Gofaizen & Sherle

Group Data Processing Policy

Gofaizen & Sherle

September 2025

INTRODUCTION

This Data Processing Policy (hereinafter – the "Policy") is issued on behalf of the Group (as defined below). The Group operates through its registered entities in various jurisdictions and hereinafter referred to as "we", "us", or "our", providing the services as defined in the General Terms of Services available at the website www.gofaizen-sherle.com and other contracts concluded (if any).

This Policy applies to all individuals whose personal data we process (hereinafter referred to as "you," "your," or "yours"), including clients, website users, business contacts, and other individuals who engage with us.

We are committed to protecting the privacy and security of your personal data. This Policy explains how we collect, use, disclose, transfer, and retain your personal data when you engage with us, use our services, or interact with our digital platforms and communication channels. This Policy ensures transparency in how we handle personal data and outlines your rights under applicable data protection laws.

This Policy applies to all personal data processing activities undertaken by us across the jurisdictions of our operations. These activities include any interaction or engagement with us, regardless of whether such engagement occurs online, offline, or in a hybrid manner. It also includes data processing activities that occur across our offices, entities, and partners located in various jurisdictions.

Our operations are governed by various privacy and data protection laws, including the General Data Protection Regulation (GDPR) and other local laws. By interacting with us, you consent to the practices described in this Policy, subject to the applicable data protection laws.

CONTROLLERSHIP ARRANGEMENTS

The following entities (hereinafter - the "Group") act as joint controllers for the purposes of personal data processing carried out under this Policy and provision of services as specified in the relevant service agreement or engagement terms concluded with you:

- **Gofaizen & Sherle OÜ**, legal entity incorporated in Estonia with registry code 16295888, address: Harju maakond, Tallinn, Lasnamäe linnaosa, Lõõtsa tn 2a, 11415;
- **UAB "Gofaizen & Sherle",** legal entity incorporated in Lithuania with registry code 306079826, address: Vilnius, Lvivo g. 25-702, LT-09320;
- **Gofaizen & Sherle Limited**, legal entity incorporated in Hong Kong with certificate of incorporation no. 3153754, address: 8th Floor, China Hong Kong Tower, 8-12 Hennessy Road, Wan Chai, Hong Kong;
- **Gofaizen & Sherle Inc.**, legal entity incorporated in Panama with certificate of incorporation no. 155766386, address: World Trade Center 200-B, Suite 266 Calle 53 Este, Marbella, Panama;
- **Gofaizen & Sherle S.A.S. DE C.V.,** legal entity incorporated under the number 243 of the book 4898, address: Av la Revolucion #piso 6 Apto. 12, Colonia San Benito, Presidente Plaza, San Salvador;
- **G&S Accounting OÜ,** legal entity incorporated in Estonia with registry code 17167098, address: Harju maakond, Tallinn, Lasnamäe linnaosa, Lõõtsa tn 2a, 11415;

- Gofaizen & Sherle Corporate Services OÜ, legal entity incorporated in Estonia with registry code 16865498, address: Harju maakond, Tallinn, Lasnamäe linnaosa, Lõõtsa tn 2a, 11415.

Under the terms of the agreement concluded between the entities, the Group jointly determines the purposes and means of processing personal data related to the provision of their services, especially in the context of cross-border operations. None of the Group entities acts solely as a data processor for another; instead, all entities collaborate equally in service delivery and operational decision-making, including data protection governance.

Each Group entity remains individually and jointly responsible for ensuring that data processing is carried out in compliance with applicable data protection laws in its respective jurisdiction, and for fulfilling its obligations to data subjects.

Details regarding the internal allocation of responsibilities between the joint controllers may be made available upon request. The designated point of contact for data protection matters across the Group is the entity established in Estonia (Gofaizen & Sherle OÜ).

WHAT PERSONAL DATA WE PROCESS

At the Group, we handle personal data with the highest standards of care and security. The personal data we collect is essential for achieving the following objectives:

- delivering and managing our services;
- fulfilling legal and regulatory obligations;
- supporting our legitimate business interests;
- ensuring compliance with contractual agreements;
- enhancing customer experience and service quality;
- conducting necessary due diligence and background checks;
- maintaining effective communication and records.

We will only process a minimal amount of relevant information that is necessary to enable us to carry out the functions, activities and objectives outlined above.

