Data Protection Concept

Classification: INTERNAL

Version: 0.1

Published by: Company Management

Published on: 06/02/2018

Foreword by the Company Management/DPO

>> optional, to be added if applicable <<

Contents

TOC

Document history

Version	Description	Author	Date
0.1	First draft preparation		XX/XX/17

1. Introduction

This Data Protection Concept describes ordinary handling of information which is internally processed by the XY Group, but also outside its premises in terms of the EU General Data Protection Regulation (GDPR) and the German Data Protection Act (*BDSG*). Hence, the Data Protection Concept is an important contribution to the legal handling of personal data for all business activities and it represents a key element of the data protection management system of XY

who considers data protection to be not only a legal duty, but an important business goal. XY must particularly and actively protect personal customer and employee data since customers and Staff must be confident that XY will not misuse their personal data.

Above all, data protection is a management responsibility which the Company Management intends to face. Since data protection cannot (only) be prescribed from the top down, but lived by every XY employee this Data Protection Concept helps Staff to consider data protection aspects at their work places through clear instructions. Staff are obliged to comply with and implement this Concept.

1.1. General Data Protection Remarks

Data protection law includes a set of rules for handling personal data to protect personal rights of data subjects. The goal is preventing “transparent individuals” and protecting the data subjects’ personal rights.

The EU General Data Protection Regulation (GDPR), the German Federal Data Protection Act and other sector- and country-specific regulations are based on the European Charter of Fundamental Rights and art. 2 clause 1 in connection with art. 1 clause 1 and art. 10 clause 1 *GG* [*Grundgesetz* – German Basic Law]. In this context, data protection is particularly guaranteed through a right to informational self-determination and the basic right to IT system confidentiality and integrity. The GDPR provides for a minimum data protection level for all EU member states. This Data Protection Concept is intended to make a particular contribution with regard to new legal GDPR requirements to ensure compliance in this area.

1.2. Scope of Application

This Data Protection Concept represents the basis for handling personal data. Any other instructions, duties, policies and company agreements concerning personal data handling shall be considered supplements, unless they are contrary to this Concept. It shall apply to

the processing of data from private and business customers, contract partners and contact persons, data from other external offices and data from Staff, apprentices, applicants and other individuals, regardless of the type of employment.

This Data Protection Concept shall apply to all group companies and it is directed at any and all Staff of the individual companies, regardless of the type of employment, including freelancers, temporary workers and other workers ("Staff").

1.3. Data Protection as a Marketing Factor

Active data protection may be used as a marketing factor, particularly in the light of increased sensitivity among (final) customers concerning the handling of their personal data. However, it has also become increasingly important for customers to have sub-contractors providing for compliance levels pursuant to data protection law and for up-to-date technical security measures provided for by the law. If XY not only fulfils their legal duties, but sees data protection an important company philosophy components, this may be used to distinguish XY from competitors vis-à-vis (potential) customers.

1.4. Data Breach Consequences

Unlawful personal data handling may lead to both claims for damages from data subjects and a loss of reputation;

such consequential damages,are difficult to quantify but must not be underestimated. Careless personal data handling may also lead to complaints which individuals submit to supervisory authorities.

Not only this, prohibited or incorrect personal data use represents either an administrative offence subject to a fine of up to EUR 20,000,000 and/or 4% of the annual turnover or even a crime subject to imprisonment of up to three years.

2. Definitions

The data protection law key element are personal data which includes any information on an individual's personal or material situation. Hence, any information can be a piece of personal data if this can be attributed to certain individuals and this may include trivial facts and both apparent and publicly available information. Statistics, however, which do not allow for the identification of individuals shall generally not be deemed personal data.

Some information on individuals is considered particularly sensitive. This special category of personal data includes information on political opinions, religious/ideological beliefs, trade union membership, genetic data, biometric data for clear identification of natural persons, health data and sexual life/orientation data. Once information on individuals relates to these sub-areas, it is necessary to pay particular attention.

Data processing includes any and all steps concerning data handling, including, but not limited to, data collection, storage, transmission, forwarding, modification, combination, analysis and deletion and any other types of use; this is a very broad term.

Data subjects in terms of data protection law shall be individuals who are identifiable based on personal data, that is, individuals affected by data processing activities. All data subjects shall be entitled to certain inalienable rights in terms of data protection law.

