

Studierendenwerk Thüringen privacy policy

(updated 05/23/2018)

Foreword

Dear Sir / Madam,

The digital age allows us the opportunity to accelerate many of our business and management processes when servicing all students of Thuringian institutes of higher education, and to manage these more efficiently. In doing this, data is gathered and processed, sometimes very extensively, on a daily basis and in every area of Studierendenwerk Thüringen's activities.

But no matter whether this is through the booking of accommodation place in one of our facilities or through an application for a student maintenance loan (BAföG), our policy remains the same: wherever data is saved and sent, a high degree of data protection and security must be upheld. This is the case for students, our business partners and for our staff. Data protection is, after all, the protection of an individual.

For this reason, we see it as our responsibility as a state-wide service provider to reflect statutory requirements regarding the gathering and processing of personal data. Every person in contact with Studierendenwerk Thüringen can be sure that we will safeguard personal rights and the privacy of the individual concerned, along with providing protection against unauthorized access. This is our agreement and the basis of all trustful cooperation.

In this data protection policy, we have set strict standards which apply to the processing of data from students, business partners and from staff. These reflect the requirements of European data protection policy as well as the applicable regulations of German national data protection law.

Our fundamental data protection policies are transparency and legality of data gathering, data economy, appropriation of data and security of data. Every member of staff is obligated to adhere to this privacy policy and to the respective data protection legislation. As the Data Protection Officer for Studierendenwerk Thüringen, I will ensure that the statutory regulations and principles regarding data protection are upheld.

I am available as a contact person for all questions pertaining to data protection and data security within Studierendenwerk.

Annett Gelbke

Data Protection Officer for Studierendenwerk Thüringen

Inhaltsverzeichnis

I.	<i>Aim of privacy policy</i>	3
II.	<i>Field of application and change to privacy policy</i>	3
III.	<i>Application of statutory rights</i>	3
IV.	<i>Principles for the processing of personal data</i>	4
	1. <i>Fairness and legality</i>	4
	2. <i>Appropriation</i>	4
	3. <i>Transparency</i>	4
	4. <i>Data reduction and data economy</i>	4
	5. <i>Deletion</i>	5
	6. <i>Factual accuracy and actuality of data</i>	5
	7. <i>Confidentiality and data security</i>	6
V.	<i>Admissibility of data processing</i>	6
	1. <i>Customer and partner details</i>	6
	1.1 <i>Data processing due to contractual relationship</i>	6
	1.2 <i>Data processing for advertising purposes</i>	7
	1.3 <i>Consent in data processing</i>	7
	1.4 <i>Data processing based on legal authorization</i>	7
	1.5 <i>Data processing due to legitimate interest</i>	7
	1.6 <i>Processing of particularly sensitive data</i>	8
	1.7 <i>User data and internet</i>	8
	2. <i>Staff data</i>	9
	2.1 <i>Data processing for employment relationships</i>	9
	2.2 <i>Data processing due to legal permission</i>	9
	2.3 <i>Collective working regulations for data processing</i>	10
	2.4 <i>Consent in data processing</i>	10
	2.5 <i>Data processing due to justified interest</i>	10
	2.6 <i>Processing of particularly sensitive data</i>	11
	2.7 <i>Automated decisions</i>	12
	2.8 <i>Telecommunication and internet</i>	12
VI.	<i>Transfer of personal details</i>	13
VII.	<i>Contract data processing</i>	13
VIII.	<i>Rights of affected individuals</i>	14
IX.	<i>Confidentiality of data processing</i>	15
X.	<i>Security of data processing</i>	16
XI.	<i>Privacy monitoring</i>	17
XII.	<i>Data security incidents</i>	17
XIII.	<i>Responsibilities and sanctions</i>	18
XIV.	<i>The Studierendenwerk Thüringen Data Protection Officer</i>	18
XV.	<i>Definitions</i>	19

Note: In the interest of better readability, neither male nor female forms are used throughout this text. All references to persons are valid for both genders.

