Flick Gocke Schaumburg

Data protection notic

of Flick Gocke Schaumburg Rechtsanwälte Wirtschaftsprüfer Steuerberater Partnerschaft mbB
for clients, potential clients and interested parties

1. Name and contact details of the controller and the data protection officer

This data protection notice applies to the processing of data by:

Flick Gocke Schaumburg
Rechtsanwälte Wirtschaftsprüfer Steuerberater
Partnerschaft mbB
(Hereinafter: "FGS")
Fritz-Schäffer-Straße 1
53113 Bonn
Germany
T +49 228/9594-0
F +49 228/9594-100
datenschutz@fgs.de

Our data protection officer can be contacted at the above address and by email at datenschutz@fgs.de.

Unless otherwise stated below, this data protection notice also applies to the initiation, establishment of client relationships and the handling and processing of engagements as well as the organization of events in person and/or virtually by:

- Flick Gocke Schaumburg GmbH Wirtschaftsprüfungsgesellschaft, Fritz-Schäffer-Straße 1, 53113 Bonn, Germany;
- FGS Digital GmbH, Fritz-Schäffer-Straße 1, 53113 Bonn, Germany;
- FGS Steuerberatungsgesellschaft mbH, Fritz-Schäffer-Straße 1, 53113 Bonn, Germany;
- FGS Revisions- und Treuhandgesellschaft mbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft, Fritz-Schäffer-Straße 1, 53113 Bonn;
- FGS Treuhandgesellschaft für Stiftungsvermögen mbH, Fritz-Schäffer-Straße 1, 53113 Bonn, Germany;

with each of the above companies being responsible for processing your data themselves. Please contact the FGS company concerned if you have any data protection questions, referring to "data protection" in the subject line, or send an email to datenschutz@fgs.de.

This data protection notice also applies to the following controllers for notary services:

- Lawyer and notary Dr. Finn Lubberich (lawyer and notary with offices in Frankfurt am Main) Friedrich-Ebert-Anlage 49, 60308 Frankfurt am Main, Germany, T: +49 69/71703-0, F: +49 69/71703-300, datenschutz@fgs.de.
- Lawyer and notary Dr. Martin Oltmanns LL.M. (University of Chicago) (lawyer and notary with offices in Berlin), Unter den Linden 10, 10117 Berlin, Germany, T: +49 30/21 00 20-0, F: +49 30/21 00 20-100, datenschutz@fgs.de.

The notaries process your personal data when carrying out official duties (such as certifications, authentications, deposits, and safekeeping) in accordance with the provisions of the General Data Protection Regulation (GDPR) and the Federal Data Protection Act, as well as the Hessian Data Protection and Freedom of Information Act (Notary Dr. Finn Lubberich) or the Berlin Data Protection Act (Notary Dr. Martin Oltmanns).

The data protection officers responsible for the processing of personal data in the course of official duties by our notaries can be contacted at the aforementioned address in Bonn and via datenschutz@fgs.de.

2. Collection and storage of personal data, and nature and purpose of their use

a) Initiation, establishment of client relationships, for handling and processing engagements, as well as the handling of events in person and/or virtually.

Personal data is processed by FGS to the extent necessary for the initiation, establishment, administration, and billing of client relationships or orders to our notaries, as well as the execution and processing engagements and orders to our notaries, or the organization of events in person and/or virtually. We process personal data also to review and respond to client inquiries, for example, to exclude potential conflicts of interest and to fulfill legal requirements, such as those related to the prevention of money laundering and financing of terrorism, and the EU Directive on cross-border tax arrangements (DAC6).

aa) Parties affected by the processing of personal data

FGS processes personal data of

- Clients and their employees and board members (supervisory boards, management boards, managing directors, advisory boards)
- Third parties to the extent their personal data are necessary to establish client relationships or handle and process an engagement or to instruct our notaries. This may include a client's direct and indirect (sleeping) shareholders or partners, business partners and contractual partners, and its advisors and representatives, (potential) opponents in a legal dispute and their legal counsel, and the employees and directors of the individuals and entities mentioned, and individuals who need to be included in our documentation or reports in relation to the prevention of money laundering and financing of terrorism, and the EU Directive on cross-border tax arrangements (DAC6).
- It also applies to a client's family members, if necessary, for example, in tax and succession matters, or in relation to the prevention of money laundering and financing of terrorism, and the EU Directive on cross-border tax arrangements (DAC6).
- Administrative and court staff
- Witnesses, experts and translators
- Potential clients and interested parties

bb) Categories of personal data processed by FGS

FGS processes the following categories of personal data:

