GUIDE D'EXPLOITATION

Microsoft Purview

À l'usage du responsable IT ou administrateur du client

Organisation	[Nom du client] — à compléter
Administrateur	[Prénom Nom] — à compléter
Email admin	[email admin] — à compléter
Consultant	[Prénom Nom, email] — à compléter
Date de déploiement	[Date] — à compléter
Prochaine révision annuelle	[Date + 1 an] — à compléter

Table des matières

Introduction :

Ce guide explique comment maintenir et prouver la conformité nLPD au quotidien. Il ne remplace pas le guide technique complet : il est conçu pour l’administrateur IT de votre organisation, sans formation Purview préalable.

Votre organisation a déployé 7 protections fondamentales :

Protection	Ce qu’elle apporte
MFA (tous les comptes)	Blocage des accès non autorisés même en cas de vol de mot de passe
Blocage partage externe SharePoint	Fermeture du vecteur de fuite via liens SharePoint
2 étiquettes de sensibilité	Classification et chiffrement AES-256 des données sensibles
Auto-labelling service	Détection et étiquetage automatique des fichiers SharePoint existants
DLP Exchange (surveillance)	Détection et traçabilité des envois de données sensibles par email
Rétention automatique 10 ans	Conservation RH + Finances conforme CO art. 958f, suppression automatique à échéance
Break-glass RMS	Accès de secours aux fichiers chiffrés en cas d’urgence ou de départ de l’administrateur

Ce guide vous explique ce que vous verrez au quotidien et comment réagir.

Partie 1 : Les 2 étiquettes, quoi et quand

Vos employés verront ces 2 étiquettes dans Word, Excel, PowerPoint et Outlook. Il est important qu’ils sachent quand appliquer laquelle.

Étiquette	Quand l’appliquer
1 - Interne	Documents internes courants : procédures, rapports internes, notes de réunion, présentations internes. Aucun chiffrement. Visible uniquement par les employés de l’organisation.
2 - Confidentiel	Tout ce qui contient des données personnelles sensibles : contrats de travail, fiches de salaire, données médicales, numéros AVS, IBAN, dossiers clients avec coordonnées. Chiffré : seules les personnes autorisées peuvent l’ouvrir.

INFO : Application automatique : Purview applique automatiquement l’étiquette 2 - Confidentiel quand il détecte un numéro AVS, un IBAN ou des termes médicaux dans un document. L’employé n’a rien à faire dans ce cas.

ATTENTION : Si un employé ne voit pas les étiquettes : dans Word, cliquez sur Fichier → Options → Centre de gestion de la confidentialité → vérifiez que le complément Sensibilité est actif. Si le problème persiste, contactez votre consultant.

INFO : Protection par chiffrement : un fichier étiqueté 2 - Confidentiel reste illisible quel que soit le canal utilisé pour le transmettre (email, clé USB, Gmail, perte d’un laptop). Tout destinataire doit s’authentifier pour l’ouvrir — soit via son compte Microsoft, soit via un code à usage unique envoyé par email. Voir Partie 6 pour le détail selon le type de destinataire.

Partie 2 : Alertes DLP dans Outlook, comment réagir

Quand un employé tente d'envoyer un email contenant des données sensibles à une adresse externe, Outlook affiche un message d'avertissement. Voici les 3 situations possibles et la marche à suivre.

Situation 1 : l'envoi est légitime

L'employé envoie un contrat à un client ou un document RH à la fiduciaire. Il clique sur Remplacer, saisit une justification courte (ex. : « Envoi du contrat demandé par M. Dupont le 12.04.2026 ») et envoie. La trace est automatiquement enregistrée dans Purview.

Situation 2 : l'employé s'est trompé de destinataire

Il clique sur Annuler, corrige le destinataire et renvoie. Aucune action supplémentaire n'est requise.

