(as of March 2022)

DATA PROTECTION - INFORMATION SHEET FOR STUDENTS

Information on data processing and the rights of data subjects

Please note that the German version of the privacy notice is recognized as legally valid.

Dear students,

we take data protection at our university very seriously and your rights in this regard are very important to us. You receive here all notifiable and worth knowing information about the data protection of the AStA at the University of Lüneburg.

Who is responsible for data protection at the AStA and whom can you contact if you have any questions?

Responsible body in the sense of the GDPR is:

Student body of the University of Lüneburg
Represented by the AStA spokespersons
Universitätsallee 1, 21335 Lüneburg
Phone: 04131 / 677 - 1510
E-mail: sprecherinnen@asta-lueneburg.de
Website: www.asta-lueneburg.de

Our Data Protection Officer:

Tobias Lange
External data protection officerBerner
Heerweg 246, 22159 Hamburg
Germany
E-mail: datenschutz@asta-lueneburg.de
Phone: 040/ 5700 3925

Organization of the AStA and various sub-organizations:

In order to carry out its activities, the AStA forms a large number of independent organizations, bodies, units or other representations or those operating under the AStA. For this purpose, the AStA, represented by the AStA spokespersons, is the responsible body in terms of data protection.

An overview of our organizations, bodies, units and other representations can be found on our website: www.asta-lueneburg.de The lists on our website do not claim to be complete. Furthermore, not every association of students at the university is basically legitimized under the AStA. Students are free to organize themselves as they wish and to be active in any legal form (university) publicly, without being subject to the AStA. If there is any doubt as to whether an organization belongs to the AStA, clarification can be obtained by contacting the AStA. This data protection information only refers to organizations, bodies, units and representations that are legitimized by the AStA.

Special protection of personal data of minors in relation to information society services:

The legislator has provided that personal data of persons under 16 years of age are in need of special protection in the processing with information society services and has expressed this in Art. 8 and in other places of the GDPR.

Our offerings, both online and offline, are not explicitly or primarily aimed at young people under the age of 16. Nevertheless, persons in this group can and do obtain information from us about study opportunities and other topics. As a matter of principle, we do not collect or process any personal data on our websites, including data from young people under the age of 16. We also do not use any third-party applications in our web pages that could do so, nor do we load content from third-party servers on web pages. In particular, we do not use tracking cookies or other technologies that could record user behavior and track it beyond applications and devices.

In the context of hardship applications, data of persons under 16 years of age may be stored and processed, namely data on students' own children or young people living in the household of a community of responsibility. This is only done in order to prove a neediness in the context of the examination of the hardship case applications. The processing and subsequent storage of such data is also carried out in a digital manner. We have taken special technical and organizational measures for such data to ensure particularly secure processing.

Purposes, legal bases and duration of the storage of personal data:

We collect and process data on the basis of the statutes and tasks that we have to fulfill at the University of Lüneburg. For this purpose, personal data is transferred to us by the university within the framework of your contracts with the university. We do not process your/your data for any other purpose

than for the performance of the tasks prescribed by the University. In particular, we do not transfer your data to unauthorized third parties nor do we create profiles from the personal data within the meaning of Art. 4 (4) GDPR.

The legal basis for the processing of the data is the contract concluded with you with the university and the Lower Saxony Higher Education Act. According to this, we are allowed to store and process all personal data of you that is directly necessary for the execution of the tasks of the AStA, as well as to receive this data from the university for this purpose, in accordance with Art. 6 Para. 1 lit. b.) and c.) GDPR.

We are required by law to document or transfer certain data from you/you to the university as part of our tasks, which is done on the basis of Art. 6 para. 1 lit. c.) GDPR. We collect personal data beyond the aforementioned data in individual cases if this is necessary for the performance of the tasks or if separate circumstances make it necessary. Such collection and processing of personal data takes place either on the basis of a voluntary express consent by you/you, within the meaning of Art. 6 para. 1. lit. a.) GDPR, on the basis of a legitimate interest pursuant to Art. 6 para. 1 lit. f.) GDPR, due to the protection of your/your vital interests according to Art. 6 para. 1 lit. d.) GDPR, due to a public interest according to Art. 6 para. 1. lit. c.) or on the basis of Art. 6 para. 1 lit. f.) in conjunction with. Art. 9 para. 2 lit. f.) GDPR, if a legitimate interest also makes the processing of particularly sensitive data necessary.