In contrast, data controller is the exact counterpart of data subjects. The companies managing data processing activities, that is, those determining in what ways data from data subjects are to be processed, shall are referred to as data controllers. Processing activities may also be outsourced to other offices (such as to XY group companies or external service providers), but the customer shall continue to be the data controller. A clear identification of the data controller is important since data subjects should have a clear, single contact.

In more detail:

Personal Data: any information relating to identified or identifiable individuals, whereby natural persons shall be deemed identifiable if they can be directly or indirectly identified through identifiers such as names, ID numbers, location data, on-line identifiers and single or several features representing such natural persons' physical, physiological, genetic, mental, economic, cultural or social identity.

Personal data may include the following:

- name, age, marital status, date of birth, profession, address, telephone number, e-mail address;
- salary information, preferred payment types, account/credit card numbers, credit standing information, payment history or liabilities;
- identifiers (customer/personnel numbers);
- biometric (height) and health (pre-existing conditions) data;
- relatives and social relationships;

- customer characteristics (existing contracts, contract history);
- consumption (consumption data, means of transport, trash bin contents);
- surfing habits (browser information, browsing history);
- video recordings and photos.

Personal Data Special Categories; Data providing information on the race, ethnic origin, political opinions, religious/ideological beliefs and trade union membership and data on the health status, sexual life or sexual orientation.

Data Controller: Any natural or legal person, authority, facility or other body solely or jointly deciding upon personal data processing purposes and means.

Processing: Any operations with or without automated processes or any series of operations relating to personal data, such as acquisition, collection, organisation, arrangement, storage, adjustment, modification, reading, retrieval, use, disclosure by transmission, distribution or any other type of provision, comparison, linking, restriction, deletion or destruction.

Anonymous and Pseudonymous Data: The opposite of personal data are "anonymous data" which cannot be attributed to any specific individuals. Unemployment rate data or public transport average usage statistics do not allow for statements on individuals, which means they are anonymous data. Since anonymous data do not relate to individuals, they are not subject to data protection law; however, they may be subject to particular confidentiality if they are company data (such as business figures, internal statistics). At a first glance, "pseudonymous data" are similar to anonymous data; pseudonyms can also be referred to as "aliases". Contrary to anonymous data, however, allocation to individuals is still possible in the case of pseudonyms. Allocation simply includes an additional step, such as comparisons with or searches in customer databases or staff registers. Hence, pseudonymous data are personal data subject to data protection law.

Example: A following statement represents pseudonymous data: "the employee no. 1241 worked 11.5 extra hours last month". Based on information available to the Personnel department, it is possible to identify the individual so this is personal data. No identification of individuals is possible through the following statement: "The German citizen consumes 121 litres of water" so this is not personal data.

3. Roles and Responsibilities

The Company Management and, on the department level, officers appointed by the Company Management shall be responsible for data protection concept implementation in every-day business operations. However, data protection is relevant for all XY staff, which means that they must protect personal data.

3.1 Managing Directors

>> to be added <<

3.2 Managerial Staff

>> to be added <<

Department	Name/Position
Legal	
IT	
Operations	
Finance	
Marketing/Sales	

3.3. Data Controller

The term of "data controller" is the link to legal rights and duties; responsibilities include the handling of data. The data controller regarding data handling under this Data Protection Concept shall be

>> to be added <<

4. Data Protection Law Classification of XY

Essentially, XY shall be subject to GDPR and *BDSG* provisions.

>> Description of main processing purposes to be added. <<

5. Company Data Protection Officer

In terms of sec. 38 *BDSG* and art. 37 GDPR, XY appointed a company data protection officer (DPO)

who shall be; >> <<

He/she shall fulfil his/her function, assigned to him by law and under this directive by applying his expertise, subject to no restrictions. For this purpose, the specialist departments shall provide the required information, documents etc., whereby this shall also apply to queries, complaints and information provision requests.

Every XY employee may refer to the DPO for any questions, remarks, suggestions or complaints which shall be, upon request, treated as a secret.

6. Data Protection Law Basic Conditions

XY is subject to the below data protection law basic conditions:

6.1. Legal Basis of Processing

Data processing shall be governed by the so-called prohibition with the reservation of authorisation provided for under GDPR and *BDSG* provisions. This means that personal data processing is generally forbidden, unless it was expressly authorised.

According to art. 6 GDPR and comparable specific sector regulations, personal data processing is only admissible if

- data subjects agreed to processing of their personal data for a single or several given purposes;
- processing is required to fulfil contracts to which data subjects are parties or to perform pre-contractual measures upon the data subjects' requests;
- processing is required to fulfil legal duties to which the data controller is subject;
- processing is required to protect data subjects' or other individuals' vital interests;
- processing is required to protect data controller's or third parties' vital interests, unless interests, fundamental rights or freedoms of data subjects requesting personal data protection prevail, in particular if data subjects are children.

