Akeneo App Certification
Security charter

By signing this document, the App partner commits to comply with the following Akeneo security recommendations:

Security checklist	Context	Commitment
PIM accesses scope	An App suggests to the PIM user the permissions that are needed to work properly. Akeneo documentation	The App owner commits to offer the PIM user only the PIM permissions needed for the App to work properly (**no unnecessary access granted**).
OAuth 2 security	The oAuth2 protocol to connect an App offered by Akeneo requires proper management of the security information. Akeneo documentation	The App owner commits to store securely the "OAuth 2.0 client credentials" issued by the App Store (client_secret and "access token") and to make every effort to ensure that no third party can access this information.
Hosting	The App owner is responsible for the App hosting.	The App owner commits to check that the App hosting service guarantees that no unwanted access to the App can be made.
Code	The App owner is responsible for the App code and code dependencies/external libraries	The App owner commits to make every effort to ensure that its code does not contain any security vulnerabilities. The App owner commits to keep its App up-to-date with the last maintained version of external libraries (not owned by the App owner) but used by the App.

		The App owner commits to fix in the shortest possible time any security vulnerability that is communicated to him.
PIM data fair usage	An App with access to PIM data via its API can cause unwanted modifications to PIM data.	The App owner commits to perform sufficient testing to avoid unwanted changes to PIM data that could result in product data corruption.
API fair usage	An App with access to PIM data via its API can cause unwanted PIM overloads.	The App owner commits to respect Akeneo PIM API fair usage recommendations.

Partner Company Name: InBetween

Date: 21 Feb, 2023

Signature: