GUIDE DE DÉPLOIEMENT

Microsoft Purview

Minimum Viable de Conformité (MVC) — PME suisse 5 à 25 personnes

Licence	Microsoft 365 Business Premium + Purview Suite
Tenant	[tenant].onmicrosoft.com — à remplacer
Client	[Nom du client] — à remplacer
Durée	4 à 6 heures (déploiement + tests)
Version	1.0 — Avril 2026

Table des matières

Préface 4
Partie 0 : Prérequis 5
0.1 Accéder au portail Purview 5
0.2 PowerShell en administrateur 5
0.3 Attribuer les rôles 5
Entra ID (entra.microsoft.com → Rôles et administrateurs) 5
Exchange Online (admin.exchange.microsoft.com → Rôles → Organization Management) 5
Purview RBAC (Paramètres → Rôles et étendues → Groupes de rôles) 5
0.4 Vérifier la licence Purview Suite 6
0.5 Activer EnableMIPLabels (une seule fois par tenant) 6
0.6 Activer le MFA sur tous les comptes 6
0.7 Bloquer le partage externe au niveau du tenant SharePoint 6
Partie 1 : Activer l'audit 7
Partie 2 : Créer les 2 étiquettes de sensibilité 8
2.1 Créer les SITs personnalisés 8
SIT 1 : AVS-Suisse-PME 8
SIT 2 : Medical-RH-Suisse 9
2.2 Créer les 2 étiquettes 9
Étiquette 1 : 1 - Interne (sans chiffrement, par défaut) 9
Étiquette 2 : 2 - Confidentiel (avec chiffrement AES-256) 10
2.3 Publier les étiquettes 11
2.4 Auto-labelling côté service (fichiers SharePoint existants) 12
2.5 Break-glass RMS (accès de secours aux fichiers chiffrés) 13
Partie 3 : DLP Exchange 14
3.1 Créer la politique DLP-PME-Surveillance 14
3.2 Règle 1 : Avertir-Donnees-Sensibles 14
3.3 Règle 2 : Avertir-IBAN-Externe 15
Partie 4 : Rétention automatique des données 16
4.1 Retention-RH-10ans 16
4.2 Retention-Finances-10ans 16
Partie 5 : Vérification et remise 17
Test 1 : Audit actif 17
Test 2 : Étiquettes visibles dans Word 17
Test 3 : Détection automatique (auto-labelling client) 17
Test 4 : Avertissement DLP 17
Test 5 : Audit 17
Test 6 : Blocage partage SharePoint 17
Checklist de remise client 18
Annexe A : Glossaire simplifié 19
Annexe B : Checklist MVC complète 20

Annexe C : Mots-clés pour les SIT personnalisés 21
C.1 : AVS-Suisse-PME (4 langues nationales + anglais) 21
C.2 : Medical-RH-Suisse (4 langues nationales + anglais) 21
Annexe E : Différences POC vs Production 22
Annexe I : Registre des activités de traitement (art. 12 nLPD) 23
Informations générales de l'organisation 23
Activité 1 : Gestion des ressources humaines et de la paie 23
Activité 2 : Comptabilité et gestion financière 24
Activité 3 : Gestion de la relation client 24
Annexe F : Adaptations sectorielles 25
F.1 : PME générique (MVC tel quel) 25
F.2 : Fiduciaire et comptabilité 25
Adaptation 1 : ajouter une étiquette 3 - Externe-Fiduciaire 26
Adaptation 2 : affiner la rétention 26
Option : ajouter un SIT IDE/UID 26
F.3 — Cabinet d'architectes et ingénieurs civils 27
Adaptation : remplacer le blocage SharePoint par le partage contrôlé avec expiration 27
F.4 : Étude d'avocats et notaires 28
Adaptation : étiquette 3 - Juridique-Externe (sans chiffrement RMS) 28
F.5 : Agence de communication et marketing 29
Adaptation 1 : exclure les sites créatifs de l'auto-labelling service 29
Adaptation 2 : exclure les comptes créatifs de la DLP Exchange 29
F.6 : Cabinet médical et paramédical 30
Adaptation : étiquette 3 - Patient-Externe (sans chiffrement RMS) 30
F.7 : Synthèse des adaptations 31
Annexe J : Soutien au travail de documentation 32

Préface

⚠ **ATTENTION :** Personnalisation obligatoire : remplacez [domaine], [tenant] et [tenant].sharepoint.com par les informations réelles du client. L'Annexe I est préremplie pour Axonix SA (POC demo.ch) ; adaptez-la au client.

Ce guide est conçu pour un consultant qui installe une protection Minimum Viable de Conformité (MVC) dans une PME suisse de 5 à 25 personnes. Objectif : une session de 4 à 6 heures, client autonome à la fin.

Qu'est-ce que le MVC ? Le Minimum Viable de Conformité est l'ensemble minimal de mesures techniques défendables devant le Préposé fédéral à la protection des données (PFPDT). Il ne vise pas la perfection technique mais la capacité de démontrer une démarche proportionnée et documentée. Pour une PME de 5 à 25 personnes sans IT dédié, c'est le point de départ réaliste et maintenable.

Piliers MVC couverts :

Pilier	Ce que ça apporte
MFA (tous les comptes)	Première barrière contre la compromission de compte
Blocage partage externe SharePoint	Fermeture du vecteur de fuite via liens SharePoint
Audit (traçabilité PFPDT)	Journal de toutes les actions sur les données, 1 an
2 étiquettes (Interne + Confidentiel)	Classification + 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
Rétention automatique	Conservation 10 ans des données RH et Finances (CO art. 958f)
Break-glass RMS	Accès de secours aux fichiers chiffrés en cas d'urgence

ⓘ **INFO :** Hors périmètre MVC : IRM, Endpoint DLP, Managed Environments, eDiscovery, Communication Compliance, DSPM for AI. Ces fonctionnalités sont documentées dans le Guide complet Microsoft Purview 2026 et peuvent être déployées progressivement après le socle MVC.

Partie 0 : Prérequis

0.1 Accéder au portail Purview

N°	Étape	Action
1	Navigateur	Microsoft Edge ou Google Chrome. Évitez Firefox.
2	URL	https://purview.microsoft.com (ou https://compliance.microsoft.com, redirige automatiquement).
3	Connexion	Compte admin M365 (Global Admin ou Compliance Admin).
⚠	Accès refusé	« Vous n'avez pas accès » → problème de rôles, allez à la section 0.3.

0.2 PowerShell en administrateur

N°	Étape	Action
1	Ouvrir	Démarrer → Windows PowerShell → clic droit → Exécuter en tant qu'administrateur. Le titre affiche « Administrateur ».
2	Autoriser les scripts	Set-ExecutionPolicy RemoteSigned -Scope CurrentUser → O → Entrée.

0.3 Attribuer les rôles

Entra ID (entra.microsoft.com → Rôles et administrateurs)

Rôle Entra ID	Pourquoi
Administrateur de la sécurité	Signaux de risque dans Purview
Administrateur de mise en conformité	Politiques Purview

→ Rôles et administrateurs → cherchez le rôle → + Ajouter des attributions → votre compte.

Exchange Online (admin.exchange.microsoft.com → Rôles → Organization Management)

+ Ajouter des membres → votre compte. Attendez 5 à 10 minutes avant de continuer.