Situation 3 : un employé a envoyé alors qu'il ne fallait pas

L'administrateur reçoit une alerte email. Marche à suivre :

Étape	Action
1. Vérifier	Purview → Protection contre la perte de données → Alertes. Identifiez le fichier envoyé et le destinataire. Ou security.microsoft.com → Enquête et réponse → Incidents et alertes → Incidents.
2. Contacter le destinataire	Demandez-lui de supprimer le fichier reçu et de confirmer par écrit. Conservez cette confirmation.
3. Documenter l'incident	Notez la date, l'employé, le fichier, le destinataire, les données concernées et les actions prises. Conservez ce document dans votre dossier de conformité.
4. Évaluer le risque	Si les données concernent des personnes identifiables et que le risque pour elles est élevé : notifier le PFPDT. Si risque faible : document interne suffisant.

INFO : Spécificité IBAN : la règle Avertir-IBAN-Externe exige une justification écrite avant tout envoi d'IBAN vers l'extérieur. Cette justification est automatiquement enregistrée dans l'Activity Explorer Purview. C'est votre preuve de contrôle au sens de l'art. 8 nLPD.

Partie 3 : Routine mensuelle de l’administrateur (15 minutes)

Ces vérifications mensuelles constituent vos mesures organisationnelles au sens de l’art. 8 nLPD. Planifiez un rappel récurrent dans votre agenda.

Vérification 1 : Incidents DLP (5 minutes)

security.microsoft.com → Enquête et réponse → Incidents et alertes → Incidents. Filtrez sur le dernier mois. Pour chaque incident DLP : vérifiez que l’envoi était légitime (justification présente et cohérente). Si un incident vous semble anormal, suivez la procédure de la Partie 2.

Vérification 2 : Partage SharePoint (5 minutes)

admin.sharepoint.com → Sites actifs. Vérifiez que la colonne Partage externe affiche Désactivé pour tous les sites sans exception. Si un site est passé à Activé sans raison :

Étape	Action
1. Identifier	Notez le nom du site et l’administrateur qui a modifié le paramètre.
2. Corriger	Cliquez sur le site → onglet Paramètres → Partage de fichiers externes → Uniquement les personnes de votre organisation → Enregistrer.
3. Documenter	Notez la correction dans votre journal mensuel.

⚠ **ATTENTION :** Le blocage du partage externe SharePoint est un paramètre tenant global. Il peut être modifié par tout Global Admin ou administrateur SharePoint. Sa vérification mensuelle est obligatoire pour maintenir la conformité nLPD.

ⓘ **INFO :** Exception selon votre secteur : si votre consultant a configuré un partage contrôlé pour certains sites de projet (cabinets d’architectes, ingénieurs), ces sites afficheront Activé. C’est normal et intentionnel. Vérifiez uniquement que les sites RH et Finances affichent Désactivé. En cas de doute sur ce qui est normal pour votre configuration : contactez votre consultant avant de modifier quoi que ce soit.

Vérification 3 : Nouveaux utilisateurs (5 minutes)

admin.microsoft.com → Utilisateurs actifs. Vérifiez que tout nouveau compte créé dans le mois a bien le MFA activé et la licence Purview Suite assignée. Un compte sans MFA est une vulnérabilité immédiate.

☑ **CONSEIL :** Archivage : après chaque vérification, notez la date et « RAS » (rien à signaler) ou décrivez les actions prises. Ce journal constitue votre preuve de surveillance active pour le PFPDT.

Vérification 4 : Politiques de rétention (5 minutes)

Purview → Gestion du cycle de vie des données → Stratégies de rétention. Vérifiez que les deux politiques suivantes sont présentes et actives :

Politique	Statut attendu
Retention-RH-10ans	Active — emplacement : https://[tenant].sharepoint.com/sites/RH
Retention-Finances-10ans	Active — emplacement : https://[tenant].sharepoint.com/sites/Finances

⚠ **ATTENTION :** Si une politique affiche Erreur ou est absente : contactez votre consultant immédiatement. Une politique de rétention désactivée signifie que les documents RH et Finances ne sont plus soumis à la conservation légale obligatoire (CO art. 958f). C’est un risque juridique immédiat.

