CLUSIS

LOI SUR LA PROTECTION DES DONNÉES

Les 10 éléments essentiels à mettre en place

Rumya / everwise

SOLÈNE TIERNY OESCH

- Partner chez Everwise
- Senior Legal Counsel (titulaire du brevet d’avocat)
- LL.M., CIPP/E, CIPM

+41 79 489 97 52
solene.tiernyoesch@everwise.ch

Rumya

AURÉLIEN TISSERAND

- + de 14 ans dans le développement de solutions digitales
- CEO et co-fondateur de Rumya depuis 2018
- Formation et Certification RGPD en 2018
- Business Analyst de Formation

+41 78 224 45 08
aurelien.tisserand@rumya.ch

GOUVERNANCE

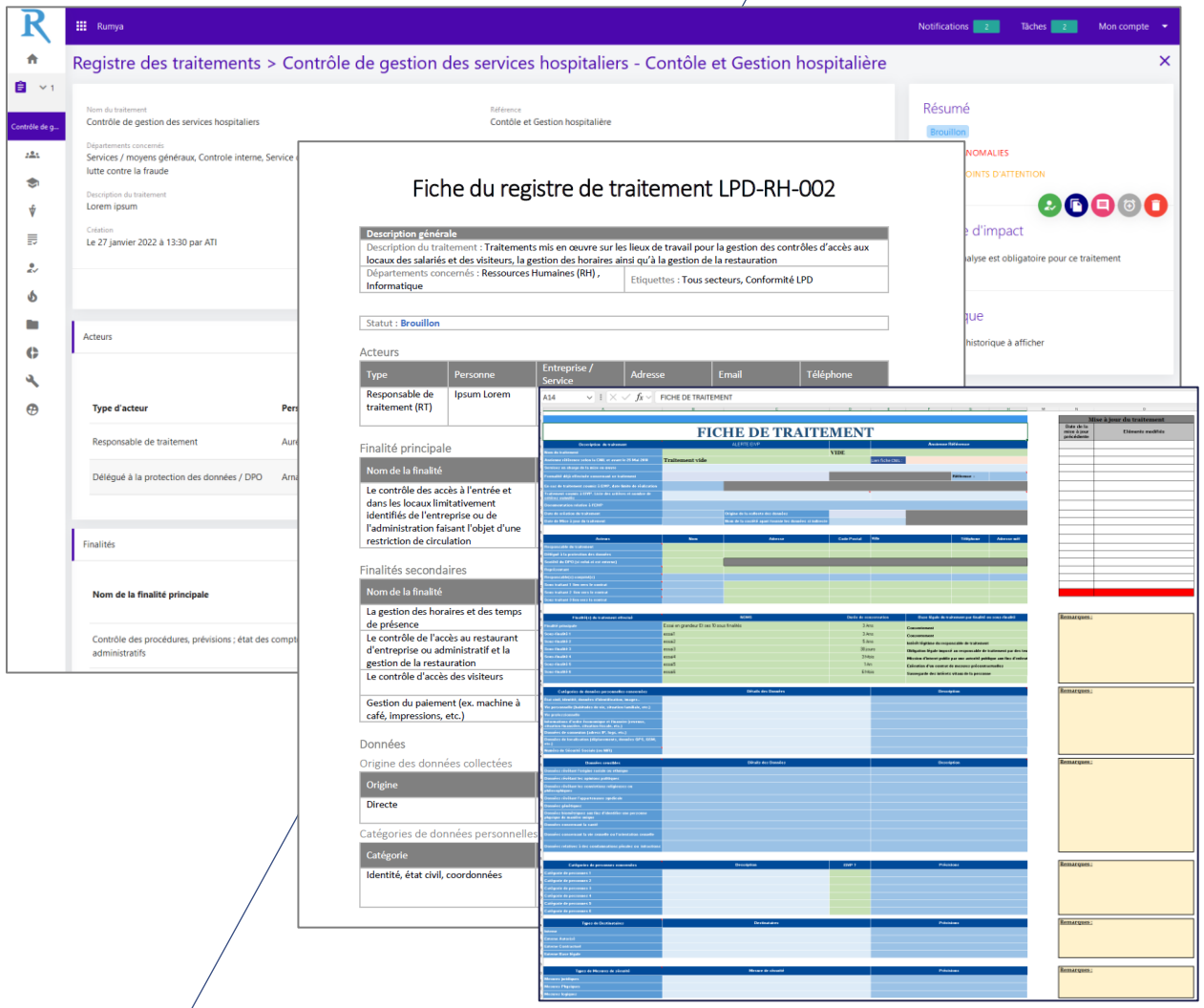
- ❑ Désignation d'un pilote (coordinateur, référent ou d'un DPO) et de son équipe
- ❑ Définition des rôles et responsabilités dans la gestion des données (ex. gestion des incidents)
- ❑ Détermination des formations nécessaires pour le pilote et son équipe
- ❑ Octroi des moyens humains et financiers nécessaires pour mener à bien sa mission
- ❑ Revue annuelle de la conformité et mise à jour de la documentation et des processus