IMPORTANT : Sans Organization Management, la commande PowerShell d'audit s'exécute sans erreur mais ne fait rien.

Purview RBAC (Paramètres → Rôles et étendues → Groupes de rôles)

Groupe Purview	Accès
Compliance Administrator	Labels, DLP, rétention, politiques
Content Explorer Content Viewer	Voir le contenu des fichiers
Content Explorer List Viewer	Voir la liste des fichiers

0.4 Vérifier la licence Purview Suite

admin.microsoft.com → Utilisateurs actifs → votre compte → Licences et applications → vérifiez que Microsoft Purview Suite est coché. Si absent : cochez et Enregistrer les modifications.

0.5 Activer EnableMIPLabels (une seule fois par tenant)

Requis pour que les étiquettes de type Groupes et sites fonctionnent (notamment si le client évolue vers le guide complet).

```
Install-Module Microsoft.Graph -Scope CurrentUser
Connect-MgGraph -Scopes "Directory.ReadWrite.All"
$t = Get-MgBetaDirectorySettingTemplate -All | Where-Object { $_.DisplayName -eq "Group.Unified" }
New-MgBetaDirectorySetting -BodyParameter @{ templateId = $t.Id; values = @(@{ name = "EnableMIPLabels"; value = "True" }) }
```

→ *Déconnectez-vous et reconnectez-vous au portail Purview avant de continuer.*

0.6 Activer le MFA sur tous les comptes

IMPORTANT : Priorité absolue : sans MFA, Purview est un château de cartes. Un mot de passe volé donne accès à toutes les données sensibles.

N°	Étape	Action
1	Accès	admin.microsoft.com → Utilisateurs actifs → Authentification multifacteurs (bouton en haut de la liste).
2	Activer	Sélectionnez tous les utilisateurs → Activer → Confirmer.
3	Alternative recommandée	entra.microsoft.com → Protection → Accès conditionnel → stratégie MFA pour Tous les utilisateurs (permet des exclusions ciblées).

0.7 Bloquer le partage externe au niveau du tenant SharePoint

Cette étape ferme le principal vecteur de fuite non surveillé : les liens SharePoint vers l'extérieur. Elle n'affecte pas les envois par email.

⚠ ATTENTION : Vérifiez au préalable qu'aucun site SharePoint actif ne dépend du partage externe. admin.sharepoint.com → Sites actifs → colonne Partage externe : identifiez les sites Activé et validez avec le client avant de bloquer.

N°	Étape	Action
1	Accès	https://admin.sharepoint.com → Stratégies → Partage.
2	Partage externe	Curseur SharePoint → Uniquement les personnes de votre organisation. Faites de même pour OneDrive.
3	Enregistrer	Cliquez sur Enregistrer.

INFO : Ce paramètre est un plafond global : aucun site ne peut être partagé en externe même si un administrateur essaie de l'activer site par site. Les envois de pièces jointes par email ne sont pas affectés et restent surveillés par la DLP Exchange (Partie 3).

Partie 1 : Activer l'audit

IMPORTANT : À faire AVANT les étiquettes : sans audit actif, vous n'avez aucune trace en cas d'incident nLPD et ne pouvez pas vérifier que vos politiques fonctionnent.

```
Install-Module -Name ExchangeOnlineManagement -Force
Connect-ExchangeOnline
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $true
Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled
```

→ *Résultat attendu : UnifiedAuditLogIngestionEnabled : True*

```
Disconnect-ExchangeOnline -Confirm:$false
```

CONSEIL : Vérification dans Purview : Purview → Audit (menu gauche) → Rechercher → bandeau vert = audit actif. Si bouton Démarrer l'enregistrement visible → cliquez dessus.

Partie 2 : Créer les 2 étiquettes de sensibilité

Ordre	Rôle
1 — 1 - Interne	Sans chiffrement. Étiquette par défaut pour tous les documents internes.
2 — 2 - Confidentiel	Avec chiffrement AES-256. Pour AVS, salaires, médical, contrats, données bancaires.

2.1 Créer les SITs personnalisés

ⓘ **INFO :** SIT = Types d'informations sensibles dans l'interface Purview. Propagation : attendez 15 à 30 minutes après création avant de configurer les étiquettes.

SIT 1 : AVS-Suisse-PME

Détecte les numéros AVS suisses au format exact 756.XXXX.XXXX.XX en 4 langues nationales + anglais. Ne valide pas le checksum EAN-13 (détection par format uniquement). Complémentaire au SIT natif Swiss Social Security Number AHV qui valide le checksum.

N°	Étape	Action
1	Navigation	Purview → Protection des données → Classifieurs → Types d'informations sensibles → + Créer un type d'informations sensibles
2	Page 1 : Nommer	Nom : AVS-Suisse-PME | Description : Détection numéro AVS suisse 756.XXXX.XXXX.XX, 4 langues nationales + anglais. → Suivant
3	Page 2 : Modèle	+ Ajouter un modèle → Niveau de confiance : Moyen → + Ajouter un élément principal → Expression régulière → ID : regex-AVS-Suisse → collez : 756\\.\\d{4}\\.\\d{4}\\.\\d{2} → Correspondance de chaîne → Terminé
4	Page 2 : Mots-clés	+ Ajouter des éléments de soutien → Liste de mots-clés → ID : recherche-AVS-Suisse → saisissez un mot-clé par ligne (voir Annexe C) → Terminé
5	Page 3 : Tester	Suivant → testez avec 756.1234.5678.94 (checksum EAN-13 valide) → vérifiez la détection → Suivant → Créer
⚠	Propagation	Attendez 15 à 30 minutes avant de configurer les règles qui utilisent ce SIT.

ⓘ **INFO :** 756.1234.5678.94 est un numéro de test au format AVS avec checksum EAN-13 valide. AVS-Suisse-PME le détecte (format uniquement). Le SIT natif Swiss Social Security Number AHV le détecte également (checksum validé). Utilisez ce numéro pour tester les deux SIT simultanément.

SIT 2 : Medical-RH-Suisse

Détecte les données médicales RH (arrêts maladie, certificats, incapacité de travail) en 4 langues nationales + anglais.

N°	Étape	Action
1	Navigation	Purview → Protection des données → Classifieurs → Types d'informations sensibles → + Créer un type d'informations sensibles
2	Page 1 : Nommer	Nom : Medical-RH-Suisse | Description : Détection données médicales RH, 4 langues nationales + anglais. → Suivant
3	Page 2 : Modèle	+ Ajouter un modèle → Niveau de confiance : Moyen → + Ajouter un élément principal → Liste de mots-clés → ID : medical-rh-suisse → saisissez un mot-clé par ligne (voir Annexe C) → Terminé
4	Page 3 : Tester	Suivant → testez avec « arrêt maladie » → vérifiez la détection → Suivant → Créer | Attendez 15 à 30 minutes avant de continuer.

2.2 Créer les 2 étiquettes

Étiquette 1 : 1 - Interne (sans chiffrement, par défaut)

N°	Étape	Action
1	Navigation	Purview → Protection des données → Étiquettes de confidentialité → + Créer une étiquette
2	Page 1 : Nommer	Nom : 1 - Interne | Description : Document à usage interne uniquement. | Couleur : Bleu → Suivant
3	Page 2 : Étendue	Cochez : Fichiers et autres ressources de données, Emails, Réunions → Suivant
4	Page 3 : Protection	Sélectionnez Aucune protection → Suivant
5	Finaliser	Laissez les pages suivantes par défaut → Créer une étiquette → Ne créez pas encore de stratégie → Terminer.

Étiquette 2 : 2 - Confidentiel (avec chiffrement AES-256)

INFO : Groupes mail-enabled requis pour le chiffrement RMS : Azure Rights Management exige que les groupes assignés aient une adresse email. En tenant cloud pur (sans AD on-prem) : créez les groupes via Exchange Online PowerShell avant de continuer :
Connect-ExchangeOnline New-DistributionGroup -Name "GRP-Confidentiel-Purview" -Alias "grp-confidentiel-purview" -Type Security -PrimarySmtpAddress "grp-confidentiel-purview@[domaine]" Add-DistributionGroupMember -Identity "GRP-Confidentiel-Purview" -Member utilisateur@[domaine]
En environnement hybride (AD on-prem) : procédure complète dans le Guide complet Microsoft Purview 2026, section 2.2.

N°	Étape	Action
1	Navigation	Purview → Protection des données → Étiquettes de confidentialité → + Créer une étiquette
2	Page 1 : Nommer	Nom : 2 - Confidentiel | Description : Données personnelles sensibles (AVS, salaires, médical, contrats, IBAN). | Couleur : Bordeaux → Suivant
3	Page 2 : Étendue	Cochez : Fichiers et autres ressources de données, Emails, Réunions → Suivant
4	Page 3 : Protection	Sélectionnez Contrôler l'accès + Appliquer le marquage de contenu → Suivant
5	Contrôle d'accès	Configurer les paramètres | Attribuer maintenant | Expiration : Jamais | Hors connexion : 30 jours | + Attribuer des autorisations → ajoutez (1) GRP-Confidentiel-Purview, (2) admin@[domaine], (3) Tous les utilisateurs authentifiés | Niveau : Éditeur (Co-auteur) → Enregistrer
6	Marquage	Filigrane : CONFIDENTIEL (40, diagonal, rouge) | En-tête : CONFIDENTIEL — Usage interne uniquement | Pied : Document protégé nLPD, Ne pas diffuser → Suivant
7	Auto-labelling client	Activez le toggle → + Ajouter une condition → Le contenu contient | Groupe : Donnees-Sensibles | Opérateur : OU | Ajoutez : AVS-Suisse-PME (min 1, Moyen) + IBAN (min 1, Élevé) + Medical-RH-Suisse (min 2, Moyen) → Ajouter → Suivant
8	Finaliser	Pages suivantes par défaut → Créer une étiquette → Ne créez pas encore de stratégie → Terminer.
⚠	Propagation	Attendez 15 à 30 minutes avant de configurer la DLP et l'auto-labelling service.

⚠ ATTENTION : Auto-labelling : deux mécanismes distincts. L'étape 7 ci-dessus configure l'auto-labelling côté client : il s'applique quand l'utilisateur ouvre un document dans Word ou Outlook. Les fichiers déjà présents dans SharePoint avant le déploiement ne sont pas couverts par ce mécanisme. La section 2.4 configure l'auto-labelling côté service qui analyse les fichiers SharePoint de façon asynchrone. Les deux mécanismes sont complémentaires et doivent être configurés.

INFO : Protection par chiffrement RMS : un fichier étiqueté 2 - Confidentiel reste illisible quel que soit le canal utilisé (email, clé USB, Gmail). C'est la mesure technique centrale au sens de l'art. 8 nLPD.

INFO : Accès des destinataires externes : le paramètre « Tous les utilisateurs authentifiés » permet à n'importe quel destinataire de s'authentifier pour ouvrir le fichier, selon deux mécanismes : **Destinataire avec un compte Microsoft (compte professionnel M365, Outlook.com) :** il ouvre le fichier normalement. Azure RMS vérifie son identité en ligne et déchiffre à la volée. Transparent pour l'utilisateur. **Destinataire sans compte Microsoft (Gmail, adresse personnelle, AFC, caisse AVS) :** Word lui affiche un message d'authentification. Il reçoit un code à usage unique par email, valable 15 minutes, qu'il saisit dans le navigateur pour accéder au contenu via une visionneuse web. En cas d'expiration : il clique à nouveau sur « Envoyer le code ». *Note : cette liste n'est pas exhaustive. D'autres scénarios existent (appareils mobiles, applications tierces) qui peuvent se comporter différemment selon la version des clients Office installés chez le destinataire. Informez le client de cette friction potentielle avant la mise en production.*

INFO : Traçabilité des accès externes : l'ouverture du fichier par un destinataire externe via code OTP n'apparaît pas dans les journaux Purview. L'authentification se passe côté infrastructure Microsoft (serveurs Azure RMS) et n'est pas exposée dans l'audit tenant. La preuve de transmission reste dans l'audit DLP côté expéditeur : expéditeur, destinataire, fichier, horodatage, règle déclenchée. **Défendabilité PFPDT :** si le PFPDT demande « qui a ouvert ce fichier et quand », vous ne pouvez pas répondre pour les destinataires externes. Mais cette question se pose uniquement en cas d'incident. Dans ce cas, la réponse est : « le fichier était chiffré, seul un utilisateur authentifié pouvait l'ouvrir, voici la trace de l'envoi. » C'est suffisant au sens de l'art. 8 nLPD.

INFO : DLP et fichiers chiffrés : pour les fichiers étiquetés 2 - Confidentiel (chiffrés RMS), Exchange peut inspecter les métadonnées d'étiquette mais pas nécessairement le contenu pour détecter les SIT. La protection repose donc sur deux niveaux complémentaires : la détection par SIT pour les fichiers non chiffrés (1 - Interne), et le chiffrement RMS lui-même pour les fichiers 2 - Confidentiel qui les rend illisibles même en cas d'envoi non intercepté.

2.3 Publier les étiquettes

Sans publication, les étiquettes sont invisibles dans Word, Outlook et SharePoint.

N°	Étape	Action
1	Navigation	Purview → Protection des données → Stratégies → Stratégies de publication d'étiquettes → + Publier l'étiquette
2	Étiquettes	Sélectionnez : 1 - Interne, 2 - Confidentiel → Ajouter → Suivant
3	Unites admin	Laissez Répertoire complet → Suivant
4	Utilisateurs	Laissez Tous utilisateurs et groupes → Suivant
5	Paramètres	Cochez : (1) Les utilisateurs doivent fournir une justification pour abaisser le niveau | (2) Obliger les utilisateurs à appliquer une étiquette à leurs courriers et documents → Suivant
6	Défauts	Étiquette par défaut documents et e-mails : 1 - Interne. Laissez le reste par défaut → Suivant
7	Nom	Nom : Politique-Labels-[client] → Suivant
8	Soumettre	Vérifiez le résumé puis cliquez sur Envoyer. Propagation : jusqu'à 24 heures.

2.4 Auto-labelling côté service (fichiers SharePoint existants)

L'auto-labelling service analyse de façon asynchrone les fichiers déjà présents dans SharePoint et OneDrive, indépendamment de leur ouverture par un utilisateur. C'est le seul mécanisme qui couvre le stock documentaire existant.