I. Aim of privacy policy

As part of its social responsibilities as a service provider and contact party for all students at Thuringian institutes of higher education as well as an employer of around 650 staff, Studierendenwerk Thüringen binds itself to the strict adherence to data protection law. This data protection policy creates, among other things, necessary and uniform parameters for the data handling processes which take place on a daily basis in all seven pillars of Studierendenwerk Thüringen's public activity (student living, institute catering, educational support, childcare facilities, psychological, legal and social counselling) but also in human resource management.

II. Field of application and change to privacy policy

This privacy policy applied to all staff of Studierendenwerk Thüringen. Due to protective purposes, this also applies to persons who, as unpaid interns, tutors or freelancers working for and in the name of Studierendenwerk Thüringen, are not employed in the strictest sense but who nevertheless come into contact with personal data. This privacy policy extends to all processing of personal data¹. Anonymous data, e.g. for statistical analysis or examination, are not subject to this policy. Changes to this policy may only take place with the agreement of the Studierendenwerk Thüringen Data Protection Officer (hereinafter DPO) and the management (e.g. in the case of changes to current data protection law).

III. Application of statutory rights

Through this privacy policy, current public data protection law is not replaced, but rather duly appropriated and supplemented in relation to the individual tasks carried out by Studierendenwerk Thüringen. Priority is always given to German national and European legislation, provided that these are more stringent requirements than those listed in the policy.

¹ see XV.

IV. Principles for the processing of personal data

1. Fairness and legality

When processing² personal data, the personal rights of the individual³ concerned must be taken into account and safeguarded. Personal data must be gathered and processed in a fair and legal manner (e.g. on the basis of legal authorization and consent of the individual).

2. Appropriation

The processing of personal data will always take place in a purposeful manner and may only fulfil the purpose set out before the data is submitted. Subsequent changes in purpose are fundamentally prohibited and require a justification (e.g. notification and express consent of the individual pertaining to the intended change of purpose).

3. Transparency

Individuals must be informed about the processing of their personal data at the time of its submittal. Fundamentally, submittal of data must be carried out by the individual themselves. The individual must then be able to understand or be informed of at least the following:

The identity of the responsible organization⁴, the purpose of the data processing, and, in the case of an authorized forwarding of data, the identity of the third party⁵, which will receive this data.

4. Data reduction and data economy

Before every case of personal data processing, it is to be assessed whether, and to what extent, this is necessary to complete the task concerned and for the intended purpose. Priority is given to the usage of anonymous or statistical data if it is sufficient for the fulfilment of a purpose or to carry out a task if no unreasonable complexity is caused.

² see XV.

³ see XV.

⁴ see XV.

⁵ see XV.

Data processing using identifiers or pseudonyms is always to be taken into consideration. Personal details are not to be saved as provision for potential future purposes, unless this is required by law or authorized.

In the application of new data processing software, priority is to be given to data protection-friendly products. Furthermore, before activating new software it is always to be ensured that preferences are selected where the minimum amount of data is gathered in order to fulfil the intended purpose or to complete the intended task.

5. Deletion

Personal data which is no longer required⁶ due to expiry of a legal or business process-related retention period must be routinely deleted without the request of the individual concerned. Every department of Studierendenwerk Thüringen ensures that an assessment of databanks used in data processing and of administrative acts takes place at least once a year for this purpose. After this, personal data and records for which there is no longer any reason for their storage are deleted. The deletion of data to be carried out is to be documented in writing: compulsory are date of deletion, member of staff responsible, and extent of deletion. The documentation of data deletion is to be kept available for possible assessments in the respective department. In the rare event of interest points worthy of protection or of personal details with historical importance, data must continue to be saved until the interest point has been legally clarified and the piece of data can then be assessed for its archival value for historical purposes.

6. Factual accuracy and actuality of data

Personal data is to be saved correct, complete and, where required, as up-to-date as possible. Across all departments it is to be ensured that non-applicable, incomplete or obsolete data is deleted, corrected, completed or brought up to date.