When processing personal data, XY guarantees that authorisation elements required for processing exist. With regard to processing employee data, this shall be art. 88 GDPR, sec. 26 *BDSG* or, for processing certain customer data, art. 6 GDPR above.

When processing data for which no legal authorisation element exists, XY ensures that it obtains legal authorisations from the respective data subjects. The prohibition of personal

data processing by automated means if processing has legal or similar effects for data subjects will be complied with.

6.2. Consent from Data Subjects

In addition to the legal data processing authorisation, consent from data subjects in terms of art. 6 clause 1a GDPR represent a possibility to process data legally. Both the GDPR and court judgements stipulate strict requirements (regulated under art. 7 GDPR) for such declarations of consent stating that data subjects must grant their consent on a voluntary and informed basis. As an example, XY ensures this for declarations of consent to data storage from applicants even beyond the application process (in a pool of applicants).

6.3. Appropriation

The data processing purpose is based on the relevant specialist tasks for the performance of which data were collected. These purposes must be clear and legitimate and be indicated at the time of data collection. Data protection law requires that personal data generally be processed only for the purpose for which they were originally collected. Data have certain purposes and XY has generally no personal data which are “free” for use for undefined purpose; if data is no longer required for their original purposes, they must be deleted, unless the law requires they be archived.

Data processing for purposes other than the original ones represents a purpose change or exception in terms of art. 6 clause 4 GDPR and shall be possible only on a legal basis or subject to the data subjects’ consent. This shall also apply if data are to be transferred to other offices performing tasks which exceed auxiliary functions.

For any and all processes, XY ensures that personal data will be processed only for those purposes for which they were collected, that legal authorisations exist or that express declarations of consent from data subjects are obtained if the purpose is supposed to be changed.

6.4. Correctness

XY guarantees that data stored by the Group are correct and that they will be updated if required.

6.5. Data Minimisation

The data minimisation principle means that only such data (quantities) are collected and processed which are required for the relevant application. XY shall consider this for all of their processes including personal data processing.

6.6. Transparency

Data subjects shall always have the right to dispose of their own personal data, they must be able to understand who stores and processes which personal data for what purposes and they must be informed about processing purposes not later than upon collection. Hence, data may never be secretly processed without data subjects being aware of this. It is important to thoroughly explain data processing steps (for example in the Data Protection Declaration) and to seriously, completely and truthfully answer any queries to guarantee transparency. For example, art. 13 GDPR states that data subjects must be particularly informed about the DPO's contact data, the purpose (for each case of data processing), processing period, rights to information and objection, legal bases of data processing and comprehensible weighing of interests. Generally, data subjects must be informed about any and all rights, that is, about the right to information, correction, deletion, processing restriction, objection and data transferability. Data subjects must also be informed about the extent to which decision-making is based exclusively on automated data processing (profiling).

In this regard, it must be considered that information is submitted to data subjects immediately upon data collection. Art. 12 GDPR requires this information to be submitted to data subjects "in a transparent, intelligible and easily accessible form, using clear and plain language", whereby verbal, written and electronic information transfer shall be sufficient. Information addressed specifically to a child must be particularly clear. Only if data subjects already dispose of required information in data processing cases shall no duty to provide information exist; XY must produce evidence in this regard.

6.7. Security

XY must prove that personal data are processed in a way which provides for reasonable data security levels. It does so by implementing technical and organisational measures.

6.8. Data Protection Impact Assessment

Art. 35 GDPR requires the performance of data protection impact assessments, meaning risk assessments which XY must perform prior to processing personal data. Generally, such data protection risk assessment must only be performed if there is a high risk for the data subjects' rights and freedoms, such as in the below cases:

- data for valuation, scoring or profiling purposes, particularly concerning work, economic situations, health, personal preferences/interests, credit standings, habits, whereabouts;
- automated decision-making having legal consequences;
- processing of sensitive data, such as health data;
- comprehensive processing procedures;
- interlinked or combined datasets;
- data from individuals in need of protection, such as children, elderly people, patients or staff;
- usage of new technologies, such as IoT developments.

Should data protection impact assessments in terms of art. 35 GDPR be required, the DPO must be involved which is why XY employees should immediately inform the DPO about the introduction of new personal data processing systems so that he/she could check them for admissibility in terms of data protection law.

