					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : PII24					Titre du document : **Politique de protection de la vie privée relative à la vidéosurveillance (CCTV) et à la surveillance physique**							
Version : 1.0		Date d'entrée en vigueur : 01.01.2025			Propriétaire du document :							
X	Politique		Norme		Procédure		Formulaire		Registre		Autre	

Historique des révisions				
Numéro de révision	**Date de révision**	**Modifications**	**Revu par**	**Propriétaire du processus**

Approbations			
Nom	**Fonction**	**Date**	**Signature**

Alignement sur les normes et réglementations

Norme / Réglementation	Clause / Contrôle / Article	Applicabilité	Type de couverture	Commentaire
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Contrôles documentés et opérationnels
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Surveillance et action corrective
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Finalité, base légale, déclencheur de risque et enregistrements
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Répartition entre sous-traitant et responsable conjoint du traitement
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	Obligations et demandes des personnes concernées
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Collecte, traitement, minimisation, conservation et élimination
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Enregistrements et demandes de divulgation
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Accords avec les sous-traitants, instructions, assistance et enregistrements
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Droits du sous-traitant et assistance relative aux divulgations
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Protection des enregistrements et journalisation
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Principes et responsabilité

GDPR	Article 6	Controller	Primary	Base légale
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparence et mentions d'information
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Demandes d'exercice des droits
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Gouvernance, sous-traitants, enregistrements, sécurité, DPIA et conseil
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Finalité, collecte, minimisation, conservation et divulgation
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparence, participation, responsabilité, sécurité et conformité
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Risque relatif à la vie privée et déclencheurs de DPIA
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Contrôles de protection de la vie privée applicables aux PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Contrôles des accès et des entrées physiques
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, surveillance physique, restriction d'accès et journalisation

1. Champ d’application

1.1 La présente politique s’applique à la vidéosurveillance (CCTV), à la surveillance vidéo, à la surveillance des visiteurs, aux journaux de contrôle d’accès physique, aux enregistrements de surveillance opérée par des agents de sécurité, aux systèmes de surveillance des locaux et aux activités connexes de surveillance physique qui collectent ou traitent autrement des PII.

1.2 La présente politique s’applique aux organisations agissant en tant que responsables du traitement pour leurs propres locaux et activités de surveillance physique.

1.3 Elle s’applique également aux activités d’assistance réalisées en qualité de sous-traitant ou de sous-traitant ultérieur lorsque l’organisation exploite, héberge, examine, stocke, divulgue, supprime ou traite autrement des enregistrements de vidéosurveillance, des données de visiteurs ou des journaux d’accès physique pour le compte d’un client.

1.4 La présente politique couvre la définition des finalités de surveillance, l’approbation, les mentions d’information et la signalétique, les restrictions d’accès, la divulgation, la conservation, la suppression, l’externalisation, l’escalade des incidents, l’orientation des demandes d’exercice des droits, la revue et la gestion des éléments de preuve.

1.5 La présente politique ne fournit pas de conseil en droit du travail, de commentaire juridique relatif aux comités d’entreprise, de procédure applicable aux autorités répressives compétentes, ni de registre dédié à la vidéosurveillance (CCTV).

1.6 Les éléments de preuve propres à la surveillance sont conservés dans les éléments de preuve canoniques du PIMS identifiés dans la présente politique.

2. Objet

2.1 L’objet de la présente politique est d’établir des contrôles de protection de la vie privée applicables à la vidéosurveillance (CCTV) et à la surveillance physique afin que les activités de surveillance reposent sur une finalité déterminée, soient transparentes et proportionnées, fassent l’objet d’un contrôle d’accès, soient conservées pendant des durées définies, ne soient divulguées que par des canaux approuvés et soient étayées par des éléments de preuve PIMS auditables.

2.2 La présente politique encadre de manière cohérente le traitement des enregistrements de vidéosurveillance, des registres de visiteurs, des journaux d’accès physique et des PII de surveillance connexes, sans créer de registres, comités, tableaux de bord ou rôles non canoniques supplémentaires.