- Contact information, particularly first and last name, potentially including titles, address, phone number, email address, payment details (account holder, IBAN, BIC), passport or ID card information (especially date of birth, issuing authority, issue date, expiration date, serial number, personal features, photo), photographs, video recordings, tax identification details, residence and domicile state, existence/non-existence of reporting obligations (DAC6), log data, metadata, IP addresses, time and duration of participation in video/audio conferences, and, if applicable, the telephone number of the line used to make a call,

  as far as they are necessary for the initiation, establishment, administration, and billing of a client engagement or order to our notaries, or for the purpose of identification obligations under the Anti-Money Laundering Act and/or the EU Directive on cross-border tax arrangements (DAC6), or for the organization of events in person and/or virtually.

  and

- information on professional activities,
- information on income and financial position,
- other personal data,

  in each case only to the extent required to process the engagement or instruct a notary in order to establish and evaluate the facts, and to advise and represent a client properly.

Personal data in particular categories defined in Art. 9 GDPR (data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data uniquely identifying a natural person, health data or data concerning the sex life or sexual orientation of a natural person) and personal data relating to criminal convictions and offenses or related security measures pursuant to Art. 10 GDPR will be processed only to the extent required to process the engagement or project in order to establish and evaluate the facts, and to advise and represent a client properly or if it is necessary within the scope of identification obligations under the Anti-Money Laundering Act and/or the EU Directive on cross-border tax arrangements (DAC6).

cc) Sources of personal data processed by FGS

We regularly receive personal data directly from the persons concerned and process these data directly.

If this is not the case (e.g. in correspondence with client contact persons and/or opponents and their representatives or counsel, and public authorities, courts), the data originate from the following sources:

- Clients and/or opponents and their representatives or counsel
- Courts and public authorities (e.g. connected with the inspection of judicial, criminal or administrative files and/or information)
- Other third parties (e.g. parties to proceedings, witnesses, experts)
- Publicly accessible sources or those accessible, for example, due to a legitimate interest (e.g. commercial register, company register, transparency register, land register, insolvency notices, internet research, credit agencies)
- Potential clients or interested parties

dd) Purposes for which FGS processes personal data

FGS processes personal data in connection with the initiation, establishment, administration, billing, execution, handling and processing engagements or instructing our notaries for the following purposes: or orders to our notaries, as well as the organization of events in person and/or virtually for the following purposes:

- Compliance with legal requirements (e.g. under the German Money Laundering Act) to identify a client, any persons acting on the client's behalf and beneficial owners of the client

The legal basis for this processing Art. 6 (1) point c GDPR (performance of a legal obligation)

- Examining potential conflicts of interest with existing or previous client relationships before accepting an engagement
- Establishing and evaluating the facts
- Advising and representing our clients
- Correspondence with clients, opposing parties and their representatives or advisors, authorities, courts, and other parties, possibly also via video/audio conferences.
- Accounting, invoicing
- Handling and establishing clients' claims
- Organization of events for clients and potential client prospects, both as in-person events and via video/audio conferences, or a combination of both formats.

The legal basis for these processing activities is Art. 6 (1) point b GDPR (performance of contract) if personal data of our clients are processed; otherwise Art. 6 (1) point f GDPR (safeguarding of legitimate interests that override those of the person concerned).

The legal basis for the processing of particular categories of personal data is Art. 9 (2) point f GDPR (processing for the establishment, exercise or defense of legal claims).

ee) Transfer of personal data to third parties, recipient of personal data

Personal data is not transferred to third parties for any purposes other than those specified under 2. a) dd) above. We transfer our clients' personal data to third parties only if:

- they have granted their explicit consent thereto pursuant to Art. 6 (1) sentence 1 point a GDPR,
- this transfer is necessary pursuant to Art. 6 (1) sentence 1 point f GDPR for the establishment, exercise or defense of legal claims and there is no reason to suppose that they have an overriding legitimate interest in their data not being transferred,
- a legal obligation exists for the transfer pursuant to Art. 6 (1) sentence 1 point c GDPR, or
- this is legally permissible and necessary for the processing of the client relationship or order in accordance with Art. 6 (1) sentence 1 point b GDPR, or for the conduct of a video/audio conference as agreed upon with the participants.

