to the employee's legitimate interests.

Monitoring measures that require the processing of employee data may only be implemented where there is a statutory obligation or reasonable grounds to do so. Even where there are reasonable grounds, the reasonableness of the monitoring measures must be reviewed. The company's legitimate interest in implementing the monitoring measure (e.g. compliance with legal provisions and internal company rules) must be weighed against a potential legitimate interest of the employee affected by the measure in being excluded from the measure and said measure may only be implemented where it is reasonable to do so. The company's legitimate interest and potential legitimate interests of the employees must be ascertained and documented prior to every measure. Any rights to participation by employee representatives and the data subject's rights to information must be taken into account during this process.

The company will provide employees with telephone systems, email accounts, intranet, internet access and internal social networks for the performance of operational tasks. These are work tools and company resources. They may be used within the framework of the legal requirements applicable in each case and the company's internal rules. Where personal use is permitted, telecommunications secrecy and telecommunications legislation must be complied with where applicable.

There will be no general monitoring of the telephone and email communication or intranet and internet use. To prevent attacks on the IT infrastructure or individual users, protective measures may be implemented at the crossovers to the CHROMOS Group network which block technically harmful content or analyse the patterns of attacks. For security reasons, the use of telephone systems, email accounts, the intranet and internet, and internal social networks may be temporarily logged. Analyses of this data relating to specific individuals may only be performed in the event of a specific justified suspicion of a breach of the law or the CHROMOS Group policies or those of its companies. Such checks may only be performed by the investigating departments having due regard to the principle of proportionality. The relevant legislation must also be complied with in each case, as must any existing company rules.

5. Transmission of personal data

A transmission of personal data to recipients outside the CHROMOS Group, or to recipients within the CHROMOS Group, will be subject to the conditions governing the admissibility of personal data processing in accordance with section 4. The recipient of the data must be obliged to only use said data for the purposes specified.

In the event of data being transmitted to a recipient outside the CHROMOS Group in a third country (see point 13 g)), a level of data protection equivalent to that in this privacy policy must be ensured by them. This will not apply where the transmission takes place on the basis of a statutory obligation. Such a statutory obligation may arise under national law or national law may acknowledge the purpose behind transmission of the data in the statutory obligation of a third country.

In the event of data being transmitted to CHROMOS Group companies by third parties, steps must be taken to ensure that the data may only be used for the intended purpose.

6. Obligations during order processing

Order processing is when a contractor is commissioned to process personal data without bearing responsibility for the associated business process. In such cases, an agreement regarding the order processing must be concluded with external contractors and between CHROMOS Group companies. In so doing, the commissioning company retains full responsibility for the correct performance of the data processing. The contractor may only process personal data within the framework of the principal's instructions. The following requirements must be met when placing the order and the commissioning division must ensure the implementation thereof.

a) The contractor must be selected based on its ability to ensure the necessary technical and organisation protective measures.
b) The order must be placed in text form. In so doing, the data processing instructions and the responsibilities of the principal and the contract must be documented.
c) The contract standards provided by the relevant responsible Data Protection Officer must be complied with.
d) Before commencing the data processing, the principal must ensure that the contractor is complying with the obligations. A contractor may provide evidence of compliance with the requirements in particular by providing a suitable certification or some other appropriate proof of data security. Depending on the risk involved in the data processing, this check may need to be repeated during the contract term.
e) In the case of cross-border contract data processing, the statutory requirements for the disclosure of personal data abroad must be fulfilled. In particular, personal data may only be processed in a third country outside the European Economic Area if the contractor provides evidence of a level of data protection that is equivalent to that provided for in this privacy policy. Suitable instruments may be:
    (1) Agreement with the EU standard contractual clauses on contract data processing in third countries between the contractor and the potential subcontractors,
    (2) The contractor's participation in a certification system recognized by the EU in order to create an adequate level of data protection.
    (3) Acknowledgement of the contractor's binding company regulations to create an adequate level of data protection by the data protection supervisory authority.