REGISTRE DU TRAITEMENT

- ❑ Lister les traitements de données qui utilisent des données personnelles

Quelques exemples :

- RH | Gestion du recrutement
- RH | Gestion du personnel
- RH | Gestion des badges
- RH | Gestion des salaires
- PROD | Gestion des fournisseurs
- COM | Gestion des clients
- QUA | Ecoute et enregistrement des conversations téléphoniques
- IT : Mise à disposition des outils informatiques
- IT : Gestion du Wi-Fi
- SEC : Vidéosurveillance



REGISTRE DU TRAITEMENT

❑ Description du traitement

Nom du traitement
Badges sur le lieu de travail

Référence du traitement
LPD-RH-002-FRA

Départements concernés
Ressources Humaines (RH) , Informatique

Etiquettes
Conformité LPD, Français

Description du traitement
Traitements mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux des salariés et des visiteurs, la gestion des horaires ainsi qu'à la gestion de la restauration

Date de démarrage du traitement
1 janvier 2025

Date de création de la fiche du traitement
Le 13 janvier 2025 à 23:45 par ATI

Dernière mise à jour
Le 13 janvier 2025 à 23:56 par ATI

EDITER LES INFORMATIONS

REGISTRE DU TRAITEMENT

- Quels sont les acteurs ?

Acteurs

+ AJOUTER UN ACTEUR

Type d'acteur	Personne	Entreprise / Service	Adresse	Email	Téléphone	Actions
Responsable de traitement (RT)	Michael Thanner	Mon Entreprise SA	Chemin de Lausanne, 1 - 1009 Pully Suisse	thanner@entreprise.ch	+41 78 241 41 41	
Délégué à la protection des données (DPO / DPD)	Amélie Miguel	DPO Externe Conseil	Route de Fleurbois, 16 - 1009 Pully Suisse	a.miguel@dpo.ch	+41 21 142 14 14	
Sous-traitant (ST)	Etienne Joly	Badges Père et Fils SARL	Avenue de Vevey, 8 - 1009 Pully Suisse	j.etienne@bpf.ch	+41 79 847 44 14	

REGISTRE DU TRAITEMENT

❑ Quelles sont les finalités des traitements, les bases légales et les durées de conservation ?

Finalités

Nom de la finalité principale	Durée de conservation	Base légale	Actions
Le contrôle des accès à l'entrée et dans les locaux limitativement identifiés de l'entreprise ou de l'administration faisant l'objet d'une restriction de circulation	3 Mois	Intérêt légitime du responsable de traitement	

+ AJOUTER UNE SOUS-FINALITÉ

Noms des sous-finalités	Durée de conservation	Base légale	Actions
La gestion des horaires et des temps de présence	1 Année(s)	Obligation légale imposée au responsable de traitement	
Le contrôle de l'accès au restaurant d'entreprise ou administratif et la gestion de la restauration	3 Mois	Intérêt légitime du responsable de traitement	
Le contrôle d'accès des visiteurs	1 Mois	Intérêt légitime du responsable de traitement	
Gestion du paiement (ex. machine à café, impressions, etc.)	5 Année(s)	Intérêt légitime du responsable de traitement	

REGISTRE DU TRAITEMENT

- Des données sensibles sont-elles concernées ? Quelles sont les catégories de personnes concernées ?

+ AJOUTER UN TYPE DE DONNÉES SENSIBLES

Données sensibles	Détails	Commentaires	Actions
Données biométriques	Empreintes / Visage / Rétine / Caractéristiques vocales	Couplée au système de badge pour les accès nécessitant le plus haut niveau d'accréditation. Ex. Datacenter	

+ AJOUTER UNE CATÉGORIE

Catégories de personnes concernées	Commentaires	Nb. personnes concernées	Actions
Collaborateurs	-	150 en moyenne	
Visiteurs	Sans données biométriques	300 par année	

REGISTRE DU TRAITEMENT

- Quelles données sont collectées ?

