

Accord de traitement des données (DPA)

Dernière mise à jour le 1er mai 2026 · Contrat au sens de l'art. 28 du RGPD.

Ceci est une traduction fournie à titre d'information. En cas de différence entre cette traduction et la version anglaise, la version anglaise prévaut.

Comment cela fonctionne

Le présent DPA fait partie des conditions d'utilisation. Il s'applique automatiquement dès qu'un espace de travail est créé et que des données à caractère personnel y sont enregistrées. L'organisation cliente propriétaire de l'espace de travail est le responsable du traitement ; Dazr est le sous-traitant. Aucune signature n'est requise ; si votre processus d'achat exige un exemplaire contresigné, écrivez à legal@dazr.eu.

1. Définitions

Les termes du présent DPA ont le sens que leur donne le règlement (UE) 2016/679 (le RGPD). Les « données personnelles du client » sont les données à caractère personnel que le responsable du traitement (ou les membres et auditeurs agissant sous son autorité) place dans l'espace de travail, y compris les données personnelles figurant dans les tâches de contrôle, les preuves, les commentaires, les fichiers, les risques, les incidents, les fiches fournisseurs, les membres et invitations, les signalements reçus via le portail public et le journal d'activité.

2. Objet, durée, nature et finalité

- **Objet** : le traitement des données personnelles du client afin que le responsable du traitement puisse gérer son programme de conformité en sécurité de l'information et en protection des données au moyen de la plateforme Dazr Compliance.
- **Durée** : la durée de l'abonnement du responsable du traitement, augmentée de la période de grâce après résiliation prévue par les conditions d'utilisation.
- **Nature et finalité** : hébergement, stockage, transmission, consultation, effacement et les opérations décrites dans les conditions d'utilisation et la politique de confidentialité.
- **Type de données personnelles** : données d'identification des membres des espaces de travail et des auditeurs invités (adresse e-mail, nom, rôle) ; le cas échéant, données d'identification des personnes qui signalent via le portail public ou qui signalent des incidents ; coordonnées d'employeurs et métadonnées opérationnelles téléversées par le responsable du traitement. Le responsable du traitement veille à ne pas téléverser de catégories particulières de données, sauf si sa propre base juridique le permet.
- **Catégories de personnes concernées** : les salariés, prestataires et auditeurs externes invités du responsable du traitement, ainsi que toute personne identifiée dans les contenus de conformité que le responsable du traitement choisit de téléverser.

3. Obligations du sous-traitant

1. Nous traitons les données personnelles du client uniquement sur instruction documentée du responsable du traitement. Ces instructions consistent en l'utilisation des fonctions prévues de la plateforme ; si nous estimons qu'une instruction enfreint le RGPD ou une autre disposition du droit de l'Union ou d'un État membre relative à la protection des données, nous en informons le responsable du traitement.
2. Nous veillons à ce que les personnes autorisées à traiter les données personnelles du client se soient engagées à respecter la confidentialité.
3. Nous prenons toutes les mesures requises par l'art. 32 du RGPD (sécurité du traitement). Les mesures actuelles sont décrites à la section 7 ci-dessous.
4. Nous respectons les conditions de l'art. 28, paragraphes 2 et 4, pour le recours à des sous-traitants ultérieurs

(voir la section 6).

5. Compte tenu de la nature du traitement et des informations dont nous disposons, nous aidons le responsable du traitement à répondre aux demandes des personnes concernées, à notifier les violations, à réaliser les analyses d'impact et à mener la consultation préalable des autorités de contrôle (art. 28, paragraphe 3, points e et f).
6. Au choix du responsable du traitement, nous supprimons ou restituons toutes les données personnelles du client au terme de la prestation de services et détruisons les copies existantes, sauf si le droit de l'Union ou d'un État membre exige leur conservation.
7. Nous mettons à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de l'art. 28 et permettons la réalisation d'audits, y compris des inspections, et y contribuons (voir la section 9).

4. Obligations du responsable du traitement

- Le responsable du traitement garantit qu'il dispose d'une base juridique au sens de l'art. 6 (et, le cas échéant, de l'art. 9) pour les données personnelles qu'il place dans l'espace de travail.
- Le responsable du traitement est responsable de l'exactitude des données personnelles du client et de la réponse aux demandes des personnes concernées portant sur son espace de travail (nous lui transmettons les demandes que nous recevons et l'assistons conformément à l'art. 28, paragraphe 3, point e).
- Le responsable du traitement contrôle les accès (rôles des membres, invitations d'auditeurs, portail public de signalement) au moyen des réglages de la plateforme.

5. Transferts internationaux

Par défaut, les données personnelles du client sont stockées dans l'Union européenne. Lorsqu'un sous-traitant ultérieur a son siège hors de l'UE, les transferts sont régis par les clauses contractuelles types de la Commission européenne (décision 2021/914), module 3 (de sous-traitant à sous-traitant), avec les mesures complémentaires décrites à la section 7. Les sous-traitants ultérieurs actuels et leur localisation figurent sur </legal/subprocessors>.