3. Objectifs

3.1 Les objectifs de la présente politique sont les suivants :

3.1.1 définir les finalités de surveillance et le périmètre du traitement avant le début de la surveillance ;

3.1.2 documenter dans REG02 les activités de vidéosurveillance (CCTV), d’accès physique, de surveillance des visiteurs et de surveillance physique ;

3.1.3 identifier les activités de surveillance qui nécessitent une revue des risques relatifs à la vie privée ou un examen préalable à la DPIA dans REG04 ;

3.1.4 conserver dans REG07 les éléments de preuve relatifs aux mentions d’information et à la signalétique transparentes ;

3.1.5 restreindre l’accès, la visualisation, l’exportation, la divulgation et la conservation des PII de surveillance ;

3.1.6 orienter les demandes des personnes concernées via REG06 ;

3.1.7 gérer les prestataires de surveillance externalisés et les éléments de preuve de partage de données via REG08 ;

3.1.8 escalader les incidents suspectés relatifs aux PII et liés à la surveillance via REG10 ;

3.1.9 consigner les revues, dérogations, non-conformités, actions correctives, constats d'audit et améliorations dans REG12.

4. Énoncés de politique

4.1 Inventaire, finalité et approbation de la surveillance

4.1.1 [Controller] The Process Owner / Business Owner DOIT enregistrer chaque activité de vidéosurveillance (CCTV), de surveillance des visiteurs, de journalisation du contrôle d'accès physique ou de surveillance physique dans REG02 avant le début de l'activité.

4.1.2 [Controller] The Privacy Lead / PIMS Manager DOIT valider l'entrée REG02 pour les champs relatifs à la finalité, à la base légale, au lieu surveillé, aux catégories de PII, aux catégories de personnes concernées, à la conservation, à la mention d'information, à l'accès et à la divulgation avant l'activation d'une activité de surveillance nouvelle ou substantiellement modifiée.

4.1.3 [Controller] The Process Owner / Business Owner DOIT enregistrer dans REG02 les zones surveillées approuvées, les zones exclues et les limites de collecte avant l'activation des caméras, capteurs, registres de visiteurs ou journaux de contrôle d'accès.

4.1.4 [Conditional] The Process Owner / Business Owner DOIT obtenir une décision de risque relatif à la vie privée dans REG04 avant d'activer une surveillance impliquant une surveillance systématique, un enregistrement audio, une identification biométrique, une détection fondée sur l'analytique, des lieux sensibles, des personnes vulnérables ou une surveillance non évidente.

4.1.5 [Joint Controller] The Privacy Lead / PIMS Manager DOIT enregistrer dans REG08 la répartition des responsabilités de surveillance conjointe avant le début d'une surveillance partagée avec un bailleur, un partenaire de gestion des installations, un client ou un autre responsable conjoint du traitement.

4.1.6 [Processor] The Privacy Lead / PIMS Manager DOIT enregistrer dans REG08 les instructions du client relatives à la surveillance et les limites de traitement autorisées avant de traiter des enregistrements de vidéosurveillance, des registres de visiteurs ou des journaux d'accès physique pour le compte d'un client.

4.2 Mention d'information et transparence

4.2.1 [Controller] The Process Owner / Business Owner DOIT s'assurer que les éléments de preuve relatifs à la signalétique de surveillance ou à une mention d'information équivalente fournie en temps utile sont enregistrés dans REG07 avant que les zones surveillées soient ouvertes aux personnes concernées.

4.2.2 [Controller] The Privacy Lead / PIMS Manager DOIT relier chaque mention d'information relative à la surveillance dans REG07 à la finalité de traitement correspondante dans REG02 avant publication ou modification substantielle.

4.2.3 [Processor] The Privacy Lead / PIMS Manager DOIT fournir dans REG08 les informations à l'appui des mentions d'information relatives à la surveillance lorsque l'organisation exploite des services de surveillance conformément aux instructions du client.

4.2.4 [Conditional] The Process Owner / Business Owner DOIT enregistrer les mesures de transparence alternatives dans REG07 et REG04 avant l'activation d'une surveillance non évidente ou d'urgence.

[... Les sections 4.3–8 ne sont pas incluses dans cet aperçu. Achetez le document complet pour accéder à l'intégralité du contenu. ...]

9. Dérogations

9.1 [All] The Privacy Lead / PIMS Manager DOIT consigner chaque dérogation à la présente politique dans REG12 avant son utilisation.

9.2 [Conditional] The Data Protection Officer / Privacy Advisor DOIT documenter un avis relatif à la vie privée dans REG04 ou REG12 avant l'approbation de dérogations impliquant une surveillance non évidente, un enregistrement audio, une identification biométrique, une surveillance fondée sur l'analytique ou des lieux de surveillance sensibles.

9.3 [All] Top Management DOIT approuver dans REG12 les dérogations dépassant 90 jours avant toute prolongation au-delà de la période initiale de dérogation.