7. Data subjects' rights

Every data subject may exercise the following rights. Any exercise of these rights must be processed immediately by the responsible department and may not result in any detriment to the data subject.

a) The data subject may request information about which personal data is being held about them, from what source and for what purpose. Where additional rights to inspect documents held by the employer (e.g. personnel records) exist under employment law within the framework of an employment relationship, these will remain unaffected.
b) If personal data is transmitted to third parties, information must also be provided about the recipient's identity or about the categories of recipients.
c) If personal data is incorrect or incomplete, the data subject may ask for it to be corrected or supplemented.
d) The data subject may object to the processing of his or her personal data for advertising purposes or for market or opinion research. In the case of an objection to such purposes, his or her data must be blocked.
e) The data subject is entitled to ask for his or her data to be erased where there is no legal basis for the data processing or where the legal basis has lapsed. The same will apply where the purpose of the data processing has lapsed due to the passage of time or for any other reason.

Existing retention obligations and any legitimate interests preventing an erasure must be complied with.

f) The data subject has a general right to object to the processing of his or her data if his or her legitimate interest overrides the interest in the processing due to his or her particular personal situation. This will not apply in the case of a legal obligation to carry out the processing.

8. Confidentiality

Personal data is subject to data secrecy. All CHROMOS Group employees are prohibited from unauthorised processing. Unauthorised processing will be any processing undertaken by an employee without being commissioned and authorised accordingly to do so during the course of his or her duties.

Employees may only be granted access to personal data where, and insofar as is, necessary for their respective duties. This requires the careful division and separation of roles and responsibilities, as well as their implementation and maintenance, within authorisation concepts.

Employees may not use personal data for their own private or commercial purposes, transmit the same to unauthorised parties, or make said data accessible to those parties by any other means.

At the start of their employment, all employees will be briefed regarding the obligation to maintain data secrecy and will be obliged to do so. This obligation will continue to apply even after termination of the employment relationship.

9. Data protection check / activity report

Compliance with the privacy policy and applicable data protection legislation will be monitored regularly, at least once a year, in data protection checks. The relevant responsible Data Protection Officer in each case will be responsible for conducting these checks, where applicable with the help of the IT security officers or possibly other company departments having audit permissions or external auditors commissioned to carry out the checks.

The relevant responsible Data Protection Officer in each case will summarise the results once a year in an activity report which must include the following points at a minimum:

- new procedure descriptions
- any privacy-related incidents
- any requests regarding specific individuals

In addition, a list of the requests to erase and amend personal data to be documented by the respective responsible Data Protection Officer must be appended to the activity report.

The management boards of the CHROMOS Group companies must be informed about the key results from the data protection checks in each case. Upon request, the results of the data protection checks

will be made available to the relevant data protection supervisory authorities. As part of the authority granted to it under national law, the relevant data protection supervisory authority may also conduct its own checks on compliance with the requirements of this policy.

10. Privacy-related incidents

Every employee must report any breaches of this privacy policy or other requirements to protect personal data (privacy-related incidents, see point 13e)) to their respective superiors and the relevant data supervisory authority immediately.

In the case of

- the unlawful transmission of personal data to third parties,
- unlawful access to personal data by third parties, or
- the loss of personal data,

where the privacy-related incident results in a risk to the data subject, the relevant responsible Data Protection Officer will organise the report provided for under Art. 33 of the GDPR to the responsible supervisory authority.

Where

- there is a high risk to the data subject's rights and freedoms as a result of the privacy-related incident,
- there are no suitable technical and organisational measures preventing unauthorised access to personal data (e.g. encryption), and
- no effective damage limitation measures have been taken to eliminate the high risk incurred at the time of the privacy-related incident,

the relevant responsible Data Protection Officer will organise the communication to the data subjects provided for in Art. 34 of the GDPR.

