**EGI CheckIn service provider registration form**

*This form needs to be filled and signed by any service provider (SP) not federated in EGI that wants to be integrated with the EGI AAI platform: CheckIn.*

The Organisation [Organisation name]

represented by [Representative name] and [Representative name]

considering that

* the Organisation wishes to connect its service to the CheckIn service in order to allow user login through the CheckIn and retrieve users’ attribute
* the CheckIn service can be integrated only with service providers who commit and fulfil the EGI security relevant to the service providers

agrees to comply with the requirements that the CheckIn data privacy (<https://wiki.egi.eu/wiki/SPG:Drafts:Data_Privacy_EGI_CheckIn>) places upon the connected service.

The registered entityID of the SP is: [URL]

The security incident response contact is: [CSIRT mail address], [CSIRT phone number]

The Organisation representatives have read and accept to fulfil the following policies:

* [EGI Security policy](https://documents.egi.eu/document/3015)
* [Service Operations Security Policy](https://documents.egi.eu/document/1475)
* [Traceability and Logging Policy](https://documents.egi.eu/document/2934)
* [Security Incident Response Policy](https://documents.egi.eu/document/2935)[[1]](#footnote-1)
* [Policy on the Processing of Personal Data](https://documents.egi.eu/document/2732)

Form provided by the representative of the Organisation:

Name: […]

Title: […]

Date & Place: […]

Signature:

1. Compliance to the security incident response policy is limited to security incidents that are relevant for the user authentication and authorization information obtained through CheckIn. For example, the compromised machine processed or stored user authentication data after being compromised. [↑](#footnote-ref-1)