Modèle de registre des activités de traitement (RoPA) RGPD

Le registre de l'article 30 prêt à compléter : un registre responsable du traitement aligné sur l'art 30(1)(a)–(g), un registre sous-traitant aligné sur l'art 30(2)(a)–(d), des colonnes base légale et transferts hors EEE, et dix exemples d'activités préremplis — conçu pour l'UE-27, double rôle, piloté par listes déroulantes.

Ce PDF est le guide des champs qui accompagne le modèle. Le fichier de travail est le XLSX (validations par listes déroulantes, feuilles responsable et sous-traitant, bloc d'identité de l'organisation) ; une variante Markdown lisible par machine est fournie pour les agents IA. Les trois fichiers sont gratuits sur orbiqhq.com/templates/gdpr-ropa-template — sans e-mail requis.

Base juridique : règlement (UE) 2016/679 (RGPD), article 30(1)–(5) ; position du G29 sur l'article 30(5) (avril 2018) ; guide RoPA de la DPC irlandaise (2023) ; les lignes directrices registre de la CNIL. Ce modèle est une aide, pas un conseil juridique.

Ce qu'exige l'article 30

Registre du responsable du traitement — article 30(1). Chaque responsable du traitement (et, le cas échéant, son représentant) tient un registre des activités de traitement effectuées sous sa responsabilité, comportant : **(a)** le nom et les coordonnées du responsable du traitement, de tout responsable conjoint, du représentant au titre de l'article 27 et du DPO ; **(b)** les finalités du traitement ; **(c)** les catégories de personnes concernées et de données à caractère personnel ; **(d)** les catégories de destinataires, y compris les destinataires dans des pays tiers ou des organisations internationales ; **(e)** le cas échéant, les transferts vers des pays tiers, l'identification du pays et, pour les transferts relevant du second alinéa de l'article 49(1), la documentation des garanties appropriées ; **(f)** dans la mesure du possible, les délais d'effacement envisagés ; **(g)** dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles de l'article 32(1).

Registre du sous-traitant — article 30(2). Chaque sous-traitant tient un registre de toutes les catégories de traitements effectués pour le compte de chaque responsable du traitement, comportant : **(a)** le nom et les coordonnées du sous-traitant, de chaque responsable pour le compte duquel il agit, ainsi que des représentants et du DPO ; **(b)** les catégories de traitements effectués pour le compte de chaque responsable ; **(c)** le cas échéant, les transferts vers des pays tiers avec identification du pays et, pour les transferts fondés sur une dérogation de l'article 49, les garanties documentées ; **(d)** dans la mesure du possible, une description générale des mesures de sécurité de l'article 32(1).

Forme et accès. Le registre se présente par écrit, y compris sous forme électronique (art 30(3)), et doit être mis à la disposition de l'autorité de contrôle sur demande (art 30(4)). La DPC irlandaise attend d'un RoPA qu'il soit autoporteur et lisible par un examinateur externe sans explication.

La dérogation « moins de 250 salariés », bien lue

L'article 30(5) exempte les organisations de moins de 250 salariés **sauf** si le traitement (i) est susceptible de comporter un risque pour les droits et libertés des personnes concernées, (ii) n'est pas occasionnel, ou (iii) porte sur des catégories particulières de l'article 9 ou des données pénales de l'article 10. La position du G29 d'avril 2018 lit ces critères comme des **alternatives** : un seul facteur suffit à déclencher l'obligation de tenue du registre pour l'activité concernée, et un traitement n'est « occasionnel » que s'il intervient en dehors de l'activité courante. La paie, les RH, le CRM, le support et le marketing relèvent de l'activité courante — c'est pourquoi, en pratique, presque toute entreprise en activité tient un RoPA pour ses traitements courants, quel que soit son effectif.

Comment compléter le registre

1. Complétez la feuille Identité de l'organisation. C'est le bloc d'identité art 30(1)(a) / 30(2)(a) : noms du responsable du traitement et du sous-traitant, coordonnées, responsables conjoints, représentants, DPO.

2. Inventoriez par finalité, pas par outil. Une ligne par activité de traitement (l'approche registre de la CNIL). Un même système peut héberger plusieurs activités ; une même activité peut s'étendre sur plusieurs systèmes.

3. Remplissez toutes les colonnes côté responsable. La base légale n'est pas une exigence textuelle de l'art 30, mais tous les modèles des autorités de contrôle européennes l'incluent — un registre qui l'omet ne passera pas une revue de complétude.

4. Consignez les transferts ligne par ligne. « Hors EEE » est le critère opérant : nommez le pays tiers et l'outil du chapitre V (adéquation, CCT, BCR), et liez les garanties documentées pour toute dérogation de l'article 49.

5. Complétez le registre sous-traitant si vous traitez pour des clients. Une ligne par responsable du traitement, avec des descriptions au niveau des catégories de traitements effectués.

6. Faites-le vivre. Désignez un propriétaire du registre, fixez des dates de revue et marquez les lignes remplacées « Obsolète — conservée » plutôt que de les supprimer, afin que le registre montre son propre historique.

