Fiche mémo · Leçon 29 · 34 min

Le RGPD dans vos flux, sous-traitants, contrats et hébergement en Europe

Dès qu'un flux lit un nom, un téléphone ou une adresse, votre entreprise est responsable de traitement et chaque outil traversé devient un sous-traitant. Il faut un contrat avec chacun, savoir dans quel pays il traite les données, n'envoyer à l'IA que l'utile et tenir une ligne de registre par flux.

Objectifs

- Dresser la liste des sous-traitants d'un flux, avec leur contrat et le pays où ils traitent les données
- Réduire les données envoyées à l'IA aux seuls champs nécessaires à sa tâche
- Rédiger la ligne du registre d'un flux et repérer quand une analyse d'impact s'impose

À retenir

- Votre entreprise est responsable de traitement ; chaque outil qui traite les données du flux pour elle est un sous-traitant, avec un contrat rangé.
- Chaque étape a son pays : la région de Make se choisit une fois pour toutes, et votre propre connexion d'IA sort de la garantie européenne.
- L'IA ne reçoit que les champs dont elle a besoin ; noms, téléphones et courriels rejoignent le résultat après elle.
- Un flux quotidien a sa ligne au registre, même dans une entreprise de 12 personnes.
- Deux critères sur neuf, et l'IA générative en compte déjà un : au deuxième, appelez votre DPO ou votre conseil.

Le trajet d'une demande de devis

1. **Formulaire Tally** — La cliente saisit nom, téléphone, commune et description du chantier.
2. **Webhook n8n** — n8n Cloud reçoit toute la demande et la garde dans son journal.
3. **Nœud qui masque** — Seuls le type d'ouvrage, la commune et la description continuent vers l'IA.
4. **IA qui classe** — Le fournisseur d'IA reçoit le texte réduit et rend un JSON.
5. **Sheets et Gmail** — Google stocke la ligne du tableur et le brouillon de réponse.
6. **Claire relit** — Rien ne part chez la cliente sans sa validation.

Chaque case est un endroit où les données de la cliente passent ou restent : chacune a son contrat et son pays.

La demande à recopier

Demande à recopier Faire préparer la ligne du registre à partir de la fiche

```
Tu aides le référent RGPD d'une PME de [effectif] salariés, [secteur], à [ville].
Voici la fiche d'automatisation d'un de nos flux, sans aucune donnée réelle de client : [collez la fiche].
Dresse la ligne de notre registre des activités de traitement, selon l'article 30 du RGPD, en huit rubriques : nom du flux et responsable, finalité, catégories de personnes, catégories de données, destinataires et sous-traitants (un par ligne, avec le pays de traitement), transferts hors UE et leur cadre, durées de conservation par endroit, mesures de sécurité.
Pour chaque information absente de la fiche, écris « à compléter » au lieu de supposer.
Termine par la liste des critères d'analyse d'impact que ce flux remplit, avec une phrase de justification pour chacun.
```

Note : Ne collez jamais une vraie demande de client dans cette demande : la fiche suffit.

Le code à recopier

Le nœud qui ne laisse passer que l'utile (n8n, nœud Code) JAVASCRIPT

```javascript
// Placé entre le Webhook (champs remis à plat) et le nœud d'IA.
// Il ne garde que ce dont l'IA a besoin pour classer la demande.
const masquer = (texte) => (texte || "")
  // retire les adresses de courriel écrites dans la description
  .replace(/[\w.+-]+@[\w-]+(?:\.[\w-]+)+/g, "[courriel retiré]")
  // retire les numéros français : 06 12 34 56 78, 0556123456, +33 6 12 34 56 78
  .replace(/(\+33\s?|0)[1-9](?:[\s.-]?\d{2}){4}/g, "[téléphone retiré]");

return $input.all().map((item) => ({
  json: {
    id_demande: item.json.id_demande,   // pour rejoindre les coordonnées après l'IA
    type_ouvrage: item.json.type_ouvrage,
    commune: item.json.commune,
    description: masquer(item.json.description),
  },
}));
```

Après l'IA, un nœud Merge rejoint le résultat et les coordonnées par le champ id_demande, pour remplir le tableur. Le masquage attrape les formats courants, pas tous : il réduit le risque, il ne le supprime pas.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Brancher l'IA du flux avec le compte gratuit et personnel d'un salarié, « le temps de tester », puis le laisser en production. Aucun contrat ne lie l'entreprise à l'éditeur, les réglages d'entraînement et de région sont ceux d'un particulier, et la clé part avec le salarié le jour où il quitte l'entreprise.	Ouvrez un compte au nom de l'entreprise dès le premier test, acceptez son DPA, refusez l'entraînement, choisissez la région, et rangez la clé dans les identifiants de la plateforme.
Créer l'organisation Make sans regarder le champ de région, puis découvrir des mois plus tard qu'elle est en US. La région de l'organisation Make ne se change plus après sa création. Tous les scénarios qu'elle contient traitent leurs données dans cette zone.	Choisissez EU à la création. Si l'organisation est déjà en US, créez-en une nouvelle en EU, reconstruisez et testez les scénarios, puis coupez l'ancienne.