This means in detail, whereby the following list is to be seen only as a list of all possible, but by no means actually collected data of each individual case:
We collect in connection with you generally when a purpose requires it:

- Name, address and contact details
- Dates of birth
- Matriculation numbers
- Subjects or data on the course of study
- Data on activities and voluntary tasks at the university

In special cases, we also collect and process biographical data (place of birth, curriculum vitae, education, schools attended and work activities as well as previous places of residence, etc.) from you if such information is necessary for the performance of certain tasks, for example, in the study financing counseling.

We will take appropriate and necessary means in the event of a medical emergency on your part, unless otherwise agreed. For this purpose, we also process your/your personal data, for example, when calling an ambulance.

If, in individual cases, a collection and processing of your personal data is carried out by us on the basis of a legitimate interest, we will only do so after weighing up your legitimate interests in protection, which must not exceed our interests, and consulting our data protection officer. In this case, the weighing of interests will be explained to you to an appropriate extent.

As part of the payment of contributions to the student body, we receive these directly from the university as a total sum for the number of enrolled students. We do not process or store any personal data in this process.

According to §4 of the statutes of the student body, students have a right of complaint. If this right is exercised, we process and store the personal data necessary for the purpose of processing such complaints. This is done in strict proximity to the best possible resolution of the complaint. Such data will not be processed for any other purpose and will be deleted after settlement. Should a possible legal claim against us or third parties arise from the complaint, we will retain such data in accordance with the statutory limitation periods.

The student body receives the personal data required to conduct the general assembly from the university administration under strict purpose limitation. The personal data received for this purpose will only be processed for the purpose of holding the General Assembly and will be deleted thereafter.

The student body forms numerous committees, boards and units. In these various sub-organizations of the student body, only the data of students who have voluntarily applied for or assumed offices are stored and processed on the basis of the respective statutes. We do not store and process any other personal data of students of the university. In particular, we do not maintain directories of all students or of students in individual areas at the university.

We have appointed an anti-discrimination officer. This person acquires knowledge of personal data, in particular also sensitive data including data requiring special protection pursuant to Art. 9 GDPR, in the course of performing this task. Anti-discrimination officers are trained separately on data protection and are committed to this in writing. Personal data obtained in this way is only processed for the purpose for which students seeking help have con-

tacted this office. The data will be stored as necessary. In the case of incidents of a certain severity with possible future legal claims arising from the incident, documentation and storage will take place. In this case, the retention period is based on the statutory limitation periods. Furthermore, documentation and storage can also take place for the purpose of defending legal claims against the anti-discrimination officers themselves. Data stored in connection with the performance of anti-discrimination counseling is stored in a particularly secure manner and protected from access by unauthorized persons. Persons performing this function are separately trained in data protection and are committed to data protection in writing.

Under the umbrella of the student body, we conduct "study career counseling" and have commissioned consultants to carry this out. Personal data obtained in connection with such counseling regularly contains health data within the meaning of Art. 9 GDPR. We process and store this data only for the purpose of carrying out the consultation. Insofar as simple inquiries are concerned, we refrain from storing them. Insofar as the inquiry has been made to us in writing, including by digital means, we delete such data after the consultation has been completed. In complicated, extensive consulting cases, we reserve the right to document the consultation for the purpose of possible later legal claims against us and to store it in accordance with the statutory limitation periods. Studium-Barriere consultants are specially trained in data protection and are obligated in writing to protect data.

We provide BAföG counseling under the umbrella of the student body. In this context, the advisors working for this service receive personal data, in particular also sensitive financial data and data of the most personal sphere of life. This may also include data that falls under Article 9 of the GDPR. We do not process such data for any other purpose than to advise on the individual case. As a matter of principle, we do not document or store personal data relating to our advice. If we are approached with complicated cases that could trigger possible legal consequences, we refer such inquiring students to the legal counsel of the student body. BAföG advisors are specially trained in data protection and are bound in writing to data protection.