+ AJOUTER UNE CATÉGORIE DE DONNÉES

Catégories de données personnelles concernées	Détails	Commentaires	Actions
Identité, état civil, coordonnées	Identité (nom, prénom), Photographie, Numéro de matricule	Pour les visiteurs : nom, prénom, date et heure de visite, société d'appartenance	
Vie professionnelle	Données RH	Service, plages horaires habituellement autorisées, zones d'accès habituellement autorisées, congés, autorisations d'absences, jours de réduction du temps de travail, décharge d'activité de service et...	
Données d'ordre économique	Paiements	Les informations relatives aux paiements, à la date du repas ainsi qu'au type de consommation, sous la forme exclusive, prix des consommations et moyen de paiement, part patronale ou de l'administrati...	
Autres données non sensibles	Date et heure	En cas d'accès à un parking : numéro d'immatriculation du véhicule, numéro de place de stationnement. Heures d'entrée et de sortie, numéro de la porte utilisée	
Données de connexion	Numéro de matricule	Numéro du badge ou de la carte, date de validité.	
Données de localisation	Date et heure, Lieu	Heures d'entrée et de sortie, numéro de la porte utilisée.	

REGISTRE DU TRAITEMENT

- ❑ Quelle est l'origine des données ? Transmettez-vous les données à des tiers ?

+ AJOUTER UNE SOURCE DE DONNÉES

Origines des données collectées	Détails	Commentaires	Actions
