

Impact assessment template: your AI tool equipped with ELYSÉA^{1,2}

A ready-to-fill template for the data protection impact assessment (DPIA) of your deployment, following the CNIL templates, with ELYSÉA's contribution already filled in.²

WHAT THIS TEMPLATE IS FOR

- **Who fills it in:** you, the controller, with your data protection officer (DPO); the assessment remains yours, ELYSÉA signs no part of it.^{1,3}
- **When it is due:** before deployment, when processing is likely to result in a high risk; under the CNIL's list this is the case when it concerns so-called vulnerable persons, employees included, or relies on an innovative use.^{1,4,5}
- **In Switzerland too:** the Federal Act on Data Protection requires the same prior assessment when there is a high risk to personality or fundamental rights.⁶
- **Our basis:** ELYSÉA carried out its own assessment before any real user; it concludes that processing is authorised under conditions, thirty measures being required before the first real user. It is handed over on request, without being published.

TO FILL IN

1. Context

ITEM	YOUR ANSWER	WHAT ELYSÉA BRINGS YOU
Controller	Your company: name, address, legal representative	ELYSÉA is your processor for everything it does for your tool: checking answers, alert, crisis evidence, attestations, kept for you; it is sole controller of its customer accounts, its billing and the security of its servers; memory from one application to another falls under joint controllership. ^{3,7}
Purpose	The precise use of the tool in your teams	ELYSÉA checks every answer of the AI model before it reaches the person; it has no other purpose.
Data subjects	The equipped teams, their number	No age verification; a minor indicator and dual consent under 15 exist for other uses.
Data	What your employees will enter	The message and the answer pass through ELYSÉA; memory from one conversation to the next exists only with the person's consent.
Recipients and processors	Your tool's publisher, your host	ELYSÉA's processors: database in Paris, model in Paris, accounts in Frankfurt; for other providers, possibly outside the EU, declared as such in the list handed over with the contract.
Vital danger alert	Your choice at installation, once the setting is built: yes or no; if yes, who receives it and under which procedure	Today, when a vital danger is confirmed, ELYSÉA writes for your application an alert with a fixed text asking for urgent human care, with the time and a fingerprint of the identifier, without conversation content; readable in your portal, kept for 90 days. Planned before the first real user: a setting of your choice; without a choice, no alert; the emergency numbers given to the person always remain.
Retention periods	Yours	ELYSÉA's are in the annex to the data processing contract.

2. Fundamental principles

QUESTION	YOUR ANSWER	WHAT ELYSÉA BRINGS YOU
Legal basis	Legitimate interest or performance of the employment contract, to be justified; an employee's consent is rarely free	— ^{1,8}
Minimisation	What the tool does not need to receive	ELYSÉA trains no model with your data.
Informing employees	Your note, and the statement that the person is talking to an AI	A reference text exists, unpublished, handed over on request. ⁹
Staff consultation	The works council (comité social et économique), before deployment	Dedicated sheet handed over with this template. ^{10,11}
Data subjects' rights	Your contact address	Requests received by ELYSÉA are passed on to you; answer within 30 days at most.

3. Risks

- **The three events to examine:** illegitimate access to data, unwanted modification, disappearance; for each, impacts, severity and likelihood. ¹²
- **The AI-specific risks the CNIL asks to examine:** data leakage through the system, misuse, bias, false content about a real person, automated decisions that cannot be checked, people losing control over their data, AI-specific attacks, serious ethical risks. ⁵
- **Prohibition to check:** inferring an employee's emotions in the workplace is prohibited by the AI Act, except for safety or health reasons. ⁹

RISK TO YOUR EMPLOYEES	YOUR MEASURE	WHAT ELYSÉA SETS AGAINST IT, AND ITS LIMIT
Reading emotions	Do not enable it in the tool	Emotion recognition locked in ELYSÉA; a voice analysis path remains on the deployed service, removed with voice in the version being prepared.
Manipulation, dependence, substitution	Your usage charter	Four prohibitions checked on every answer, which you can tighten, never weaken.
An employee in distress	Your internal support procedure, and your choice on the alert	Pointing to public helplines, without taking charge, always; today, when a vital danger is confirmed, an alert without content to your application; planned: only if you have chosen it.
Individual monitoring	Do not do it	No individual monitoring dashboard provided by ELYSÉA.
Contesting an answer	Your complaints channel	Every answer carries an attestation tied to the exact software version.
Real effectiveness of the safeguards	Track it in your review	No measured result to date: measurement to be done, published after the campaign.

4. Sign-off

1. Opinion of your data protection officer, written and dated. ¹
2. Opinion of the works council, attached. ¹⁰
3. Decision of the controller: refuse, authorise under conditions or authorise; date of the review. ²
4. Review at every change in risk, in particular at every new version of the tool. ¹

WHAT THIS TEMPLATE DOES NOT SAY

- **It does not replace your assessment:** the right-hand columns describe ELYSÉA alone, not your publisher's tool or your use. ³
- **It does not prove effectiveness:** no published measurement, no third-party validation, no customer to date.
- **ELYSÉA's measures are not all done:** those its assessment requires will be done before the first real user, otherwise no opening.

NEXT STEP

Ask for our assessment and the retention annex; we review yours with your officer. contact@elysea.app · elysea.app

