Teufelberger data protection guidelines

Table of Contents

1 Purpose

The Teufeberger Group undertakes to comply with data protection laws within the scope of their social responsibility. These data protection guidelines apply for the Teufelberger Group worldwide. The compliance with data protection is a basis for trustworthy business relationships and the reputation of the Teufelberger Group as an attractive employer.
Data protection guidelines create the required framework conditions for data transmissions[1] between Group companies worldwide. They ensure that there is an appropriate data protection standard for cross-border data traffic as required by EU general data protection regulations (GDPR) and those required by the respective national laws and for countries where there are no appropriate legal standards for data protection.

2 Area of application and changes to data protection guidelines

The data protection guidelines apply for all companies in the Teufelberger Group, i.e. for Teufelberger Holding AG and all associated companies including their employees.

The data protection guidelines extend to all processing of person-related data[2]. Anonymized[3] data, e.g. for statistical analyses or research, are not subject to these data protection guidelines.

Individual Group companies are not entitled to determine regulations deviating from these data protection guidelines. Supplementary data protection guidelines may only be determined in agreement with the authorized Group data protection officer (GDPO) should these be required for compliance with the respective national law. Any change to these data protection guidelines are to be determined only with the agreement of the GDPO.

3 Validity of statutory law

These data protection guidelines contain the provisions of the GDPR as well as the application of the national legislation. It supplements and specifies the data protection law of the respective countries. The contents of these data protection guidelines also apply should there be no corresponding statutory law. Existent reporting obligations required by statutory law for processing of data need to be observed.

Each company of the Teufelberger Group is responsible for compliance with these data protection guidelines and the legal obligations. Should there be reason to believe that legal obligations conflict with the obligations arising from these data protection guidelines, then the Group company concerned is to notify the GDPO without undue delay. Should national legal provisions contravene the data protection guidelines, then the Teufelberger Holding AG is to find a practical solution together with the Group company concerned complying with the objectives of the data protection guidelines.

4 Principles applicable to the processing of person-related data

4.1 Fairness and legitimacy

The processing of person-related data requires the compliance with the personal rights of those concerned[4]. Person-related data needs to be collected and processed in a legitimate and fair manner.

4.2 Appropriate purpose

The processing of person-related data is only permitted on the basis of the purpose established for the collection of the data. Retrospective changes to the purpose are restricted and require justification.

[1] See 15.1
[2] See 15.2
[3] See 15.3
[4] See 15.4

4.3 Transparency

The person concerned is to be notified of the use of their data. In principle person-related data is to be compiled together with those concerned. The person concerned by the collection of data needs to be aware or be appropriately notified of the following minimum information:

- The identity of the responsible office5
- Purpose of the data processing
- Third parties or category of third parties also receiving the data transmission

4.4 Data avoidance and minimization

The processing of person-related data needs to be examined as to whether and to what extent this is necessary to achieve the required purpose of the processing. Should it be possible for the achievement of the purpose and the effort involved is in relation appropriate to the purpose, then anonymized or statistical data is to be used.
Person-related data may not be stored for use in potential purposes in the future unless this is prescribed or permitted by statutory law.

4.5 Deletion

Person-related data which is no longer required on expiry of the legal or business related prescribed retention periods[6] are to be deleted. Should in individual cases there be aspects related to data protection or data of historical significance, then the data is to remain stored until these data protection aspects are legally clarified.

4.6 Data accuracy and topically

Person-related data is to be stored in a correct, complete and if required up-to-date manner. Appropriate measures are to be undertaken to ensure that data which is no longer applicable, incomplete or obsolete is deleted, corrected, supplemented or brought up to date.

4.7 Data confidentiality and security

Person-related data is subject to data privacy. The data is to be handled confidentially and appropriate organizational and technical measures controlled by authorized access, secure from unauthorized processing or transfer as well as any accidental loss, alteration or destruction.

5 Data reliability and processing

The collection, processing and use of person-related data is only then permitted should one of the following authorized circumstances exist. Such circumstances are also required should the purpose of the collection, processing and use of person-related data is changed in respect of the original intended purpose.