Partie 4 : En cas d'incident de données

IMPORTANT : Définition d'un incident (art. 24 nLPD) : une violation de la sécurité des données est tout accès non autorisé, toute divulgation, perte ou destruction de données personnelles. Exemples : laptop volé avec des données non chiffrées, email envoyé au mauvais destinataire, accès d'un ancien employé non supprimé.

Étape	Action immédiate
1. Contenir	Bloquez immédiatement l'accès concerné (supprimez les droits, changez le mot de passe, révoquez le partage). Ne tardez pas.
2. Révoquer l'accès RMS si le fichier est chiffré	Si le fichier étiqueté 2 - Confidentiel a été envoyé à un mauvais destinataire : vous pouvez révoquer immédiatement son accès, même s'il a déjà reçu le fichier. Voir section 4.1 ci-dessous.
3. Évaluer	Quelles données ? Combien de personnes concernées ? Les données étaient-elles chiffrées (si oui, risque très faible) ?
4. Documenter	Rédigez un compte-rendu d'incident : date et heure, données affectées, personnes concernées, cause probable, actions prises, mesures correctives.
5. Notifier le PFPDT	Si le risque pour les personnes concernées est élevé : notifiez le PFPDT dans les meilleurs délais (art. 24 nLPD). Formulaire sur www.edoeb.admin.ch.
6. Informer les personnes	Si le risque pour elles est élevé : informez-les de l'incident, des données touchées et des mesures prises.

4.1 : Révoquer l'accès à un fichier chiffré (RMS)

Si un fichier étiqueté 2 - Confidentiel a été envoyé par erreur à un mauvais destinataire, vous pouvez interdire immédiatement toute tentative de déchiffrement de ce document, même s'il est déjà dans la boîte mail du destinataire. Le fichier devient définitivement inaccessible pour lui, sans avoir à le récupérer physiquement.

INFO : Comment ça fonctionne : chaque fois que quelqu'un tente d'ouvrir un fichier chiffré RMS, son application contacte les serveurs Microsoft pour obtenir une autorisation de déchiffrement. La révocation dit à ces serveurs : « refusez toutes les demandes pour ce document précis, peu importe qui les fait. »

Étape 1 : récupérer l'identifiant du document (ContentId)

Purview → Content Explorer → recherchez le document par nom → cliquez dessus → notez la valeur ContentId affichée dans les détails. Alternative via PowerShell :

```
Connect-AipService
Get-AipServiceDocumentLog -ContentName "nom-du-fichier.docx"
```

Étape 2 : révoquer l'accès

```
Revoke-AipServiceDocumentAccess -ContentId "[GUID du document]" -Force
```

ATTENTION : La révocation est immédiate et définitive. Elle s'applique à tous les destinataires, y compris les membres internes autorisés. Si vous devez rétablir l'accès pour les membres internes, vous devrez renvoyer une nouvelle version du document avec l'étiquette réappliquée.

4.2 : Utiliser le compte Break-glass en cas de gros problème

Le compte Break-glass est un compte de secours configuré lors du déploiement (section 2.5 du guide de déploiement). Il dispose du rôle Super User RMS : il peut ouvrir et déchiffrer n'importe quel fichier du tenant, même si l'administrateur habituel a quitté l'organisation ou perdu son accès.

Situation	Quand utiliser le compte Break-glass
Administrateur quitte l'organisation	Son départ révoque ses droits. Les fichiers chiffrés avec son compte restent accessibles via le Break-glass.
Fichiers inaccessibles après réorganisation	Restructuration des groupes ou suppression accidentelle d'un groupe autorisé → le Break-glass permet de récupérer les fichiers.
Audit judiciaire ou PFPDT	Accès urgent à des fichiers chiffrés dans le cadre d'une demande légale.
Test annuel	Une fois par an, testez que le compte Break-glass fonctionne toujours avant d'en avoir besoin.