We offer the possibility of a free legal consultation. This advice is provided by a law firm commissioned for this purpose. We do not receive any personal data in this context. For the purpose of billing for the service, we are only provided with the name and address data of the service recipients together with the invoices issued by the commissioned law firm.

In the context of hardship applications, we store and process data of the applicants for the purpose of processing applications for grants or reimbursements according to the hardship regulations of the university. In this context, special data within the meaning of Art. 9 GDPR may also be processed. The legal basis for this is Art. 6 para. 1 lit. e.) GDPR, if applicable in conjunction with Art. 9 para. 2. lit. a.) GDPR. The data processed and stored as part of the processing of hardship applications serve only the purpose of carrying out the processing and the possibility of a subsequent verification of accuracy. The processing is only carried out by separately trained employees of the AStA who are committed to data protection. Particularly high security standards apply to the storage and retention of data. The storage of data for the clarification of possible legal claims is 3 years.

We offer a so-called "bed exchange" as a service. Here, temporary rooms are arranged for new students at the university. Requests as well as offers are not published. The name, contact and address data received in this context are only processed manually in the AStA and appropriate contacts are established for this purpose. If necessary, we also use automated procedures for this purpose. The legal basis is provided by your/your explicit or also tacit consent, for example within the framework of the contact form on our website. The personal data required for this purpose will only be stored and processed for this purpose. If the purpose is fulfilled or no longer exists, the data will be deleted. A storage does not take place.

We offer counseling on "Parents in Studies (EliStu)". This is carried out by specific advisors appointed for this purpose. In this context, these advisors become aware of information relating to the highly personal sphere of the students' lives as well as information about minors or children. Information obtained in this way is only processed for the purpose of this consultation and, if necessary, stored for a short period of time. In principle, personal data obtained in this context will not be documented and stored. If inquiries are made in writing, including digitally, the data will be destroyed/deleted after the consultation has been completed. Advisors for "EliStu" are specially trained in data protection and are committed to data protection in writing.

We operate a bicycle repair shop under the umbrella of the student body. This operates commercially and is also registered accordingly. For the purpose of the implementation and on the basis of the AO (Abgabenordnung) and the HGB (Handelsgesetzbuch), invoices with personal data are created and customer correspondence is kept. Documents relevant to accounting and customer correspondence are

kept for 6 years. Documents relevant to the annual financial statements are kept for 10 years. Name and address data are processed. If contact data such as telephone numbers and e-mail addresses are processed, they are only retained for as long as there is a purpose for doing so.

We rent out rooms on the university premises for events and other purposes. In this context, we process the name, contact and address data required for this purpose, and possibly also matriculation numbers. This data is also transferred to the university in connection with the rental of the rooms and the purpose of the rental. Storage and processing only takes place as long as a purpose for this continues to exist. Such a purpose includes, in particular, storage and processing for subsequent complaints about the rooms in connection with the rental. If a purpose no longer exists, the data will be deleted. The university may have different regulations regarding storage, which should be enquired about there.

We rent out lockers in a building of the university. In this context, we process the name, contact and address data required for this purpose, and possibly also matriculation numbers. Storage and processing only takes place as long as a purpose for this continues to exist. Such a purpose includes in particular the storage and processing for subsequent complaints about the lockers in connection with the rental. If a purpose no longer exists, the data will be deleted.

We operate a sound and light rental service for events on the university campus under the umbrella of the student body. This is done without the intention of making a profit and without a commercial character. For this purpose, we process the name, address and contact data of the persons renting the equipment, as well as any expense allowances received for this purpose. Amounts received are recorded with personal data in the student body's accounts and processed and stored there in accordance with the statutes and legal provisions.
If we process data from you that fall under Art. 9 of the General Data Protection Regulation (GDPR) or have a special need for protection for any other reason, this will only be done on the basis of special technical and organizational measures that ensure the lawful storage and processing and, if necessary, also the onward transfer of this data.

We further regulate the specific processing of personal data and its purpose as well as storage in our statutes and regulations.

