

## ARCLINE PRIVACY STATEMENT

### 1 ABOUT THIS PRIVACY STATEMENT

This privacy statement explains how Arcline AS ("Arcline", "we") processes personal data in connection with our legal services. Arcline is committed to safeguarding your privacy and processes personal data in accordance with the General Data Protection Regulation (GDPR) and applicable Norwegian law. This statement gives you an overview of how we process personal data, for what purposes, and your rights as a data subject.

### 2 WHO IS RESPONSIBLE FOR PROCESSING YOUR PERSONAL DATA?

Arcline is the data controller for personal data processed in connection with our services. This means that we determine the purposes and means of the processing and are responsible for ensuring that your personal data is processed in compliance with applicable law.

#### Contact details:

Arcline AS

Edvard Storms gate 2, 0166 Oslo

E-mail: [contact@arcline-ai.com](mailto:contact@arcline-ai.com)

Enterprise registration number: 932 227 339

### 3 WHICH PERSONAL DATA DO WE PROCESS AND FOR WHICH PURPOSES?

#### 3.1 Legal services

In connection with the provision of our services and Solution, Arcline collects and processes personal data about Customers, their employees, owners, and other individuals referred to in documents or correspondence.

We process personal data to the extent necessary for legitimate interests, including:

- Establishing and managing Customer relationships
- Performing conflict of interest checks and mandatory Customer due diligence (KYC/AML)
- Assisting external third-party lawyers with their legal services using our Solution
- Invoicing and administration
- IT operations, information security, and file retention
- Improving our services through analysis of anonymized and redacted Customer materials to enhance templates, workflows, internal knowledge management and service quality
- We may also process personal data where required by law, e.g., anti-money laundering obligations, bookkeeping requirements, or other legal duties.

The types of personal data processed may include:

- Contact details (name, email, phone number, title, company affiliation)
- Identification details (e.g., ownership information, ID documentation)
- Case-related information (contained in agreements, correspondence, and other documents)
- Invoicing information (e.g., billing contact)

Special categories of personal data may be processed where necessary for the establishment, exercise, or defence of legal claims, or where otherwise permitted by law.

### **3.2 Suppliers and other business partners**

We will process personal data in connection with our agreements with suppliers and other business partners. The personal data that will typically be processed are contact details (such as name, position, telephone number, and email address) and other information considered necessary in order to respond to communications, or to conclude or perform agreements.

For individuals, the basis for processing will be the agreement entered into with the individual or it's employer. Where the supplier or other business partner is a company, personal data are processed based on Arcline's legitimate interest. Said legitimate interest is the need to administer the contractual relationship and maintain a professional dialogue in connection with a potential or existing agreement.

## **4 WHO DO WE SHARE YOUR PERSONAL DATA WITH?**

### **4.1 Data processors**

Your personal data may be made available to service providers that process data on our behalf. These include the individual lawyer handling your case, providers of IT systems, cloud hosting, authentication services, and other technical infrastructure necessary for the provision of our services.

To protect your rights, we enter into data processing agreements with all such suppliers, which, among other things, ensure that your personal data cannot be used for purposes other than those we have specified. Our suppliers are also required to impose the same obligations on their subcontractors.

None of our suppliers are located outside the EU/EEA. This means that personal data will not be transferred to or become accessible from jurisdictions that do not provide the same level of protection of personal data as Norwegian law.

### **4.2 Other third parties**

Arcline will not disclose your personal data to third-parties beyond the lawyers serving your legal matter, unless there is a lawful basis for such disclosure. Such a basis may include your consent, disclosure being necessary to provide legal services, or disclosure being required by law.

Examples of third parties with whom we may share your personal data include courts, public authorities, counterparties, and external lawyers, but only to the extent necessary in connection with a specific case or to fulfil legal obligations.

## **5 YOUR RIGHTS**

You have the following rights under data protection law (subject to conditions and exceptions):

- **Access** – to know what data we process about you
- **Rectification** – to have inaccurate or incomplete data corrected
- **Erasure** – to request deletion of your personal data
- **Restriction** – to limit processing in certain circumstances
- **Portability** – to receive data in a structured, machine-readable format
- **Objection** – to object to processing based on our legitimate interests
- **Complaint** – to lodge a complaint with the Norwegian Data Protection Authority (Datatilsynet)

You may exercise your rights by contacting us at [contact@arcline-ai.com](mailto:contact@arcline-ai.com).

## **6 HOW LONG DO WE STORE YOUR PERSONAL DATA?**

We retain personal data only for as long as necessary to fulfil the purposes described above or as required by law. For case documents, this may typically be for 10 years to protect Customer interests and to comply with legal obligations (e.g., lawyers archiving obligations, AML).

Anonymized and redacted information used for service improvement may be retained for longer but cannot be traced back to individuals.

## **7 MEASURES TO SAFEGUARD YOUR PERSONAL DATA**

We use technical and organizational security measures, including encryption, access controls, and secure hosting, to protect personal data against unauthorized access, misuse, or disclosure. Internal routines are established to ensure ongoing compliance and security.

## **8 CHANGES TO THIS PRIVACY STATEMENT**

We may update this privacy statement when necessary. The latest version will always be available at our website.