Procédure d'activation et d'utilisation

IMPORTANT : Le compte Break-glass dispose de droits absolus sur tous les fichiers chiffrés du tenant. Chaque utilisation doit être documentée dans le registre des incidents. N'utilisez ce compte que si aucune autre solution n'est disponible.

Étape	Action
1. Récupérer les identifiants	Ouvrez le coffre-fort physique où sont stockés les identifiants du compte Break-glass. Ne stockez jamais ces identifiants dans un gestionnaire de mots de passe numérique.
2. Ouvrir PowerShell en administrateur	Démarrer → Windows PowerShell → clic droit → Exécuter en tant qu'administrateur.
3. Se connecter et réactiver le Super User	Install-Module -Name AIPService -Force Connect-AipService -Credential (Get-Credential) Enable-AipServiceSuperUserFeature Add-AipServiceSuperUser -EmailAddress [email du compte Break-glass]
4. Accéder aux fichiers	Connectez-vous à Microsoft 365 avec le compte Break-glass. Ouvrez les fichiers chiffrés normalement depuis Word ou SharePoint. Le chiffrement est levé automatiquement pour ce compte.
5. Désactiver après utilisation	Disable-AipServiceSuperUserFeature Disconnect-AipService
6. Documenter	Notez dans votre registre : date, heure, raison, fichiers accédés, durée d'activation. Cette entrée est obligatoire — chaque activation est tracée dans l'audit Purview.

CONSEIL : Test annuel recommandé : une fois par an lors de la révision annuelle (Partie 7), activez le Super User, ouvrez un fichier test chiffré, puis désactivez immédiatement. Cela confirme que le compte fonctionne et que les identifiants sont toujours valides. Documentez le test dans votre journal.

Contacts en cas d’urgence

Contact	Coordonnées
Votre consultant Purview	[Prénom Nom] — [email] — [téléphone]
PFPDT (signalement)	www.edoeb.admin.ch — +41 58 462 43 95
Support Microsoft	admin.microsoft.com → Support → Nouvelle demande de support

Partie 5 : Produire les preuves pour le PFPDT

Si le PFPDT vous contacte, vous devrez produire des preuves que vos données sont protégées. Voici ce qu’il faut avoir, où le trouver et comment l’archiver.

Preuve	Comment la produire
Registre des activités de traitement	Le document Annexe I remis par votre consultant. À mettre à jour si une nouvelle activité de traitement démarre. Conserver la version signée.
Preuves de chiffrement	Purview → Protection des données → Étiquettes de confidentialité → capture d’écran montrant les 2 étiquettes actives et leur configuration.
Journal d’audit	Purview → Audit → Rechercher → plage de dates demandée → exporter en CSV. Montre que les accès sont tracés.
Contrôle des partages	admin.sharepoint.com → Stratégies → Partage → capture d’écran du curseur sur Uniquement les personnes de votre organisation.
Preuves de rétention	Purview → Gestion du cycle de vie des données → Stratégies de rétention → capture d’écran de Retention-RH-10ans et Retention-Finances-10ans actives. Démontre la conformité à CO art. 958f.
Journal des incidents	Votre journal mensuel (Partie 3) + les comptes-rendus d’incidents (Partie 4). Un simple fichier Word ou une feuille Excel suffisent.
Preuve de surveillance active	Les emails d’alerte DLP reçus + les actions prises. Conservez-les dans un dossier dédié.

☑ **CONSEIL :** Archivage recommandé : créez un dossier partagé interne « Conformité nLPD ». Mettez-y : ce guide, le registre des activités, les captures d’écran annuelles, et le journal mensuel. En cas de contrôle PFPDT, vous avez tout en un endroit.

Partie 6 : Envoyer des documents à des clients ou partenaires externes

Avec le MVC déployé, le partage externe via liens SharePoint est bloqué au niveau du tenant. L'unique canal de transmission externe est l'email avec pièce jointe. Ce choix est volontaire : il concentre tous les envois externes dans un canal surveillé par la DLP Exchange.