7. Confidentiality and data security

Data secrecy is applied when dealing with personal data. Data must be handled confidentially in personal contact and must be secured through appropriate

⁶ Siehe XV.

organizational and technical measures against unauthorized access, unlawful processing or transfer, as well as accidental loss, change or destruction.

V. Admissibility of data processing

The gathering, processing and usage of personal data is only admissible if one of the following permissions exists. Such permissions are also required if the purpose for the gathering, processing and usage of personal data must be changed from the original intended purpose.

1. Customer and partner details

1.1 Data processing due to contractual relationship

Personal details of the interested parties concerned or of contractual partners may be processed for the justification, implementation and ending of a contract. This also extends to the written and telephone support of interested parties or contractual partners, as long as this is in context with the purpose of the contract. Prior to a contract, i.e. in the phase of initiation, the processing of personal data is allowed in order to create offers, to prepare contracts or to otherwise fulfil interested parties' wishes pertaining to the signing of a contract. Data given may be used to contact interested parties during the phase of initiation. Any restrictions given by interested parties must always be taken into account. For advertising measures which exceed this, the following requirements in part V.1.2. must be heeded.

1.2 Data processing for advertising purposes

Should an individual contact Studierendenwerk Thüringen with an information query (e.g. requesting for information to be sent), data processing in order to fulfil this request is permissible. After the information query has been dealt with, the handled data is to be deleted immediately, unless the individual concerned has expressly given consent to in future be provided with further information regarding a certain topic (e.g. newsletters) through Studierendenwerk Thüringen. Data gathered in this way will not be forwarded to third parties.

1.3 Consent in data processing

Data processing may also take place with the consent⁷ of the individual concerned. According to IV.3., the individual must, prior to giving consent, be informed of this privacy policy. For purposes of proof, declaration of consent must always take place in writing or electronically.

1.4 Data processing based on legal authorization

Processing of personal data is also permissible if national law demands, requires or allows for this. The type and extent of data processing must be necessary for the legally authorized data processing and must comply with the relevant statutory regulations.

1.5 Data processing due to legitimate interest

Processing of personal data may also take place when this is necessary for the realization of a justified interest of Studierendenwerk Thüringen. Legitimate interests are usually legal (e.g. enforcement of claims) or commercial (e.g. avoidance of breaches of contract). Processing of personal data due to justified interests may not take place when, in isolated cases, there is reason for the protected interests of the individual concerned which outweigh its need. Protected interests must be assessed in every case of data processing.

1.6 Processing of particularly sensitive data

Processing of particularly sensitive⁸ personal data may only take place when required by law or when the individual concerned has given express consent. Processing of this data is also permissible when it is imperative to do so in order to satisfy, exercise or defend legal rights of the individual concerned. If the processing of particularly sensitive data is intended, the Studierendenwerk Thüringen DPO is to be informed in advance of the planned measures.

⁷ see XV

⁸ see XV

1.7 User data and internet

When personal data is gathered, processed and used on Studierendenwerk Thüringen websites, individuals are to be informed of this through corresponding data protection notices and, where applicable, cookie notices. Data protection and cookie notices are to be integrated in such a way that they are easy to recognize by the individual, understandable, immediately reachable and always available.

If usage profiles are to be created for the assessment of user behavior on Studierendenwerk Thüringen websites (i.e. tracking), individuals concerned must be advised of this in every case through privacy policy notices.

Personal tracking may only take place when legally permissible or when the individual has expressed consent. Should tracking take place under a pseudonym, the individual is to be informed through privacy policy notices of the possibility to object to this (i.e. opt-out).

If access to personal data is enabled through registration-only areas of Studierendenwerk Thüringen websites, the identification and authentication of individuals is to be technically designed in a way that a suitable level of protection is attained for the particular access to data. The corresponding department which offers the service concerned is responsible for reaching the technically appropriate level of protection. The Information Technology department is to be involved in this.