9.4 [All] The Privacy Lead / PIMS Manager DOIT revoir dans REG12 les dérogations ouvertes relatives à la surveillance au moins une fois par mois jusqu'à leur clôture.

10. Mise en application

10.1 [All] The Privacy Lead / PIMS Manager DOIT consigner dans REG12 les défaillances des contrôles de surveillance en tant que non-conformités dans un délai de cinq jours ouvrés à compter de leur confirmation.

10.2 [Both] The Information Security Lead DOIT suspendre l'accès non autorisé au système de surveillance dans un délai d'un jour ouvré à compter de la confirmation et consigner l'action dans REG10 ou REG12.

10.3 [All] Top Management DOIT attribuer dans REG12 la responsabilité des actions correctives dans un délai de 10 jours ouvrés en cas de manquements répétés ou substantiels à la politique.

10.4 [Conditional] The Incident Response Coordinator DOIT initier le workflow d'incident relatif aux PII dans REG10 en cas de suspicion de divulgation non autorisée, de perte ou de compromission de PII de surveillance.

11. Revue et maintenance

11.1 [All] The Privacy Lead / PIMS Manager DOIT revoir la présente politique et les éléments de preuve de surveillance connexes dans REG12 au moins une fois par an.

11.2 [Controller] The Process Owner / Business Owner DOIT revalider chaque finalité de surveillance active, mention d'information, périmètre géographique et entrée de conservation dans REG02 et REG07 au moins une fois par an.

11.3 [Both] The System Owner / Application Owner DOIT revalider les contrôles d'accès, de journalisation, de suppression et d'exportation des systèmes de surveillance dans REG12 au moins une fois par an et après toute modification substantielle du système.

11.4 [Conditional] The Vendor / Procurement Owner DOIT revalider les éléments de preuve relatifs aux prestataires de surveillance externalisés dans REG08 au moins une fois par an et avant le renouvellement du contrat.

11.5 [All] The Privacy Lead / PIMS Manager DOIT mettre à jour les éléments de preuve connexes dans REG02, REG04, REG07, REG08, REG10 ou REG12 dans un délai de 30 jours calendaires suivant les modifications approuvées de la politique.

12. Politiques associées

12.1 PII02 - Politique relative aux rôles, responsabilités et à la responsabilité en matière de protection de la vie privée

12.2 PII03 - Politique d'inventaire des traitements de PII et de base légale

12.3 PII04 - Politique relative aux mentions d'information et à la transparence

12.4 PII06 - Politique de gestion des droits des personnes concernées

12.5 PII07 - Politique d'appréciation des risques relatifs à la vie privée et de DPIA

12.6 PII08 - Politique de protection de la vie privée dès la conception et par défaut

12.7 PII09 - Politique de collecte, d'utilisation, de divulgation et de partage des PII

12.8 PII10 - Politique de conservation, de suppression et d'élimination des PII

12.9 PII12 - Politique de gestion de la protection des données pour les sous-traitants, sous-traitants ultérieurs et tiers

12.10 PII13 - Politique de transfert international de PII

12.11 PII14 - Politique de sécurité des PII et de contrôle d'accès

12.12 PII15 - Politique de gestion des incidents et violations de PII

12.13 PII17 - Politique de gestion des informations documentées et des éléments de preuve du PIMS

12.14 PII18 - Politique de surveillance, d'audit et d'amélioration du PIMS

12.15 PII19 - Politique de protection de la vie privée des employés

12.16 PII21 - Politique de protection de la vie privée relative à l'AI et à la prise de décision individuelle automatisée