Canal unique : email avec pièce jointe

Pour transmettre un document à un client ou à un partenaire externe, appliquez l'étiquette 2 - Confidentiel avant d'envoyer. Outlook avertit si le document contient des données sensibles détectées (AVS, IBAN, médical).

Point	Détail
Protection	Le fichier est chiffré par Azure RMS. Il reste illisible même si l'email est intercepté, transmis via une clé USB ou reçu sur un appareil non autorisé.
Destinataire avec compte Microsoft	Compte professionnel M365 ou Outlook.com : le destinataire ouvre le fichier normalement dans Word ou la visionneuse web. Azure RMS vérifie son identité en ligne et déchiffre automatiquement. Aucune action supplémentaire requise.
Destinataire sans compte Microsoft	Gmail, adresse personnelle, AFC, caisse AVS : Word affiche un message d'authentification. Le destinataire reçoit un code à usage unique par email (expéditeur : microsoft.com), valable 15 minutes. Il le saisit dans le navigateur pour accéder au contenu. Si le code expire : cliquer à nouveau sur Envoyer le code.
Traitement IBAN	L'avertissement DLP s'affiche et exige une justification écrite avant l'envoi. La justification est enregistrée automatiquement dans Purview.
Impression par le destinataire	Possible avec le niveau Co-auteur (configuration actuelle). Pour bloquer l'impression : contactez votre consultant.

⚠ **ATTENTION :** Cette description couvre les cas les plus fréquents mais n'est pas exhaustive. Le comportement peut varier selon la version des clients Office installés chez le destinataire, son système d'exploitation (iOS, Android, Mac) ou l'application utilisée pour ouvrir le fichier. En cas de difficulté d'ouverture signalée par un destinataire externe : demandez-lui d'essayer via un navigateur web sur office.com.

ⓘ **INFO :** Traçabilité des accès externes : l'ouverture du fichier par un destinataire externe via code OTP n'apparaît pas dans vos journaux Purview. L'authentification se passe côté infrastructure Microsoft et n'est pas visible dans votre audit tenant. Seule la transmission est tracée dans Purview : expéditeur, destinataire, fichier, horodatage, règle DLP déclenchée.

☑ **CONSEIL :** Défendabilité PFPDT : si le PFPDT vous demande « qui a ouvert ce fichier et quand », vous ne pouvez pas répondre pour les destinataires externes. Mais cette question ne se pose qu'en cas d'incident. Dans ce cas, votre réponse est : « le fichier était chiffré, seul un utilisateur authentifié pouvait l'ouvrir, voici la trace de l'envoi. » C'est défendable au sens de l'art. 8 nLPD.

Règle de décision simple

Type de document	Action
Fiche de salaire, données AVS, médical, IBAN	Email avec étiquette 2 - Confidentiel + justification DLP si demandée
Bilan, déclaration fiscale, rapport de gestion	Email avec étiquette 2 - Confidentiel
Contrat individuel avec données personnelles	Email avec étiquette 2 - Confidentiel
Contrat-cadre ou conditions générales	Email avec étiquette 1 - Interne ou 2 - Confidentiel selon le contenu
Document de travail générique sans données personnelles	Email standard, étiquette 1 - Interne

INFO : Défendabilité PFPDT : concentrer tous les envois externes dans l’email surveillé par la DLP garantit une traçabilité complète. Chaque envoi de données sensibles génère une trace horodatée (expéditeur, destinataire, fichier, justification). C’est la preuve documentaire exigée par le PFPDT en cas de contrôle (art. 24 nLPD).

Partie 7 : Révision annuelle

Une fois par an, effectuez cette révision complète. Planifiez-la à la même période chaque année (exemple : chaque janvier).