N°	Étape	Action
1	Navigation	Purview → Protection des données → Stratégies → Stratégies d'étiquetage automatique → + Créer une stratégie d'étiquetage automatique
2	Catégorie	Faites défiler la liste → sélectionnez Personnaliser → Suivant
3	Nommer	Nom : Auto-Label-Confidentiel | Description : Détection automatique AVS, IBAN, médical dans SharePoint et OneDrive. → Suivant
4	Étiquette	Cliquez sur choisir une étiquette → sélectionnez 2 - Confidentiel → Appliquer → Suivant
5	Emplacements	Activez : Sites SharePoint (Tous les sites), Comptes OneDrive (Tous les utilisateurs), Courrier Exchange (Tous les utilisateurs) → Suivant
6	Règles	Sélectionnez Règles communes → Suivant → + Nouvelle règle
7	Règle AVS	Nom : Règle-Donnees-Sensibles | Le contenu contient → + Ajouter → Types d'infos confidentielles → AVS-Suisse-PME (Moyen, min 1) + IBAN (International Banking Account Number, Élevé, min 1) + Medical-RH-Suisse (Moyen, min 2) → Enregistrer
8	Mode	Sélectionnez Exécuter la stratégie en mode de simulation → Suivant → Créer une stratégie

INFO : Après 24 à 48 heures de simulation : Purview → Stratégies d'étiquetage automatique → cliquez sur Auto-Label-Confidentiel → Afficher les résultats de simulation. Vérifiez que les fichiers RH et Finances apparaissent dans la liste. Si résultat correct → cliquez sur Activer la stratégie.

2.5 Break-glass RMS (accès de secours aux fichiers chiffrés)

Si l'administrateur qui a configuré le chiffrement quitte l'organisation, les fichiers chiffrés avec l'étiquette 2 - Confidentiel peuvent devenir inaccessibles. Le rôle Super User RMS permet à un compte de secours de lever le chiffrement de n'importe quel document du tenant en cas d'urgence.

IMPORTANT : Cette procédure est obligatoire avant mise en production. Sans compte Break-glass configuré, un départ conflictuel ou une corruption du tenant peut entraîner une perte irréversible des données chiffrées.

Étape 1 : Installer le module et se connecter (Windows PowerShell 5.1 uniquement, pas Cloud Shell) :

```
Install-Module -Name AIPService -Force
Connect-AipService
```

Étape 2 : Activer la fonctionnalité Super User et désigner le compte de secours :

```
Enable-AipServiceSuperUserFeature
Add-AipServiceSuperUser -EmailAddress admin@[domaine]
```

Étape 3 : Vérifier et désactiver après configuration :

```
Get-AipServiceSuperUser
Disable-AipServiceSuperUserFeature
```

⚠ **ATTENTION :** Réactivez le Super User uniquement en cas d'urgence réelle. Chaque activation est tracée dans les journaux d'audit Purview. Documentez chaque utilisation dans votre registre des incidents. Stockez les identifiants du compte de secours dans un coffre-fort physique.

Partie 3 : DLP Exchange

La politique DLP Exchange surveille les envois d'emails contenant des données sensibles vers des destinataires externes. Elle contient deux règles : une règle d'avertissement général, et une règle spécifique IBAN avec justification obligatoire. Les deux partent en simulation 2 à 4 semaines avant activation.

INFO : Canal de sortie unique : dans ce MVC, l'email est le seul canal légitime d'envoi de données vers l'extérieur (SharePoint est bloqué). Une fiduciaire doit pouvoir envoyer des IBAN par email. Le blocage strict sans période de rodage bloquerait l'activité. Après simulation, les deux règles passent en avertissement avec justification obligatoire horodatée, conforme art. 8 nLPD.

ATTENTION : Prérequis : les SIT (section 2.1) doivent être créés et propagés (30 minutes) avant de créer cette politique.

3.1 Créer la politique DLP-PME-Surveillance

N°	Étape	Action
1	Navigation	Purview → Protection contre la perte de données → Stratégies → + Créer une stratégie → Personnalisé → Personnalisé → Suivant
2	Nommer	Nom : DLP-PME-Surveillance → Suivant
3	Emplacements	Activez uniquement : Courrier Exchange (Tous les utilisateurs). Désactivez SharePoint, OneDrive, Teams. → Suivant
4	Paramètres	Sélectionnez Créer ou personnaliser des règles DLP avancées → Suivant
5	Règles	Cliquez + Créer une règle. Créez les 2 règles détaillées ci-dessous.
6	Mode	Page Mode : Exécuter en mode simulation → Suivant
7	Soumettre	Vérifiez et cliquez Soumettre.

3.2 Règle 1 : Avertir-Donnees-Sensibles

Paramètre	Configuration
Nom de la règle	Avertir-Donnees-Sensibles
Condition 1	Le contenu contient → OU : AVS-Suisse-PME (Moyen, min 1) + IBAN (International Banking Account Number, Élevé, min 1) + Medical-RH-Suisse (Moyen, min 2)
Condition 2	Du contenu est partagé avec des personnes extérieures à mon organisation
Actions	Aucune (avertissement seulement)
Notifications utilisateur	Activez les conseils de stratégie → message : Ce document contient des données sensibles. Vérifiez que le destinataire est autorisé.
Remplacements	Activez + exigez justification.
Rapport d'incident	Niveau Moyen. Alerte email : admin@[domaine].

→ Cliquez sur Enregistrer. Puis + Créer une règle pour la règle suivante.

3.3 Règle 2 : Avertir-IBAN-Externe

Paramètre	Configuration
Nom de la règle	Avertir-IBAN-Externe
Condition 1	Le contenu contient → IBAN (International Banking Account Number, confiance Élevée, min 1)
Condition 2	Du contenu est partagé avec des personnes extérieures à mon organisation
Actions	Aucune (avertissement seulement en phase simulation)
Notifications utilisateur	Activez les conseils de stratégie → message : Ce document contient un IBAN. Toute transmission externe est enregistrée conformément à la nLPD. Assurez-vous d'avoir l'accord du responsable.
Remplacements	Activez + exigez justification → la justification est enregistrée dans l'Activity Explorer.
Rapport d'incident	Niveau Élevé. Alerte email : admin@[domaine].

→ *Cliquez sur Enregistrer.*

INFO : Après 2 à 4 semaines : consultez l'Activity Explorer → si les faux positifs sont acceptables → modifiez la politique → Mode → Activer immédiatement.

Partie 4 : Rétention automatique des données

Les politiques de rétention définissent combien de temps les documents sont conservés et ce qui se passe à l'échéance (suppression automatique). C'est une obligation directe de la nLPD (art. 6 al. 4) et du droit comptable suisse (CO art. 958f).

IMPORTANT : Sans politique de rétention configurée, le registre des activités de traitement (Annexe I) indique « 10 ans (CO art. 958f) » sans mesure technique correspondante. C'est une incohérence documentaire immédiatement visible en audit PFPDT. Ces deux politiques ferment ce gap.

4.1 Retention-RH-10ans

Conserve les documents du site SharePoint RH pendant 10 ans puis supprime automatiquement.