We transfer third party personal data to our clients and other third parties if:

- they have granted their explicit consent thereto pursuant to Art. 6 (1) sentence 1 point a GDPR,
- the transfer is necessary pursuant to Art. 6 (1) sentence 1 point f GDPR for the establishment, exercise or defense of legal claims, notably those of our clients, and there is no reason to suppose that they have an overriding legitimate interest in their data not being transferred,
- a legal obligation exists for the transfer pursuant to Art. 6 (1) sentence 1 point c GDPR, or
- this is legally permissible and necessary for the processing of the client relationship or order in accordance with Art. 6 (1) sentence 1 point b GDPR, or for the conduct of a video/audio conference as agreed upon with the participants.

In addition to our clients, the following parties may receive personal data:

- Our clients' employees and directors (supervisory boards, management boards, managing directors, advisory boards), and their direct and indirect (sleeping) partners or shareholders, business and contractual partners and advisors and representatives, (potential) opponents in a legal dispute and their legal counsel, and the employees and directors of the above persons and entities
- Family members of the client
- Public authorities and courts, including those which maintain (non-) public registers, credit agencies
- Experts and translators
- Order processors who process personal data on our behalf and according to our documented instructions (esp. IT service providers, marketing service providers, catering service providers)
- Providers of video conferencing and webinar solutions
  aaa) Microsoft Teams
  In the context of meetings with our clients and/or third parties as well as our events, we use the software Microsoft Teams to conduct video or audio conferences, if necessary accompanied by an exchange of participants in text form via chat. We also use Microsoft Teams for identification purposes as part of the legally required prevention of money laundering and financing of terrorism.
  For this purpose, we process certain personal data such as participants' email addresses, first and last names in order to send invitations to the video or audio conferences and to connect the participants with each other and make them known or recognisable to each other. However, email addresses are not transmitted to other participants.
  In addition, when using Microsoft, further personal data such as log data, metadata, IP addresses, time and duration of participation and, in the case of telephone dial-in, the telephone number of the calling connection, if applicable, are processed.
  The provider Microsoft may process further personal data if the participant logs in via a Microsoft account or is logged in to a Microsoft account when using Microsoft Teams (e.g. address and payment data) or uses an app provided by Microsoft (e.g. hardware identifiers such as MAC addresses, device identifiers). Such registration is not required on the part of FGS and the processing of personal data in this context is carried out by Microsoft as the responsible party. The same applies to certain log data, which Microsoft always processes for its own business purposes.
  Video or audio conferences are only recorded in exceptional cases if this has been agreed in advance with all participants. Video conferences that take place as part of the identification process for the prevention of money laundering and financing of terrorism are always recorded. In the event of a recording, this will be indicated by a corresponding overlay or, in the case of dial-in by telephone, by an announcement.
  Microsoft Teams is operated by Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18 D18 P521, Ireland. The data processing for the operation of Microsoft Teams takes place on servers in data centers in the European Union in Ireland and the Netherlands. For this purpose, we have concluded a commissioned processing agreement with Microsoft Ireland Operations Limited in accordance with Art. 28 GDPR. However, it cannot be ruled out that personal data may also be transmitted outside the European Union or the European Economic Area, e.g. in the event of a failure of data centers, official and/or court orders. For these cases, we have concluded a data protection agreement with Microsoft Ireland Operations Limited on the basis of the "standard data protection clauses" pursuant to Art. 46 (2) point c GDPR as well as further suitable guarantees and supplementary measures in accordance with the judgment of the European Court of Justice in Case C-311/18 (Schrems II).
  bbb) GoTo Webinar
  In the context of our events, we use the GoTo Webinar software to conduct video or audio conferences, possibly accompanied by an exchange of participants in text form via chat. For this purpose, we process certain personal data such as the participants' email addresses, first and last names in order to send invitations to the video or audio conferences and to connect the participants with each other and make them known or recognisable to each other. However, email addresses are not transmitted to other participants.
  In some cases, participants can also register directly for an event offered by us using a link via GoTo Webinar. To do this, participants are required to enter their first name, last name, email address, company/organisation and job title.
  In addition, when using GoTo Webinar, further personal data such as log data, metadata, IP addresses, time and duration of participation and, in the case of telephone dial-in, the telephone number of the calling connection, if applicable, are processed.
  The provider GoTo may process further personal data if the participant registers via a GoTo account or is registered with a GoTo account when using GoTo Webinar (e.g. address and payment data) or uses an app provided by GoTo (e.g. hardware identifiers such as MAC addresses, device identifiers). Such registration is not required on the part of FGS and the processing of personal data in this context is carried out by GoTo as the responsible party. The same applies to certain log data which GoTo processes for its own business purposes.
  A recording of the video or audio conferences will only take place in exceptional cases if this has been agreed in advance with all participants. In the event of a recording, this will be indicated by a corresponding overlay or, in the case of dial-in by telephone, by an announcement.
  GoTo Webinar is operated by LogMeIn Ireland Unlimited Company, The Reflector, 10 Hanover Quay, Dublin 2, D02R573, Ireland. The data processing for the operation of GoTo Webinar takes place on servers that are distributed worldwide.
  For this purpose, we have concluded a commissioning agreement with LogMeIn Ireland Unlimited Company in accordance with Art. 28 GDPR as well as a data protection agreement based on the "standard data protection clauses" in accordance with Art. 46 (2) point c GDPR as well as further suitable guarantees and supplementary measures in accordance with the ruling of the European Court of Justice in Case C-311/18 (Schrems II).
- In individual cases, personal data may also be transferred to recipients in third countries outside the European Union or the European Economic Area for which the European Commission has not formally established an adequate level of data protection via an adequacy decision pursuant to Art. 45(3) GDPR or, pursuant to Art. 46 (5) GDPR, before 25 May 2018. If the transfer is not necessary for the establishment, exercise or defense of legal claims (Art. 49 (1) point e GDPR) and there is no other reason for transfer under Art. 49 (1) GDPR, we will obtain consent in accordance with Art. 49 (1) point a GDPR or provide applicable guarantees that the recipient will protect the personal data. This is regularly done in the form of data protection contracts based on "standard data protection clauses" pursuant to Art. 46 (2) point c of the GDPR and, if legally required, further suitable guarantees or supplementary measures in accordance with the ruling of the European Court of Justice in Case C-311/18 (Schrems II). For further information on these guarantees, please contact our data protection officer at datenschutz@fgs.de.