12.17 PII23 - Politique relative aux sous-traitants de PII dans le cloud

13. Normes et référentiels de référence

13.1 La présente politique est mise en correspondance avec les normes et réglementations suivantes. Cette correspondance explique comment la politique soutient les exigences citées et identifie les clauses internes qui les mettent en œuvre ou les appuient.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mis en correspondance avec les éléments de preuve documentés relatifs à la surveillance, la planification opérationnelle, les contrôles d'activation, les enregistrements de finalité, le lien avec les mentions d'information, la configuration des accès, la configuration de la conservation et le contrôle des changements pour les activités de vidéosurveillance (CCTV) et de surveillance physique. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Mis en correspondance avec la mesure des contrôles de surveillance, la revue des prestataires, la revue des accès, les constats d'audit, les non-conformités, les actions correctives, l'escalade des actions en retard et les éléments de preuve d'amélioration. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Mis en correspondance avec la définition, par le responsable du traitement, des finalités de surveillance, la documentation de la base légale, les décisions relatives aux déclencheurs de risque relatif à la vie privée et les enregistrements des activités de traitement de surveillance dans REG02 et REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8** - Mis en correspondance avec la répartition applicable aux prestataires de surveillance externalisés, la répartition des responsabilités de surveillance conjointe et les éléments de preuve relatifs aux sous-traitants ou aux responsables conjoints du traitement dans REG08. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Mis en correspondance avec les obligations relatives aux personnes concernées liées à la surveillance, l'orientation des demandes, la préservation nécessaire à l'évaluation des demandes et les éléments de preuve de gouvernance pour l'assistance relative aux droits. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Mis en correspondance avec la limitation de la collecte de surveillance, les limites de traitement, la minimisation, les durées de conservation, la suppression, l'écrasement, les gels de

conservation et le contrôle des copies extraites. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Mis en correspondance avec les enregistrements des divulgations externes, le traitement des demandes de divulgation, la minimisation avant divulgation et les divulgations liées à des incidents impliquant des PII de surveillance. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Mis en correspondance avec les instructions du client pour le sous-traitant, les limites de traitement autorisées, l'assistance aux mentions d'information, les instructions de conservation et de suppression, l'assistance relative aux droits et les enregistrements du sous-traitant pour les services de surveillance externalisés. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mis en correspondance avec l'assistance du sous-traitant aux obligations du client, l'autorisation de divulgation, les enregistrements de divulgation, la notification des demandes de divulgation et le traitement des divulgations juridiquement contraignantes relatives aux PII de surveillance. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Mis en correspondance avec la protection des enregistrements de surveillance, les accès restreints, la revue des accès à privilèges, la journalisation des accès, le confinement des accès non autorisés et les éléments de preuve de journalisation pour les systèmes de surveillance. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Mis en correspondance avec la licéité, la loyauté, la transparence, la limitation des finalités, la minimisation des données, la limitation de la conservation et les éléments de preuve de responsabilité pour les activités de surveillance. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Mis en correspondance avec la documentation de la base légale pour la vidéosurveillance (CCTV), la surveillance des visiteurs, les journaux d'accès physique et les autres activités de surveillance physique. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Mis en correspondance avec les mentions d'information transparentes relatives à la surveillance, les éléments de preuve de signalétique, le lien entre les mentions d'information et les finalités de traitement, les informations à l'appui des mentions d'information fournies par le sous-traitant et les mesures de transparence alternatives. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Mis en correspondance avec l'accès, la rectification, l'effacement, la limitation, l'opposition, l'orientation des demandes, la préservation nécessaire à l'évaluation des demandes et l'assistance au client liée à la surveillance. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Mis en correspondance avec la gouvernance du responsable du traitement, la répartition entre responsables conjoints du traitement, la gouvernance des sous-traitants, les registres des activités de traitement, la sécurité des systèmes de surveillance, la revue des risques relatifs à la vie privée, les déclencheurs de DPIA et l'avis relatif à la vie privée. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mis en correspondance avec la spécification des finalités, la limitation de la collecte, la minimisation des données, la limitation de l'utilisation, la limitation de la conservation et la limitation de la divulgation pour les PII de surveillance. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Mis en correspondance avec la transparence, la participation des personnes, la responsabilité, la sécurité de l'information, la revue de conformité, la revue des accès, l'orientation des demandes d'exercice des droits, l'escalade des incidents et les éléments de preuve d'actions correctives. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 5.1; Clause 6.2** - Mis en correspondance avec le risque relatif à la vie privée et l'examen des déclencheurs de DPIA pour la surveillance physique systématique, non évidente, audio, biométrique, fondée sur l'analytique, dans des lieux sensibles, concernant des personnes vulnérables ou présentant autrement un risque plus élevé. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Mis en correspondance avec les contrôles de protection des PII pour la finalité, la collecte, la minimisation, la conservation, la divulgation et la participation des personnes concernées dans les contextes de surveillance. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Mis en correspondance avec le provisionnement des accès, la restriction de l'accès à l'information et les contrôles d'entrée physique pertinents pour l'accès aux systèmes de surveillance et les enregistrements de contrôle des accès physiques. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Mis en correspondance avec la protection de la vie privée et des PII, l'entrée physique, la surveillance de la sécurité physique, l'accès à privilèges, la restriction de l'accès à l'information et les contrôles de journalisation pour les systèmes de vidéosurveillance (CCTV) et de surveillance physique. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].