Information Security Management System

General Data Protection Regulation

Data Protection Policy

Reference Number	GDPR-R001
Version / Revision	1.0
Classification	Public
Document Owner	M. Haas , Chief Operating Officer
Approved By / Date	M.Haas / 13.04.2018
Editor	T. Mathew
Status / Date	Released / 13.04.2018

I. AIM OF THE DATA PROTECTION POLICY 3
II. SCOPE AND AMENDMENT OF THE DATA PROTECTION POLICY 3
III. APPLICATION OF NATIONAL LAWS 3
IV. PRINCIPLES FOR PROCESSING PERSONAL DATA 4
1. Fairness and lawfulness 4
2. Restriction to a specific purpose 4
3. Transparency 4
4. Data reduction and data economy 4
5. Deletion 4
6. Factual accuracy; up-to-date status of data 5
7. Confidentiality and data security 5
V. RELIABILITY OF DATA PROCESSING 5
1. Customer and partner data 5
1.1 Data processing for a contractual relationship 5
1.2 Data processing for advertising purposes 5
1.3 Consent to data processing 6
1.4 Data processing pursuant to legal authorization 6
1.5 Data processing pursuant to legitimate interest 6
1.6 Processing of highly sensitive data 6
1.7 Automated individual decisions 7
1.8 User data and internet 7
2. Employee data 7
2.1 Data processing for the employment relationship 7
2.2 Data processing pursuant to legal authorization 8
2.3 Collective agreements on data processing 8
2.4 Consent to data processing 8
2.5 Data processing pursuant to legitimate interest 8
2.6 Processing of highly sensitive data 9
2.7 Automated decisions 9
2.8 Telecommunications and internet 9
VI. TRANSMISSION OF PERSONAL DATA 10
VII. CONTRACT DATA PROCESSING 10
VIII. RIGHTS OF THE DATA SUBJECT 11
IX. CONFIDENTIALITY OF PROCESSING 12
X. PROCESSING SECURITY 12
XI. DATA PROTECTION CONTROL 12
XII. DATA PROTECTION INCIDENTS 13
XIII. RESPONSIBILITIES AND SANCTIONS 13
XIV. DATA PROTECTION OFFICER 13
XV. DEFINITIONS 14

I. Aim of the Data Protection Policy

As part of its social responsibility, CSF is committed to international compliance with data protection laws. This Data Protection Policy applies worldwide, based on globally accepted, basic principles on data protection. Ensuring data protection is the foundation of trustworthy business relationships and the reputation of CSF as an attractive employer.

The Data Protection Policy provides one of the necessary framework conditions for cross-border data transmission[1]. It ensures the adequate level of data protection prescribed by the European Union Data Protection Directive[2] and the national laws for cross-border data transmission, including in countries that do not yet have adequate data protection laws[3].

II. Scope and amendment of the Data Protection Policy

This Data Protection Policy applies to CSF AG, affiliated companies and their employees. The Data Protection Policy extends to all processing of personal data. In countries where the data of legal entities is protected to the same extent as personal data[4], this Data Protection Policy applies equally to data of legal entities. Anonymized[5] data, e.g. for statistical evaluations or studies, is not subject to this Data Protection Policy.

The latest version of the Data Protection Policy can be accessed with the data privacy information at CSF's website: www.csf.ch.

III. Application of national laws

This Data Protection Policy comprises the internationally accepted data privacy principles without replacing the existing national laws. It supplements the national data privacy laws. The relevant national law will take precedence in the event that it conflicts with this Data Protection Policy, or it has stricter requirements than this Policy. The content of this Data Protection Policy

[1] Refer XV.
[2] Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
[3] Refer XV.
[4] Refer XV.
[5] Refer XV.

must also be observed in the absence of corresponding national legislation. The reporting requirements for data processing under national laws must be observed.

IV. Principles for processing personal data

1. Fairness and lawfulness

When processing personal data, the individual rights of the data subjects[6] must be protected. Personal data must be collected and processed in a legal and fair manner.

2. Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

3. Transparency

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:

- The identity of the Data Controller[7]
- The purpose of data processing
- Third parties[8] or categories of third parties to whom the data might be transmitted

4. Data reduction and data economy

Before processing personal data, you must determine whether and to what extent the processing of personal data is necessary in order to achieve the purpose for which it is undertaken.

Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

5. Deletion

Personal data that is no longer needed[9] after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the

[6] Refer XV.
[7] Refer XV.
[8] Refer XV.
[9] Refer XV.

interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

6. Factual accuracy; up-to-date status of data

Personal data on file must be correct, complete, and - if necessary - kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

7. Confidentiality and data security

Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

V. Reliability of data processing

Collecting, processing and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

1. Customer and partner data

1.1 Data processing for a contractual relationship

Personal data of the relevant prospects, customers and partners can be processed in order to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract - during the contract initiation phase - personal data can be processed to prepare bids or purchase orders or to fulfil other requests of the prospect that relate to contract conclusion. Prospects can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospects must be complied with. For advertising measures beyond that, you must observe the following requirements under V.1.2.

1.2 Data processing for advertising purposes

If the data subject contacts CSF AG to request information (e.g. request to receive information material about a product), data processing to meet this request is permitted.

Customer loyalty or advertising measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The data subject must be informed about the use of his/her data for advertising purposes. If data is collected only

for advertising purposes, the disclosure from the data subject is voluntary. The data subject[10] shall be informed that providing data for this purpose is voluntary. When communicating with the data subject, consent shall be obtained from him/her to process the data for advertising purposes. When giving consent, the data subject should be given a choice among available forms of contact such as regular mail, e-mail and phone (Consent, see V.1.3).

If the data subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

1.3 Consent to data processing

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed in accordance with IV.3. of this Data Protection Policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

1.4 Data processing pursuant to legal authorization

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed in accordance with IV.3. of this Data Protection Policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

1.5 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary for a legitimate interest of the CSF AG. Legitimate interests are generally of a legal (e.g. collection of outstanding receivables) or commercial nature (e.g. avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

1.6 Processing of highly sensitive data

Highly sensitive[11] personal data can be processed only if the law requires this or the data subject has given express consent. This data can also be processed if it is mandatory for asserting, exercising or defending legal claims regarding the data subject. If there are plans to process highly sensitive data, the 0 must be informed in advance.

[10] Refer XV.
[11] Refer XV.

1.7 Automated individual decisions

Automated processing of personal data that is used to evaluate certain aspects (e.g. credit-worthiness) cannot be the sole basis for decisions that have negative legal consequences or could significantly impair the data subject. The data subject must be informed of the facts and results of automated individual decisions and the possibility to respond. To avoid erroneous decisions, a test and plausibility check must be made by an employee.

1.8 User data and internet

If personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a privacy statement and, if applicable, information about cookies. The privacy statement and any cookie information must be integrated so that it is easy to identify, directly accessible and consistently available for the data subjects.

If use profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy statement. Personal tracking may only be effected if it is permitted under national law or upon consent of the data subject. If tracking uses a pseudonym, the data subject should be given the chance to opt out in the privacy statement.

If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.

2. Employee data

2.1 Data processing for the employment relationship

In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorized data processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws have to be observed. In cases of doubt, consent must be obtained from the data subject.

There must be legal authorization to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the company.

2.2 Data processing pursuant to legal authorization

The processing of personal employee data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorized data processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

2.3 Collective agreements on data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorized through a collective agreement. Collective agreements are pay scale agreements or agreements between employers and employee representatives, within the scope allowed under the relevant employment law. The agreements must cover the specific purpose of the intended data processing activity, and must be drawn up within the parameters of national data protection legislation.

2.4 Consent to data processing

Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented. In the event of informed, voluntary provision of data by the relevant party, consent can be assumed if national laws do not require express consent. Before giving consent, the data subject must be informed in accordance with IV.3. of this Data Protection Policy.

2.5 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary to enforce a legitimate interest of CSF AG. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature.

Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection.

Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion, and cannot be performed unless appropriate. The legitimate interest of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (e.g. rights of co-determination for the employee representatives and information rights of the data subjects) must be taken into account.

2.6 Processing of highly sensitive data

Highly sensitive personal data can be processed only under certain conditions. Highly sensitive data is data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be filled out differently. Moreover, data that relates to a crime can often be processed only under special requirements under national law.

The processing must be expressly permitted or prescribed under national law. Additionally, processing can be permitted if it is necessary for the responsible authority to fulfil its rights and duties in the area of employment law. The employee can also expressly consent to processing.

If there are plans to process highly sensitive data, the Data Protection Officer must be informed in advance.

2.7 Automated decisions

If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g. as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee. To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The data subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

2.8 Telecommunications and internet

Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the company primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the CSF network that block technically harmful content or that analyse the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person can be made only in a concrete, justified case of suspected violations of laws or policies of the CSF AG. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met. The relevant national laws must be observed in the same manner as the company regulations.

VI. Transmission of personal data

Transmission of personal data to recipients outside or inside the CSF AG is subject to the authorization requirements for processing personal data under Section V. The data recipient must be required to use the data only for the defined purposes.

In the event that data is transmitted to a recipient outside the CSF AG to a third country[12], this country must agree to maintain a data protection level equivalent to this Data Protection Policy. This does not apply if transmission is based on a legal obligation.

If data is transmitted by a third party to the CSF AG company, it must be ensured that the data can be used for the intended purpose.

VII. Contract data processing

Data processing on Behalf means that a provider is hired to process personal data, without being assigned responsibility for the related business process. In these cases, an agreement on Data Processing on Behalf must be concluded with external providers and among companies within the CSF AG. The client retains full responsibility for correct performance of data processing. The provider can process personal data only as per the instructions from the client. When issuing the order, the following requirements must be complied with; the department placing the order must ensure that they are met.

1) The provider must be chosen based on its ability to cover the required technical and organizational protective measures.
2) The order must be placed in writing. The instructions on data processing and the responsibilities of the client and provider must be documented.
3) The contractual standards for data protection provided by the Data Protection Officer must be considered.
4) Before data processing begins, the client must be confident that the provider will comply with the duties. A provider can document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.
5) In the event of cross-border contract data processing, the relevant national requirements for disclosing personal data abroad must be met. In particular, personal data from the European Economic Area can be processed in a third country only if the provider can

[12] Refer XV.

prove that it has a data protection standard equivalent to this Data Protection Policy. Suitable tools can be:

a. Agreement on EU standard contract clauses for contract data processing in third countries with the provider and any subcontractors.

b. Participation of the provider in a certification system accredited by the EU for the provision of a sufficient data protection level.

c. Acknowledgment of binding corporate rules of the provider to create a suitable level of data protection by the responsible supervisory authorities for data protection.

VIII. Rights of the data subject

Every data subject has the following rights. Their assertion is to be handled immediately by the responsible unit and cannot pose any disadvantage to the data subject.

1) The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected.
2) If personal data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.
3) If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.
4) The data subject can object to the processing of his or her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use.
5) The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.
6) The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

Additionally, every data subject can assert the rights under III. Para. 2, IV. V., VI. IX., X and XIV. Para. 3 as a third-party beneficiary if a company that has agreed to comply with the Data Protection Policy does not observe the requirements and violates the party's rights.

IX. Confidentiality of processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The "need to know" principle applies. Employees may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

X. Processing security

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification).

In particular, the responsible department can consult with the Chief Information Security Officer (CISO). The technical and organizational measures for protecting personal data are part of Corporate Information Security management and must be adjusted continuously to the technical developments and organizational changes.

XI. Data protection control

Compliance with the Data Protection Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the Data Protection Officer, and other company units with audit rights or external auditors hired. The results of the data protection controls must be reported to the CISO. CSF AG's Board must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the responsible data protection authority. The responsible data protection authority can perform its own controls of compliance with the regulations of this Policy, as permitted under national law.