We keep personal data only as long as the purpose of processing. After this time, your data will be irretrievably deleted. If we are required by law to retain your data beyond this period, your data will be archived. Such data is restricted in processing and continues to exist only for the purpose of complying with the retention periods. They are only processed insofar as a request in this regard arises due to legal or other provisions or a legal defense is necessary.

When collecting and processing your personal data, we strictly adhere to the principle of data economy and minimal use. This principle is also the basis for the processing of your personal data by our employees and representatives. Employees and representatives only receive the personal data necessary for the provision of the respective service on the basis of the minimum principle.

Based on the principle of data economy, we also only transfer personal data to third parties if we are authorized or obligated to do so. The following is a list of possible authorized recipients, but not necessarily actual recipients of your personal data:

- Authorized representatives or contact persons named by you to us in writing
- Other students
- University jobs
- External third responsible parties

Whether a transfer to one of these recipients takes place in an individual case and with which scope of personal data, is based on the agreements made with you and the authorizations, consents and legal provisions available in the individual case.

We retain personal data that is subject to retention in accordance with the existing statutory provisions. According to this, certain data must be retained for up to 10 years. In detail:

- Business and commercial letters 6 years
- Accounting records 6 years
- Documents relevant to annual financial statements 10 years
- Accounting records 10 years
- Election documents according to the bylaws regularly for the existing election period
- Declarations of commitment to data protection or similar documents in accordance with the limitation periods 3 years

Furthermore, on the basis of §§ 195ff BGB (German Civil Code), a retention period of up to 30 years may be possible for the purpose of preserving legal evidence within the framework of statutory limitation periods in legal disputes. If we store personal data on this basis beyond the actual period of mandatory

retention, this is done on the basis of Art. 6 para. 1 lit f.) GDPR.

Personal data for which there are no retention obligations, no purpose of processing and no legitimate or public interest will be irrevocably deleted. If you exercise a right to which you are entitled with respect to individual personal data, for example, revoke consent or demand the deletion of certain data, this deletion will take place immediately and irrevocably upon exercise of the right.

For purposes of advertising and external presentation, we operate a website on the Internet:

www.asta-lueneburg.de
www.kritische-festschrift.de
www.queereringvorlesung.de

The aforementioned website is additionally and primarily governed by the privacy policy executed on the website. We do not collect any personal data on this website nor do we use such techniques via third-party providers. A data transfer to third parties, especially outside the EU, also does not take place.
On the website we operate a so-called "bulletin board". Here, advertisements can be placed in various categories. Within the scope of such advertisements, name and contact data are processed and published on the website. This is done after your explicit consent when submitting the online form by confirming the consent to the publication and the privacy policy.

For contact purposes, we store and process your private e-mail addresses. This is done only after an explicit voluntary consent by you. We also consider this consent to be given in the sense of conclusive behavior if you provide us with e-mail addresses for contacting you or for specific purposes and the desire to communicate by e-mail is clearly recognizable. We store and use your private e-mail addresses only for the purpose for which they were transmitted to us. As a matter of principle, we do not publish e-mail addresses. If in certain cases a publication takes place, this happens only after a voluntary informed consent by you/you. With regard to possible risks in e-mail communication or the publication of e-mail addresses, we ask you to read Appendix A2 "Risks in e-mail communication" to this information sheet.

As a matter of principle, we do not process e-mail addresses in mass e-mails or the dispatch to several persons in such a way that e-mail addresses of one recipient are disclosed to other recipients. We make exceptions to this rule if the e-mail addresses of all other recipients are already known to a group of recipients or if it can be assumed that the disclosure of e-mail addresses within a group is clearly intended by all recipients involved for the purpose of this communication. In the latter sense, therefore, if consent can be clearly inferred from the conclusive expression of the recipients. E-mails are received and sent via an SSL-encrypted connection. We do not use any techniques that enable the e-mails to be followed up by tracking methods. We also do not send e-mails that load data from third insecure sources.

In special cases, we publish your names, images (photos and videos) or other information in the press (online and offline), on our websites, social media portals or other places on the Internet. We do this only after your explicit, informed and voluntary consent. For each publication granted, you/they will be informed separately about the nature and scope of the publication. An informed and voluntary consent includes an appropriate instruction about possible risks of such a publication. This can be found in Appendix 1 to this information sheet.