Point de révision	Action
Registre des activités	Vérifiez si de nouvelles activités de traitement ont démarré dans l'année (nouveaux logiciels, nouveaux fournisseurs, nouveaux types de données). Mettez à jour le registre.
Comptes utilisateurs	Vérifiez que tous les comptes d'anciens employés ont été supprimés ou désactivés. Aucun compte ne devrait rester actif plus de 30 jours après un départ.
DLP : passage en mode actif	Si la DLP est encore en mode simulation : consultez l'Activity Explorer pour évaluer les faux positifs. Si le taux est acceptable, passez en mode actif (contactez votre consultant).
MFA : nouveaux comptes	Vérifiez que tous les comptes créés dans l'année ont bien le MFA actif et la licence Purview Suite.
Partage SharePoint	Vérifiez que le curseur tenant SharePoint est toujours sur Uniquement les personnes de votre organisation. Capture d'écran à archiver.
Rétention : vérification des politiques	Purview → Gestion du cycle de vie des données → Stratégies de rétention. Confirmez que Retention-RH-10ans et Retention-Finances-10ans sont actives. Capture d'écran à archiver dans votre dossier Conformité nLPD.
Auto-labelling service : vérification	Purview → Protection des données → Stratégies d'étiquetage automatique. Confirmez que Auto-Label-Confidentiel est actif (pas en simulation). Si encore en simulation, contactez votre consultant pour l'activer.
Break-glass RMS : test annuel	Activez le Super User RMS avec le compte Break-glass, ouvrez un fichier test chiffré, désactivez immédiatement. Documentez le test. Confirme que les identifiants sont valides avant d'en avoir besoin en urgence.
Archivage de preuves	Capturez les politiques Purview actives (DLP, étiquettes, rétention, auto-labelling). Exportez le journal d'audit de l'année écoulée. Archivez dans votre dossier Conformité nLPD.

Partie 8 : Spécificités selon le secteur d'activité

Selon le secteur d'activité de votre organisation, votre consultant a adapté la configuration MVC standard. Cette partie décrit ce qui change dans votre utilisation quotidienne et votre routine mensuelle. Lisez uniquement la section correspondant à votre secteur.

> **INFO :** Si votre secteur n'est pas listé ici, votre configuration est le MVC standard (Parties 1 à 7 suffisent).

8.1 : Fiduciaire et comptabilité

Votre configuration inclut une 3ème étiquette spécifique : 3 - Externe-Fiduciaire. Elle permet d'envoyer des documents aux institutions (AFC, caisses AVS, banques) sans le système d'authentification OTP qui les bloquerait.

Quelle étiquette utiliser ?

Type de document	Étiquette à appliquer
Documents internes, notes, procédures	1 - Interne
Dossiers RH, contrats de travail, données AVS, médicales	2 - Confidentiel (chiffré)
Bilans, déclarations fiscales, décomptes TVA envoyés à l'AFC	3 - Externe-Fiduciaire (non chiffré)
Documents bancaires envoyés à une banque	3 - Externe-Fiduciaire (non chiffré)
Décomptes envoyés à une caisse AVS ou assureur	3 - Externe-Fiduciaire (non chiffré)
Documents envoyés à un client particulier ou entreprise	2 - Confidentiel ou 3 - Externe-Fiduciaire selon accord client

> **INFO :** Pourquoi deux étiquettes pour l'externe ? L'étiquette 2 - Confidentiel chiffre le fichier et oblige le destinataire à s'authentifier (OTP). L'AFC, les banques et les caisses AVS ne supportent pas ce système. L'étiquette 3 - Externe-Fiduciaire envoie le document sans chiffrement mais avec un marquage visuel et une traçabilité DLP obligatoire. La conformité nLPD est assurée par la justification enregistrée dans Purview.

Routine mensuelle adaptée

Vérification 1 (incidents DLP) : les envois avec l'étiquette 3 - Externe-Fiduciaire déclenchent aussi des incidents DLP. La justification saisie par l'employé doit être cohérente (ex. : « Bilan 2025 envoyé à l'AFC conformément à la demande du 12.01.2026 »).

Vérification politiques de rétention : dans votre configuration, la rétention 10 ans s'applique uniquement aux documents portant les étiquettes 2 - Confidentiel ou 3 - Externe-Fiduciaire. Les brouillons et mémos non étiquetés ne sont pas conservés 10 ans. C'est intentionnel et conforme à l'art. 6 nLPD (minimisation).