XII. Data protection incidents

All employees must inform the CISO immediately about cases of violations against this Data Protection Policy or other regulations on the protection of personal data (data protection incidents)[13].

In cases of

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

the required company reports (Information Security Incident Management) must be made immediately so that any reporting duties under national law can be complied with.

XIII. Responsibilities and sanctions

The employees are responsible for data processing in their area of responsibility. Therefore, they are required to ensure that the legal requirements, and those contained in the Data Protection Policy, for data protection are met. Management staff are responsible for ensuring that organizational, HR, and technical measures are in place so that any data processing is carried out in accordance with data protection. Compliance with these requirements is the responsibility of the relevant employees. If official agencies perform data protection controls, the CISO must be informed immediately.

Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted in many countries and result in claims for compensation of damage. Violations for which individual employees are responsible can lead to sanctions under employment law.

XIV. Data Protection Officer

The Data Protection Officer, being internally independent of professional orders, works towards the compliance with national and international data protection regulations. He is responsible for the Data Protection Policy, and supervises its compliance. The Data Protection Officer is appointed by the CSF AG Board of Management.

[13] Refer XV.

Any data subject may approach the Data Protection Officer, or the relevant data protection coordinator, at any time to raise concerns, ask questions, request information or make complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially.

If the data coordinator in question cannot resolve a complaint or remedy a breach of the Policy for data protection, the Data Protection Officer must be consulted immediately. Decisions made by the Data Protection Officer to remedy data protection breaches must be upheld by the management of the company in question. Inquiries by supervisory authorities must always be reported to the Data Protection Officer.

Contact details for the Data Protection Officer and staff are as follows:

CSF Computer Solutions Facility AG,

Markus Haas, Data Protection Officer,

Güterstrasse 107,

4133 Pratteln.

Email: markus.haas@csf.ch

XV. Definitions

- Data is anonymized if personal identity can never be traced by anyone, or if the personal identity could be recreated only with an unreasonable amount of time, expense and labour.
- Consent is the voluntary, legally binding agreement to data processing.
- Data protection incidents are all events where there is justified suspicion that personal data is being illegally captured, collected, modified, copied, transmitted or used. This can pertain to actions by third parties or employees.
- Data subject under this Data Protection Policy is any natural person whose data can be processed. In some countries, legal entities can be data subjects as well.
- The European Economic Area (EEA) is an economic region associated with the EU, and includes Norway, Iceland and Liechtenstein.
- Highly sensitive data is data about racial and ethnic origin, political opinions, religious or philosophical beliefs, union membership or the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be structured differently. Moreover, data that relates to a crime can often be processed only under special requirements under national law.

- Personal data is all information about certain or definable natural persons. A person is definable for instance if the personal relationship can be determined using a combination of information with even incidental additional knowledge.
- Processing personal data means any process, with or without the use of automated systems, to collect, store, organize, retain, modify, query, use, forward, transmit, disseminate or combine and compare data. This also includes disposing of, deleting and blocking data and data storage media.
- Processing personal data is required if the permitted purpose or justified interest could not be achieved without the personal data, or only with exceptionally high expense.
- Data Controller is the legally independent company CSF AG, whose business activity initiates the relevant processing measure.
- A sufficient level of data protection in third countries is acknowledged by the EU Commission if the core of personal privacy, as unanimously defined in the member countries of the EU is adequately ensured. When making its decision, the EU Commission accounts for all circumstances that play a role in data transmission or a category of data transmission. This includes the opinions under national law and relevant applicable professional standards and security measures.
- Third countries under the Data Protection Policy are all nations outside the European Union/ EEA. This does not include countries with a data protection level that is considered sufficient by the EU Commission.
- Third parties are anyone apart from the data subject and the Data Controller. In a case of Data Processing in Behalf data processors in the EU are not third parties under the data protection laws, because they are assigned by law to the responsible entity.
- Transmission is all disclosure of protected data by the responsible entity to third parties.

End of document.