N°	Étape	Action
1	Navigation	Purview → Gestion du cycle de vie des données → Stratégies de rétention → + Nouvelle stratégie de rétention
2	Nommer	Nom : Retention-RH-10ans | Description : Rétention documents RH, 10 ans CO art. 958f. → Suivant
3	Unites admin	Répertoire complet → Suivant
4	Type	Sélectionnez Statique → Suivant
5	Emplacements	Activez uniquement Sites SharePoint classiques et de communication → Modifier → saisissez https://[tenant].sharepoint.com/sites/RH → cliquez + → Terminé. Désactivez tous les autres emplacements. → Suivant
6	Paramètres	Conserver les éléments pendant une période spécifique → 10 ans → Démarrer la période fondée sur : Lorsque les éléments ont été modifiés en dernier lieu → À la fin : Supprimer automatiquement les éléments → Suivant → Soumettre.

4.2 Retention-Finances-10ans

Conserve les documents du site SharePoint Finances pendant 10 ans puis supprime automatiquement. Même procédure que 4.1 avec les adaptations suivantes :

Paramètre	Valeur
Nom	Retention-Finances-10ans
Description	Rétention documents Finances, 10 ans CO art. 958f.
URL SharePoint	https://[tenant].sharepoint.com/sites/Finances
Durée et action	10 ans → Supprimer automatiquement

INFO : Les politiques de rétention s'appliquent dans un délai variable selon le tenant (quelques minutes à plusieurs jours). Elles n'affectent pas les fichiers tant que la durée de rétention n'est pas écoulée. Un fichier soumis à une politique de rétention ne peut pas être supprimé manuellement avant l'échéance.

Partie 5 : Vérification et remise

Effectuez ces tests dans l'ordre indiqué, qui correspond à l'ordre de déploiement. Attendez les délais de propagation avant chaque test.

Test 1 : Audit actif

PowerShell :

Get-AdminAuditLogConfig | FL UnifiedAuditLogIngestionEnabled

→ résultat attendu : True.
Alternative : Purview → Audit → Rechercher → bandeau vert.

Test 2 : Étiquettes visibles dans Word

Ouvrez Word sur un PC utilisateur. Ruban → Sensibilité (ou Fichier → Sensibilité). Les 2 étiquettes doivent être présentes. Si absent : propagation jusqu'à 24 heures, vérifiez la publication (section 2.3).

Test 3 : Détection automatique (auto-labelling client)

Dans Word, tapez 756.1234.5678.94 (numéro fictif avec checksum EAN-13 valide). Attendez 30 secondes. L'étiquette 2 - Confidentiel doit s'appliquer automatiquement via l'auto-labelling client. Ce test ne couvre pas l'auto-labelling service (section 2.4) : celui-ci se valide dans Purview → Stratégies d'étiquetage automatique → résultats de simulation.

Test 4 : Avertissement DLP

Envoyez par email à une adresse externe un document contenant 756.1234.5678.94. Le message « Ce document contient des données sensibles… » doit apparaître dans Outlook avant l'envoi. Si absent : la DLP peut prendre jusqu'à 1 heure à s'activer après création.

Test 5 : Audit

Purview → Audit (menu gauche) → Rechercher. Aujourd'hui. Activités : noms conviviaux → Fichier accédé. Des entrées doivent correspondre à vos tests.

Test 6 : Blocage partage SharePoint

Dans SharePoint, ouvrez un fichier et tentez de cliquer sur Partager → Personnes spécifiques → saisissez une adresse externe. Le partage doit être refusé : Votre organisation ne permet pas le partage avec des personnes extérieures.

Checklist de remise client

Cette checklist suit l'ordre de déploiement. Voir Annexe B pour la référence complète avec les sections correspondantes.

	Élément à valider	Statut
☐	MFA activé sur tous les comptes	à valider
☐	Partage externe SharePoint bloqué au niveau tenant	à valider
☐	Audit actif (True dans PowerShell)	à valider
☐	SITs AVS-Suisse-PME et Medical-RH-Suisse créés et propagés	à valider
☐	Étiquettes 1 - Interne et 2 - Confidentiel créées et publiées	à valider
☐	Auto-labelling service activé en mode simulation (section 2.4)	à valider
☐	Politiques de rétention RH et Finances créées (section 4)	à valider
☐	DLP-PME-Surveillance créée en mode simulation (2 règles)	à valider
☐	Break-glass RMS configuré (section 2.5)	à valider
☐	Étiquettes visibles dans Word sur un PC utilisateur (Test 2)	à valider
☐	Détection AVS fonctionnelle avec 756.1234.5678.94 (Test 3)	à valider
☐	Avertissement DLP déclenché sur envoi externe (Test 4)	à valider
☐	Partage SharePoint externe refusé (Test 6)	à valider
☐	Registre des activités (Annexe I) remis et adapté au client	à valider

Annexe A : Glossaire simplifié

Terme	Définition
MVC (Minimum Viable de Conformité)	Ensemble minimal de mesures techniques défendables devant le PFPDT. Ne vise pas la perfection technique mais la capacité de démontrer une démarche proportionnée et documentée.
SIT	Détecteur de motifs qui cherche des numéros AVS, IBAN, etc. dans les documents.
Étiquette de sensibilité	Marqueur appliqué à un document qui indique son niveau de confidentialité et active les protections associées (chiffrement, filigrane).
Auto-labelling client	S'applique quand l'utilisateur ouvre un document dans Word ou Outlook. Configure lors de la création de l'étiquette (section 2.2).
Auto-labelling service	Analyse asynchrone des fichiers déjà présents dans SharePoint et OneDrive par Purview, indépendamment de leur ouverture. Configure via une stratégie dédiée (section 2.4).
Chiffrement AES-256 / Azure RMS	Technologie qui verrouille le contenu d'un document. Sans la clé, le fichier est illisible même s'il est volé, transmis via Gmail ou copié sur une clé USB.
DLP (Data Loss Prevention)	Politique qui surveille et peut bloquer les envois de données sensibles par email ou partage.
Rétention Purview	Politique qui définit la durée de conservation des documents et déclenche leur suppression automatique à l'échéance.
Break-glass RMS	Procédure de secours permettant à un compte désigné d'accéder aux fichiers chiffrés en cas d'urgence (départ admin, perte d'accès).
Audit log	Journal qui enregistre toutes les actions sur les données. Obligatoire nLPD art. 24.
PFPDT	Préposé fédéral à la protection des données. Autorité de contrôle suisse nLPD.
nLPD	Nouvelle loi fédérale sur la protection des données (en vigueur depuis septembre 2023).

Annexe B : Checklist MVC complète

INFO : Cette annexe est la référence de déploiement du consultant avec les sections correspondantes. La checklist de remise client (Partie 5) en est la version simplifiée sans références de section.