>> process to be adjusted, if need be; reference to the guidelines<<

Attention: the consultation duty under art. 36 GDPR must be considered for risky data processing. Hence, the DPO and/or the Company Management shall contact the supervisory authority if the data protection impact assessment shows that data processing entails high risks in terms of data protection law.

7. Reporting Duty according to the GDPR

Personal data protection is of utmost importance to XY. However, if data breaches do occur, XY is aware of its reporting duty which it fulfils without undue delay. Such breaches occur if

data security violations (unintentionally or illegally) lead to the destruction, loss, modification or unauthorised disclosure of/access to personal data which was transferred, stored or processes in any other way. Mit anderen Worten ein unbefugter Datenzugriff, eine „Datenpanne".

Art. 33 and 34 GDPR indicates how to proceed in cases of data breaches: the supervisory authority must always be informed; an exception shall only exist if data breaches will probably not lead to risks for data subjects. Therefore, XY employees must inform the DPO immediately of data breaches for him/her to assess the risk for data subjects resulting from such breach. Data subjects need only be informed if there is a high risk for their rights and freedoms. Even though information of data subjects may be omitted if technical and organisational measures preventing authorised third parties from accessing personal data exist, but the DPO shall be responsible for the relevant evaluation.

Since data breaches must be reported to supervisory authorities in charge within 72 hours, staff should not delay to quickly inform the DPO about any data breach.

8. Data Transfer to Third Parties

Data transfers to other bodies, such as external service providers, authorities, the police of public prosecution offices, shall also be processes relevant in terms of data protection law requiring factual justifications in every individual case. Hence, any data transfers must be thoroughly assessed and approved by the supervisor or the DPO.

8.1. Group-Internal Transfer

Data transfers to other XY group companies, too, must be examined since data may not be simply transferred between group companies, combined, compared or made available in other ways; there is no comprehensive group privilege. Transfers within XY must also be justified in the context of weighing interests.

Since only those departments which require the data for their activities may access this data, transfer to other group companies shall be admissible only if legal bases exists in individual cases. Companies must check individual procedures for legal admissibility and consider the data subjects' interests.

Data transfers between XY companies shall be complemented by data protection contracts (if required) to guarantee legally admissible processing.

8.1. External Service Providers and Commissioned Data Processing

If external service providers are to be engaged to whom XY must transfer personal data or who is granted a right to access any stored data, managers of the relevant departments must ensure that the DPO is informed and that a commissioned data processing contract is concluded, if required.

>> process to be adjusted, if need be; reference to the guidelines<<

In addition, particular aspects of data processing or transmission to "insecure" third countries (such as the US) must be considered and supplementary contracts must be concluded, if need be.

If external service providers are to be engaged to whom XY must transfer personal data (contract data processor) or who are granted a right to access personal data, a written contract must be concluded. Commissioned data processors must be chosen with care under consideration of the technical and organisational measures and they may process data only pursuant to XY's instructions. Requirements as to the contents of such contracts under art. 28 GDPR must be considered and, to ensure this, the DPO should be informed about the intention of concluding such commissioned data processing contracts.

9. Confidentiality and Data Protection Compliance Duty

The XY staff shall be instructed about their confidentiality and data protection duty when signing their employment contract and they shall sign a relevant declaration to be added to the personnel files.

In addition, XY shall perform regular data protection training courses.

>> to be adjusted, if need be; more detailed description <<

10. Personal Data Description and Appropriation

XY processes the below personal data and/or data categories:

>> to be adjusted by more details, if need be <<

10.1. Applicant Data

The affected group of persons includes applicants and parties interested in vacancies.

These data relate to individual information on the applicants' personal and factual situations provided during the application process, that is:

- name;
- address;
- date of birth;
- photo;
- parents' name/dates of birth/profession/religious or political beliefs (not required, but often voluntarily provided);
- education: final marks and education institutions;
- former employers, references and testimonials;
- current notice periods, desired salaries and availability;
- for applicants from third countries: type and term of valid residence/work permits;
- passport copies.

Data will be used for applicant management purposes.

10.2. Employee Data

The affected group of persons includes staff (permanent employees, working students, trainees) and freelancers.