⚠ **ATTENTION :** Numéros IDE/UID : si votre consultant a configuré le SIT IDE-UID-Suisse, les documents contenant des numéros CHE-XXX.XXX.XXX déclencheront aussi des alertes DLP. C’est normal et voulu pour tracer les transmissions de données d’entreprises clientes.

8.2 : Cabinet d’architectes et ingénieurs civils

Votre configuration n’inclut pas le blocage global du partage externe SharePoint. À la place, les partages sont autorisés avec des personnes spécifiques et expirent automatiquement après 30 jours. Les sites RH et Finances restent bloqués individuellement.

Partager un dossier de projet avec un sous-traitant

Étape	Action
1. Ouvrir le dossier	Dans SharePoint, naviguez jusqu’au dossier de projet à partager.
2. Partager	Cliquez sur Partager → sélectionnez Personnes spécifiques → saisissez l’adresse email du sous-traitant → permission : Consultation → Envoyer.
3. Durée	L’accès expirera automatiquement après 30 jours. Aucune action nécessaire à l’échéance.
4. Renouveler	Si le projet se poursuit au-delà de 30 jours : répétez l’étape 2. Le sous-traitant reçoit un nouveau lien.

⚠ **ATTENTION :** Ne partagez jamais les sites RH et Finances avec des sous-traitants. Ces sites sont bloqués individuellement. Si SharePoint refuse le partage sur ces sites, c’est le comportement attendu.

Routine mensuelle adaptée

Vérification 2 (partage SharePoint) : dans votre configuration, les sites de projet affichent Activé dans la colonne Partage externe. C’est normal. Vérifiez uniquement que les sites RH et Finances affichent Désactivé. Si un site RH ou Finances affiche Activé, corrigez immédiatement.

ⓘ **INFO :** Traçabilité des partages : chaque partage externe vers un sous-traitant est enregistré dans l’audit SharePoint. Purview → Audit → Rechercher → Activités : Fichier partagé avec un utilisateur externe. C’est votre preuve de contrôle des accès au sens de l’art. 8 nLPD.

8.3 : Étude d'avocats et notaires

Votre configuration inclut une 3ème étiquette spécifique : 3 - Juridique-Externe. Elle permet d'envoyer des pièces de procédure aux tribunaux, aux parties adverses et aux greffes, sans le système d'authentification OTP qui serait incompatible avec les délais judiciaires.

Quelle étiquette utiliser ?

Type de document	Étiquette à appliquer
Documents internes, notes, dossiers en cours	1 - Interne
Dossiers clients avec données personnelles sensibles	2 - Confidentiel (chiffré)
Pièces de procédure envoyées à un tribunal	3 - Juridique-Externe (non chiffré)
Correspondance vers une partie adverse	3 - Juridique-Externe (non chiffré)
Actes notariés envoyés à un greffe	3 - Juridique-Externe (non chiffré)
Correspondance inter-cabinets	3 - Juridique-Externe (non chiffré)

INFO : Justitia.swiss : pour les dépôts officiels via le portail Justitia.swiss, déposez directement via le portail. Réservez l'étiquette 3 - Juridique-Externe aux transmissions par email vers les tribunaux, parties adverses et greffes.

CONSEIL : La protection nLPD est assurée : même sans chiffrement RMS, la DLP enregistre chaque transmission (expéditeur, destinataire, document, justification). Le marquage visuel du document engage la responsabilité du destinataire. En cas de divulgation non autorisée par la partie adverse, la responsabilité est sur elle, pas sur votre étude.

Routine mensuelle adaptée

Vérification 1 (incidents DLP) : les envois avec l'étiquette 3 - Juridique-Externe génèrent des incidents DLP avec justification obligatoire. Vérifiez que la justification est présente et cohérente avec le dossier (ex. : « Conclusions envoyées au Tribunal civil, dossier n° 2026/1234 »).

