

Modèle d'AIPD — RGPD article 35

Filtrage · description · nécessité & proportionnalité · matrice de risques · visa · annexe IA

MODÈLE GRATUIT — DOCX · PDF · MD | Version 1.0 · Mise à jour 2026-07-22

À compléter AVANT le début du traitement (art 35(1)).

Les sections 4 à 11 portent le contenu obligatoire de l'art 35(7)(a)–(d).

Lorsqu'un DPO est désigné, son avis est obligatoire (art 35(2)).

Risque résiduel élevé → consultez d'abord votre autorité de contrôle (art 36 : 8 semaines + 6).

Revue au moins lorsque le risque change (art 35(11)).

1. Contrôle du document

Référence de l'AIPD	ID interne, p. ex. DPIA-2026-004
Nom du traitement / de la fonctionnalité	Nom court du traitement analysé
Responsable / évaluateur	Entité juridique ; personne qui complète cette AIPD
Date de début / d'approbation	Dates de cycle de vie

2. Filtrage — une AIPD est-elle requise ?

2a. Cas toujours-AIPD de l'article 35(3)

Cas	S'applique ?
35(3)(a) Évaluation/profilage systématique et approfondi avec effets juridiques ou similaires significatifs	Oui / Non
35(3)(b) Traitement à grande échelle de données de catégories particulières (art 9) ou relatives aux condamnations pénales (art 10)	Oui / Non
35(3)(c) Surveillance systématique à grande échelle d'une zone accessible au public	Oui / Non

2b. Les neuf critères de risque élevé WP248 rév.01 (règle générale : deux remplis → AIPD)

Critère	Rempli ?
1. Évaluation ou notation (y compris profilage, prédiction)	Oui / Non
2. Décision automatisée avec effet juridique ou similaire significatif	Oui / Non
3. Surveillance systématique	Oui / Non
4. Données sensibles ou données à caractère hautement personnel	Oui / Non
5. Données traitées à grande échelle	Oui / Non
6. Croisement ou combinaison d'ensembles de données	Oui / Non
7. Données concernant des personnes vulnérables	Oui / Non
8. Usage innovant / solutions technologiques ou organisationnelles nouvelles (y compris l'IA)	Oui / Non
9. Traitement empêchant l'exercice d'un droit ou l'utilisation d'un service/contrat	Oui / Non

Consultez aussi la liste de l'art 35(4) de votre autorité de contrôle — p. ex. la liste de 14 catégories de la CNIL (FR), la liste britannique à risque élevé de l'ICO, la liste norvégienne du Datatilsynet.

3. Résultat du filtrage

AIPD requise ?	Oui / Non — avec le(s) déclencheur(s) : cas de l'art 35(3), nombre de critères WP248 remplis, ou entrée d'une liste art 35(4)
Si non	Consignez le raisonnement et conservez ce document ; refiltrez si le traitement change

4. Description systématique du traitement (art 35(7)(a))

Nature, portée, contexte, finalités	Ce que fait le traitement, pour qui, à quelle échelle et pourquoi
Catégories de données personnelles	Signaler explicitement les catégories particulières (art 9)
Catégories de personnes concernées	Signaler les groupes vulnérables (enfants, salariés, patients)
Destinataires	Équipes internes, sous-traitants, tiers
Transferts internationaux	Pays tiers + mécanisme de transfert (CCT, adéquation)
Conservation	Durée et déclencheur de suppression
Systèmes et flux de données	Où les données résident et circulent
Intérêt légitime poursuivi	Uniquement si l'art 6(1)(f) est invoqué

5. Dossier de consultation (art 35(2), 35(9))

Avis du DPO	Obligatoire lorsqu'un DPO est désigné — consigner l'avis et la date
Point de vue des personnes concernées	Le cas échéant ; si non recueilli, consigner pourquoi
Sous-traitants / fournisseurs consultés	P. ex. documentation du fournisseur d'IA examinée

6–7. Nécessité et proportionnalité (art 35(7)(b))

Base légale	Base de l'art 6 ; condition de l'art 9 si catégories particulières
Nécessité	Pourquoi ce traitement atteint la finalité ; minimisation des données appliquée
Proportionnalité	Alternatives moins intrusives envisagées et pourquoi elles ne suffisent pas
Transparence & droits	Comment les personnes concernées sont informées ; comment l'accès, l'effacement, l'opposition et la portabilité sont honorés

8–10. Évaluation des risques (art 35(7)(c))

Des risques pour les droits et libertés des personnes concernées — pas des risques pour l'entreprise. Cotez probabilité × gravité sur une matrice 3×3.

	Gravité : faible	Gravité : moyenne	Gravité : élevée
Probabilité : élevée	Moyen	Élevé	Élevé
Probabilité : moyenne	Faible	Moyen	Élevé
Probabilité : faible	Faible	Faible	Moyen

Exemple de ligne complétée :

ID	Risque	P	G	Mesure	Résiduel
EX1	Accès non autorisé aux journaux d'un assistant IA de support client contenant des données personnelles	M	É	Accès restreint au rôle de support d'astreinte ; journaux pseudonymisés après 24 h ; conservation réduite à 30 jours ; accès audités	Faible

11. Mesures d'atténuation (art 35(7)(d))

Une mesure spécifique par risque. Les formulations génériques ne réduisent pas les scores ; les MTO spécifiques (art 32), les contrôles d'accès, la pseudonymisation et la réduction des durées de conservation, si.

12. Risque résiduel & décision au titre de l'article 36

Risque résiduel global	Faible / Moyen / Élevé — après toutes les mesures
Consultation préalable requise ?	Si le risque résiduel reste ÉLEVÉ : consultez l'autorité de contrôle AVANT le traitement (art 36) — avis écrit sous 8 semaines, prolongeables de 6
Autorité consultée / réponse	Date, référence, issue — ou n/a

13–14. Visa & journal de revue (art 35(2), 35(11))

Approbation du responsable	Nom, rôle, date
Avis du DPO consigné	Oui / Non — date
Déclencheurs de revue	Nouvelle catégorie de données, nouveau modèle d'IA, nouveau destinataire, nouvelle finalité
Prochaine revue planifiée	Date

Annexe IA — fonctionnalités IA/LLM et règlement IA de l'UE

À compléter pour tout traitement piloté par l'IA (critère WP248 n° 8, plus typiquement les n° 1, 2 et 5). Pour les systèmes d'IA à haut risque lorsque vous êtes un déployeur dans le champ de l'art 27 du règlement IA de l'UE, la FRIA peut être documentée conjointement avec cette AIPD — aucune analyse ne remplace l'autre.

Modèle / système	Fournisseur, modèle, version
Provenance des données d'entraînement	Données personnelles dans les données d'entraînement/de fine-tuning ? Documentation du fournisseur examinée ?
Décisions automatisées & effets	Effets juridiques ou similaires significatifs (art 22 RGPD) ? Humain dans la boucle ?
Explicabilité & supervision	Les résultats peuvent-ils être expliqués aux personnes concernées ? Quelles mesures de supervision s'appliquent ?
Risques de biais / d'exactitude	Tests réalisés ; modes de défaillance connus ; plan de surveillance
Classification au titre du règlement IA	Interdit / Haut risque / Limité (transparence) / Minimal
Référence FRIA (art 27)	Si haut risque et dans le champ : référence de la documentation conjointe