

Workshop on Solid Pods for AI Agents: Building GDPR-Compliant Data Backends

No Institute Given

Abstract. Solid is a W3C specification designed to operationalise GDPR principles at the architectural level: users control their data in personal Pods, grant and revoke granular access permissions, and can exercise the right to erasure through instant deletion. For AI agent systems, this architecture offers a principled alternative to storing personal data in model weights or vector databases, where GDPR compliance is effectively impossible. Yet deploying Solid Pods as data backends for AI agents remains practically difficult. This tutorial examines that gap directly, drawing on hands-on experience integrating Solid Pods with LLM agents via the Model Context Protocol. We cover Solid architecture, WebID and Solid-OIDC authentication, Web Access Control, and SPARQL query patterns, then walk through the practical challenges of deployment across server interoperability, authentication flows, and agent access patterns. The goal is to equip participants with the knowledge to build with Solid today, and a clear picture of where the ecosystem is headed.

Keywords: Solid Pods, AI agents, GDPR compliance, data sovereignty, Model Context Protocol, Web Access Control, decentralised data storage

1 Motivation

Large language models are increasingly deployed as agents that access personal data. Current architectures absorb this data into model weights or vector databases, making GDPR compliance — particularly the Right to Be Forgotten — effectively impossible for production systems. Solid Pods offer a principled alternative: personal data remains in user-controlled storage, agents access it at runtime via standardised protocols, and deletion is instant. This tutorial is a hands-on introduction to deploying that vision in practice, including the rough edges that documentation does not always cover.

The tutorial draws on direct experience building the EHDS Linked Health Data Portal (mcp.linkeddata.es), an ISWC 2026 Resource Track submission connecting LLM agents to 21.2 million RDF triples across 30 clinical cohorts. Integrating Solid Pods into that architecture surfaced practical challenges across authentication, server interoperability, and agent access patterns.

2 Topics Covered

The first part introduces Solid: WebID, Web Access Control, RDF storage, and why this architecture operationalises GDPR Articles 15–17 at the infrastructure

level. It also covers the Model Context Protocol as a standardised interface for agent-data access, and situates Solid Pods within the European Data Spaces landscape.

The second part is hands-on. Participants work through pod deployment across Community Solid Server, Enterprise Solid Server, and Node Solid Server; Solid-OIDC authentication flows; WAC permission management at scale; SPARQL query patterns and their limits; and the mismatch between how LLM agents invoke tools and how Solid expects clients to behave.

The third part is an open discussion on the relationship between well-designed standards and the friction of real-world adoption — directly engaging the Summer School theme of regulation and innovation as catalysts or antagonists.

3 Target Audience and Expected Outcomes

The tutorial targets researchers and practitioners working in privacy management; no prior Solid or MCP experience is required. Participants will leave with a working understanding of Solid Pod deployment for AI agent backends and a clearer view of where the ecosystem stands today.

4 Presenters

Meem Arafat Manab, Marie Skłodowska-Curie doctoral fellow, Ontology Engineering Group, Universidad Politécnica de Madrid (HARNESS network).

Víctor Rodríguez-Doncel, Associate Professor, Department of Artificial Intelligence, Universidad Politécnica de Madrid.

Beatriz Esteves, postdoctoral researcher, KNoWS group, IDLab, Ghent University–imec; co-chair W3C DPVCG.

Marlin Kisia, Marie Skłodowska-Curie doctoral fellow, IDLab, Ghent University–imec (HARNESS network).

5 Equipment and Format

One to two hours. Laptop and projector. A live demo connecting an LLM agent to a Solid Pod is planned, with a recorded fallback.

This work is supported by HARNESS, funded from the European Union’s Horizon Europe research and innovation programme under grant agreement no. 101169409.