Directe	Personnes concernées	Lors du scan par badge	
Directe	Visiteurs	Lors du remplissage du formulaire de visite	
Indirecte	Collaborateurs	Saisie des informations en amont par la personne qui invite le visiteur : nom, prénom, motif et adresse email	

+ AJOUTER UN DESTINATAIRE

Type	Destinataires	Précisions	Actions
Interne	Les services internes qui traitent les données dans la limite de leur champs d'action professionnels	Direction, Ressources humaines (RH), Personnes habilitées	
Tiers habilités	Partenaires institutionnels	Tiers autorisés de par leur mission ou fonction (conseil, juges, justices, huissier, commissaire aux comptes, etc....)	
Externe dans le cadre d'un contrat	Sous-traitants	Les personnes habilitées des services gérant la sécurité des locaux : identité, badge, temps de présence et déplacement des personnes, si entreprise extérieure.	

REGISTRE DU TRAITEMENT

- Existe-t-il des transferts internationaux ? Licéité du transfert ?

+ AJOUTER UN TRANSFERT INTERNATIONAL

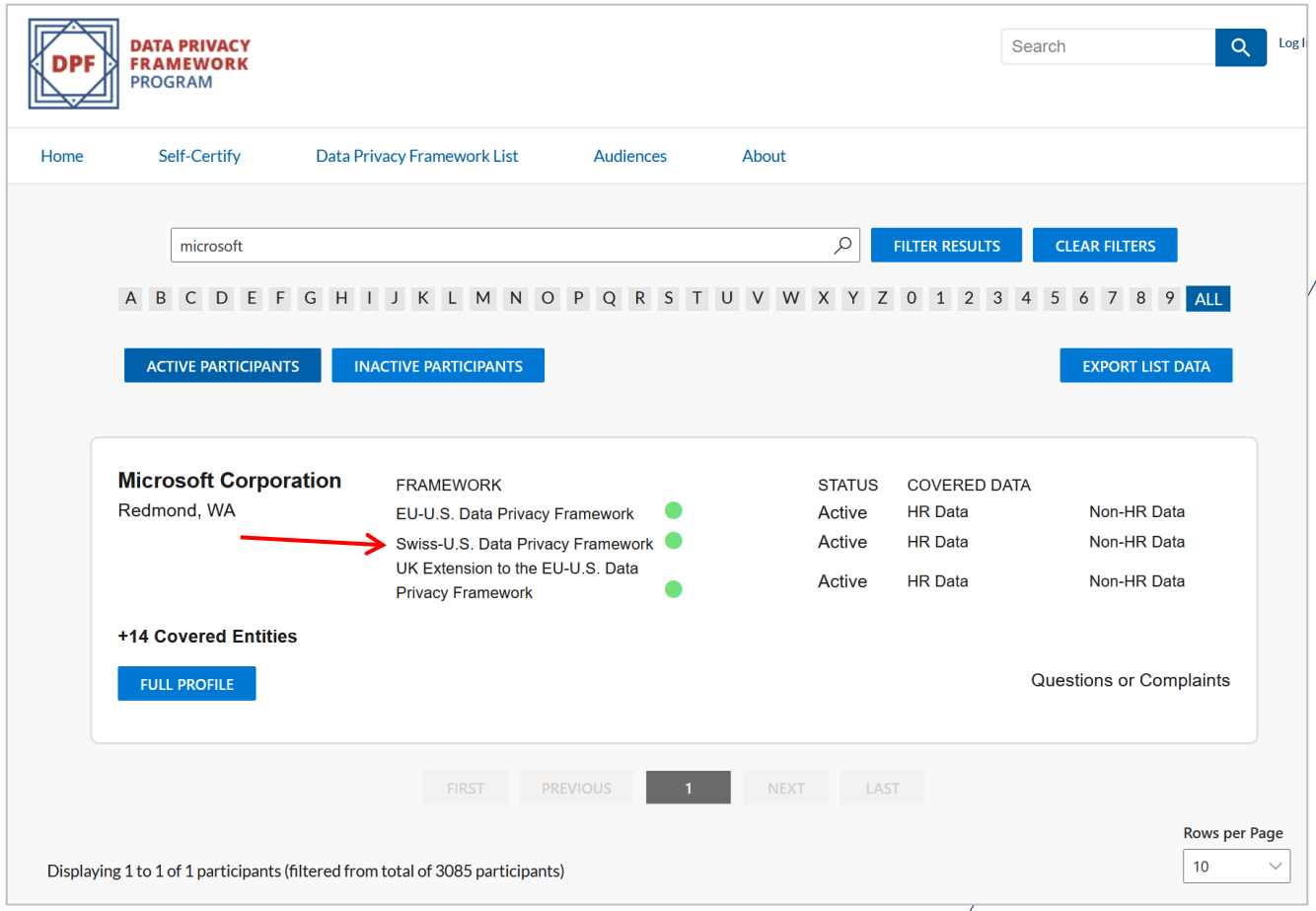
Destinataire	Pays	Zone	Garantie	Documentation	Détails	Actions
Stempeluhr AG	Allemagne	Pays de l'UE	-	0	Logiciel des badgeuses	
Amazon	États-Unis	Adéquation partielle (*voir plus*)	Clauses Contractuelles Types	3	Système de backup	
Deep Spirit Inc.	Inde	Non adéquat	Aucune	1	Analyse de risque lié aux badges assisté par IA	

