Fiche mémo · Leçon 7 · 36 min

Répondre à une demande d'exercice de droits et réagir à une fuite de données

Une personne peut demander ce que vous avez fait de ses données, IA comprise : vous répondez en un mois, gratuitement, en cherchant aussi dans les conversations et chez le sous-traitant. Une fuite se confine dans l'heure, se documente toujours, se notifie sous 72 heures si le risque n'est pas improbable, et s'annonce aux personnes s'il est élevé.

Objectifs

- Traiter une demande d'accès, d'effacement ou d'opposition dans le délai d'un mois, conversations d'IA comprises
- Décider, après un incident, s'il faut notifier la Commission nationale de l'informatique et des libertés (CNIL) et informer les personnes
- Rédiger l'accusé de réception, la notification et le message aux personnes concernées en langage clair

À retenir

- Une demande de droits reçoit une réponse dans un délai d'un mois, gratuite, prolongeable de deux mois en prévenant la personne dans le premier mois.
- La recherche couvre les conversations d'IA, les fichiers envoyés, la mémoire de l'outil et ce que garde le sous-traitant.
- Toute violation se documente ; elle se notifie à la CNIL sous 72 heures si le risque n'est pas improbable, et s'annonce aux personnes s'il est élevé.
- Le délai court à partir du moment où l'entreprise sait ; un sous-traitant prévient son client responsable dans les meilleurs délais.
- Avant de supprimer une conversation ou un lien, consignez ce qu'ils contenaient : c'est ce qui permet d'évaluer le risque.

Une demande d'accès traitée en un mois

1 — J0, réception
Date notée, accusé de réception envoyé.

→

2 — Identité
Pièce demandée seulement en cas de doute raisonnable.

→

3 — Recherche
Dossiers, messagerie, conversations d'IA, sous-traitants.

→

4 — Réponse
Copie des données et informations de l'article 15.

→

5 — Avant J+30
Envoi, ou prolongation motivée dans le mois.

Article 12 du RGPD : un mois à compter de la réception, prolongeable de deux mois si la demande est complexe, en prévenant la personne dans le premier mois.

La demande à recopier

Demande à recopier **Rédiger l'accusé de réception puis la réponse à une demande d'accès**

```
Rôle : tu aides une PME de [secteur] à répondre à une demande d'accès au titre de l'article 15 du RGPD, en langage clair.
Contexte : demande reçue le [date] de [Personne A], [qualité : candidat, client, salarié]. Ce que nous avons trouvé, sans donnée réelle : [catégories de données et lieux : dossier, messagerie, conversations de l'outil d'IA]. Ligne du registre : finalité [finalité] ; destinataires [services internes, éditeur de l'outil d'IA en tant que sous-traitant] ; durée de conservation [durée] ; origine [source] ; décision automatisée : [aucune / description].
Tâche 1 : écris l'accusé de réception, qui indique la date de réception et le délai d'un mois.
Tâche 2 : écris la réponse qui donne, rubrique par rubrique, les informations de l'article 15 et annonce la copie jointe des données.
Format : vouvoiement, phrases courtes, aucune information que je n'ai pas donnée, crochets laissés là où il manque une information.
```

Note : Le modèle se remplit sans le nom ni les données de la personne : ils restent dans votre réponse finale, pas dans la demande à l'IA.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Supprimer la conversation fautive dans la minute, sans rien noter. Vous ne pouvez plus dire quelles données sont parties ni combien de personnes sont touchées, alors que la documentation et la notification le demandent.	Consignez d'abord l'heure, le contenu et le nombre de personnes, ou faites une capture conservée par le référent, puis supprimez le lien et la conversation.
Attendre d'avoir tout compris pour notifier la CNIL. Les 72 heures courent depuis la prise de connaissance, week-end compris. Une enquête complète dépasse souvent ce délai.	Faites une notification initiale dans le délai avec ce que vous savez, puis une notification complémentaire quand l'enquête avance, comme le téléservice le permet.
Répondre à une demande d'accès avec le seul dossier principal. Les conversations d'IA, les fichiers joints et ce que garde le sous-traitant sont aussi des données de la personne. Une réponse incomplète méconnaît l'article 15.	Partez de la ligne du registre : chaque destinataire et chaque outil cités sont un endroit où chercher, outil d'IA compris.
Exiger une copie de pièce d'identité avant de répondre à toute demande. L'article 12 ne permet de demander des informations supplémentaires qu'en cas de doute raisonnable sur l'identité. Exiger une pièce sans raison collecte une donnée de plus et retarde la réponse.	Répondez à l'adresse connue de la personne ; ne demandez un élément supplémentaire que si un doute réel existe, et seulement ce qui suffit à le lever.