5.1 Customer and partner data

5.1.1 Data processing for a contractual relationship

The person-related data of those concerned, customers or partners, may be processed for the creation, implementation and termination of a contract. This also includes the maintenance of a contractual relationship, provided it is commensurate with the contractual purpose. In the preliminary stages of a contract - that is in the preliminary approach - the processing of person-related data for drawing up an offer, preparation of a purchase order or the fulfillment of requirements related to the conclusion of a contract is permitted. The parties may be contacted by using the data they provided

[5] See 15.5
[6] See 15.6

during the contractual preparation phase. Any probable restrictions expressed by the parties involved require compliance. Any additional advertising measures require compliance with the following under 5.1.2.

5.1.2 Data processing for advertising purposes

Should the person concerend approach a company of the Teufelberger Group for information (e.g. requesting the dispatch of information material on a product), then data processing is permitted for the fulfillment of this request.
Uncalled for customer retention or advertising measures are subject to additional legal requirements. Processing of person-related data for the purpose of advertising or market and opinion research is permitted provided it reconciles with the original purpose of data compilation. The person concerned is to be advised of the use of their data for advertising purposes.

The person concerned is to be advised the disclosure of data for this purpose is of a voluntary nature. Consent[7] to the processing of their data for advertising purposes is to be obtained of the person concerned while in communication with that person. The person concerned is to have the option of choosing between the available contact channels such as post, electronic mail and telephone regarding the scope of the consent (for consent see 5.1.3).

Should the person concerned disagree with the use of their data for advertising purposes, then any further use of their data for those purposes is not permitted and are to be blocked for those purposes. Any additional restrictions existing in some countries in respect of the use of data for advertising purposes need to be observed.

5.1.3 Consent to data processing

Data processing may proceed based on the consent of the person concerned. The person concerned is to be advised before their consent pursuant to 4.3 of these data protection guidelines. In principle the declaration is to be obtained in writing or by electronic means for proof of consent. Consent may be obtained verbally under certain circumstances, such as during consultation by telephone. The consent is to be recorded in writing.

5.1.4 Data processing based on legal authorization

Processing of person-related data is also permitted when national legal provisions require, assume or permit processing. The nature and extent of data processing are essential for lawful data processing and are to comply with these legal provisions.

5.1.5 Data processing based on a legitimate interest

Processing of person-related data is also permitted when required to realize a legitimate interest of the Teufelberger Group. Legitimate interests are as a rule legal (e.g. enforcement of outstanding claims) or economic (e.g. prevention of breaches of contract). Processing of person-related data based on a legitimate interest is not permitted when in an individual case there are indications that the legitimate interests of the person concerned prevail over the interest in processing. The legitimate interests need to be reviewed for every processing.

5.1.6 Processing of highly sensitive data

Processing of highly sensitive[8] person-related data is only permitted when required by law or the person concerned explicitly agrees.
Processing of these data is also permitted when it is mandatory in order to assert, exercise or maintain legal claims against the person concerned.
Should processing of highly sensitive data be planned then the GDPO is to be advised in advance.

[7] See 15.7
[8] See 15.8

5.1.7 User data and internet

Should person-related data be collected, processed and used then the persons concerned need to be advised by data protection references or cookie notices. The data protection references or cookie notices are to be integrated in such a way that they are easily identifiable, directly accessible and constantly available to the persons concerned.

Should user profiles be compiled from websites and apps for the evaluation of user behaviour (tracking) then the persons concerned are to be advised in the data protection references in each case. Person-related tracking may only take place when permitted by national law or the person concerned agrees.
Should websites or apps permit access to person-related data where registration in a mandatory section, then identification and authentication of the persons concerned need to be designed in such a way that adequate protection is obtained for the respective access.

5.2 Employee data

5.2.1 Data protection for the employment relationship

Person-related data relating to the employment relationship may be processed that is required for the justification, implementation and termination of the employment contract.
Person-related data of applicants may be processed when initiating an employment relationship. The data of the applicant is to be deleted after rejection under consideration of evidential deadlines, unless the applicant agrees to continued storage for a later selection process. Consent is also required for the utilization of data for further application procedures or prior to transferring the application to other Group companies.
Data processing is always to refer to the purpose of the employment contract when there is an existing employment relationship provided any of the following facts for permitting data processing do not intervene.
Should collection of additional information on the applicant/employee from a third party be required during the initiation of the employment relationship or in an existing employment relationship, then the respective legal requirements need to be taken into account. In case of doubt approval of the person concerned is to be obtained.
Legal legitimation is required for the processing of person-related data in context of the employment relationship, though not directly serving the fulfillment of the employment contract. This may be legal requirements, collective arrangements with employee representatives, an approval of the employee or the legitimate interests of the company.