ff) Storage period for personal data

FGS will store personal data for as long as necessary to process them for the purposes mentioned under 2. a) bb). In individual cases, this may be necessary for up to 30 years. Additionally, we store personal data if we are required by law to do so. As a result, we must store manual files due to professional regulations (regularly for six calendar years after the end of an engagement pursuant to Sec. 50 of the German Federal Code for the Legal Profession; regularly for ten years after the end of a project under Sec. 66

of the German Tax Advisors Act / Sec. 51b of the German Public Auditors Act. We must retain personal data which we have collected in the course of an identification in accordance with the Money Laundering Act for up to 10 years after termination of the client relationship. Our notaries are obligated to keep files for up to 100 years, pursuant to Sec. 5 of the German Notaries' Professional Code of Conduct. In addition, certain personal data must be stored for six or ten years pursuant to Secs. 238, 257 of the German Commercial Code or Sec. 147 of the German General Tax Code, respectively. If personal data are stored only due to a legal obligation to keep records, the processing is limited to this purpose.

The log data from Microsoft Teams is deleted by us after 30 days, unless it is stored by Microsoft Ireland Operations Limited. Microsoft Ireland Operations Limited stores log data for a maximum of 13 months.

Log data from GoTo Webinar is only stored by LogMeIn Ireland Unlimited Company and for up to 365 days.

b) No legal requirement / consequences of failing to provide data

We collect the personal data mentioned above under 2. a) bb) without there being a legal or contractual obligation for you to do so within the meaning of Art. 13 (2) point e GDPR. In the event that you do not wish to provide us with certain information, we inform you here in accordance with Art. 13 (2) point e GDPR that we reserve the right to provide the service in question and may even be obliged to refuse to do so due to legal requirements or the Money Laundering Act.

