Business name of the actor	Role in the hosting service (Host/processor of the Host)	HDS certified (yes / no / exempted)	SecNumCloud 3.2 qualified	Hosting activities in which the player is involved	Access to personal health data from countries outside the European Economic Area, by the Host or one of its processors (Requirement No 29 of the HDS framework)	Host or processor subject to a risk of access to personal health data from countries outside the European Economic Area, imposed by the legislation of a third country in breach of EU law (Requirement no 30 of the HDS framework)
Namirial S.p.A.	Host and Processor of the Host	Yes	No	Activities 3,4, 5 and 6	No For the services included within the HDS certification scope, no access to personal health data from countries outside the European Economic Area (EEA) is performed by the Host or by any of its processors. All systems hosting personal health data within the HDS scope are located within the EEA. Access to personal health data within the HDS scope is carried out exclusively by personnel based in the EEA. All processors and service providers involved in the HDS-certified services operate exclusively within the EEA. No remote support, administration, maintenance, assistance, or monitoring activities involving access to personal health data are carried out from countries outside the EEA.	Yes For the services included within the HDS certification scope, the Host relies on sub-processors that may be subject to the legislation of third countries outside the European Economic Area (EEA), in particular the United States of America (USA). The potential risk of access to personal health data arising from the legislation of such third countries has been identified and assessed through dedicated Transfer Impact Assessments (TIAs) covering all relevant sub-processors. The applicable non-European legislation that could, in specific circumstances, result in access to personal health data in breach of Union law is identified and documented in the contractual documentation, including the Data Processing Agreements (DPAs) concluded with the sub-processors. Appropriate technical, organisational, and contractual safeguards have been defined and implemented in order to mitigate the identified risks and to prevent any unauthorised access to personal health data. In light of the measures adopted, the residual risk of unauthorised access to personal health data arising from non-European legislation is considered limited and acceptable.