5.2.2 Data processing based on legal authorization

Processing of person-related data of employees is also permitted when
national legal provisions require, assume or permit data processing. The nature and extent of data processing are essential for lawful data processing and are to comply with these legal provisions.
Should there be legal scope of action then the legitimate interests of the employee are to be taken into consideration.

5.2.3 Collective arrangements for data processing

Should processing exceed the purpose of concluding the contract then it is also legitimate when permitted by collective arrangements. Collective arrangements are agreements between employer and employee representatives within the scope of the respective labour law options. The arrangements are to encompass the specific purpose of the desired processing and their structure in compliance with the national data protection law.

5.2.4 Consent to data processing

Processing of employee data may be concluded when based on the approval of the person concerned. Declarations of approval are to be voluntary. Involuntary approvals are not effective. In principle the declaration is to be obtained in writing or by electronic means for proof of consent. Should this not be possible due to exceptional circumstances then the approval may be granted verbally. The consent is to be properly recorded in writing in each case. An approval by the person concerned may be assumed in case of voluntary information on data when national law does not prescribe an explicit approval. The person concerned is to be advised before their consent pursuant to 4.3 of these data protection guidelines.

5.2.5 Data processing based on a legitimate interest

Processing of person-related employee data may also occur when required for the realization of a legitimate interest of the Teufelberger Group. Legitimate interests are as a rule legally justified (e.g. establishment, exercise or defense of legal claims) or economic (e.g. evaluation of companies).

Processing of person-related data based on a legitimate interest is not permitted when in an individual case there are indications that the legitimate interest of the employee concerned prevails over the interest of the processing. Legitimate interests need to be reviewed for every processing.

Control measures requiring the processing of employee data may only be conducted when there is a legal obligation, a relatively legitimate interest or a justifiable reason. The comparative relation of the control measures also needs to be examined in cases where there is a justifiable reason. The legitimate interests of the company in the implementation of the control measures (e.g. compliance with legal provisions and internal company procedures) need to be balanced against the possible legal interest of the employee affected by the measures in the exclusion process and may only be conducted if appropriate. The legitimate interest of the company and the possible legitimate interest of the employee need to be determined and documented before each process. Additionally any further requirements in conjunction with statutory law (e.g. co-determination rights of the employee representatives and the tights to information of those concerned) need to be considered.

5.2.6 Processing of highly sensitive data

Highly sensitive person-related data may only be processed under certain conditions. Highly sensitive data refers to data concerning racial and ethnic origins, political opinions, religious or philosophical convictions, membership of trade unions or the health or sexual life of those concerned. Equally data relating to criminal acts may only be processed under certain conditions governed by statutory law. The processing must be specifically permitted or prescribed under statutory law. Processing may also be additionally permitted should it be necessary for the responsible authority to comply with their rights and duties in the area of labour law. The employee may voluntarily explicitly approve the processing.

Should processing of highly sensitive data be planned then the GDPO is to be advised in advance.

5.2.7 Telecommunication and internet

Telephone systems, email addresses, intranet and internet as well as internal social networks are provided by the company in the first instance for business operations. They are a means of work and a company resource. They may be used within the scope of the respective legal provisions and internal company policy. Should permission be granted for private purposes then compliance with telecommunications privacy and the respective current national telecommunications law is to be observed if applicable.

There is no general monitoring of telephone and email communication or intranet and internet use. Protective measures for the defense against attacks on IT infrastructure or on individual users may be implemented at interfaces in the Teufelberger network in order to block technically damaging content or to analyze the pattern of attack.

Person-related evaluations of this data may only occur when there is a specific justified suspicion of an infringement of the law or guidelines of the Teufelberger Group. These controls may only be exercised by the investigating departments in compliance with the principle of comparative relation. Compliance is also required with the respective national laws as is the case with these company provisions.

6 Transmission of person-related data

Transmission of person-related data to a recipient outside the Teufelberger Group or a recipient within the Teufelberger Group is subject to requirement of prior approval of the person-related data processing as under section 5. The recipient of the data is obliged to only apply the data for the purposes stipulated.
Should data be transmitted to a recipient outside the Teufelberger Group in a third country[9] then the recipient is to guarantee a data protection level equal to these data protection guidelines. Should this not apply then the transmission is only to occur on the basis of a legal requirement.
Should data be transmitted from third parties to a company of the Teufelberger Group then it is necessary to ensure that the data is used only for the intended purposes.