The personal data that we process about you may vary depending on the function, activity and objectives. In relation to the objectives above and purposes outlined further in this Policy, we will process the following personal data relating to you:

- contact details (e.g., full name, job title, company, address, phone numbers, email);
- identity documents (e.g., passports, national ID cards, driver's licenses, KYC documentation);
- statutory register information (e.g., directorships, shareholdings, beneficial ownership, trustee positions);
- tax and financial data (e.g., tax ID numbers, bank account details, financial statements, payment history);
- accounting records (e.g., invoices, payroll, bookkeeping records, tax returns);
- professional and employment details (e.g., employment history, job role, qualifications, professional licenses);

- contractual and transactional data (e.g., legal agreements, client onboarding documents, transaction records);
- communications data (e.g., phone calls, emails, client instructions, meeting recordings, transcripts);
- website and technical data (e.g., IP address, device identifiers, session logs, cookie preferences);
- third-party data (e.g., information from legal counsel, financial institutions, regulatory authorities, public records).

We may process the following categories of special data relating to you, depending on the nature of our services and whether you choose to share such information with us or it is required for compliance purposes:

- political opinions or status (e.g., information indicating political exposure or classification as a PEP);
- criminal offence data (e.g., records of criminal convictions or allegations, sanctions, anti-money laundering and counter-terrorist financing screening results);
- health or medical information (e.g., health declarations required to support certain legal claims, or for the employment purposes);
- biometric data (e.g., facial scans or fingerprint data, if used for identity verification or electronic onboarding);
- racial or ethnic origin (e.g., data disclosed in KYC documents such as national ID or passport where visible);
- trade union membership (e.g., when relevant in the context of employment or labour law advice).

We only process sensitive personal data when necessary for legal or regulatory compliance, or with your explicit consent. Such data is handled with strict confidentiality and in accordance with applicable data protection laws.

You are not legally obliged to provide any of the personal data that is outlined in this Policy and the provision of personal data is not a contractual requirement, neither is it necessary to enter into a contract. However, not providing certain data may limit our ability to offer services or reach the desired business relationship results.

HOW WE COLLECT PERSONAL DATA

We collect personal data from a variety of sources in order to provide our services, comply with legal and regulatory obligations, and maintain effective business relationships. We collect personal data from the following sources (incl., direct and indirect):

- when you communicate with us directly (e.g., via email, phone calls, messengers, web forms, phone or online meetings, or consultations);
- from trusted external sources (e.g., business partners, legal or financial advisors, regulators, or publicly available records and databases);
- through your engagement with our digital presence (e.g., social media platforms such as LinkedIn or WhatsApp, or when you browse or interact with our website);

- when you attend events where we are present (e.g., conferences, webinars, seminars, or informal networking sessions);
- in the course of providing our legal and professional services (e.g., during transactions, compliance checks, onboarding processes, or legal representation).

We are committed to ensuring that all personal data collected, whether directly or through third parties. is relevant, up to date, and handled in accordance with applicable data protection laws.

PURPOSES AND LEGAL BASES

We will process your personal data for a specified, explicit and legitimate purposes, and will not further process your personal data in a way that is incompatible with those purposes.

We collect and use personal data only where it is relevant and necessary for the following purposes:

- providing our legal, corporate, and advisory services (e.g., onboarding clients, drafting legal documents, advising on regulatory matters, and representing clients in transactions or disputes);
- complying with legal and regulatory obligations (e.g., fulfilling requirements under anti-money laundering laws, maintaining tax and accounting records, conducting sanctions and PEP screening);
- managing internal operations and administration (e.g., maintaining client files, invoicing and payments, IT support, and managing business continuity);
- maintaining effective communication and client relationships (e.g., responding to queries, organising consultations or meetings, and managing ongoing engagements);
- improving our services, monitoring quality, and maintaining accurate records (e.g., recording and analyzing conversations);
- conducting marketing and business development (e.g., sharing newsletters, event invitations, or legal insights, where legally permitted or consented to);
- ensuring security and protecting legal rights (e.g., monitoring systems for fraud, conducting audits, pursuing or defending legal claims).

Depending on the context, we rely on one or more of the following lawful bases to process personal data:

- when processing is necessary to enter into, or perform, a contract with you or your organization;
- where processing is required to meet statutory duties (e.g., under anti-money laundering regulations, tax laws, or court orders);
- where we have a genuine business reason to process your data, such as to provide high-quality service, manage operations, or protect our legal rights, and where this does not override your fundamental rights and freedoms;
- where you have explicitly given us permission to process your data for a specific purpose (e.g., subscribing to marketing communications).