2. Staff data

2.1 Data processing for employment relationships

Personal data may be processed for employment relationships when it is required for the justification, execution and termination of an employment contract. In the preliminary stages of an employment contract, personal data of applicants may be processed. Data is to be deleted according to legislative deadlines after rejection of a candidate, unless the applicant has expressly consented to their data being saved for a later selection process.

In an existing working relationship, data processing must always be related to the employment contract, as long as none of the following permission clauses interferes with this. Should the gathering of further information about the applicant through a third party be necessary during the period prior to or after the start of an employment relationship, the corresponding national legal requirements are to be taken into account. In case of

doubt, the consent of the individual concerned is to be gained. A corresponding legal legitimization must always be present in the case of processing of personal data which is related to the context of the employment relationship but which does not distinctly serve to fulfil the employment contract. This may be statutory requirements, collective working regulations with employee representatives, a consent from the member of staff or the justified interests of Studierendenwerk Thüringen.

Staff data is always to be handled confidentially by the department of Human Resources. Access is to only be allowed for the purpose of task completion by the party responsible.

2.2 Data processing due to legal permission

Processing of personal staff data is also permissible if statutory regulations demand, require or allow for this. The type and extent of data processing must be necessary for the legally permissible data processing and depend on these statutory regulations. The protected interests of the member of staff concerned must be taken into account in the case of a legal flexibility.

2.3 Collective working regulations for data processing

If the processing of a piece of data extends beyond the purpose of contract implementation, it is still permissible if allowed by a collective working regulation.

Collective working regulations are labor contracts or agreements between employers and employee representatives within the scope of possibility from the current labor legislation. The regulations must extend to the exact purpose of the desired processing and are designed within the scope of statutory data protection law.

2.4 Consent in data processing

Processing of staff data may take place with the consent of the individual concerned. According to IV.3., the individual must, prior to giving consent, be informed of this privacy policy. For purposes of proof, declaration of consent must always take place in writing or electronically. If exceptional circumstances do not allow for this, consent may also be provided verbally. Every case of expression of consent must be correctly documented. In the case of an informed voluntary submittal of data by the individual concerned, consent may be assumed if state law does not stipulate this explicitly. According to IV.3., the individual must, prior to giving consent, be informed of this privacy policy.

2.5 Data processing due to justified interest

Processing of personal staff data may also take place when this is necessary for the realization of a justified interest of Studierendenwerk Thüringen. Justified interests are usually legal (e.g. enforcement of claims) or commercial (e.g. avoidance of breaches of contract). Processing of personal data due to justified interests may not take place when, in isolated cases, there is reason for the protected interests of the individual concerned which outweigh its need. Protected interests must be assessed in every case of data processing.

Assessment measures which require the processing of staff member data may only be carried out where there is a legal requirement or a justified reason to do so. Even when a justified reason is given, the proportionality of the assessment measure must be checked. The justified interests in the execution of the assessment measure (e.g. adherence to legal guidelines and rules internal to the organization) must be balanced against a possible protected interest of the member of staff concerned and may only be executed if deemed appropriate. In addition, further requirements according to statutory law (e.g. rights of co-determination of the workers' representation, information rights of the individual) must be taken into account.

2.6 Processing of particularly sensitive data

Processing of particularly sensitive personal data may only take place under certain conditions. Particularly sensitive data is data pertaining to racial and ethnic background, political opinion, union membership or about the health or sexual activity of the individual. This also includes genetic and biometric data which may clearly identify a person, or healthcare data.

Data pertaining to criminal offenses may often be handled only in compliance with special requirements set out in the applicable national laws. Processing of this data must be expressly permissible or required according to national law. Processing of data may also be authorized when it is necessary in order to fulfil the rights and obligations of the responsible body in the area of labor law. The member of staff concerned may also voluntarily express consent to data processing. The Studierendenwerk Thüringen Data

Protection Officer is to be informed if the processing of particularly sensitive data is intended.