Data transmission within the Group is regulated in a separate master agreement for data transmission.

7 Processing of order data

Processing of order data occurs when a contractor is mandated with the processing of person-related data without the transfer of responsibility for the related business process. Should this be the case then an agreement is to be concluded regarding the order data processing between the external contractor and the Teufelberger Group company. The mandating company retains the full responsibility for the correct conduct of the data processing. The contractor is only permitted to process person-related data within the scope of the instructions provided by the principal. The following provisions are to be complied with in the issue of the order; the mandating department is to ensure its implementation.

- The contractor is to be selected in accordance with their suitability in guaranteeing the required technical and organizational protective measures.
- The order is to be issued in writing. In the process, the instructions related to the data processing and the responsibilities of the principal and those of the contractor are to be documented.
- Compliance with the contractual standards drawn up by the GDPO is required.
- The principal needs to be satisfied that the contractor is in compliance with the requirements before the start of data processing. Compliance with the requirements of data security may be proven by the contractor through submission of suitable certification. Verification of compliance is to be regularly conducted during the contractual period proportionate to the level of risk attached to the data processing.
    a. The respective national requirements concerning the transmission of person-related data to a foreign country are to be complied with when transmitting order data across borders. The processing of person-related data from the European Economic Area to a third country is only to occur when the contractor certifies a data protection standard equal to these data protection guidelines. The following means may be suitable: Agreement on EU standard contract clauses on the processing of order data in third countries between the contractor and possible sub-contractors.

[9] See 15.9

b. The commitment of the contractor to a certification system acknowledged by the EU for the creation of appropriate data protection standards.
c. Acknowledgement of binding company regulations by the contractor for the creation of an appropriate data protection standard by the responsible data protection supervisory authorities.

8 Rights of the person concerned

Each person concerned is entitled to the following rights. Their enforcement is to be processed without undue delay by the responsible department and may not lead to any disadvantage for the person concerned.

- The person concerned may request information as to the origin of the person-related data and the reason for storing the data. Should there be a provision for additional access rights to the documentation of the principal in accordance with the respective labour law (e.g. personnel file) in a case of employment then these remain unaffected.
- Should person-related data be transmitted to a third party then information on the identity of the recipient or the category of the recipients need to be provided.
- Should person-related data be incorrect or incomplete then the person concerned is permitted to demand its correction or completion.
- The person concerned may object to the processing of their person-related data for the purposes of advertising or market and opinion research. In this case the data is to be blocked.
- The person concerned is entitled to demand the deletion of their data should the legal basis for the processing of the data be lacking or no longer applicable. The same applies should the purpose of the data processing be no longer applicable due to the lapse of time or other reasons. Existing retention requirements and the extinction of opposing legitimate interests need to be observed.
- The person concerned possesses a fundamental right to object to the processing of their data which needs to be taken into consideration when their legitimate interest prevails over the interest in processing on the basis of specific personal circumstances. This does not apply should the legal provisions require the completion of the processing.

9 Confidentiality of processing

Person-related data is subject to data privacy. Unauthorized collection, processing or use by the employees of the Teufelberger Group is not permitted. Any processing undertaken by an employee without being entrusted or entitled to the fulfillment of the task is unauthorized. The need-to-know principle applies. Employees are only permitted to receive access to person-related data should and provided it is required for their respective tasks. This requires care in the asignment and separation of roles and responsibilities as well as in their implementation and maintenance in relation to authorization concepts.

Employees are not permitted to use person-related data for their own private or business purposes, transmit to or provide access to unauthorized persons in any way. Superiors are to instruct their employees on the duties of complying with data privacy on commencement of the employment relationship. This obligation also continues to apply following termination of the contract.

10 Security of processing

Person-related data is to be protected at all times against access, unauthorized processing or transfer, as well as against loss, falsification or destruction. This applies independently of whether the data is processed in electronic or paper form.