Data Privacy Framework Program : https://www.dataprivacyframework.gov/list

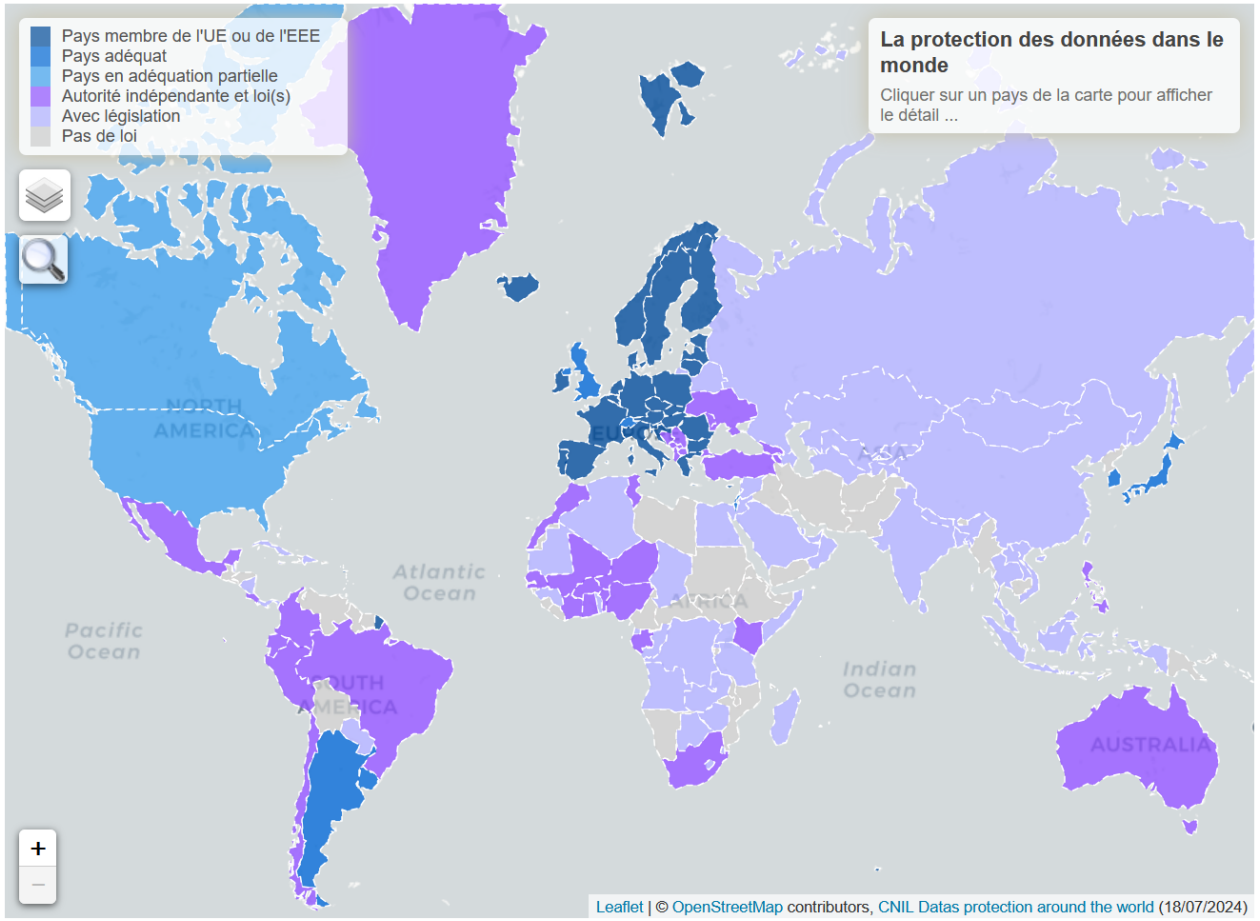
REGISTRE DU TRAITEMENT

- Existe-t-il des transferts internationaux ? Licéité du transfert ?

Data Privacy Framework Program : https://www.dataprivacyframework.gov/list



ADÉQUATION DANS LE MONDE



DEVOIR D'INFORMATION

- Obligation d'informer la personne concernée, par exemple :
  - clients et prospects, employés, candidats, fournisseurs, visiteurs (y compris du site internet), etc.

  De manière adéquate de la collecte de données personnelles, notamment sur :
  - l'identité et les coordonnées du responsable du traitement ;
  - la finalité du traitement ;
  - les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises
  - les pays et garanties en cas de transferts à l'étranger, etc.
- Rédaction et publication de déclarations de confidentialité claires et accessibles
- Elaborations de notices d'information complémentaire si nécessaire
- Mise à jour des documents en fonction des changements

MESURES TECHNIQUES ET ORGANISATIONNELLES

- Assurer la confidentialité :
  - Contrôle de l'accès aux données limité
  - Contrôle de l'accès aux locaux et aux installations
  - Contrôle d'utilisation
- Assurer la disponibilité et l'intégrité :
  - Protection des supports de données contre la copie, la modification ou la destruction
  - Contrôle de la mémoire et du transport
  - Disponibilité des fonctions du système de traitement
  - Signalement des dysfonctionnements (fiabilité)
  - Restauration rapide en cas d'incident et préservation de l'intégrité des données
  - Sécurité par des systèmes et logiciels régulièrement mis à jour
- Assurer la traçabilité :
  - Contrôle de la saisie, des modifications et de la communication des données.
  - Détection rapide des violations et actions correctives

SOUS-TRAITANTS ET CONTRATS

- ❑ Identification de tous les sous-traitants impliqués dans le traitement de données personnelles
- ❑ Vérification de la conformité des sous-traitants avec les exigences de la LPD
- ❑ Vérification des mesures organisationnelles et techniques pour assurer un niveau de sécurité adéquat
- ❑ Élaboration de clauses contractuelles spécifiques et claires sur la protection des données (respect des instructions, responsabilités, mesures de sécurité, etc.)
- ❑ Sous-traitance du sous-traitant uniquement avec l'accord du responsable de traitement
- ❑ Surveillance des sous-traitants pour assurer une protection continue des données