Guide des champs — Registre responsable (art 30(1))

Colonne	Quoi renseigner
Fonction métier / activité de traitement	Regroupez les lignes par fonction (RH, ventes, finance...) et nommez l'activité de sorte qu'un lecteur externe la comprenne sans poser de question — « Administration du personnel et paie », pas « SAP ».
Finalité(s) — art 30(1)(b)	Pourquoi les données sont traitées, en termes opérationnels. Une ligne par finalité lorsque les finalités diffèrent sensiblement.
Base légale (art 6(1))	Liste déroulante : consentement, contrat, obligation légale, intérêts vitaux, mission d'intérêt public, intérêts légitimes. Bonne pratique exigée par tous les modèles des autorités de contrôle.
Données de catégories particulières / pénales	Signalez les données art 9 / art 10 et consignez la condition de l'art 9(2) invoquée (p. ex. art 9(2)(b) pour les traitements relevant du droit du travail). C'est l'un des trois facteurs qui font tomber l'exemption de l'art 30(5).
Personnes concernées / données personnelles — art 30(1)(c)	Des catégories, pas des individus : « salariés ; candidats », « données d'identification ; coordonnées bancaires ». Suffisamment granulaire pour que les réponses conservation et sécurité aient un sens ligne par ligne.
Destinataires — art 30(1)(d)	Catégories de destinataires, y compris les sous-traitants, les sociétés du groupe et les autorités publiques — et les destinataires dans des pays tiers.
Colonnes transfert — art 30(1)(e)	Si les données quittent l'EEE : le pays de destination ou l'organisation internationale, l'outil du chapitre V (adéquation / CCT / BCR) et, pour les dérogations de l'art 49, un lien vers les garanties documentées.
Conservation — art 30(1)(f)	Le délai d'effacement envisagé ou les critères (« durée du contrat de travail + conservation légale »). « Dans la mesure du possible » ne veut pas dire « facultatif » — les régulateurs lisent une case vide comme une lacune.
Mesures de sécurité — art 30(1)(g)	Une description générale des TOM de l'art 32(1) protégeant cette activité : chiffrement, contrôle d'accès, MFA, journalisation. Renvoyez à votre document TOM pour le détail.
Statut AIPD (art 35)	Le résultat de la pré-analyse par activité. Toute activité identifiée comme « susceptible d'engendrer un risque élevé » exige une AIPD avant son lancement.
Propriétaire / dernière revue / statut de la ligne	Les champs de workflow qui font vivre le registre — et la première chose qu'un auditeur vérifie pour détecter l'obsolescence.

Guide des champs — Registre sous-traitant (art 30(2))

Colonne	Quoi renseigner
Nom + coordonnées du responsable — art 30(2)(a)	Une ligne par responsable du traitement pour lequel vous traitez. SaaS B2B : une ligne par client, ou par segment de clients lorsque le traitement est identique.
Catégories de traitements — art 30(2)(b)	Ce que vous faites pour le compte du responsable du traitement, au niveau des catégories : hébergement, sauvegarde, accès du support, reporting — pas le détail par enregistrement.
Sous-traitants ultérieurs	Qui vous engagez en aval, avec les localisations. Restez cohérent avec votre liste publique de sous-traitants ultérieurs et vos engagements de notification au titre de l'art 28(2).
Transferts — art 30(2)(c)	La même logique du chapitre V que le registre responsable, vue du côté du sous-traitant.
Mesures de sécurité — art 30(2)(d)	Les TOM de la plateforme ; renvoyez à votre certificat ISO 27001 ou à votre rapport d'assurance lorsque les preuves y figurent.
Référence DPA	Le contrat de l'art 28(3) sous lequel chaque ligne opère, avec version et date de signature.

Au-delà de l'UE-27 : Royaume-Uni et Norvège

Royaume-Uni. Le UK GDPR conserve l'article 30 à l'identique, et l'ICO publie des modèles de documentation pour responsables du traitement et sous-traitants. Ce registre fonctionne comme RoPA UK : prenez « hors du Royaume-Uni » comme critère de transfert et l'ICO comme autorité de contrôle. Le modèle de l'ICO est centré responsable et cadré UK ; ce fichier ajoute le registre sous-traitant et les colonnes de transfert hors EEE dans un seul document.

Norvège. Le RGPD s'applique en Norvège via l'accord EEE et le Personal Data Act (personopplysningsloven) ; le Datatilsynet attend le même registre de l'article 30 — le protokoll over behandlingsaktiviteter — et l'examine lors de ses enquêtes. Les transferts EEE vers la Norvège ne sont pas des transferts vers un pays tiers pour les responsables du traitement de l'UE, et inversement.

Pourquoi maintenir le RoPA à jour en vaut la peine

Le RoPA relève du palier inférieur d'amendes — jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial (art 83(4)) — mais son poids réel est probatoire : c'est régulièrement le premier document qu'une autorité de contrôle demande, et les manquements à l'article 30 sont cités comme facteurs aggravants dans les constats relatifs à la responsabilité (accountability). Un registre à jour répond aussi aux questions de due diligence de l'article 28 que posent vos clients grands comptes — c'est pourquoi des extraits du RoPA ont leur place dans votre trust center, à côté de votre DPA, de vos TOM et de votre liste de sous-traitants ultérieurs.

Gardez le registre connecté aux preuves vivantes — mesures de sécurité, changements de sous-traitants ultérieurs, statut AIPD — dans Orbiq, et publiez le volet destiné aux acheteurs sur un Trust Center européen : orbiqhq.com.