Participation in video or audio conferences via Microsoft Teams or GoTo Webinar is in any case voluntary and not a prerequisite for the processing of the mandate by FGS. However, if the use of Microsoft Teams is not consented to, it may be necessary to identify the person in another way, e.g. in person, in order to establish a client relationship for the legally prescribed prevention of money laundering and financing of terrorism.

If we offer events exclusively virtually or if the capacities for attendance are exhausted, participation in the event is not possible without the use of Microsoft Teams or GoTo Webinar.

c) Automated decision-making / profiling

FGS does not use any profiling or mechanisms for automated decision-making.

3. Rights of data subjects

You have the right:

- pursuant to Art. 15 GDPR to obtain from us confirmation as to whether your personal data are being processed. In particular, you have the right to obtain information on the purposes of the processing; the categories of personal data concerned; the categories of recipients to whom your data have been or will be disclosed; the envisaged storage period; the existence of a right to request rectification or erasure or restriction of processing, or to object to such processing; the existence of a right to lodge a complaint; the source of your data if not collected by us; and on the existence of automated decision-making;
- pursuant to Art. 16 GDPR to demand from us the immediate rectification of inaccurate personal data concerning you held by us, or to have incomplete personal data completed;
- pursuant to Art. 17 GDPR to demand from us the erasure of your personal data stored by us unless the processing is necessary for exercising the right of freedom of expression and information; for compliance with a legal obligation; for reasons of public interest; or for the establishment, exercise or defense of legal claims;
- pursuant to Art. 18 GDPR to demand that we restrict the processing of your personal data if you contest the accuracy of the data or the processing is unlawful but you oppose the erasure of the personal data, or we no longer need the data, but they are required by you for the establishment, exercise or defense of legal claims; or if you have objected to processing pursuant to Art. 21 GDPR;
- pursuant to Art. 20 GDPR to receive the personal data which you have provided to us in a structured, commonly used and machine-readable format, or – to the extent technically possible – to demand their transfer to another controller;
- pursuant to Art. 7 (3) GDPR at any time to withdraw your consent given to us. In consequence of withdrawal, we shall no longer be allowed to process the data in future on the (sole) basis of such consent; and
- pursuant to Art. 77 GDPR to lodge a complaint with a supervisory authority. As a rule, you can contact the supervisory authority of your usual place of residence or place of work or our office or the office of our notaries.

4. Right to object / Right to withdraw consent

If your personal data are being processed on the basis of legitimate interests pursuant to Art. 6 (1) sentence 1 point f GDPR, you have the right to object to the processing of your personal data pursuant to Art. 21 GDPR on grounds relating to your particular situation, or if the objection relates to direct marketing. In the second of these two cases, you have a right to object in general without invoking a particular situation and we shall comply with the objection. If you wish to exercise your right to withdraw consent or object, simply send an email to datenschutz@fgs.de.

If you wish to revoke your consent pursuant to Art. 7 (3) GDPR, it is also sufficient to send an email to datenschutz@fgs.de. However, we would like to point out that in the event of revocation, we may be required by law to continue processing your personal data, e.g. in the case of video recordings in the context of identification for the prevention of money laundering and terrorist financing.

5. Data security

We use transport encryption (SSL/TLS) as standard for email correspondence. However, a requirement for end-to-end transport encryption is that it is also used by the recipient. For an even higher level of encryption, content encryption (S/MIME) can be used for email correspondence by special arrangement.

Otherwise we take suitable technical and organizational security measures to protect your data against coincidental or intentional manipulation, partial or complete loss, destruction, and unauthorized access by third parties. We continuously improve our security measures in keeping with technological progress.

6. Validity and revision of this data protection notice

This is the currently applicable version of the data protection notice as of May 2023. The evolution of the services we offer, and changes to statutory or official requirements, can make it necessary for us to revise this data protection notice from time to time. You can retrieve and print the current version of the data protection notice from the website at any time: www.fgs.de/mandanten-datenschutzerklaerung (in German) or #enter URL here# (in English).

As of May 2023