Ref.	Action à valider	Statut
[0.3]	Rôles Entra ID (Sécurité + Conformité) attribués	☐
[0.3]	Organization Management Exchange attribué	☐
[0.3]	Compliance Administrator Purview attribué	☐
[0.4]	Licence Purview Suite attribuée au compte admin	☐
[0.5]	EnableMIPLabels activé (PowerShell)	☐
[0.6]	MFA activé sur TOUS les comptes (pas seulement admin)	☐
[0.7]	Partage externe bloqué au niveau tenant SharePoint	☐
[1]	Audit actif : UnifiedAuditLogIngestionEnabled = True	☐
[2.1]	SIT AVS-Suisse-PME créé et propagé (30 min)	☐
[2.1]	SIT Medical-RH-Suisse créé et propagé (30 min)	☐
[2.2]	Groupe GRP-Confidentiel-Purview créé (mail-enabled)	☐
[2.2]	Étiquette 1 - Interne créée	☐
[2.2]	Étiquette 2 - Confidentiel créée (chiffrement + auto-labelling client)	☐
[2.3]	Les 2 étiquettes publiées (Politique-Labels-[client])	☐
[2.4]	Stratégie Auto-Label-Confidentiel créée et simulée	☐
[2.5]	Break-glass RMS configuré (Super User RMS désigné)	☐
[3]	DLP-PME-Surveillance créée (2 règles, mode simulation)	☐
[4]	Retention-RH-10ans créée (SharePoint RH)	☐
[4]	Retention-Finances-10ans créée (SharePoint Finances)	☐
[5]	Test 1 : Audit actif vérifié	☐
[5]	Test 2 : Étiquettes visibles dans Word	☐
[5]	Test 3 : Détection AVS avec 756.1234.5678.94 fonctionnelle	☐
[5]	Test 4 : Avertissement DLP sur envoi externe déclenché	☐
[5]	Test 6 : Partage SharePoint externe refusé	☐
[I]	Registre des activités adapté et remis au client	☐

Annexe C : Mots-clés pour les SIT personnalisés

INFO : Astuce copier-coller : copiez les mots-clés dans un document Word vierge, Ctrl+H : Rechercher « / » → Remplacer par « ^p ». Vous obtenez la liste prête à coller dans Purview, un mot-clé par ligne.

C.1 : AVS-Suisse-PME (4 langues nationales + anglais)

Expression régulière : 756\\.\\d{4}\\.\\d{4}\\.\\d{2} | Niveau de confiance : Moyen | min : 1

Langue	Mots-clés (un par ligne dans Purview)
Français	AVS / numéro AVS / No. AVS / N° AVS / assurance vieillesse / assurance sociale / numéro d'assurance
Allemand	AHV / AHV-Nummer / AHV-Nr / Altersvorsorge / Sozialversicherung / Versicherungsausweis / AHV-Ausweis
Italien	AVS / numero AVS / No. AVS / assicurazione vecchiaia / assicurazione sociale / numero d'assicurazione
Romanche	numer AVS / AVS / assicuranza da vegliadetgna / assicuranza sociala / document d'assicuranza / attest d'assicuranza
Anglais	AHV number / AVS number / Swiss social security / social security number CH / Swiss insurance number

C.2 : Medical-RH-Suisse (4 langues nationales + anglais)

Niveau de confiance : Moyen | min : 2

Langue	Mots-clés (un par ligne dans Purview)
Français	arrêt maladie / certificat médical / incapacité de travail / congé maladie / aptitude au travail / inapte au travail / convalescence / accident de travail / maladie professionnelle
Allemand	Krankmeldung / ärztliches Zeugnis / Arbeitsunfähigkeit / Krankheitsfall / Arbeitsunfähigkeitszeugnis / Genesungsurlaub / Berufsunfall / Berufskrankheit / arbeitsunfähig
Italien	certificato medico / incapacità lavorativa / congedo malattia / idoneità al lavoro / inidoneità al lavoro / convalescenza / infortunio professionale / malattia professionale
Anglais	sick leave / medical certificate / incapacity to work / fit for work / unfit for work / occupational accident / occupational disease / sick note / medical leave
Romanche	annunzia da malsogna / certificat medical / incapacità da lavurar / congedi da malsogna / abilita da lavurar / nun abel da lavurar / convalescenza / accident da lavur / malsogna professiunala

Annexe E : Différences POC vs Production

Point	En production
Compte admin dans le chiffrement	Supprimez admin@[domaine] des autorisations de chiffrement. Gérez l'accès via le rôle Super User RMS uniquement (Guide complet, section 2.6).
DLP mode simulation	Après 2 à 4 semaines : modifiez la politique → Mode → Activer immédiatement. Vérifiez l'Activity Explorer avant.
Noms des groupes	Remplacez par les groupes réels du client. Créez-les mail-enabled via Exchange Online (Guide complet, section 2.2).
Registre des activités	Complétez l'Annexe I avec les activités réelles du client. Supprimez les références à Axonix SA et demo.ch.
Auto-labelling service	Vérifiez les résultats de simulation après 48h avant d'activer. Ajustez les sites SharePoint inclus aux sites réels du client.
Rétention	Remplacez les URLs SharePoint par les URLs réelles des sites RH et Finances du client. Ajoutez une politique Email-3ans si la messagerie Exchange doit être couverte.
Break-glass RMS	Utilisez un compte cloud-only dédié (non nominatif). Stockez les identifiants dans un coffre-fort physique. Documentez chaque activation.
MFA	Préférez l'Accès conditionnel Entra (stratégie MFA) pour permettre des exclusions ciblées.
Évolution vers guide complet	Si le client souhaite ajouter IRM, Endpoint DLP, eDiscovery ou Communication Compliance, référez-vous au Guide complet Microsoft Purview 2026.

Annexe I : Registre des activités de traitement (art. 12 nLPD)

⚠ **ATTENTION :** Exemple pré-rempli pour Axonix SA (demo.ch) : remplacez Axonix SA, demo.ch et admin@demo.ch par les données réelles du client.

Informations générales de l'organisation

Champ	À compléter par l'organisation
Raison sociale	[Nom de la société]
Responsable du traitement (art. 5 let. j nLPD)	[Nom, Prénom, Fonction]
DPO / Conseiller en protection des données	[Nom, Prénom ou Externe / Pas de DPO désigné]
Date de dernière mise à jour	[JJ/MM/AAAA]

Activité 1 : Gestion des ressources humaines et de la paie

Champ	Valeur — Axonix SA
Finalité	Administrer les contrats de travail, calculer et verser les salaires, gérer les absences.
Personnes concernées	Employés actifs et anciens employés.
Catégories de données	Numéro AVS, coordonnées, salaire, évaluations, données médicales (certificats), IBAN.
Destinataires	Fiduciaire, caisse AVS, assureur LAA, assureur maladie, Microsoft (sous-traitant).
Conservation	10 ans après fin du contrat (CO art. 958f).
Base légale	Exécution du contrat de travail (art. 31 al. 2 let. a nLPD).
Mesures techniques	Étiquette 2 - Confidentiel (chiffrement AES-256, Azure RMS). DLP-PME-Surveillance (surveillance envois externes). Retention-RH-10ans (suppression automatique). MFA actif.

Activité 2 : Comptabilité et gestion financière

Champ	Valeur — Axonix SA
Finalité	Tenir la comptabilité, gérer paiements fournisseurs et encaissements clients.
Personnes concernées	Fournisseurs, clients (contacts de facturation), employés (notes de frais).
Catégories de données	IBAN, coordonnées de facturation, montants, références de contrats.
Destinataires	Fiduciaire, banque, AFC, administrations fiscales cantonales, Microsoft (sous-traitant).
Conservation	10 ans (CO art. 958f).
Base légale	Obligation légale (CO art. 957 ss).
Mesures techniques	Étiquette 2 - Confidentiel (chiffrement AES-256, Azure RMS). Règle DLP Avertir-IBAN-Externe (justification obligatoire, traçabilité horodatée). Retention-Finances-10ans (suppression automatique). MFA actif.

Activité 3 : Gestion de la relation client

Champ	Valeur — Axonix SA
Finalité	Exécuter les contrats de prestation, suivi commercial, facturation.
Personnes concernées	Contacts clients (personnes physiques, contexte B2B principalement).
Catégories de données	Nom, coordonnées professionnelles, historique des commandes et contrats.
Conservation	Durée du contrat + 5 ans (prescription CO art. 127).
Base légale	Exécution du contrat (art. 31 al. 2 let. a nLPD).
Mesures techniques	Étiquette 1 - Interne. Accès restreint par site SharePoint. DLP-PME-Surveillance.

→ *Ajoutez ici les activités supplémentaires spécifiques au client.*

Annexe F : Adaptations sectorielles

Le MVC tel que décrit dans ce guide est conçu pour une PME générique de 5 à 25 personnes sans flux externes complexes. Certains secteurs ont des contraintes métier incompatibles avec certains choix architecturaux du MVC. Cette annexe documente les adaptations nécessaires par secteur.

> ℹ **INFO :** Mode d'emploi : chaque section décrit les points de rupture, les adaptations à appliquer et ce qui reste valide sans modification. Appliquez uniquement les adaptations correspondant au secteur du client.

F.1 : PME générique (MVC tel quel)

Profil : commerce, services administratifs, petite industrie, association. Flux externes limités à des emails ponctuels vers des clients ou fournisseurs.

Point	Statut
Blocage SharePoint externe	☑ Adapté — pas de besoin de partage externe volumique
Chiffrement RMS + OTP	☑ Adapté — destinataires peu nombreux, flux occasionnel
DLP Exchange avertissement	☑ Adapté
Auto-labelling	☑ Adapté
Rétention 10 ans	☑ Adapté si les sites SharePoint contiennent uniquement des documents formels

> ☑ **CONSEIL :** Aucune adaptation requise. Déployez le MVC tel quel.

F.2 : Fiduciaire et comptabilité

Profil : fiduciaire, bureau de comptabilité, conseil fiscal. Flux externes fréquents vers AFC, caisses AVS, banques, clients particuliers et entreprises.

Point de rupture	Impact
Chiffrement RMS vers AFC et banques	Ces institutions refusent les flux OTP Microsoft. Un bilan chiffré envoyé à l'AFC sera inaccessible.
Rétention globale SharePoint	Conserver 10 ans toute l'URL SharePoint inclut les brouillons et mémos sans valeur légale, ce qui viole le principe de minimisation nLPD art. 6.

Adaptation 1 : ajouter une étiquette 3 - Externe-Fiduciaire

Cette étiquette permet d'envoyer des documents aux institutions (AFC, banques, caisses AVS) sans chiffrement RMS bloquant, tout en garantissant la traçabilité nLPD via la DLP.

Paramètre	Configuration
Nom	3 - Externe-Fiduciaire
Chiffrement RMS	Aucun
Marquage visuel	Filigrane : CONFIDENTIEL — USAGE EXTERNE AUTORISÉ | En-tête : Transmission autorisée nLPD
Usage	Bilans, déclarations fiscales, décomptes TVA, documents bancaires
Protection	Assurée par la DLP (justification obligatoire) + marquage visuel + audit

Procédure : identique à la création de l'étiquette 1 - Interne (section 2.2), sans chiffrement, avec marquage visuel activé. Ajoutez une règle DLP dédiée : tout document étiqueté 3 - Externe-Fiduciaire envoyé à l'externe exige une justification obligatoire enregistrée dans l'Activity Explorer.

Adaptation 2 : affiner la rétention

Remplacez la rétention globale par URL par une rétention couplée aux étiquettes : conservez 10 ans uniquement les documents étiquetés 2 - Confidentiel ou 3 - Externe-Fiduciaire dans les sites RH et Finances. Les documents non étiquetés (brouillons, mémos) suivent le cycle de vie normal.

Purview → Gestion du cycle de vie des données → Stratégies de rétention → modifiez Retention-RH-10ans et Retention-Finances-10ans → page Paramètres → Condition : appliquer uniquement aux éléments qui correspondent → Étiquette de confidentialité → sélectionnez 2 - Confidentiel et 3 - Externe-Fiduciaire.

Option : ajouter un SIT IDE/UID

Les fiduciaires traitent des numéros d'identification des entreprises (format : CHE-123.456.789). Créez un SIT regex spécifique pour les détecter et les inclure dans les conditions DLP.

Paramètre	Valeur
Nom du SIT	IDE-UID-Suisse
Expression régulière	CHE-\\d{3}\\.\\d{3}\\.\\d{3}
Niveau de confiance	Moyen, min : 1
Mots-clés de soutien	IDE / UID / numéro IDE / numéro UID / Unternehmens-Identifikationsnummer / numero IDI

F.3 — Cabinet d'architectes et ingénieurs civils

Profil : bureau d'architectes, ingénierie civile, géomètres. Collaboration constante avec des dizaines de sous-traitants extérieurs (plans CAD, modèles BIM, rapports techniques volumineux).

Point de rupture	Impact
Blocage SharePoint externe (section 0.7)	Les sous-traitants n'ont pas de compte Microsoft. Bloquer SharePoint force le recours à WeTransfer, Dropbox ou autres outils non contrôlés (Shadow IT), rendant l'audit inutile.
Fichiers volumineux (BIM, CAD)	Les pièces jointes email sont limitées à 25 Mo dans Exchange Online. Incompatible avec les flux métier.

Adaptation : remplacer le blocage SharePoint par le partage contrôlé avec expiration

⚠ **ATTENTION :** Ne pas appliquer la section 0.7 (blocage tenant SharePoint) pour ce secteur. Remplacez par la configuration suivante.

Procédure : Centre d'administration SharePoint → Stratégies → Partage.

N°	Étape	Action
1	Partage externe SharePoint	Curseur SharePoint → Personnes spécifiques (personnes spécifiées par l'utilisateur uniquement). Curseur OneDrive → Personnes spécifiques. → Suivant
2	Type de lien par défaut	Section Liens des fichiers et des dossiers → sélectionnez Personnes spécifiques. Permission par défaut : Consultation.
3	Paramètres supplémentaires	Dépliez Paramètres de partage externe supplémentaires → cochez L'accès invité expirera automatiquement après ce nombre de jours → saisissez 30.
4	Enregistrer	Cliquez sur Enregistrer.
5	Restreindre par site	Pour les sites contenant des données sensibles (RH, Finances) : admin.sharepoint.com → Sites actifs → cliquez sur le site → Paramètres → Partage → Uniquement les personnes de votre organisation. Le blocage est appliqué site par site, pas au niveau tenant.

ⓘ **INFO :** Ce paramètre permet le partage de dossiers de projet avec des sous-traitants via des liens expirés à 30 jours. Chaque partage est tracé dans l'audit SharePoint. Les sites RH et Finances restent bloqués individuellement. La DLP SharePoint (si activée) surveille les contenus partagés.

Ce qui reste valide sans modification	
MFA	Aucun changement
Audit	Aucun changement
Étiquettes et chiffrement RMS	Aucun changement, les fichiers CAD ne contiennent généralement pas de données personnelles sensibles
DLP Exchange	Aucun changement
Rétention	Aucun changement

F.4 : Étude d’avocats et notaires

Profil : avocat, notaire, huissier. Communication avec tribunaux, parties adverses, greffes et administrations via des systèmes judiciaires cantonaux qui n’acceptent pas les flux OTP Microsoft.

