

Modèle de registre des sous-traitants ultérieurs RGPD

Articles 28(2), (4) & 30(2), règlement (UE) 2016/679 · Avis 22/2024 du CEPD

MODÈLE GRATUIT — XLSX · PDF · MD | Version 1.0 · Mise à jour 2026-07-24

Ce que contient le classeur

Registre des sous-traitants	Une ligne par sous-traitant ultérieur — y compris les sous-traitants de rang inférieur plus bas dans la chaîne : identité et adresse du siège, contact, description du service et du traitement, catégories de données personnelles, lieux de traitement, mécanisme et détail de transfert, garanties de sécurité, parent et niveau dans la chaîne, date du contrat de répercussion, statut et référence de notification. Cette feuille est la source de votre liste publique et de votre page Trust Center.
Journal des modifications	Une ligne par ajout, remplacement, retrait ou changement substantiel : référence de la notification, date d'envoi, canaux, responsables du traitement concernés, date limite d'opposition, oppositions reçues, issue, date d'effet. Votre piste de preuve au titre de l'article 28(2).
Diligence raisonnable	Une ligne par évaluation : garanties revues, certifications vérifiées, référence des TOM, analyse d'impact des transferts lorsque le chapitre V s'applique, divulgation des sous-traitants de rang inférieur, résultat et date de la prochaine revue — le dossier continu des « garanties suffisantes ».

L'échelle juridique

Art 28(2)	Autorisation écrite préalable — générale ou spécifique — pour recruter un autre sous-traitant. Sous autorisation générale, le sous-traitant doit informer le responsable du traitement des ajouts ou remplacements envisagés, en lui donnant une possibilité réelle de s'opposer avant que le changement ne prenne effet.
Art 28(3)(d) & (4)	Le contrat oblige le sous-traitant à respecter les conditions du paragraphe 2 ; les mêmes obligations de protection des données se répercutent sur chaque sous-traitant ultérieur, et le sous-traitant initial demeure pleinement responsable envers le responsable du traitement de l'exécution par le sous-traitant ultérieur.
Art 30(2)	Le registre des activités de traitement du sous-traitant couvre les traitements effectués pour le compte de chaque responsable du traitement — les colonnes service, catégories de données et transfert du registre alimentent directement ces registres.
Chapitre V	Tout traitement hors de l'EEE nécessite une décision d'adéquation (art 45), des garanties appropriées — le plus souvent les CCT de la décision (UE) 2021/914 (art 46) — ou, à titre exceptionnel, une dérogation de l'art 49. Le registre enregistre le mécanisme et la date de l'analyse d'impact des transferts par sous-traitant ultérieur.
Avis 22/2024 du CEPD	Adopté le 7 octobre 2024 : les responsables du traitement doivent disposer de l'identité, de l'adresse et du contact de chaque acteur de la chaîne, avec les descriptions de traitement, les lieux, les garanties de transfert et les garanties de sécurité — tenus à jour en permanence et fournis de manière proactive, pas sur demande.

Pourquoi une liste PDF statique échoue

La plupart des sous-traitants tiennent leur liste de sous-traitants ultérieurs dans une annexe PDF, mise à jour quand quelqu'un y pense. L'avis 22/2024 du CEPD a fermé cette voie : la liste doit être à jour en permanence, couvrir toute la chaîne, et une mise à jour silencieuse de page web ne décharge de rien si elle ne s'accompagne pas d'une alerte active envoyée aux responsables du traitement à temps pour s'opposer. La colonne statut du registre (« Annoncé — délai d'opposition ouvert » → « Actif ») et le journal des modifications existent pour rendre cette séquence auditable.

Le délai de notification est contractuel, pas légal : la pratique européenne se concentre autour de ~15 jours comme délai typique, 30 à 60 jours négociés par les clients grands comptes et réglementés, et 90 jours de plus en plus rares. Quoi que dise votre DPA, le critère du CEPD est de savoir si le délai permet une opposition éclairée et effective.

Ce que la CNIL attend

Le guide du sous-traitant de la CNIL et son clausier type exigent une autorisation écrite préalable — spécifique ou générale — avant tout recrutement d'un sous-traitant ultérieur ; sous autorisation générale, le sous-traitant doit informer le responsable du traitement de tout ajout ou remplacement envisagé afin qu'il puisse s'y opposer. La CNIL attend en outre que le responsable du traitement puisse identifier à tout moment chaque sous-traitant ultérieur de la chaîne, le sous-traitant fournissant cette information et la tenant continuellement à jour — c'est exactement la fonction de ce registre, dont les colonnes identité, chaîne et statut correspondent une à une à cette attente.

Royaume-Uni & Norvège

Le UK GDPR reprend l'article 28 tel quel, sous la supervision de l'ICO, dont les lignes directrices sur les contrats attendent une date limite d'opposition explicite. La Norvège applique le RGPD via l'accord sur l'EEE (personopplysningsloven), sous la supervision du Datatilsynet. Les transferts de l'EEE vers le Royaume-Uni reposent sur les décisions d'adéquation britanniques renouvelées (prorogées en 2025, expiration le 27 décembre 2031) ; un traitement interne à l'EEE, Norvège comprise, ne nécessite aucun mécanisme de transfert.

Du registre au workflow

Un registre résout le problème de la tenue des dossiers ; il ne notifie pas les responsables du traitement, n'applique pas les délais d'opposition et ne prouve pas qui a vu quoi. Orbiq publie votre registre des sous-traitants ultérieurs dans un Trust Center avec notifications aux abonnés, suivi des dates limites d'opposition et piste d'audit — orbiqhq.com/platform/trust-updates. La variante Markdown lisible par machine de ce modèle permet à un agent IA de maintenir le registre aux côtés de votre registre des activités de traitement et de vos notifications de changement.