



CERTIFICATE

no. 438/23

ePrivacyseal GmbH
Große Bleichen 21, 20354 Hamburg, Germany

hereby certifies* that

as determined in the certification decision of 20 March 2023

Sen Spirit Technology Limited
9/F, The Whitney, 183 Wai Yip Street, Kwun Tong, Kowloon, Hong Kong

operates its product or service

„Openhive Federated Learning (OHFL) v3“

version 6 December 2022

as defined in annex 1 and to the exclusion of the processing activities in annex 2 to this certificate.

final audit day: 30/03/2023

next planned monitoring by 29/03/2025

period of validity: 30/03/2023 – 29/03/2025

The certification decision takes place under the validity condition described in Annex 3 and in conformity with the criteria catalogue for the “ePrivacyseal EU” (version 3.0 of May 2022) of ePrivacyseal GmbH.

Annex 1 to certificate no. 438/23

Definition of processing activities

The product to be certified is called Openhive Federated Learning (OHFL) and is the flagship product of Openhive (OH). Openhive (OH) is a technology brand that provides enterprise software solutions primarily focused on multi-party data collaboration and synergy, AI, and data protection. Sen Spirit Technology Limited (SST), based in Hong Kong, is Openhive's official business representative in Hong Kong and Macau. Karin and SST only provide the OHFL software to the companies, but do not operate the infrastructure and are not involved in the operation of OHFL.

Openhive Federated Learning (OHFL) is a machine learning (ML) technology that enables organizations to collaboratively build and train AI models while keeping their respective proprietary data at the source. The data sets to be processed vary on a case-by-case basis, depending on the specific business use cases or business questions to be answered.

Data storage is the responsibility of the individual participants.

Annex 2 to certificate no. 438/23

Excluded processing activities

The following processes are not within the scope of this evaluation:

- relationships between end user organizations and their third party-service providers and partners
- any further data processing and other product behaviour not covered by the scope (see below)
- any data storage practices of OHFL users (database services/cloud services)
- the technical security of the local OHFL infrastructure (every OHFL user is responsible for their own security)
- any support services for the installation and further product assistance
- communications and contract negotiations among cooperating businesses using the product
- the billing infrastructure and associated data transfers, such as receiving application data for billing purposes in the SaaS (Software as a Service) model (see technical factual description)

Annex 3 to certificate no. 438/23

Validity condition

Businesses using the product must (1) obtain (voluntary and explicit) consent from all data subjects before using their data, and (2) provide transparency to data subjects through a valid privacy notice.

In case of a deletion request from a data subject, all involved businesses must fully delete and re-train the model.