GESTION DES DROITS

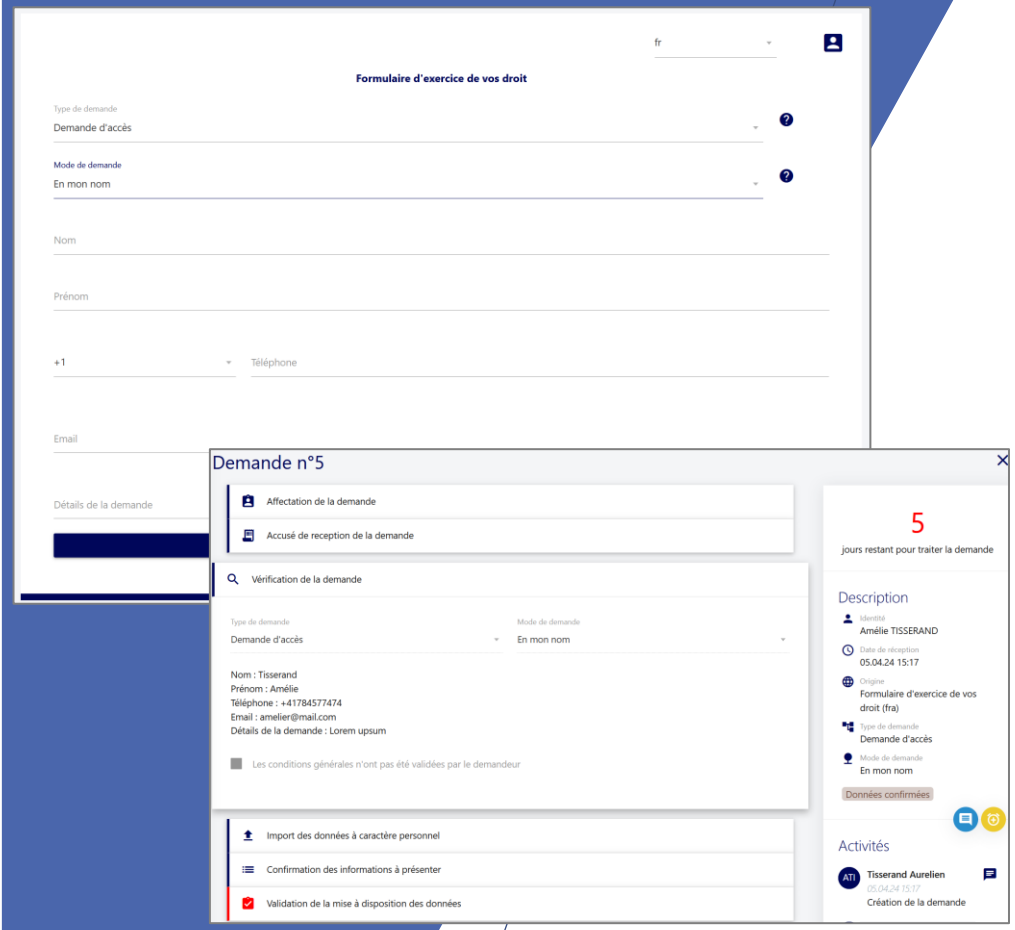
- Connaître les droits des personnes concernées
  - Droit d'être informé
  - Droit d'accès
  - Droit de rectification
  - Droit à l'effacement
  - Droit à la limitation du traitement
  - Droit à la portabilité des données
  - Droit d'opposition
  - Droit de ne pas faire l'objet d'une décision fondée exclusivement sur une décision automatisée ou un profilage

GESTION DES DROITS

- ❑ Mettre en place une procédure et la documenter

Comment faire :

- Identifier les points d'entrées / les canaux de communication
- Définir les responsabilités
- Identifier les données
- Préparer des scenarios et des modèles de réponse
- Attention au délai de réponse / prolongation du délai de réponse possible à certaines conditions
- Attention au mode de réponse (papier / digital)



GESTION DES DROITS

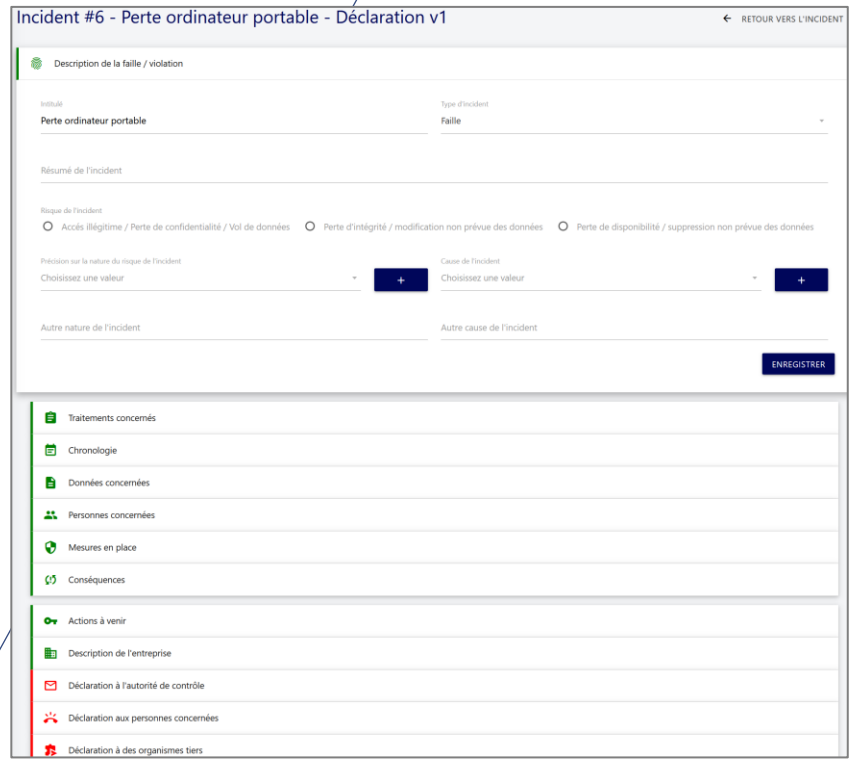
- ❑ Mettre en place une procédure et la documenter