The data relate to individual information on the staff's personal and factual situation, that is:

- names and names at birth;
- addresses (official addresses);
- date of birth;
- account details;
- tax number, tax class, denomination, civil status, nationality;
- education level;
- health and social security insurance data;
- job level/salary;
- mobile/land line phone number; private e-mail address (voluntarily), emergency contacts (name and phone number (voluntarily));
- for special cases: passport copy (residence permit for staff from third countries;

- activity-related employee data e.g. payroll data, expense invoices, holidays and sickness periods, work-time registration, warnings, evaluations.

These data will be used for processing employment contracts and registering Staff with tax offices, health/pension insurance companies.

10.3. Accounting Data

The affected group of persons includes accounting and finance staff, suppliers and customers.

The data relate to individual information on the staff's, suppliers' and customers' personal and factual situation, that is:

Accounting and finance staff

- contact partner names;
- contact partner addresses;
- invoice information, including tax numbers and account details.

Suppliers

- contact partner names;
- address;
- invoice information, including tax numbers and account details.

Customers

- contact partner names;
- (e-mail) addresses;
- communication contents.

Data will be used for accounting purposes.

10.4. Usage Data

The affected group of persons includes users of the XY website at www.XY.com.

>> to be adjusted by more details, if need be <<

The data relate to individual information on the users' personal and factual situation, that is:

usage data in terms of sec. 15 clause 1 *TMG* [*Telemediengesetz* – German Telemedia Act], such as:

- the IP address from accessing computers;

- access date and time;
- name and URL of the downloaded file;
- data transfer quantity;
- successful retrieval notification;
- browser and operating system recognition data.

These data will be used to enable users to use the XY website and for advertising, market research and adequate XY company website structuring purposes.

10.5. Customer Data

The affected group of persons includes XY customers. XY mainly operates in the B2B sector so that personal data will be affected in this context only to a small extent, for example in the form of contact partner names and e-mail addresses:

- contact partner names;
- (e-mail) addresses;
- communication contents.

10.6. Special Categories of Personal Data

Art. 9 clause 1 GDPR defines special categories of personal data as data providing information on the race, ethnic origin, political opinions, religious/ideological beliefs, trade union membership, health and sexual life/orientation; however, this shall also include genetic and biometric data.

XY business operations may entail the processing of special categories of personal data in the following cases:

- employee data (health, religion);
- applicant data (health, religious/ideological beliefs).

11. Protection of Data Subject Rights

Data subjects shall have a right to information, correction, deletion, processing restriction, objection and data transferability.

XY ensures that any data required for justified requests will be quickly and completely provided within one month; third-party personality rights must be protected in this regard.

11.1. Information

In terms of art. 15 GDPR, data subjects have a right to receive information from the the data controller on what personal data from them are stored for what purposes, to whom data are transferred and from where they come,

For this, it is of utmost importance to securely identify data subjects since customers/staff being provided with information on other customer/staff would represent a severe data breach. Complete and true data shall be provided on a non-paid basis.

11.2. Correction

Under art. 16 GDPR, data subjects may request the immediate correction of their personal data and XY shall, upon request, immediately correct any incorrect data.

11.3. Processing Restrictions

According to art. 18 GDPR, data may no longer be processed if data subjects contest data correctness, if processing is illegal but data subjects object to data deletion, if data subjects still require the data in order to pursue legal claims or if data subjects objected to their processing and a decision in this regard is still pending. However, XY shall also limit processing if storage is admissible, but processing is not.

11.4. Deletion

Under art. 17 GDPR, data subjects may request the data controller to immediately delete the personal data, whereby the latter must immediately delete any personal data if one of the four reasons below applies:

- data storage is not longer required for data collection purpose achievement;
- data subject revoke their consent to data processing;
- data were illegally processed;
- data must be deleted by XY due to legal deletion duties.

XY needs not implement the right to deletion if:

- freedom of opinion and information prevails;

- data storage corresponds to legal duties;
- public interest in the field of health prevails;
- scientific or historic research purposes prevail;
- data are required to protect legal claims.

Should deletion, in the case of automated data processing, be possible not at all or only by applying unreasonable efforts due to the special way of storage and should the interests of data subjects in deletion be considered inferior, data subjects have no right and the data controller has to duty to delete such data. In this case, XY complies with processing restrictions in terms of art. 18 GDPR (see above), but the DPO should be contacted for this.

11.5. Data Transferability

Data transferability is regulated under art. 20 clause 1 GDPR; this includes, on the one hand, the right to request the provision of individual datasets and the right to transfer this to other data controllers. XY shall provide data subjects with the relevant dataset in a structured, standard and machine-readable system. If data subjects want to transfer this dataset to other data controllers, XY shall not impede or prevent this process.