The rights due to you/you:

According to Art. 15 GDPR in conjunction with § 35 BDSG (German Data Protection Law), you have the right to receive information from us about your personal data stored by us and the information specified in Art. 15 GDPR. You can exercise this right by informal written or (remote) oral request to us. The information can be limited to the extent that data concerning the fundamental rights of third parties will not be transmitted. The response to the information may be provided in electronic form.

Your right of access, in the case of collection and processing of personal data based on a legitimate or public interest, also extends to requesting a detailed explanation of the balance between our interests and your protection rights, regardless of whether these explanations have already been provided to you previously.

According to Art. 16 GDPR you have the right to correct inaccurate personal data about your person and to have incomplete personal data completed.

According to Art. 17 GDPR you have the right to delete your data. However, this right is limited and primarily concerns data that has been voluntarily provided to us. As a rule, you/you cannot request deletion of personal data that has been collected and processed on the basis of a legal obligation or for the performance of a service and continues to be processed. More details on a legally effective possible deletion are contained in Art. 17 GDPR.

If we store and process personal data from you on the basis of your voluntary consent, you can revoke this consent at any time. The revocation may also be partial or limited to specific processing purposes. The revocation of consent does not constitute an exercise of the right to erasure pursuant to Art. 17 GDPR. If you/they also want to demand the deletion of data with the objection, you/they must declare this separately. Such a declaration can be made together with the exercise of the objection.

According to Art. 18 GDPR you have the right to demand the restriction of the processing of your personal data, if one of the conditions determined for this in Art. 18 GDPR is present. We are then still permitted to store your personal data, but are subject to strict limitations in the processing that result from the nature of the circumstances.

According to Art. 20 GDPR, you can request the transfer of your data to a third party responsible. For this purpose, we can either provide you with the data in a common structured digital form or, in accordance with an existing order, transfer it directly to a third party. Another form of transfer, if technically possible for us, would have to be discussed in the individual case. Art. 20 GDPR contains further regulations on the type and scope of the rights and our obligations in this regard.

According to Art. 21 GDPR, you have the right to object if we process your personal data according to Art. 6 para. 1. lit e.) or f.), i.e. on the basis of a legitimate own or public interest. Unless we can cite compelling reasons that outweigh your rights requiring protection, for example the exercise or defense of legal claims, against this, we will immediately cease collecting and processing this personal data. If you exercise further rights, for example the right to deletion, we will carry out this deletion immediately.

Unless there are existing circumstances pursuant to Art. 12 (5) sentence 2 GDPR, the exercise of your/your rights is free of charge. Circumstances within the meaning of Art. 12 GDPR would be manifestly unfounded or, especially in the case of frequent repetition, excessive requests by a data subject. In this case, the controller may either charge a reasonable fee, taking into account the administrative costs of informing, notifying or implementing the requested measure, or refuse to act on the request.

As a data subject, you also have, according to Art. 77 GDPR in conjunction with. § 19 BDSG (German Data Protection Law), without prejudice to further and other, also judicial remedies, the right to lodge a complaint with a competent data protection supervisory authority if you suspect a breach of data protection with us. The competent supervisory authority is:

The State Commissioner for Data Protection in Lower Saxony
Prinzenstr.
530159 Hannover
Tel. 0511 / 120 45 00
Fax. 0511 / 120 45 99
E-mail: poststelle@lfd.niedersachsen.de
Website: www.lfd.niedersachsen.de

If you discover a data protection violation that is related to us, without being personally affected, you can report this violation ex officio to the competent supervisory authority for processing.

Technical and organizational measures for your protection:

In all our processes, we care about the security, availability and accuracy of your personal data. We have therefore taken extensive measures to ensure this for you. Likewise, it is our goal to finally delete personal data that is no longer needed and no longer subject to retention.

For each process of processing activities of personal data, we conduct a risk analysis in which we assess the worthiness of protection under aspects of loss, falsification, unauthorized inspection by third parties or publication. As a matter of principle, a high level of protection applies to your health data that we collect and process as part of the implementation of hardship applications.