Exemple :

1. Récolte de la demande via un formulaire en ligne
2. Quittance de réception de la demande à la personne concernée
3. Affectation de la demande à l'interne
4. Vérification de la demande
5. Identification de la personne
6. Validation ou refus de la prise en charge
7. Collecte des informations / transmission de la demande de suppression / etc.
8. Vérification des informations collectées / analyse de la suppression / etc.
9. Transmission des informations / quittance de traitement / etc.
10. Conservation des informations transmises, réponse et métadonnée avec durée de conservation adéquate

GESTION DES VIOLATIONS

- Failles et Violations
  - Définir ce qu'est une violation ou une faille et savoir les catégoriser
  - Avoir les outils pour pouvoir détecter une faille ou une violation
  - Informer les sous-traitants de leurs obligations
  - Définir un plan d'action pour réagir en cas de violation
- Gérer et documenter la violation dès la détection ou la suspicion de survenance d'un incident
  - Avoir défini au préalable une "task force" et des tiers de confiance
  - Décrire l'incident
  - Détailler la chronologie des évènements.
  - Evaluer les traitements les données et les personnes concernées.
  - Analyse des mesures en place.
  - Evaluation du risque et des conséquences prévisibles.
  - Mesures appliquées et actions à venir
  - Notifications selon le risque évalué aux
    - autorités de contrôle,
    - personnes concernées,
    - organismes tiers,
    - responsable de traitement dans le cas d'un traitement en tant que sous-traitant.



FORMATION DES COLLABORATEURS

- Sensibiliser et former les collaborateurs
  - Mise à niveau à l'engagement
  - Formation continue tout au long de la vie du collaborateur dans l'entreprise
  - Personnaliser les formations
  - Documenter !

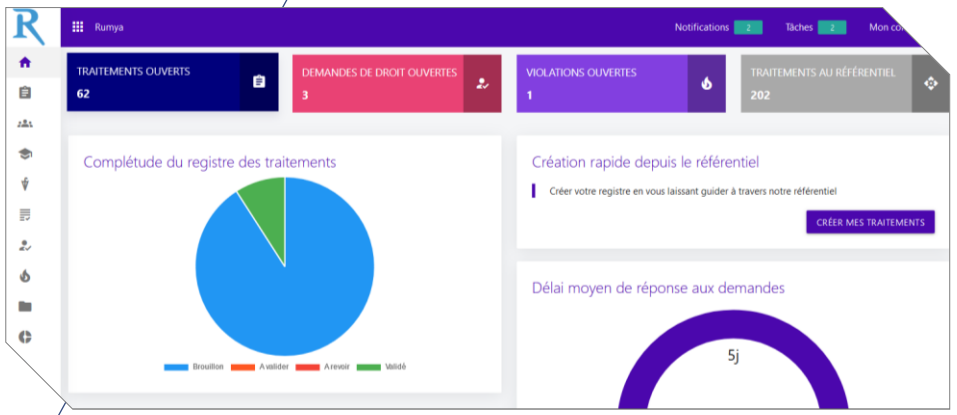
Quelques recommandations :

  - Campagnes de phishing éducatif récurrente
  - Formation en ligne
  - Démonstration de hacking

- Ne pas oublier
  - Revoir la documentation juridique : charte d'utilisation des outils informatiques, politique interne de protection des données
  - Gestion des habilitations (à l'embauche, en fin de contrat et en cas de changement)

