Project Security & Compliance for: UNICARE BiH (Inform and Primero)

Last Updated: 2025-03-25

Security should be a top priority at every stage of data integration implementation–from analysis & planning and design, to the build, testing, and deployment phases.

Implementers must support their partners to ensure that the data integration solution is in compliance with relevant security requirements and adhering to best practices. See the below checklist for project-specific implementation and security considerations.

How to use this document:

- Depending on your partners' specific requirements, early on in the implementation consider if other items should be added to this checklist to revisit before deployment and go-live to reinforce compliance.
- As each item is completed, document the date completed, who completed the task, and provide links to relevant documentation.
- When complete, seek partner sign-off on the below document and save with other project documentation where it can be accessed by relevant parties, if needed.

Checklist Item	Comments	Timeline	Status
1. **Documentation** is finalized and made accessible to relevant parties	Documentation on solution requirements, design (solution architecture diagram, data flow/BPMN diagrams, data element mapping specifications, job triggers are confirmed, business value and country implementation are identified), and test scenarios are finalized, approved, and shared in a way where all parties can access it.	Before go-live	Completed on {DATE} Workflow Diagram
2. Consider data residency and storage requirements; **adjust retention periods** in OpenFn, as needed.	Ensure compliance with data residency and storage policies **UNICEF has opted to turn on "zero-persistence" to ensure NO input/output data is retained.**	Immediately	Completed on {DATE}

3. Seek partner sign-off on the **field-level data to be processed** via OpenFn	Ensure only necessary data will be extracted and processed via OpenFn. Seek sign-off from all implementing partners before integration setup begins. Typically documented in the Information Sharing Protocol (ISP).	Before integration setup begins	Completed on {DATE} (see data element mapping specifications - LINK)
4. Seek partner sign-off on **data logged** in OpenFn History.	In the workflows' job code, do not log any personally identifiable information - only system IDs and date timestamps that may be required for transaction auditing. *For developers: Avoid unnecessary "console.log()" statements & conduct log testing to verify.* **To enable a retry mechanism for failed instances, OpenFn will retain the form ID and submission ID. Example:** **{** **"_id": 9448242** **"_xform_id": 7205** **}**	Before go-live and connection to production systems	Completed on {DATE}
5. Confirm with partners that OpenFn credential is granted **only relevant API access**	Limit scopes and permissions where possible to ensure no overly broad/ unnecessary permissions are granted to the OpenFn credential used to access the partner systems. Consider API-only access credentials and access to test environments for partner systems.	Before go-live and connection to production systems	Configuration & credential testing completed on {DATE}
6. Consider the need for **Webhook authentication for additional security.**	Require either Basic HTTP or API Key authentication from external systems sending data to a	Before go-live and connection to production systems	Completed on {DATE}

	Workflow. If authentication is enabled, update the webhook configuration in the external app that points to OpenFn, **Inform platform does not have a mechanism to add webhook authentication**		
7. Configure **Github repository** & connect with OpenFn project for version control	Github provides version control and management of different development pipelines and change request unicare-bih	Before integration setup begins	Completed on {DATE}
8. Confirm with partners what are the appropriate **access settings & administrators** for the Github repository	Github repositories should never contain data, only code for OpenFn "job" scripts used to process data. Consider making the repository "private" and only granting read/write access to the relevant project administrators. **Janani Panchalingam has been added as administrator to the repository**	Before go-live and connection to production systems	Completed on {DATE}
9. Seek **partner User Acceptance Testing (UAT)** sign-off	Ensure partner(s) have tested the solution end-to-end and have provided sign off that the functionality is working according to the requirements.	Before go-live and connection to production systems	Completed on {DATE}
10. Seek **partner Security Testing** sign-off	Ensure that security-specific testing has been conducted to validate the security requirements & alignment with policies. The appropriate testing approach should be decided in partnership with Technical Leads and relevant partner Security Leads.	Before go-live and connection to production systems	Completed on {DATE}

11. Confirm list of administrator **users who need access** to OpenFn project	Only project admins who need access to OpenFn for ongoing integration monitoring should require access to the production project on OpenFn.org.	Before go-live and connection to production systems	Completed on {DATE}
12. Confirm project administrators have **enabled notifications** for error monitoring	OpenFn project collaborators can enable email notifications for real-time alerts and/or weekly digests of any integration errors or failures.	Before go-live and connection to production systems	Completed on {DATE}
13. Confirm support structures & **key security contacts**	Ensure support processes and contacts are documented and accessible to relevant parties. Know how to report and escalate security risks and breaches.	Before go-live	Completed on {DATE}
14. Document the **change management process**	Ensure partners have aligned on a process for change management and ongoing governance. Document this process so it's accessible for all relevant parties.	Before go-live	Completed on {DATE}
15. **Train administrators** on OpenFn platform administration, user management, integration activity monitoring, and the change management process.	Training is critical to total solution handover and ensuring security best practices are maintained during the project lifetime.	Before go-live	Completed on {DATE}

Solution documentation: Github README

Support contacts: {detail or add link to where this is captured}