ANNEX to the Data Processing Agreement for Kabal Field Services (IronSight)

REVISION LOG

Rev.	Date	Nature of Changes
1.0	10.08.2025	Created document for IronSight
1.1	12.03.2026	Updated Section 1 to clarify Controller`s notification obligations for indirect data collection
1.2	02.06.2026	Updated Section 1 to authorize automated integration and cross-platform synchronization
1.3	29.07.2026	Updated module-name in heading
1.4	30.07.2026	Updated section 4 to include Zendesk, and locations updated
1.5	30.09.2026	Updated section 4 to reflect HubSpot CRM and customer account management role

1. PURPOSE AND NATURE OF THE PROCESSING OPERATIONS

The Controller will

1) provide the Processor own information,
2) provide the Processor lawfully obtained information about Controller's other contractors / suppliers, ensuring all necessary notices have been provided to the data subject as required by applicable law,
3) provide its other contractors / suppliers with access to the software system covered by the Main Agreement, and
4) make sure such other contractors / suppliers are secured the rights and obligations equal to Controller under this Data Protection Agreement and have provided required information to their personnel with regard to Processing of Personal Data belonging to such other contractors / suppliers, in order to handle and execute its logistics operations.
5) authorize and instruct the Processor to conduct automated synchronization, transfer, and integration of Personal Data between the Controller's Kabal environment and other platforms within the Kabal product suite (including, without limitation, Kabal Offshore, Kabal Personnel, Kabal Onshore, Kabal Field Operations, Kabal Supplier and Kabal Base) as well as authorized external third-party registries or platforms, provided that such integration has been enabled or requested by the Controller at a company or systemic level.

2. CATEGORIES OF DATA SUBJECTS

The Processor may Process Personal Data on the following categories of Data Subjects:

Data Subjects	Control and limitations
Controller's employees and consultants	Controller's super user will approve/reject user request and regulate access privileges by assigning application roles to the users.
Controller's contractors and subcontractors	Controller's super user will approve/reject user request and regulate access privileges by assigning application roles to the users.
Controller's data processor	Limited to Kabal employees providing services according to contract.

3. CATEGORIES OF PERSONAL DATA

The Personal Data processed on behalf of the Controller concerns the following categories of data. Except online tracking data, all data is collected and submitted by the Controller or the end-user.

Categories	Description	Purpose
System Data	e.g username, password, audit logs	Security
Contact data	e.g name, company, address, phone number, email	Contact information provided to the end-users in the application to support the work-flows.
Online Tracking Data	e.g cookies, IP address, domain name	To improve the usability, accessibility, and website performance for Controllers benefit, and to support Kabal`s security monitoring, including screening source IP addresses against threat-intelligence sources to help detect and prevent unauthorised access.IP address is used to derive approximate geolocation for these purposes only
Location data	e.g. the geographic position of a user that is «on duty» in a resource	To show position of resources on the map, aid with efficient scheduling

4. LOCATION(S), INCLUDING NAME OF COUNTRY/COUNTRIES OF PROCESSING

Company	Country of processing	Nature of processing	Additional Information
Kabal	Norway, USA, Canada, and Malaysia	To support the system and provide system support.	GDPR compliant. EU Standard Contractual Clauses (SCC) in place and TIA performed.

			Data processing is governed by Kabal`s DPA including SCC.
Microsoft Azure	Canada and USA (test, production, and failover)	Hosting of IronSight platform	GDPR compliant. EU adequacy decision for Canada and EU SCC. TIA performed. https://azure.microsoft.com/en-us/explore/trusted-cloud/privacy
HubSpot	Germany, USA, and Canada	CRM and customer account management for the IronSight platform, including customer contracts, account-management information and historic support tickets,	GDPR compliant. EU-US Data Privacy Framework (DPF) and EU Standard Contractual Clauses (SCC) in place and TIA performed. https://legal.hubspot.com/privacy-policy
Postmark	USA	Email communication between the system and the user.	GDPR compliant. EU-US Data Privacy Framework (DPF) and EU Standard Contractual Clauses (SCC) in place and TIA performed. https://www.activecampaign.com/legal/privacy-policy
Firebase	USA	Chat communication between users.	GDPR compliant. EU-US Data Privacy Framework (DPF) and EU Standard Contractual Clauses (SCC) in place and TIA performed. https://firebase.google.com/support/privacy
Twilio	USA	In-app notifications to users	GDPR compliant. EU-US Data Privacy Framework (DPF) and EU Standard Contractual Clauses (SCC) in place and TIA performed. https://www.twilio.com/en-us/legal/privacy
Auth0	USA	Authentication service for user access	GDPR compliant. EU-US Data Privacy Framework (DPF) and EU Standard Contractual Clauses (SCC) in place and TIA performed. https://www.okta.com/legal/privacy-policy/
Google Cloud Platform	USA (failover)	Hosting of IronSight data	GDPR compliant. EU-US Data Privacy Framework (DPF) and EU Standard Contractual Clauses (SCC) in place and TIA performed. https://cloud.google.com/terms/cloud-privacy-notice
Mapbox	USA	GIS Engine for application maps	GDPR compliant. EU-US Data Privacy Framework (DPF) and EU Standard Contractual Clauses (SCC) in place and TIA performed. https://www.mapbox.com/legal/privacy
Zendesk	Canada, USA and Malaysia	Handling of support requests	GDPR Compliant. Resold and implemented by Kundelab AS (Norway) under Zendesk Reseller Customer Agreement, governed by Zendesk DPA incorporating the EU SCC. https://www.zendesk.com/company/data-processing-agreement/

5. DURATION OF PROCESSING

The Processor processes the Personal Data for the term of the governing main agreement. On termination, the personal data are returned or deleted in accordance with the governing Data Processing Agreement.