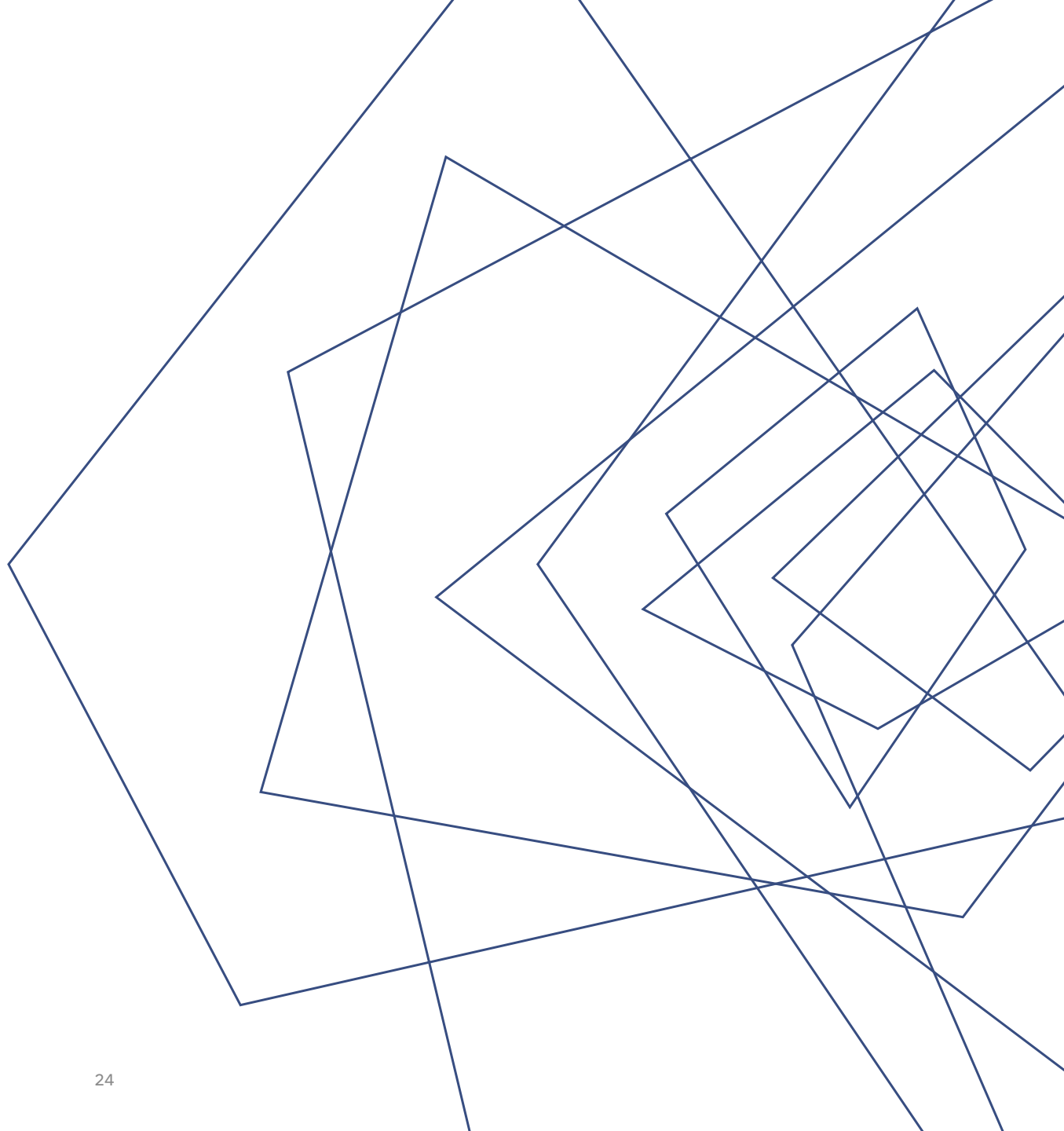
DOCUMENTATION

- Centralisation de toute la documentation relative à la protection des données :
  - Moyens d'information des personnes concernées (déclaration de protection des données, etc.)
  - Registre de traitement
  - Exercice de droit
  - Sauvegardes des informations en lien avec l'analyse des sous-traitants (due diligence)
  - Contrats
  - Encadrement des transferts hors EU
  - Procédures internes
  - Analyses d'impact
  - Consentements
  - Formations des collaborateurs
  - Audits de conformité et des rapports de sécurité
  - Documentation des potentielles violations de la sécurité des données
- Suivi des modifications documentaires et traçabilité des mises à jour
- Préparation de la documentation requise en cas de demande des autorités de contrôle



RÉSUMÉ DES 10 ÉLÉMENTS

1. Gouvernance
2. Registre du traitement
3. Transferts internationaux
4. Devoir d’information
5. Mesures techniques et organisationnelles
6. Sous-traitants et contrats
7. Gestion des droits
8. Gestion des violations
9. Formation des collaborateurs
10. Documentation



MERCI POUR VOTRE ATTENTION

AURELIEN TISSERAND

CEO et Co-founder de Rumya

+41 78 224 45 08

aurelien.tisserand@rumya.ch

www.rumya.ch

« La simplicité est la sophistication suprême »

Léonard de Vinci

SOLENE TIERNY OESCH

Partner

Senior Legal Counsel (titulaire du brevet d'avocat)

LL.M., CIPP/E, CIPM

EPFL Innovation Park – Building C

CH-1015 Lausanne – Switzerland

+41 79 489 97 52

solene.tiernyoesch@everwise.ch

www.everwise.ch