Point de rupture	Impact
Chiffrement RMS vers tribunaux et parties adverses	Les systèmes judiciaires suisses (Justitia.swiss, systèmes cantonaux legacy) ne supportent pas l’authentification OTP Microsoft. Un document inaccessible dans un délai judiciaire peut constituer une faute professionnelle.
Chiffrement RMS vers partie adverse	L’avocat adverse peut ne pas avoir de compte Microsoft. Le document reste inaccessible, bloquant la procédure.

Adaptation : étiquette 3 - Juridique-Externe (sans chiffrement RMS)

Créez une étiquette dédiée aux transmissions judiciaires et inter-cabinets, sans chiffrement RMS, avec marquage visuel et DLP obligatoire.

Paramètre	Configuration
Nom	3 - Juridique-Externe
Chiffrement RMS	Aucun
Marquage visuel	Filigrane : CONFIDENTIEL — TRANSMISSION AUTORISÉE | En-tête : Document juridique — Destinataire unique
Usage	Pièces de procédure, actes notariés, correspondance inter-cabinets, transmissions aux greffes
Protection	DLP avec justification obligatoire + audit horodaté + marquage visuel dissuasif

INFO : La protection nLPD reste assurée : la DLP trace chaque transmission (expéditeur, destinataire, document, justification). Le marquage visuel engage la responsabilité du destinataire. L’absence de chiffrement RMS est compensée par la nature professionnelle et légalement encadrée de la relation avocat-tribunal.

CONSEIL : Pour les transmissions via Justitia.swiss : utilisez le portail Justitia.swiss directement pour les dépôts officiels. Réservez l’étiquette 3 - Juridique-Externe aux transmissions informelles et inter-cabinets.

F.5 : Agence de communication et marketing

Profil : agence de communication, studio créatif, agence marketing. Centaines d'allers-retours sur des visuels, textes et contenus publicitaires avec des clients, médias et imprimeurs.

Point de rupture	Impact
Auto-labelling sur contenus métiers	Un visuel publicitaire contenant un IBAN de facturation dans le footer sera automatiquement étiqueté 2 - Confidentiel et chiffré. Le client qui reçoit le BAT (Bon À Tirer) devra s'authentifier OTP pour voir une publicité.
DLP sur échanges créatifs fréquents	Chaque envoi externe de document contenant un IBAN (devis, facture) déclenche une demande de justification. Sur 50 envois par jour, c'est une friction insoutenable.

Adaptation 1 : exclure les sites créatifs de l'auto-labelling service

Dans la stratégie Auto-Label-Confidentiel (section 2.4) : étape 5 Emplacements → Sites SharePoint → ne pas sélectionner Tous les sites. Saisissez uniquement les URLs des sites contenant des données sensibles (RH, Finances). Excluez les sites de production créative (Projets, BAT, Assets).

Adaptation 2 : exclure les comptes créatifs de la DLP Exchange

Dans DLP-PME-Surveillance → étape 3 Emplacements → Courrier Exchange → Modifier → Exclure → ajoutez les comptes des créatifs et chargés de projet. Seuls les comptes RH, Finances et Direction restent sous surveillance DLP.

⚠ **ATTENTION :** Cette exclusion est un compromis : les envois des comptes créatifs ne sont plus surveillés par la DLP. Compensez par une charte informatique signée qui interdit explicitement l'envoi de données personnelles depuis les comptes créatifs. Documentez ce choix dans le registre des activités (Annexe I).

Ce qui reste valide sans modification	
MFA	Aucun changement
Audit	Aucun changement
Blocage SharePoint tenant	Aucun changement — les agences partagent par email, pas par liens SharePoint
Étiquettes	Aucun changement — les comptes RH et Finances continuent d'utiliser 2 - Confidentiel
Rétention	Aucun changement

F.6 : Cabinet médical et paramédical

Profil : médecin généraliste, spécialiste, physio, dentiste. Deux types de flux externes : (1) échanges inter-professionnels (médecin → spécialiste → hôpital) via HIN (Health Info Net), (2) échanges avec les patients (résultats, rappels, factures).

Point de rupture	Impact
Chiffrement RMS vers les patients	Un patient sur Gmail ou Bluewin ne comprend pas le flux OTP Microsoft. Génère une surcharge du secrétariat pour dépannage technique.
Chiffrement RMS vers HIN	Non applicable : les échanges inter-professionnels via HIN utilisent leur propre infrastructure chiffrée indépendante de Microsoft. Le MVC n'interfère pas avec HIN.

Adaptation : étiquette 3 - Patient-Externe (sans chiffrement RMS)

Créez une étiquette dédiée aux communications avec les patients, sans chiffrement RMS mais avec marquage et traçabilité DLP.

Paramètre	Configuration
Nom	3 - Patient-Externe
Chiffrement RMS	Aucun
Marquage visuel	En-tête : Document médical personnel — Confidentiel | Pied : Ne pas transmettre à des tiers
Usage	Résultats d'analyses, ordonnances, rappels de consultation, factures patients
Protection	DLP trace l'envoi. Le marquage visuel engage la responsabilité du patient destinataire.

INFO : Justification nLPD : les données médicales envoyées au patient concerné sont couvertes par le droit d'accès (art. 25 nLPD). La base légale est le consentement du patient. La traçabilité DLP (qui a envoyé quoi à qui et quand) constitue la preuve de contrôle au sens de l'art. 8 nLPD.

CONSEIL : Flux HIN : pour les échanges interprofessionnels (médecin → hôpital, médecin → spécialiste), utilisez HIN Mail directement. Ces flux sont couverts par l'infrastructure HIN et n'ont pas besoin d'être gérés par Purview. Le MVC Purview couvre les données internes et les communications patients uniquement.

F.7 : Synthèse des adaptations

Secteur	Blocage SharePoint	RMS externe	Auto-labelling	DLP	Complexité
PME générique	✅ Bloquer	✅ OTP	✅ Tous sites	✅ Tous comptes	Aucune
Fiduciaire	✅ Bloquer	⚠️ Étiquette ext.	✅ Tous sites	✅ Tous comptes	Faible
Architectes	⚠️ Partage contrôlé	✅ OTP	✅ Tous sites	✅ Tous comptes	Modérée
Avocats	✅ Bloquer	⚠️ Étiquette ext.	✅ Tous sites	✅ Tous comptes	Faible
Communication	✅ Bloquer	✅ OTP	⚠️ Sites ciblés	⚠️ Comptes ciblés	Faible
Cabinet médical	✅ Bloquer	⚠️ Étiquette ext.	✅ Tous sites	✅ Tous comptes	Faible

☑ **CONSEIL :** Pour tous les secteurs avec étiquette externe (Fiduciaire, Avocats, Médical) : la procédure de création est identique à celle de l'étiquette 1 - Interne (section 2.2) avec marquage visuel activé. Comptez 30 minutes supplémentaires de déploiement.

Annexe J : Soutien au travail de documentation

Ce document est mis à disposition gratuitement. Il est le fruit de plusieurs semaines de travail incluant des tests techniques terrain sur Microsoft 365 / Purview, une validation méthodologique orientée PME et une prise en compte des exigences de la nLPD (Suisse).

À titre strictement optionnel :

https://ko-fi.com/doit4everyone

Ce soutien n’implique aucune obligation, aucun service associé et aucune différence de traitement dans l’accès au contenu.