11. Technical and organisational security measures

Personal data must be protected against unauthorised access, unlawful processing or disclosure and loss, tampering or destruction at all times. This will apply regardless of whether data processing is performed electronically or in paper format. Prior to introducing new data processing procedures, in particular new IT systems, technical and organisational measures to protect personal data must be established and implemented. Such measures must be based on state-of-the-art technology, the risks posed by the processing and the level of protection required for the data (see protection levels pursuant to section 12).

The measures will be reviewed annually and amended as necessary. The review and any changes will be documented.

The following technical and organisational measures are in place within the CHROMOS Group companies:

Physical access controls	Access by individuals to rooms is restricted to prevent unauthorised persons gaining access to the data processing systems on which personal data is processed or used.	• Protection level A data: Building locking system or caretaker; rooms within the building not lockable, normal workstations • Workstations with access to protection level C and D data; additional lockable room doors, • Server rooms; intruder detection system, secured access with log, no windows, for data of all protection levels
System access controls	Restricted access to data and data processing devices to prevent unauthorised parties from being able to use data processing systems	• Protection level A-C data; normal workstation (incl. virtual environment) with AD controls and no external access. • Protection level A and B data; normal workstation with external access via the web. Additional separate security layer (NetScaler). • Server access; for data of all protection levels, separate authentication (either AD plus admin AD or AD for PC for local server login)
Data access controls	Restricted access to data within an application to ensure that only individuals authorised to use a data processing system can access the data underlying their data access authorisation, and that personal data cannot be read, copied, modified or removed without authorisation during the processing and use or after being stored .	• Application for protection level A data: no allocation of permissions and roles • Application for protection level B data: simple application login • Application for protection level C data: permissions and roles concept • Application for protection level D data: permissions and roles concept, two-factor authentication • For personal data processing of all protection levels of a public law nature (social security, employment office, court, etc.), the data access controls stipulated by the public law authority must be used.

Transfer controls	Steps must be taken to prevent personal data from being read, copied, modified or deleted without authorisation during electronic transmission, during transportation or when stored on data media and that it is possible to determine where such data is to be transmitted within the data processing system.	• Protection level A and B data: no additional restrictions, transport encryption when transmitted via the web (https) • Protection level C data: additional transmission logging (logged in Microsoft Navision) • Protection level D data: additional content encryption • For personal data processing of all protection levels of a public law nature (social security, employment office, court, etc.), the transfer controls stipulated by the public law authority must be used.
Data entry controls	Steps must be taken to ensure that it will be subsequently possible to check and verify whether personal data was entered, modified or erased, and by whom.	• Protection level A data: data entry controls are not necessary • Protection level B and higher data: logging of processing activities • For personal data processing of all protection levels of a public law nature (social security, employment office, court, etc.), the data entry controls stipulated by the public law authority must be used.
Order controls	Steps must be taken to ensure that personal data that is processed under contract is processed in accordance with the Principal's instructions.	• Creation of a data security concept (TOM) based on the protection level in accordance with this list
Availability controls	Steps must be taken to ensure that personal data is protected against accidental destruction or loss.	• Protection level A data: virus protection • Protection level B and higher data: plus snapshots, backup concept • Protection level C and higher data: plus air conditioning system, UPS • Protection level D and higher data: plus storage at separate locations • For personal data processing of all protection levels of a public law nature (social security, employment office, court, etc.), the availability controls stipulated by the public law authority must be used.

Separation requirements	Steps must be taken to ensure that personal data that is collected for different purposes can be processed separately.	• For data of all protection levels: separation by client, company codes

12. Protection levels

To enable analysis of the technical and organisational security measures (see point 11) in terms of adequacy, personal data will be divided into the following damage classes/protection levels depending on the potential for damage (severity of the potential impact to legitimate interests):

Level A:
Freely accessible data to which access is granted without the person consulting the data having to prove a legitimate interest, e.g. address books, list of members, print and online directories.

Level B:
Personal data that, if misused, no particular impact would in fact be expected but data for which a legitimate interest is required in order to view it, e.g. public files with restricted access, customer orders, contracts with business partners.

