



# Privacy Policy of DUR Consulting GmbH

As of January 2026

## 1. Introduction and scope

DUR Consulting GmbH takes the protection of your personal data very seriously. As a consulting company in the high finance sector, we are subject to strict regulatory requirements (e.g.. AML/FATF). We process your data in accordance with the Swiss Federal Data Protection Act (DSG) and, if applicable, the EU General Data Protection Regulation (GDPR).

This Privacy Policy explains how we collect, process and protect data, particularly with regard to our compliance obligations and the implementation of security standards according to ISO 27001 and SOC2.

## 2. Responsible body

Responsible for data processing on this website and within the scope of our mandates is:

DUR Consulting GmbH Kapellstraße 1 8853 Lachen SZ Switzerland E-Mail: [contact@dur-consulting.com](mailto:contact@dur-consulting.com)

Note for EU customers: Since our core business is not primarily focused on systematic monitoring of persons in the EU, we have not currently appointed a specific EU representative. If you have any questions, please contact the above address directly.

## 3. What types of personal data do we collect?

Based on industry standards in the financial sector, we collect the following data categories, depending on our business relationship:

- **Identification data:** name, address, date of birth, nationality, copies of ID documents (passport/ID) for KYC purposes.
- **Contact information:** email address, telephone number, business contact details.
- **Financial Information & Economic Background:** Source of Wealth/Funds information on beneficial owners (UBOs), tax domicile, as well as information on transactions, provided that they are the subject of our advice or compliance audit.
- **Compliance & risk data:** results from background checks, hits on sanctions lists, PEP status (politically exposed persons), results of adverse media checks.
- **Technical data:** IP addresses, log data when using our digital services (e.g. Zoho Workdrive) or website.



## 4. Sources of data

We not only collect data directly from you, but also use external sources to fulfill our legal due diligence:

1. **Directly from you:** By submitting documents, contracts or using our forms / data rooms.
2. **Public registers:** commercial registers, company register.
3. **Specialized third-party providers** (background checks): We use databases and services from LexisNexis, iDenfy, Amlbot.com, OpenSanctions.com.

## 5. Purposes of processing and legal bases

We always process your data specifically and based on legal bases:

### 5.1 Fulfillment of contractual obligations (Art. para. 6 lit. 1 b GDPR / Art. para.31 lit.2 DSG)

Processing is carried out to provide our consulting services in the high finance sector, for mandate management and communication with you.

### 5.2 Legal obligations & compliance (Art. para. 6 lit. 1 c GDPR / Art. para.31 DSG)

As a company subject to AML (anti-money laundering) and FATF regulations, we are legally obliged to:

- Conduct identity and economic checks (KYC).
- monitor transactions and business relationships.
- Suspected reports to competent authorities (e.g. B. MROS via goAML).

### 5.3 Legitimate interests (Art. para. 6 lit. 1 f GDPR / Art. para.31 DSG)

We process data to safeguard our legitimate interests, in particular:

- Ensuring IT security and network protection (as part of our ISO 27001 and SOC2 implementation).
- assertion of legal claims and defence in legal disputes.
- Development of our services and risk management.

## 6. Decision-making and profiling

We use specialized software solutions (such as scorechain, Amlbot.com) to create risk profiles and analyze transactions (profiling). (Important: A fully automated decision-making that has legal effect on you like automatic rejection of a mandate does not take place). The software serves as support; the final decision is always the responsibility of an employee of DUR Consulting GmbH.



## 7. Transfer of data and data transfers

We will only pass on your data if this is necessary for the performance of the contract or we are legally obliged to do so.

### 7.1 External service providers

We use carefully selected service providers who are contractually obliged to maintain confidentiality and security. Currently we use:

- **Cloud & CRM:** Zoho Corporation (Zoho CRM, Zoho Workdrive, Mail). The data is hosted on servers within the EU.
- **Web hosting:** Hostinger International Limited (Cyprus/EU).
- **Compliance tools:** The vendors mentioned in Section 4 (e.g. B. LexisNexis) receive data only for the purpose of comparison.

### 7.2 Authorities

In the event of a suspicion of money laundering, we are obliged to report to the Money Laundering Reporting Office (MROS) via the goAML system or to other competent supervisory and law enforcement authorities.

### 7.3 International data transfers

Our primary data storage (Zoho, Hostinger) takes place on servers in the EU and/or Switzerland. There are no international data transfers to insecure third countries. If this is necessary in the future, we ensure that appropriate guarantees (e.g. EU-standard clauses).

## 8. Data security (ISO 27001 / SOC2)

In order to protect your data from loss, misuse or unauthorized access, we implement technical and organizational measures (TOMs) based on the standards of ISO 27001 and SOC2. (SSL/TLS for the website and data transmission) and regular security checks. This includes access controls, encryption, storage.

## 9. Retention periods

We store your personal data for as long as is necessary for the fulfillment of our contractual and legal obligations. Following the deadlines customary in the financial sector (e.g. B. Art. 957 OR, Money Laundering Act) we usually keep business-relevant documents and compliance files for a period of ten years after termination of the business relationship. After the deadline, the data will be deleted or anonymized.



## 10. Your rights

You have the right at any time:

- **Information** about your data stored by us.
- **Correction** of incorrect data.
- **Deletion** of your data (unless there is a legal retention obligation).
- **Restriction** of processing.
- **Objection** to the processing (esc. marketing).direct
- **Data portability** (issue in a common format),.

To exercise your rights, please contact: [contact@dur-consulting.com](mailto:contact@dur-consulting.com).

## 11. Data collection on our website

### 11.1 Cookies

Our website uses cookies. These are small text files that your browser stores. (e.g. Some are technically necessary for the security or functionality of the site), others serve for analysis. Technically necessary cookies are stored on the basis of our legitimate interest (Art. para. 6 lit. 1 f GDPR).

### 11.2 Hosting

Our website is hosted by Hostinger. The provider processes IP addresses and log files to ensure the security and stability of the website. We have concluded a contract processing contract (AVV) with Hostinger.

### 11.3 Google Fonts

We use Google Fonts for the uniform presentation of fonts. When you visit our site, a connection to Google servers is established, whereby your IP address can be transmitted to Google. The use is based on our legitimate interest in a uniform presentation of our online offer. (e.g. If consent is requested via cookie banners), this legal basis.

### 11.4 Zoho SalesIQ (Tracking & Chat)

We use or intend to use Zoho SalesIQ and Zoho PageSense to analyze visitor behavior and communicate (chat). Zoho SalesIQ/PageSense uses cookies and tracking technologies to analyze how visitors use our website. The information generated by the cookie is transmitted to Zoho servers (in the EU) and stored there. This service is only possible with your consent (opt-in).