# Data protection impact assessment

For the model choice Azure global (incl. US): a prompt may be processed in any Azure region worldwide, including the US. GDPR Article 35.

**Template.** Fill in every field marked in brackets, read every section against how your company uses Fundarem, and have it signed by the person responsible before you switch the model choice on. A DPIA is your document as controller; we fill in only what the product itself does.

CONTROLLER (YOU)

[your company's legal name]

ORGANISATION NUMBER
[organisation number]

DATA PROTECTION OFFICER OR RESPONSIBLE PERSON
[name and e-mail]

PROCESSOR

[given in the agreement we sign with you]

CONTACT
mg@fundarem.com

## What is assessed

| | |
|---|---|
| MODEL CHOICE | Azure global (incl. US) (`global-after-dpia`) |
| SENT TO THE MODEL | The prompt and the context for that one call, with personal data masked by the anonymiser |
| WHERE PROCESSED | Any Azure region worldwide, including the US (Azure AI Foundry, Global Standard deployment) |
| STORED DATA | Built to stay in your own Azure tenant, in the EU/EEA region chosen at install |
| TEMPLATE | Version 1.1, made 2026-11-11 |

## 01 Description of the processing

**Nature.** Fundarem connects your business systems, describes their data as one map of objects, links and actions, and lets AI agents and an assistant read it and propose changes. Every change is proposed, approved and then committed.

**Purposes.** [the purposes your company uses Fundarem for, e.g. reporting, invoice follow-up, answering questions about customers]

**Systems connected.** [the systems connected, e.g. accounting, CRM, e-mail]

**Data subjects.** [whose data is in those systems, e.g. staff, customers' and suppliers' contact persons]

**Personal data in prompts.** A prompt carries the question and the records it needs. Before every model call the anonymiser masks the columns tagged as personal data and the names and patterned values it

recognises (names, national ids, e-mail addresses, phone numbers, bank accounts); the masked values are replaced by placeholders and put back only inside your tenant. [any column class your admin has switched the anonymiser off for on this route, or “none”]

**Special categories (Art. 9).** [whether prompts may contain health, union, biometric or other special-category data; if yes, keep those classes on a model inside your tenant]

## 02 Necessity and proportionality

**Why this model choice.** [the reason, e.g. the models you need are served only worldwide, or answer quality]

**Alternatives considered.** Azure Europe (EU data zone, every prompt processed in the EU) and a self-hosted model in your own region keep processing in the EU. [why they are not enough for this purpose]

**Lawful basis.** [the lawful basis per purpose (Art. 6)]

**Minimisation.** Each connector maps only declared fields; each role sees only the object types its access allows; the model gets only the context for one call and keeps no state between calls.

## 03 Transfer outside the EU/EEA

With this model choice a prompt may be processed outside the EU/EEA by Microsoft, your own provider under your own Azure agreement, not a sub-processor we engage. Record the safeguard you rely on (GDPR Chapter V):

- **Adequacy:** the EU-US Data Privacy Framework, if the provider is certified under it. [checked on dataprivacyframework.gov on (date)]
- **Standard contractual clauses:** in Microsoft's Data Protection Addendum (Products and Services DPA). [version and date of the DPA you accepted]
- **Supplementary measures in the product:** the anonymiser on every route by default; masked values never leave your tenant; a call that would carry an unprotected value is refused; the model keeps no state.

**Provider-side handling.** How the provider stores prompts (for example for abuse monitoring) follows your agreement with it. [what your Azure agreement says, and any exemption you have applied for]

## 04 Risks and the measures against each

- **Personal data reaches the model and is exposed or reused.** Measures: the anonymiser on by default, per column class per route, changes logged and under your approval rule; per-model policy refuses a weaker model. Residual: [low / medium / high]
- **Access by authorities in a third country.** Measures: masking before the call; only the prompt for one call leaves; stored data is built to stay in your EU tenant. Residual: [low / medium / high]
- **Wrong or unfair output used for a decision.** Measures: agents propose, a person approves before anything is written; every answer names its sources. Residual: [low / medium / high]
- **Other risks for your use.** [risk, measure, residual]

## 05 Conclusion

**Residual risk overall.** [low / medium / high]

**Decision.** [accepted / accepted with these extra measures / not accepted]

**Prior consultation.** If a high residual risk remains, the controller consults the data protection authority before processing (Art. 36; in Norway, Datatilsynet). [needed: yes / no]

**Next review.** [date, and at the latest when the model choice, the connected systems or the purposes change]

> The product facts in this template match our DPIA, data processing agreement and data-flow pages on the Trust page of our website.

## 06 Sign-off

Signed for the controller after the data protection officer (or the person responsible for data protection) has given an opinion.

| FOR THE CONTROLLER | DATA PROTECTION OFFICER'S OPINION |
|---|---|
| Name | Name |
| Title | Title |
| Date | Date |
| Signature | Signature |