2.7 Automated decisions

If automated processing of data, through which personality traits are evaluated (e.g. due to staff assessment) takes place within a contractual relationship, this automated processing may not be the sole basis for decisions resulting in negative consequences or considerable adverse effects for the member of staff concerned. To avoid errors, it must be ensured within automated processes that content of the assessment of facts is carried out by a real person and that decisions are based on this assessment. The member of staff concerned must also be notified of the nature and result of an individual automated decision and given the opportunity to respond to this.

2.8 Telecommunication and internet

Studierendenwerk Thüringen provides telephone systems, email addresses, intranet and internet along with social networks as part of its primary activities. These are working tools and company resources and may be used within the scope of the corresponding legal provisions and the company agreements and business directives internal to Studierendenwerk Thüringen. In the case of authorized usage for private purposes, secrecy of telecommunications and the corresponding current national telecommunication law are to be heeded as applicable.

A general monitoring of telephone and email communication, along with intranet and internet usage, will not take place. In order to protect the IT infrastructure or individual users from attacks, protective measures may be implemented at gateways to network interfaces which block technically damaging content or which analyze the pattern of attacks. For security reasons, the use of telephone systems, email addresses, intranet and internet as well as internal social networks may be logged for limited time periods. Assessments of this data specific to individual persons may only take place due to a tangible justified suspicion of a violation of laws or of the guidelines / service agreements of Studierendenwerk Thüringen. These audits may only take place through determined areas while abiding by the principle of proportionality. The coordinating national laws or contractual provisions must be heeded.

VI. Transfer of personal details

Transfer of personal details to parties external to Studierendenwerk Thüringen is subject to the prerequisites of the processing of personal data according to part V.. The party receiving data must always (contractually) be obliged only to use data for the purposes outlined. In the case of a data transfer to a party located in a third country⁹, an level of data protection equal to in these guidelines must be provided by this party. This does not apply when transfer takes place due to legal requirement.

VII. Contract data processing

Contractual data processing takes place when a party other than Studierendenwerk Thüringen is tasked with processing personal data without carrying the responsibility of executing the related business process. In such cases, an agreement regarding contract data processing is to be signed with external contractors. Prior to signing, contractual agreements are always to be presented to the Legal Affairs department and the DPO in order to ensure that legal data protection requirements are complied with.

The client Studierendenwerk Thüringen retains full responsibility for the correct execution of data processing. The contractor may only process data according to instructions from Studierendenwerk Thüringen. At the issuance of the contract, the following specifications are to be adhered to; the relevant department of the client must ensure their implementation.

- 1. The contractor is to be selected according to its ability to implement the necessary technical and organizational protective measures.*
- 2. The contract is to be issued in written form. Instructions regarding data processing and the responsibilities of the client and the contractor are to be documented here.*
- 3. The contractual standards provided by the DPO must be heeded.*
- 4. Before commencement of data processing, the client must be satisfied with the contractor's adherence to responsibilities. Adherence to data protection requirements*

⁹ see XV.

may be verified by providing a relevant certification. Depending on the risk factor of data processed, this assessment may be repeated regularly for the duration of the contract.

5. In the case of transnational data processing, the corresponding national requirements for the international transfer of personal data are to be heeded. In particular, data processing in countries outside of the European Economic Area may only take place when the contractor is able to verify a level of data protection equal to that outlined in this data protection policy. Suitable instruments may include:

- a. Arrangement of the EU Standard Contractual Clauses for data processing in non-EEA countries with the contractor and possible subcontractors.*
- b. Participation of the contractor in an EU-approved certification system to maintain an appropriate level of data protection.*
- c. Approval of mandatory company rules to maintain an appropriate level of data protection through the responsible data protection regulatory body.*

VIII. Rights of affected individuals

Every individual may exercise the following rights regarding Studierendenwerk Thüringen free of charge. Their enforcement is to be processed immediately by the corresponding responsible department and may not cause the individual concerned any kind of detriment.