6. Sous-traitants ultérieurs

1. Le responsable du traitement nous autorise à recourir à des sous-traitants ultérieurs pour fournir le service. La liste actuelle figure sur </legal/subprocessors>.
2. Nous informons le responsable du traitement de tout ajout ou remplacement envisagé au moins 30 jours à l'avance, via l'abonnement par e-mail proposé sur cette page ou par e-mail au propriétaire de l'espace de travail.
3. Le responsable du traitement peut s'y opposer pour des motifs raisonnables liés à la protection des données. Si nous ne pouvons pas donner suite à l'objection, il peut résilier le service concerné et obtenir le remboursement au prorata de la partie non utilisée de la période de facturation en cours.
4. Nous imposons par contrat écrit à chaque sous-traitant ultérieur des obligations de protection des données au moins aussi protectrices que celles du présent DPA, et nous restons responsables envers le responsable du traitement de l'exécution des obligations du sous-traitant ultérieur.

7. Mesures de sécurité (art. 32)

- Chiffrement. Les données personnelles du client sont chiffrées au repos en AES-256-GCM au niveau applicatif, en plus du chiffrement du fournisseur de stockage. Tout le transport passe par HTTPS avec HSTS en préchargement, sans repli en clair. Les clés sont dérivées par HKDF d'un secret principal conservé uniquement dans les variables d'environnement de l'infrastructure de production.
- Contrôle d'accès. Contrôle d'accès par rôle dans la plateforme (propriétaire, administrateur, membre, auditeur) ; sessions d'auditeur limitées dans le temps et révocables. L'accès opérationnel est réservé à une

petite équipe de support via le portail de support, qui ne montre que des métadonnées par conception.

- Authentification. Connexion sans mot de passe par code à usage unique. Jetons de session signés par HMAC à durée limitée. Limitation du débit sur chaque point d'accès public, y compris la connexion d'administration.
- Résilience et intégrité. Journal d'activité en ajout seul de chaque action modifiant un état. Sauvegardes dans l'UE. L'intégrité des données stockées est vérifiée par les étiquettes d'authentification AEAD ; un texte chiffré altéré produit une erreur et n'est pas servi.
- Réseau et en-têtes. Content-Security-Policy stricte avec une liste d'autorisation de scripts en ligne hachés, X-Frame-Options strict, X-Content-Type-Options nosniff et HSTS en préchargement.
- Gestion des vulnérabilités. Les dépendances sont figées à des versions précises ; nous suivons les avis de sécurité et appliquons les correctifs selon un calendrier adapté à leur gravité.

8. Violation de données à caractère personnel

Si nous avons connaissance d'une violation de données à caractère personnel touchant les données personnelles du client, nous en informons le propriétaire de l'espace de travail dans les meilleurs délais et au plus tard 72 heures après en avoir pris connaissance (art. 33, paragraphe 2). La notification décrit, dans la mesure où elles sont connues : la nature de la violation, ses conséquences probables, les mesures prises ou proposées et le point de contact pour obtenir plus d'informations. Nous assistons le responsable du traitement dans ses propres obligations de notification au titre des articles 33 et 34.

9. Audits

Le responsable du traitement (ou un auditeur tiers qu'il a mandaté) peut auditer notre respect du présent DPA une fois tous les douze mois, avec un préavis écrit d'au moins 30 jours et pendant les heures ouvrables, d'une manière qui ne perturbe pas indûment nos activités et qui respecte la confidentialité des données des autres clients. Nous pouvons facturer des frais raisonnables pour tout audit au-delà de cette limite. Lorsqu'une obligation d'audit au titre de l'art. 28, paragraphe 3, point h, peut être satisfaite par une attestation d'un tiers dont nous disposons, nous la fournissons à la place d'un audit sur place.

10. Responsabilité

La responsabilité de chaque partie au titre du présent DPA est soumise aux limites prévues par les conditions d'utilisation. Ces limites ne plafonnent en rien la responsabilité pour les dommages subis par les personnes concernées au titre de l'art. 82 du RGPD.

11. Durée et résiliation

Le présent DPA s'applique tant que nous traitons des données personnelles du client et survit à la résiliation des conditions d'utilisation dans la mesure et pour la durée où nous détenons encore de telles données. Les sections 8 (violations), 9 (audits) et 12 (restitution et suppression) survivent à la résiliation.

12. Restitution et suppression

À la fin du service, le responsable du traitement peut exporter les données de l'espace de travail avec les outils d'export de la plateforme pendant la période de grâce de 30 jours prévue par les conditions d'utilisation. Après cette période, nous supprimons les données personnelles du client ; les sauvegardes expirent selon notre calendrier de conservation. Les données que nous sommes tenus de conserver (par exemple la facturation au titre du droit commercial italien) ne sont conservées que pendant la durée de cette obligation.

13. Ordre de priorité

En cas de contradiction entre le présent DPA et les conditions d'utilisation ou la politique de confidentialité, le

présent DPA prévaut pour les questions de traitement des données. Les clauses contractuelles types intégrées pour un transfert hors de l'UE prévalent sur le présent DPA et sur les conditions d'utilisation pour les questions qu'elles régissent.

14. Notifications

- À Dazr : privacy@dazr.eu (protection des données) ou security@dazr.eu (incidents).
- Au responsable du traitement : l'adresse e-mail du propriétaire de l'espace de travail enregistrée au moment de la notification.