8.4 : Agence de communication et marketing

Votre configuration a été adaptée pour éviter les fausses alertes DLP sur vos flux créatifs. Les comptes des créatifs et chargés de projet sont exclus de la surveillance DLP Exchange. Les sites SharePoint créatifs sont exclus de l’auto-labelling automatique.

Ce qui est surveillé et ce qui ne l’est pas

Compte / Site	Surveillance DLP
Comptes RH, Finances, Direction	☑ Surveillés — alertes DLP actives
Comptes créatifs et chargés de projet	✗ Non surveillés — exclusion intentionnelle
Sites SharePoint RH et Finances	☑ Auto-labelling actif
Sites SharePoint créatifs (Projets, BAT, Assets)	✗ Auto-labelling désactivé — intentionnel

IMPORTANT : Compensation obligatoire : les comptes créatifs ne sont pas surveillés par la DLP. En contrepartie, tous les employés concernés doivent avoir signé la charte informatique interdisant explicitement l’envoi de données personnelles depuis les comptes créatifs. Conservez ces signatures signées dans votre dossier Conformité nLPD. C’est votre mesure organisationnelle compensatoire au sens de l’art. 8 nLPD.

Routine mensuelle adaptée

Vérification 1 (incidents DLP) : vous verrez peu ou pas d’incidents DLP depuis les comptes créatifs. C’est normal. Concentrez votre attention sur les incidents provenant des comptes RH, Finances et Direction.

Vérification supplémentaire : vérifiez une fois par trimestre que les chartes informatiques des comptes créatifs sont à jour (nouveaux employés, prestataires). Un compte créatif sans charte signée est un risque non couvert.

INFO : Factures et devis avec IBAN : les envois de factures ou devis contenant un IBAN depuis les comptes créatifs ne déclenchent pas d’alerte DLP. Si vous souhaitez surveiller ces envois également, contactez votre consultant pour réintégrer certains comptes dans le périmètre DLP.

8.5 : Cabinet médical et paramédical

Votre configuration inclut une 3ème étiquette spécifique : 3 - Patient-Externe. Elle permet d'envoyer des documents aux patients sans le système OTP Microsoft que la plupart ne sauraient pas utiliser.

Quelle étiquette utiliser ?

Type de document	Étiquette à appliquer
Documents internes, procédures, notes de réunion	1 - Interne
Dossiers patients internes, historiques médicaux	2 - Confidentiel (chiffré)
Résultats d'analyses envoyés au patient	3 - Patient-Externe (non chiffré)
Ordonnances envoyées au patient	3 - Patient-Externe (non chiffré)
Rappels de consultation, factures patients	3 - Patient-Externe (non chiffré)
Échanges interprofessionnels via HIN	Hors Purview — utilisez HIN Mail directement

INFO : Réseau HIN (Health Info Net) : les échanges entre professionnels de santé (médecin → spécialiste → hôpital) passent par HIN Mail qui dispose de sa propre infrastructure chiffrée. Purview ne gère pas ces flux. Continuez à utiliser HIN Mail pour ces échanges comme avant.

CONSEIL : Base légale : les données médicales envoyées au patient concerné sont couvertes par son droit d'accès (art. 25 nLPD). La DLP trace chaque envoi (expéditeur, destinataire, horodatage). C'est votre preuve de contrôle suffisante même sans chiffrement RMS.

Routine mensuelle adaptée

Vérification 1 (incidents DLP) : les envois avec l'étiquette 3 - Patient-Externe génèrent des incidents DLP avec justification obligatoire. Vérifiez que la justification est cohérente avec l'envoi. Un volume important de justifications « résultats demande patient » est normal pour un cabinet actif.

ATTENTION : Si un patient signale ne pas avoir reçu ses résultats : vérifiez dans Purview → Audit que l'email a bien été envoyé. Si l'envoi est tracé, le problème est côté destinataire (filtre anti-spam, boîte pleine). Renvoyez depuis Outlook et demandez une confirmation de réception.