- 1. An individual may request information regarding which personal data from which source are saved about them for what purpose. In the case that in a working contract, ongoing document inspection rights (e.g. for personal files) are provided according to the corresponding labor laws, these remain unaffected.*
- 2. If personal data is authorized to be forwarded to third parties, the identity of the recipient or the category of recipients of data must be made known.*
- 3. If personal data is incorrect or incomplete, the individual may request its correction or completion.*

4. *The individual retains at all times the right to withdraw consent regarding the processing of their personal data. This must always be noted in the declaration of consent. In the case of a withdrawal of consent, personal data must be deleted after a maximum of 3 days.*

5. *The individual has the right to request the deletion of their data when the legal basis for the processing of data is missing or no longer apparent. This also applies in cases where the purpose of data processing has lapsed due to expiry or for other reasons. Existing retention obligations and legitimate interests which prevent deletion must be taken into account and communicated to the individual in a comprehensible manner.*

6. *The individual has a statutory right of objection to the processing of their data which is always to be taken into consideration when legitimate interest due to a personal situation outweighs the interest of data processing. This does not apply when a legal regulation requires the processing of data.*

IX. Confidentiality of data processing

It is statutory that personal data is subject to data secrecy. Members of staff are prohibited from unauthorized gathering, processing or usage of data. Every instance of data processing in which a member of staff is not consigned to and authorized to carry out the task is prohibited. The 'need-to-know' principle applies here.

Members of staff may only gain access to personal data when, and as long as, this is necessary for their respective tasks. This requires the careful delegation and separation of roles and responsibilities as well as their application and maintenance within the authorization concept.

Members of staff may not use personal data for their own private or commercial needs, pass data on to unauthorized persons or make data accessible by other means. Supervisors must instruct members of staff at the beginning of a working relationship of their obligation to adhere to data secrecy, which is to be documented in writing in the form of a confidentiality agreement. This obligation continues to exist after the termination of a working relationship.

X. Security of data processing

Personal data is to be protected at all times against unauthorized access, wrongful handling or transfer, loss, falsification or deletion. This applies irrespective of whether the data is stored in electronic or paper form.

Prior to the introduction of new data handling processes, especially in the case of new IT systems, it is compulsory that technical and organizational measures for the protection of personal data are stipulated in writing and to be implemented (data protection impact assessment). These measures must be oriented to the status of the technology, the risks associated with the processing and the level of protection required by the data (ascertained through the information classification process). The responsible department must always consult the Information Technology department and the DPO in this matter. The technically organizational measures for the protection of personal data are part of information security management and are to be continually adapted to technical developments and to organizational changes.

XI. Privacy monitoring

Adherence to data protection policies and to the applicable data protection laws will be regularly assessed through monitoring. This will be carried out by the DPO as well at the head of the IT department. Results of privacy monitoring are to be documented in writing and to be notified to the management, which has an independent right to supervision of this at any time. Upon request, results of privacy monitoring may be made available to the responsible data protection authority. The responsible data protection authority may, as part of its powers according to national law, also carry out its own monitoring of the adherence to regulations outlined in this policy.

XII. Data security incidents

Every member of staff is obligated to immediately inform their supervisor or the Studierendenwerk Thüringen DPO of breaches of this data privacy policy or of other regulations pertaining to the protection of personal data (data security incidents¹⁰) The

¹⁰ see XV.

responsible department leader is obligated to inform the DPO immediately regarding data security incidents.

An immediate report is particularly necessary in the case of:

- unauthorized forwarding of personal data to third parties;
- unauthorized access to personal data through third parties (e.g. data theft);
- loss of personal data.

According to law, such cases must be immediately reported by members of staff in order to fulfil obligations to individuals and to state supervisory bodies regarding the reporting of data security incidents (**72-hour rule**).

XIII. Responsibilities and sanctions

The management is responsible for data processing within Studierendenwerk Thüringen in its entirety. The management is therefore obligated to ensure that both legislative requirements and those contained in this privacy policy are upheld (e.g. national reporting obligations). It is a responsibility of the management to ensure lawful data processing which heeds data protection standards.

