The General Data Protection Regulation (GDPR) went into effect on 25 May 2018. What has changed?

Records of processing activities – Article 30 GDPR
The procedure description is replaced by the obligation to maintain a record of processing activities. All processing of personal data must be recorded, including that from research, teaching, studies administration and general administration. Even procedures that are used for general office work (word processing, management of address and telephone directories, etc.) have to be recorded.

Data protection impact assessment
The previously undertaken pre-checking will be replaced by the data protection impact assessment (Article 35 GDPR). This has to be carried out when a form of processing is likely to result in a high risk to personal data, especially when novel technologies are used. For example, a data protection impact assessment pursuant to Article 35 (3) GDPR is mandatory in the case of CCTV or extensive processing of specific categories of personal data (e.g. health data, ethnic origin and trade union membership).

Right to be informed under GDPR
The fundamental principle of the rights of the data subjects anchored in the GDPR is that the data subjects are informed about the purposes for which the information collected and used about them is intended, thus enabling them to track and verify data collection and processing.
The new information obligations pursuant to Articles 13 and 14 GDPR include:

- Identity of the controller
- Contact information of the Data Protection Officer
- Processing purposes and legal basis
- Potential data recipients
- Transfer to third countries, if relevant
- Duration of storage
- Rights of the data subject, cf. Articles 15 – 21 GDPR
- Ability to withdraw consent
- Right to lodge a complaint with a supervisory authority, cf. Article 77 GDPR
- Obligation to provide personal data

When collecting personal data from other sources pursuant to Article 14 GDPR, the controller shall indicate the source from which the personal data originate and whether it is a publicly accessible source.
Where data are obtained directly, the data subject must be immediately informed pursuant to Article 13 (1) GDPR at the time the data are obtained. This information obligation is omitted pursuant to Article 13 (4) GDPR, if the data subject has already been informed. If the data are not obtained from the data subject, the information pursuant to Art. 14 (3) GDPR must be provided within a reasonable deadline, after one month at the latest.
The concrete procedures for information provision have to be worked out in a nuanced way. **As a first step, a master declaration form is to be made available on the website of the data protection officer.**

Safeguarding the rights of data subjects
Pursuant to Article 15 (1) GDPR, the data subject may obtain confirmation from the controller whether personal data have been processed and, if so, what data exactly are involved. Pursuant to Article 12 (3) GDPR, information must be provided without delay, but at the latest within one month. **Inquiries must be forwarded to the data protection officer immediately.**
Pursuant to Article 17 GDPR, personal data must be erased without delay upon the request of the data subject and/or, under certain circumstances, by the controller themselves independently without request by the data subject. This particularly applies if there is no longer any need for data processing and no statutory retention period is in effect.

For each case of personal data processing, it must be ascertained for what purpose the data processing is intended, which retention period is necessary for the intended purpose and whether statutory retention periods preclude the erasure after the intended purpose has been achieved. This should be documented in writing in an erasure concept.

Process for the notification of any personal data breach
Pursuant to Article 33 (1) GDPR, the University of Göttingen is obligated to inform the competent supervisory authority within 72 hours of becoming aware of personal data breaches that are likely to endanger the rights and freedoms of natural persons. Even if no risk to the rights and freedoms of natural persons is to be expected from the data protection breach, there is an obligation to document all personal data breaches.
All data breaches and security incidents related to the processing of personal data are to be reported immediately to the Data Protection Officer and the IT Department of the Central Administration. For this purpose, a central email address shall be established: datenschutzvorfall@uni-goettingen.de
The Data Protection Officer in cooperation with the IT department will then evaluate the risk to the rights and freedoms of data subjects, what measures are to be undertaken and what notification obligations apply.

Technical and organizational data protection and proof of data security

Pursuant to Article 5 (2) GDPR, the University of Göttingen is obligated to document and provide proof of the technical and organisational data security measures. **Pursuant to Article 38 (1) GDPR, the Data Protection Officer is to be involved "properly and in a timely manner, in all issues which relate to the protection of personal data".** In addition to the involvement of the Data Protection Officer, the development of IT systems must also comply with the principles of **"data protection by design" and "data protection by default" (privacy-friendly default settings)** (Article 25 GDPR). The Data Protection Officer must therefore be involved in any questions relating to technical data protection. The communication of IT security remains the responsibility of the central IT security officer of the University of Göttingen.

Obligations for documentation

Pursuant to Articles 5 and 24 GDPR records of all data protection-relevant processes must be created. This shall apply, in particular, to declarations of consent.

Tasks of the Data Protection Officer

Support in:

- Creating records of processing activities
- Implementing the data protection impact assessment
- Fulfilling the information requirements pursuant to Article 13, 14 GDPR
- Safeguarding the rights of data subjects

· Checking if the technical measures have been undertaken according to the current state of the art in order to ensure the processing of personal data in accordance with the provisions of GDPR

· Participating in the preparation of service instructions or service agreements related to data protection, including the monitoring of compliance with these provisions

· Training of persons involved in the processing of personal data on basic privacy issues

· Participating in the establishment of requirement profiles for workplaces where sensitive

personal data are processed or used

· Advising on the questions of secure file management, on designing informative and clearly worded forms, destruction of files as well as the erasure of files in compliance with data protection regulations

· Advising and monitoring data protection by carrying out research projects when commissioned

· Engaging with the IT Security Working Group (AGITSI)

· Liaising between the department and the Staff Council (SAP/R3; video surveillance etc.) in accordance with the various employment agreements

Contact Information

Data Protection Officer:
Professor Andreas Wiebe, LL.M. (Virginia)
Chair for Civil Law, Intellectual Property Law, Media
Law and Information and Communications
Technology Law
Platz der Göttinger Sieben 6,
37073 Göttingen, Germany
Phone: +49 (0)551 39-7381

Deputy Data Protection Officer:
Florian Hallaschka
Nikolausberger Weg 17
37073 Göttingen, Germany
Phone: +49 (0)551-39-4689

Email: datenschutz@uni-goettingen.de

More information is provided on our homepage for

- Creating records of processing activities and standardised forms
- Implementing the data protection impact assessment
- Fulfilling the information requirements pursuant to Article 13, 14 GDPR
- Safeguarding the rights of data subjects
- Training events
- The Website of the State Representative for Data Protection of the State of Lower Saxony for further information: www.lfd.niedersachsen.de
- The EU-GDPR text