We practice manual and automated procedures that ensure deletion of your data that is no longer needed and no longer required to be kept. Hereby we realize your right to "digital oblivion" and thus minimize risks, because data that no longer exists cannot be lost. The final deletion of digital data or paper documents is carried out in accordance with the regulations prescribed for this purpose by shredding in accordance with DIN standard 66399.

We have adequately secured our premises against theft and burglary through alarm systems, security locks, and access restrictions and controls.

The data collected from you by us, if available in paper form, is stored securely in locked cabinets protected from fire and water. We endeavor to digitize paper documents promptly and completely in order to provide additional security against loss. If paper documents are no longer required after digitization, we destroy them by a certified

document destruction company or by shredding in accordance with the prescribed DIN standard 66399.

If we commission third parties (shredders) to destroy personal data, whether in digital or paper form, we generally conclude a contract processing agreement (CPA) with these companies when awarding the contract.

Digitally stored data is only stored in encrypted form in accordance with the general state of the art. If processing requires the transfer of digital data to employees or other authorized persons or institutions, this transfer is encrypted.

We log every change to digital data in a log file. Such a log file contains at least the day and time of the change, the device on which the change was made, the user who made the change, and information about the type and scope of the change. Such log files are created automatically and are only accessible to the AStA spokespersons.

We have purchased computer equipment for the storage and processing of data, the functionality and scope of which meet the requirements. The EDP equipment ensures that, from a purely technical point of view, your data is stored in an appropriately secure manner and is available at all times. This is also ensured when a maximum load capacity of the EDP systems is practiced.

We protect your data against technical and intentional unlawful interference, as well as cases of natural disasters or other accidents, including fire, by making backup copies. We create internal as well as external backup copies. Backup copies are only created in encrypted form. In the case of external or offline backups, we ensure that the physical media are stored in secure locations with appropriate safeguards.

If we commission third parties to make backup copies, maintain our IT systems or provide other IT services with access to our IT system, this will only be done after we have concluded an order processing agreement (AVV) with these companies.

A procedure is regularly run through by our internal or external data backup officers, taking into account a wide range of scenarios, which practically tests and ensures the reinstatement of backup copies in our IT systems. Thus we are able to maintain business operations even in the case of a destruction of the EDP systems or to re-establish them in the shortest possible time.

Furthermore, we have implemented additional measures to safeguard automated data processing in:

- Server rooms are locked separately.
- Persons from outside the company are not permitted to stay unaccompanied in office premises
- Server and end devices are password protected
- Logins to our IT system can only be made by user names in combination with secure passwords and in particularly sensitive areas two-factor authentication is used
- User accounts are limited in such a way that the respective users have access only to the personal data absolutely necessary for the performance of their activities
- Our computer system is protected by firewall and anti-malware software and only authorized processes can transfer data out of the closed system.

In addition, we have taken other appropriate measures to control input, transmission and transport, as well as other measures to ensure the reliability of the systems.

We have developed an emergency procedure in the event of a data breach or incident involving personal data, which also includes notification of the competent supervisory authority.

We have introduced a procedure for regularly reviewing, assessing, and evaluating the effectiveness of technical and organizational measures and for ensuring the security of processing. As part of this implementation, the AStA spokespersons are in regular exchange with the data protection officer and the IT officers/service providers. At least once a year, an as-is analysis of the processes is carried out and compared with the target specifications. The results are documented and any deviations are remedied by appropriate measures.

The data protection officer and the persons involved in IT security undergo ongoing training and take appropriate measures to ensure that the technology and organization in the AStA are always promptly adapted to the currently required status or to recommend necessary, required measures to the AStA spokespersons.

AStA Universität Lüneburg

(as of March 2022)

(as of March 2022)

Appendix 1 - Risks in the publication of personal data on the Internet

In principle, there is a risk that personal data, in particular name data and images, will be recognized and approached when published. In this respect, a connection to our university can be inferred and other persons could draw the conclusion that a study is taking place at the university or that services of the AStA are being used. Insofar as you also release information about yourself or the services used by us for publication with this data, third parties may associate this information with you and also store and process it in relation to your person (profiling) without this being technically or organizationally preventable. As a rule, such practice by third parties or companies is illegal and you can take legal action against this if necessary.