Prior to the introduction of new procedures of data processing, especially new IT systems, the GDPO

is to determine and implement technical and organizational measures for the protection of person-related data. These measures are to be in alignment with the level of technology, risks arising from the processing and the protection requirement for the data (determined by the information classification process). The technical and organizational measures for the protection of person-related data are part of group-wide information security management and need to be aligned continuously to all technical developments and to organizational changes.

11 Data protection control

Compliance with the data protection guidelines and the current data protection laws is reviewed on a regular basis through data protection audits and other controls. The GDPO is responsible for their implementation.

12 Data protection incidents

Every employee reports to their respective superior who in turn reports to the GDPO without undue delay any cases of infringement of these data protection guidelines or other provisions for the protection of person-related data (data protection incidents[10]).

Should there be cases of unintentional or unauthorized access/transfer/changes/destruction/loss then the GDPO is to initiate the prescribed company reporting procedure (Information Security Incident Management) without undue delay in order to comply with the obligations to report data protection incidents pursuant to statutory law.

13 Responsibilities and sanctions

The executive board and the management of the Group companies are responsible for data processing in their area of responsibility. They are therefore obliged to ensure that the legal data protection requirements and those contained in the data protection guidelines are taken into consideration (e.g. national reporting obligations).

It is the responsibility of the management to ensure proper data processing in compliance with data protection by means of organizational, personnel and technical measures based on those guidelines.

The GDPO is to be notified immediately should there be data protection reviews by the authorities. The respective management and factory management are to designate a data protection coordinator to the GDPO. The data protection coordinators are the persons of contact for data protection on site. They may conduct reviews and are to familiarize the employees with the contents of the data protection guidelines. The respective management is obliged to support the GDPO and the data protection coordinators in their work.
The persons responsible for business processes and projects are to advise the data protection coordinators in due time on new processing of person-related data. The officer responsible for data protection is to participate in data processing projects that include the processing of person-related data prior to processing. This applies especially for highly sensitive person-related data, in which case a risk impact assessment is to be concluded. Management is to ensure that their employees receive training in data protection to the appropriate extent. A misuse of person-related data in processing or other infringements of data protection law are prosecuted in many countries and may cause claims for damages. Contraventions caused by individual employees may lead to disciplinary actions.

[10] See 15.10

14 The group data protection officer (GDPO)

The GDPO together with the respective management and the data protection coordinators are to ensure compliance wit the national and international data protection provisions. The GDPO is responsible for guidelines relating to data protection and monitors their compliance. The GDPO is appointed by the board of Teufelberger AG. The GDPO is to be notified by the data protection coordinators regularly and consulted on all material data protection subjects without undue delay. Any person concerned may approach the data protection coordinator responsible for their area or the GDPO with any proposals, inquiries, requests for information or complaints in connection with questions on data protection or data security.

Should the responsible data protection coordinator be unable to assist with a complaint or remedy an infringement of the data protection guidelines, then the GDPO is to intervene. The decisions of the GDPO in remedying the infringement to data protection are to be taken into consideration by the respective management. The GDPO is always involved in any inquiries by the supervisory authorities.

15 Definitions

15.1 A transmission is any notification of protected data by the office responsible to third parties.

15.2 Person-related data all information relating to a particular or determinable natural person. Determinable relates to a person e.g. when a reference to the person may be determined by a combination of information and also even when supplementary knowledge is available by chance.

15.3 Anonymized is data when a reference to a person either permanently or from any person be determined any longer or when a reference to a person is only possible to reestablish with relatively great effort in time, cost and labour.

15.4 A person concerned in the meaning of these data protection guidelines is any natural person subject to the processing of data.

15.5 The responsible office is the independent legal entity within the Teufelberger Group arranging for the respective processing measures in their business activities.

15.6 Required is the processing of person-related data, when the approved purpose or the legitimate interest is not achievable without the respective person-related data or only with relatively great effort.

15.7 Consent is a voluntary legally binding consensual declaration to data processing.

15.8 Highly sensitive data refers to data concerning racial and ethnic origins, political opinions, religious or philosophical convictions, membership of trade unions or the health or sexual life of those concerned.

15.9 Third party countries in the meaning of the data protection guidelines are all stated external to the European Union/EER. Exceptions are countries where their data protections standards are appropriately acknowledged by the EU Commission.

15.10 Data protection incidents are all events where there is justified suspicion that person-related data is unlawfully exposed, collected, changed, copied, transmitted or used. This also includes actions by third parties as well as employees.