Data Protection Declaration
General information
When you register for the admissions process and when you actually apply to the University of Göttingen, any personal data you provide (your name, address, e-mail address, as well as all other application data) will be processed by Georg August Universität Göttingen, Wilhelmsplatz 1, 37073 Göttingen.

The purpose of this data processing is admissions and enrolment.

The initial legal justification for the data processing is your consent in accordance with Art. 6 paragraph 1 subsection a and Art. 7 of the European General Data Protection Regulation (EU-GDPR) as well as Art. 17 paragraph 1 of the Higher Education Act of Lower Saxony (NHG) and the University's own regulations for the collection and processing of personal data of applicants, secondary school students who are enroled in university courses, university students, examination candidates, former university members (not counting university employees) and those auditing courses at the Georg August University of Göttingen - PersDatO -*(in the version of the official announcement made on 20 October 2010, official announcement 29/2010, page 2,473, last amended by the decision of the Senate on 14 March 2018, official announcement I 21/2018 p. 320).*

Data recipients within the university are the Faculty of Physics, the Department of Teaching and Learning, the IT Department and the Göttingen International Department. Data recipient outside the university for degree programmes within the dialogue-oriented service process is the Foundation for University Admissions (Dortmund). There are no other data recipients, especially not abroad.

Your data will be kept for up to six months after your application/enrolment. In the event your application/enrolment is successful, it will become part of the files we keep on you. The data will be deleted as soon as they are no longer required for the fulfilment of the aforementioned purposes, unless statutory requirements mandate longer storage.

Information related to the data protection rights of the individuals concerned
You have the right to information about and of your data stored by the University of Göttingen. You may object to the processing of your data if certain conditions are met and/or request the correction, deletion or restriction of the processing of your data.

If you have any questions or complaints, please contact the Data Protection Officer for the University of Göttingen, Prof. Dr. Andreas Wiebe, Platz der Göttinger Sieben 6, Tel. 0551/39-4689, datenschutz@uni-goettingen.de.

The University of Göttingen is responsible for the data processing. The University is represented by its President, Prof. Dr. Ulrike Beisiegel, Wilhelmsplatz 1, 37073 Göttingen.

Under data protection laws, you have the right to complain to a supervisory authority, for example to the State Commissioner for Data Protection of Lower Saxony, Prinzenstrasse 5, 30159 Hanover, Tel. 0511/120-4500, poststelle@lfd.niedersachsen.de.

You have the right to revoke your consent at any time; the data processing that has been carried out up to that point remains compliant. The University of Göttingen would like to call your attention to the fact that if you do exercise this option, we will have no other choice but to exclude you from the application process.

Information related to the individual processing steps
Processing of log data (access data): When using the website, the access to pages, whether the access was successful, the time, the data volume transmitted and the IP address of the requesting computer are collected to detect bugs. A truncated version of the IP address is stored, such that specific identification cannot be performed or would only possible with an amount of effort that would be totally disproportionate to the knowledge gained by requesting the connection. The actual processing only takes place internally and on the basis of Art. 6 paragraph 1 f) EU GDPR, whereby the legitimate interest lies in bug detection. Log data that has been stored will be automatically deleted after seven calendar days.

Account
The prerequisite for the use of non-public areas of the website, e.g. application and enrolment management, is the existence of a user account. To create an account, the following personal data is absolutely required: Title, surname, first name, e-mail address and a password of your choice. If this data is incomplete, we are not able to assign an account and therefore the non-public areas of our web offering cannot be used. The data processing is carried out on the basis of Art. 6 paragraph 1 e) EU GDPR for the purpose of limiting access to registered users for the non-public, protected parts of the University of Göttingen's website. Account data will not be transferred to third parties. The data will be deleted either upon explicit request by the user or, at the latest, after the expiry of six months.

Automatic login with smartphones
If you use the website with an account, you are authorised to remain logged on with your smartphone. To enable this, a cookie with the encrypted access data will be stored on your mobile device. At the same time, a digital fingerprint of the mobile device will be stored on the server. The digital fingerprint is composed of several parameters. The following information is evaluated for this purpose:

- SCREEN_SIZE_AND_COLOR_DEPTH (screen size and colour depth)
- DEVICE_ATTRIBUTES: ID, model, vendor, build, device_os_version (attributes for the mobile device used: The model number (not the IMEI), the model name, the manufacturer, the series, and the version of operating system used)
- ACCEPT_LANGUAGE (language settings)
- TIME_ZONE (time zone)
- DEVICE_TYPE (mobile device used)
- BROWSER_TYPE (program used for internet access)

This data is used to identify the device and it is stored on the university's server. The data is stored and processed on the basis of a consent pursuant to Art. 6 paragraph 1 a) EU GDPR, which is granted upon activation of the automatic login by the user of the mobile device. There will be no transfer of data to third parties. The data will be used solely for the unique identification of the terminal device used in connection with the automatic login. An automatic login will only work if the digital fingerprint matches, and if the user name and password can be decrypted and match the actual access data. If the automatic login is not used for 4 weeks, it will be automatically deleted. In addition, the user can remove the automatic login credentials at any time by using the settings in his/her account, e.g. if the smartphone has been lost. By storing the above data for the relevant mobile device, the user can also differentiate between several of his/her mobile devices in his/her account and, if necessary, deactivate the automatic login for some of his/her mobile devices. Before such consent is revoked, data processed prior to the revocation shall be considered compliant.

Cookies
This application uses cookies, i.e. small files with short texts that are used for technical processing. For example, if cookies have been disabled in the browser, the full application cannot be used.