Information about you/you that third parties obtain through our publications may lead to targeted contact with you/you for purposes of advertising, marketing, job placement, and political/religious solicitation or ideological influence.

For the publication of image recordings on the Internet (online publications), it is generally the case that third parties can take unlawful possession of these images and videos by simple technical means (screenshot/video recording) and use them for their own purposes. In this context, publication on other websites or social media portals with uncontrolled distribution on the Internet cannot be ruled out. We cannot prevent such misuse either technically or organizationally, and the possibilities of taking legal action against these persons who unlawfully reproduce and use image recordings may also be more difficult or completely impossible.

In addition, social media platforms and other portals are regularly operated on servers in countries outside the European Union. The General Data Protection Regulation (GDPR) does not apply here and only very few providers have a corresponding level of data protection. You therefore run the risk that images published in this way may be used by the providers for their own purposes, in particular for advertising purposes, but may also be resold or transferred to any third party. In this context, image recordings could also be merged with other data from you/you to form a profile of your person. This is also the case if a name has not been published for the image, as an identification of the person is nevertheless carried out by technical methods. In this context, biometric recognition and storage of facial data cannot be ruled out. As a rule, you have no legal recourse against this, and in such a case it will not be possible, or only with great difficulty, to withdraw the image recordings/data from unauthorized processing and uncontrolled dissemination on the Internet.

On social media platforms (Facebook, Instagram, Twitter, etc.), images as well as text contributions can be disseminated by sharing and thus very quickly reach a very large number of people and very high attention. In the process, we have only limited influence on the comments of other people in the publication on social media platforms. We cannot exclude the possibility that there may be negative or abusive comments on text contributions or images and the persons shown on them. This applies in particular to the further dissemination by sharing as well as in the case of illegal duplication and uncontrolled dissemination on the Internet by third parties.

In the worst case, image recordings can be modified or completely distorted by technical means (Photoshop, etc.), so that persons are shown in embarrassing, shameful or humiliating situations and also in completely false situations that never took place in the first place, which can be compromising for a person.

(as of March 2022)

Appendix 2 - Risks associated with e-mail addresses

When processing e-mail addresses, absolute security cannot be guaranteed, even if SSL or other forms of encryption are used for transmission or retrieval. SSL encryption exists in principle only with the retrieval or dispatch server and does not represent end-to-end encryption.

Since end-to-end encryption cannot be guaranteed, the reading of e-mails by third parties, in particular a technical scan of the contents of an e-mail, cannot be ruled out. This also applies to non-encrypted or unsecured attachments to an e-mail.

In the context of the foregoing, it is also possible for email addresses to be technically intercepted in an individual, group or mass mailing in order to misuse these addresses for sending SPAM of any kind, including sending links or attachments to/with malware.

We can only ensure the protection of your e-mail on our systems. If there is an authorized sending of group emails with the disclosure of addresses to multiple recipients, we cannot influence the security of the business or private devices of third parties that are used to retrieve the emails. These devices may be infected by malware and thus read e-mail addresses of an entire group and use them for SPAM purposes.

SPAM e-mails that you may receive by tapping your own e-mail address from third parties may be designed in such a way that they cannot be distinguished from legitimate e-mails. They regularly try to obtain your passwords or bank details and install malware on your end device. The latter can happen in particular by opening attachments and clicking on links. This also applies to links that pretend to lead to an unsubscribe function of the distribution list or an imprint, etc.

E-mail addresses are generally a personal characteristic in the sense of data protection. They can be assigned to specific natural persons. Via the source code, the IP address and the location as well as the end device used for sending or retrieving can be traced.

If we publish e-mail addresses on the basis of the consent given for this purpose, we cannot technically prevent these addresses from being tapped by third parties. Published e-mail addresses can spread uncontrolled in the network and for SPAM purposes of any kind.

E-mail addresses may also be used for profiling purposes and may lead to direct, unwanted contact by third parties. This contact can be for purposes of advertising, job placement, gambling, etc. It cannot be excluded that the e-mail address is also used for purposes of stalking, bullying or hate and incitement against you / you.