

Planday AI connector legal notice

How this connector works

This notice describes what data and actions this connector can access, your responsibilities and the safeguards Planday provides at the platform level; it is not legal advice and does not assess your specific use case.

You're enabling an AI system to act in your Planday account.

This connector allows the AI assistant you're using to read data from, and take actions in, your Planday account at your instruction. Planday provides the data and action interface that the AI system connects to; Planday does not control, and is not responsible or liable for the AI system's behaviour, outputs, or the terms of the tool provider you've chosen to connect through. Refer to the provider's own terms and disclosures for how their AI system operates. Where an AI system generates content, makes suggestions, or takes actions using this connector, that output is AI-generated or AI-assisted.

Your responsibility when using the connector

By enabling this connector, you represent that you have assessed, or will assess, whether your specific configuration - including any use involving scheduling, absence management, or other data about identifiable employees - falls within a high-risk category under Annex III of the EU AI Act (this is more likely where decisions apply automatically without human review) and that you will fulfil any resulting obligations as deployer. You are also responsible for assessing compliance with data protection law and any other applicable requirements for your specific use case.

Data this connector can access

When enabled the connector can access the following data categories within your Planday account: Employee and organisational data, scheduling, absence and contract rules. xx

It cannot access any data outside these categories, including data not covered by the connection's configured scopes, and it cannot access data belonging to other Planday customers or accounts. Every call is re-checked against the authorizing user's Planday permissions before it runs, for example if viewing absence data is restricted to admin roles in your portal, a non-admin user's connection will not be able to retrieve it, exactly as if they'd opened that screen in Planday directly.

Access control enforcement

The connector acts strictly within the access rights of the Planday user or account that authorizes the connection. Every call is authenticated with that user's own credentials and checked against their current Planday permissions - it cannot read, change, or delete anything that user couldn't themselves read, change, or delete manually. If the authorizing

user's permissions change or are revoked, the connector's access changes or is revoked accordingly.

You configure and control access

Planday provides the data and action tools; you determine the business purpose for which they are configured and used. As the customer you determine:

- which data scopes and actions the connector is granted
- whether specific actions require human approval before execution (eg. modifications and shift publication) versus running autonomously;
- which users or roles in your organization may authorize or manage connectors;
- when to disable or revoke a connector's access

Logging and audit

Actions taken by the user are logged by Planday, including which data was accessed and which actions were taken (the commands, not the agent's reasoning).