When we process special category personal data relating to you, we can only do so if we have a lawful basis and process it under one of the specified conditions contained in the data protection legislation

because it requires higher levels of protection. For the purposes we have outlined in this Policy, the conditions for processing that we rely on are:

- where you have given us clear, informed, and specific consent to process your special category data for a particular purpose;
- where processing is necessary for legal or regulatory reasons (e.g., AML/CTF checks, KYC obligations);
- where the processing is necessary for reasons of substantial public interest and is authorised by law (e.g., detecting fraud, preventing crime, or ensuring regulatory compliance);
- where it is required in connection with actual or anticipated legal proceedings or advice;
- where relevant, and under the supervision of a professional, for employee health or fitness to work.

There are some circumstances where we may need to further process your personal data in ways that are beyond what is described in this Policy, or without your consent. If we need to do this, we will only do so when it is necessary, lawful and in compliance with the requirements set out in the data protection legislation. We will consider each circumstance on a case-by-case basis.

HOW WE SHARE YOUR PERSONAL DATA

We will only share your personal data with other organisations or individuals with your consent, or when it is necessary to fulfil our purposes, where we are required by law or where we have another legitimate interest for doing so.

When we use a data processor, we will have a contract with them which requires them to take appropriate security measures to protect your personal information in line with our internal policies. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

For the purposes outlined in this Policy, we may share your personal data in the following cases:

- we may share your personal data between the Group entities on a confidential basis where such sharing is required for the purpose of providing legal advice or other services;
- other law firms or specialist legal counsel for the purpose of obtaining specialist/foreign legal advice, as required in the context of the engagement and as approved by you in advance;
- If we have collected your personal data in the course of providing legal services to a third party entity which is our client, we may disclose it to that third party entity;
- we may share your personal data with third parties in respect of anti-money laundering checks and verification, credit reference agencies, background check agencies and government/ regulatory bodies with whom such personal data is required to be shared.

We will otherwise only disclose your personal data when you direct us or give us permission to do so, when we are required by an obligation under applicable law or regulations or judicial or official request to do so, or as required to investigate actual or suspected fraudulent or criminal activities.

HOW LONG WE KEEP YOUR PERSONAL DATA

We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected, as outlined in this Policy, or as required by applicable legal, regulatory, or contractual obligations.

We apply defined internal retention policies and schedules based on the type of data, the nature of our relationship with you, and the legal and operational requirements in the jurisdictions in which we operate. In cases where you have provided consent for processing, we will retain the data until such consent is withdrawn, unless we are required or permitted to retain it for longer under applicable law.

Once the relevant retention period has expired, or if you withdraw your consent (where applicable), we will securely delete, destroy, or anonymise your personal data so that it can no longer be associated with you, in accordance with our internal data retention and disposal procedures.

YOUR RIGHTS

As a data subject, you have a number of rights specified below under applicable data protection laws regarding the personal data we process about you. These rights are not absolute and may be subject to conditions and limitations. We consider each request on a case-by-case basis and will act in accordance with legal obligations.

- You have the right to receive clear, transparent, and easily understandable information about how we process your personal data. This Policy and other related notices serve to fulfil this obligation.
- You may request access to the personal data we hold about you, including confirmation of whether we process your data and, if so, the purposes and scope of that processing.
- You have the right to request that we correct any inaccurate personal data or complete any incomplete information we hold about you.
- You may ask us to delete your personal data under certain circumstances, for example where the data is no longer necessary for the purposes for which it was collected/ you withdraw consent (where processing was based on consent)/ you object to processing and there are no overriding legitimate grounds. This right does not apply where we have a legal obligation to retain the data or other lawful grounds for continued processing.
- You may request that we limit the processing of your personal data in certain situations. When processing is restricted, we may store your data but will not use it further without your consent, unless otherwise permitted by law.
- You have the right to receive the personal data you provided to us in a structured, commonly used, and machine-readable format, and to transmit that data to another controller, where technically feasible.
- You have the right to object to the processing of your personal data in situations where the processing is based on our legitimate interests/ the data is used for direct marketing (this right is absolute and always applies).

- You have the right not to be subject to decisions based solely on automated processing, including profiling, which produce legal or similarly significant effects on you, unless certain conditions apply.

To exercise any of these rights or to obtain more information about your data protection rights, please contact us using the contact details set out in the "Contact Us" section of this Policy.

We may need to request specific information to confirm your identity and ensure your right to access the data. This is a security measure to protect your information.

You will not be charged for exercising your rights. However, we may charge a reasonable fee or decline the request if it is manifestly unfounded or excessive.

Where a right is not applicable in certain circumstances, we will inform you of the reasons and the legal basis for our position.