Application of these guidelines is the responsibility of the corresponding member of staff. The DPO is to be informed immediately in the case of privacy monitoring through an authority. Every department must appoint a Data Protection Coordinator, who will function as a contact person for the DPO and who will execute, document and manage regular data deletion cycles.

The management is obligated to support the DPO and the departmental Data Protection Coordinators in their work. Staff responsible for business processes and projects must inform the DPO promptly regarding new processing of personal data. The DPO is always to be involved before the commencement of planned data processing which poses particular risks to the personal rights of individuals. The corresponding managers must ensure that their members of staff are educated to a sufficient extent regarding data protection and that they are instructed about changes to data processing. Unlawful processing of personal data or other breaches of data protection law may result in

criminal prosecution and payments for damages. Infringements caused by individual members of staff may furthermore lead to sanctions as part of labor law.

XIV. The Studierendenwerk Thüringen Data Protection Officer

The Studierendenwerk Thüringen Data Protection Officer serves as an internal body who, independent of directives, works towards the adherence to national and international data protection regulations. They are responsible for data protection regulations and survey compliance to these. The DPO is nominated and appointed by the management. Contact details of the DPO are to be notified to the corresponding regulatory authority by the management.

Any individual or member of staff may contact the DPO or their department's Data Protection Coordinator with suggestions, queries, requests for information or complaints pertaining to questions about data protection and data security.

Queries and complaints may be handled with confidentiality if desired. Should the DPO be unable to remedy a situation or to take corrective action against a breach of data protection regulations alone, the management must be informed immediately in order to discuss and initiate the correct measures. Queries from authorities must always be reported to the DPO.

XV. Definitions

¹ *Personal data is all information pertaining to an identified or identifiable natural person. A person is identifiable when the reference to the person, as well as the identification, may only be put together through a combination of factors and only with coincidentally available knowledge.*

² *Processing of personal data is every instance, with or without the aid of automated processing, of data gathering, saving, organization, storage, alteration, retrieval, usage, transfer, forwarding, or distribution, as well as the combination and comparison of data. Also a part of this are the disposal, deletion and blocking of data and data storage devices.*

³ *An individual person, in the case of this data privacy policy, is any natural person whose data is processed.*

⁴ *The responsible body, in the case of this data privacy policy, is Studierendenwerk Thüringen, as far as their business activity brings about the processing measures in question.*

⁵ *Third parties are every natural or juristic person / authority / place external to the individual concerned and to the organization responsible for data processing. Contract data processors are not third parties according to data protection law, as they are legally assigned to the responsible body.*

⁶ *Processing of personal data is required when the valid purpose or legitimate interest cannot be achieved, or may only be achieved through unreasonable complexity, without the personal data in question.*

⁷ *Consent is a voluntary, legally-binding declaration of consent in an instance of data processing.*

⁸ *Sensitive information is data pertaining to racial and ethnic background, political opinion, religious or philosophical beliefs, membership of trade unions or the health or sexual activity of the individual concerned. This also applies to genetic and biometric data which may easily identify a person, and to health data. Due to national law, further categories of data may also be classified as sensitive information, or the content of data categories may vary. Data pertaining to criminal offenses may often be processed only under special requirements outlined by national law.*

⁹ *Third countries, in the case of this data privacy policy, are all states external to the European Union or the European Economic Area. Excluded are states where the level of data protection has been acknowledged as acceptable by the EU Commission.*

¹⁰ *Data protection incidents are all incidences in which a justified suspicion exists of the unauthorized spying out, gathering, alteration, copying, transfer or usage of personal data. This pertains to acts by third parties as well as by members of staff.*


Studierendenwerk Thüringen Data Protection Officer contact details

Studierendenwerk Thüringen

- Datenschutzbeauftragte -

Philosophenweg 22

07743 Jena

 *03643/58156303643 581563*

 *datenschutzbeauftragter@stw-thueringen.de*