11.6. Objection

Data subjects may, at any time, object to the processing of personal data based on art. 6 clause 1e or f GDPR. If data were legally collected pursuant to either requirements above, data subjects may, at any time, object to such data being processed even though data collection was legal. XY shall respect such objections and discontinue data processing if the right to objection results from the data subjects' "particular situation", whereby the latter shall not only produce evidence showing the particular situation, but also "predominance".

Art. 21 clause 2 GDPR grants a non-paid right to objection which may be exercised at any time if processing of the data subjects' personal data relates to direct advertising activities. XY shall respect such objection and discontinue data processing activities.

12. Processing Activities Register/Documentation Duties

Overviews of the below information must be provided for automated processes:

- (company) name of the data controller;
- owner, board members, managing directors, other managers appointed on the basis of the law or the articles of association and data protection officers;
- the data controller's address;
- data collection, processing or use appropriation;
- data collection, processing or use legal basis;
- description of affected groups of persons and related data (categories);
- data recipients (categories);
- regular data deletion periods;
- scheduled data transfer to third countries;
- general description enabling preliminary evaluations of adequacy of measures in terms of sec. 9 to ensure processing security;
- data collection purpose;
- contents;
- description of affected groups of persons;
- regular deletion periods;
- information of processing types and protection measures.

Required process overviews can be obtained from XY.

13. Technical and Organisational Data Protection Measures

According to art. 32 GDPR, Technical and organisational measures must be taken which, depending on the type of personal data (categories) to be protected, provide for adequate protection levels.

Art. 32 GDPR provides for a non-conclusive list of different technical and organisational measures representing a minimum measures catalogue of concrete and abstract measures similar to objectives. Since these are minimum requirements, they depend on individual cases, but they are not required all the time. This catalogues includes

- personal data pseudonymisation and encryption: Pseudonymisation is supposed to enable identification of individuals only by "including additional data", such as identification keys. In the case of encryption, identification of individuals is still possible, but data are changed in a way that they cannot be read if not decrypted;

- system and services confidentiality, availability and reliability: This is supposed to prevent third-party access, but it also includes technical aspects, such as data the prevention of processing system overload. The relevant measures depend on the intended protection purpose and confidentiality may be guaranteed by access controls. To ensure integrity protection, electronic signatures should be used and XY guarantees data system availability through investments in double and triple redundancy of all data processing components;
- ability to quickly restore personal data availability and access after physical or technical disruptions: In addition to several back-ups of datasets, this matter mainly relates to such technical and organisational measures that representation plans for staff shortages are prepared or that outages can be prevented through emergency power supply;
- processes to monitor and evaluate technical and organisational measures effectiveness in order to guarantee processing security: It must be ensure that the above security measures can be regularly and thoroughly monitored and checked for which purpose internal and external audit reports are prepared and evaluated. If need be, this shall be followed by adequate measures.

For XY, implementation of technical and organisational data protection measures is of the utmost priority, not only for protecting staff and customers, but also for effectively combating industrial espionage.

13.2. Technical and Organisational Measures Taken by XY

13.2.1. Pseudonymisation Measures

>> to be adapted by more details <<

13.2.2. Encryption Measures

>> to be adapted by more details <<

13.2.3. Confidentiality Measures

>> to be adapted by more details <<

13.2.4. Integrity Protection Measures

>> to be adapted by more details <<

13.2.5. Measures for Protecting Availability and Capacities

>> to be adapted by more details <<

13.2.6. Regular Data Processing Security Evaluation Measures

>> to be adapted by more details <<

13.3. Information Security Management

XY bases its information protection activities, in particular for personal data, on an information security management system (ISMS) pursuant to the ISO/IEC 27001:2013(E) and the ISO/IEC 27002:2013(E) standards and which is partially aligned to the BSI IT basic protection catalogues regarding action recommendations. Details can be found in >> to be adapted by more details <<

13.4. Classification Based on Protection Needs

To protect information and personal data, XY makes a classification based on protection needs. Categories on the basis of which information is visibly identified include: "public", "internal", "confidential" and "secret" In some cases, categories include "strictly confidential" or "top secret" which must be allocated to the "secret" category. If documents show no category, they fall into the "internal" category; for more details, please refer to ....

>> to be adapted by more details <<

14. Additional Data Protection Concept Elements

The below policies and company agreements represent additional data protection concept elements:

- Communication Media Usage Policy
- >> to be adapted by more details <<
-