INTERNATIONAL TRANSFERS

We may transfer your personal data to entities outside the European Economic Area (EEA) and beyond the jurisdictions in which we operate, including Estonia, Hong Kong, and Panama. These transfers may be necessary for the purposes outlined in this Policy and to provide our services effectively.

When transferring personal data internationally, we ensure that the data is protected in accordance with applicable data protection laws for EU-based clients and other data subjects. To ensure the security and legality of these transfers, we rely on the safeguards described below.

- We transfer data to countries or regions that have been recognized by the relevant authorities (e.g., the European Commission) as offering an adequate level of data protection, ensuring that your personal data is treated with the same level of protection as within the EEA.
- When personal data is transferred to countries or entities that do not have an adequacy decision, we implement Standard Contractual Clauses (SCCs) or other legally accepted safeguards, which provide contractual obligations on the recipient to protect your personal data.

In certain cases, we may transfer your personal data to third parties in countries outside of the EEA, with your explicit consent or where such transfers are necessary for the performance of a contract.

If you have any questions or concerns regarding international data transfers, please contact us for more information about the specific measures we take to protect your personal data.

AUTOMATED DECISION-MAKING

The Group may use automated decision-making processes, including profiling, in certain circumstances. We ensure that such processes comply with applicable data protection laws and regulations, and we implement safeguards to protect your rights and freedoms.

If a decision made solely on automated processing significantly affects you, you have the right to contest the decision and request a human review. This applies in cases where the decision is based on sensitive data or has legal implications.

You have the right to receive meaningful information about the logic involved in any automated decision-making processes. If automated decision-making is based on consent, you have the right to withdraw that consent at any time.

If you wish to learn more or exercise your rights regarding automated decision-making, please contact us.

AUTOMATED RECORDING

The Group may record calls, meetings, or other communications for purposes such as quality assurance, training, compliance, or security. These recordings may be processed using automated tools, for example, to generate transcripts, identify action items, or support analytics.

We ensure that any processing of recorded communications complies with applicable data protection laws and regulations. Recordings are retained only as long as necessary for the stated purposes and are protected using appropriate technical and organizational measures.

You have the right to request access to any recordings containing your personal data, to request correction of inaccuracies, to object to certain processing, or to exercise any other applicable data protection rights. For more information or to exercise your rights, please contact us.

MARKETING ACTIVITIES

We may process your personal data for marketing purposes, including promoting our services, events, and legal updates that we believe may be of interest to you.

In certain cases, we may seek your explicit consent before processing your personal data for marketing purposes. You can withdraw your consent at any time without affecting the lawfulness of any processing based on consent before its withdrawal.

In other cases, we may process your personal data for marketing based on our legitimate interests, such as informing you about services that may be relevant to you or promoting industry-related events.

You can opt out of receiving marketing communications at any time by clicking the unsubscribe link in any marketing email or by contacting us directly. We will respect your preferences and stop sending marketing materials.

You are under no obligation to provide your personal data for marketing purposes, and choosing not to engage in marketing communications will not affect your ability to use our services.

DATA SECURITY

We have put in place measures to protect the security of your information. For more details of these measures, please contact us directly.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Additionally, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process personal information on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator where we are legally required to do so.

CONTACT US

If you would like further information relating to your data protection rights, how we process your personal data, any other data protection or matter related to this privacy notice, or would like to make a rights request, please contact us at our designated point of contact:

- Email: info@gofaizen-sherle.com;
- Phone: +3726028423;
- Address: Lõõtsa tn 2a, 11415 Tallinn, Estonia.

Each entity from the Goup will cooperate promptly to ensure the data subject's rights are respected, and appropriate actions are taken in response to complaints or requests.

If you’re not satisfied with our response where you have contacted us, or you think we’re not processing your personal data in accordance with the law, you may be able to escalate the matter to our Data Protection Officer (DPO) at:

- dpo@gofaizen-sherle.com.

In the unlikely event that your concern remains unresolved after internal escalation, you may contact the relevant supervisory authority. If you are unsure which authority to contact, please reach out to our DPO for guidance. We will ensure that your matter is escalated appropriately to the relevant authority in your jurisdiction.

We are committed to handling your concerns in a timely and transparent manner.

CHANGES OR UPDATES TO THIS POLICY

This Policy may be updated from time to time to reflect changes in legal requirements, business practices, or the way we process personal data. When such updates occur, the revised version will be published on this page.

We recommend that you consult this Policy regularly to ensure that you are aware of the most recent version and understand how your personal data is being used. Continued use of our services following the publication of an updated Policy will be understood as acknowledgment of the changes.

All amendments will take effect from the date they are made available on this page, unless otherwise stated.