Level C:
Personal data that, if misused, may impact upon the data subject in his or her position within society or his or her financial circumstances ("reputation"), e.g. income, social security benefits, property tax, misdemeanours, employment contracts (excluding health-related data).

Level D:
Personal data that, if misused, may significantly impact upon the data subject in his or her position within society or his or her financial circumstances ("existence"), e.g. serious misdemeanours, performance appraisals, results of psychological and medical examinations, debts, attachments, insolvencies.

Level E:
Data that, if misused, may affect the health, life or freedom of the data subject, e.g. data about people who may be potential victims of a criminal offence.

13. Definitions

a) **Adequate level of data protection** in third countries will be a level of protection in a non-EU country which has been approved by the EU Commission under which the core elements of privacy, as agreed upon unanimously within the EU member states, are predominantly protected. The EU Commission will base its decision on all of the circumstances that play a role

in the data transmission or a category of data transmissions. This will include an evaluation of the national legislation and the professional ethics and security measures applicable in each case.

b) **Anonymised data** is data which can no longer be connected to a person, or where such a connection can only be restored with a disproportionate amount of time, cost and effort.

c) **Particularly sensitive information** is information about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership or the health or sex life of the data subject. Other categories of data may be classified as particularly sensitive under national law or the content of the categories may differ. Similarly, information about criminal offences may often only be processed under special conditions set by national law.

d) **Data subject**, for the purposes of this policy, will mean any individual about whom data is processed.

e) **Privacy-related incidents** are all incidents in which there are reasonable grounds to suspect that personal data has been unlawfully exposed, collected, modified, copied, transmitted or used. This can relate to both actions by third parties and by employees.

f) **Third party** is anyone other than the controller and the data subject. Contract data processors are not third parties within the EU for the purposes of data protection legislation because they are legally assigned to the controller.

g) **Third countries**, for the purposes of this privacy policy, will be all countries outside the European Union and EEA. Countries whose data protection level has been acknowledged by the EU Commission as adequate are excluded.

h) **Necessary**: the processing of personal data will be deemed necessary where the permitted purpose or legitimate interest cannot be achieved without the personal data in question, or can only be achieved without said data with a disproportionate amount of expense and/or effort.

i) **European Economic Area (EEA)** is an economic area associated with the EU to which Norway, Iceland and Liechtenstein belong.

j) **Respective responsible Data Protection Officer** will be the Data Protection Officer appointed for the CHROMOS Group company in question.

k) **Personal data** is all information about a specific or identifiable individual. An individual is identifiable, e.g. when a connection to a person can be restored by combining information with additional knowledge, even where such knowledge is only available by coincidence.

l) **Transmission** means any disclosure of protected data by the controller to third parties.

m) **Processing of personal data** is any procedure, carried out with or without the help of automated processes, to collect, save, organise, retain, modify, request, use, forward, transmit, distribute or combine and compare data. This also includes disposing of, erasing and blocking data and data media.

n) **Controller** will be the legally independent CHROMOS Group company whose business activities arrange the processing measure in question.

Appendix 1: PCI DSS Compliance

Credit card data is processed within the CHROMOS Group in compliance with the following PCI DSS compliance requirements:

- SAQ 12.8.1:
  A list of service providers must be maintained. The list must include a description of the services provided in each case. The list must be maintained by IT security. All department heads are obliged to report any changes regarding service providers to IT security immediately.

- SAQ 12.8.2:
  Every service provider must conclude a written agreement with the CHROMOS Group in question regarding the protection of cardholder data. IT security must review the agreement and the guidelines for implementing the agreement.

- SAQ 12.8.3:
  IT security must establish a procedure which must be complied with when selecting service providers.

- SAQ 12.8.4:
  IT security will review service providers' PCI DSS compliance once a year and will document the same.

- SAQ 12.8.5:
  IT security will document all PCI DSS requests and, in so doing, will note down the responsibility (in-house or service provider).

- SAQ 12.10.1:
  IT security will ensure that any disruptions are implemented within the framework of the incident response procedure.