Nouvelle Loi sur la Protection des Données

Mode d'emploi

Rumya × datago

TECH4TRUST
TRUST VALLEY

CLUSIS

Rumya

Aurélien Tisserand

- + de 13 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

swiss made software
+hosted in switzerland

Spécialisation RGPD UE Certifiée
C GDPR P
Certifiée ISO 17024:2012

Présentation

datago

Anna Ploix

- Consultante juridique
- Experte en protection des données personnelles
- Formation en droit international et européen
- DPO externe spécialisée dans les données de santé

+41 22 552 82 30
apl@datago.ch

SWISS DPO ASSOCIATION

AGENDA

- **Contexte**
- Concepts et définitions
- Quelques principes
- Mener son projet de mise en conformité
- Etat des lieux interne
- Commencer par ce qui est visible depuis l'extérieur
- Respecter les droits des personnes
- Gérer les violations de données
- Outils de mise en conformité
- Questions

CONTEXTE

Protéger la personnalité et les droits fondamentaux des personnes physiques.

Règlement général sur la protection des données (RGPD)

25.05.2018

- Octroie des droits aux personnes concernées.
- Définit des obligations pour les responsables de traitements (sécurité, licéité, ...).

Loi fédérale sur la protection des données (LPD)

01.09.2023

- Applicable immédiatement
- S'applique à toutes les entreprises qui traitent des données personnelles
- S'aligne aux exigences européennes pour faciliter les échanges de données.

AGENDA

- Contexte
- **Concepts et définitions**
- Quelques principes
- Mener son projet de mise en conformité
- Etat des lieux interne
- Commencer par ce qui est visible depuis l'extérieur
- Respecter les droits des personnes
- Gérer les violations
- Outils de mise en conformité
- Questions

CONCEPTS ET DÉFINITIONS

DONNÉES PERSONNELLES

Données d'entreprise / d'organisation

Informations générées ou recueillies dans le cadre des activités, incluant des données financières, opérationnelles et relatives aux employés et clients.

Données personnelles

Informations permettant d'identifier, directement ou indirectement une personne physique.

Données sensibles

Informations révélant :

- La religion, les convictions politiques/philosophique
- L'état de santé
- La vie intime
- L'origine ethnique
- Les poursuites judiciaires
- Les aides sociales
- Des informations biométriques/génétiques d'une personne.

CONCEPTS ET DÉFINITIONS

TRAITEMENT DE DONNÉES PERSONNELLES

Profil: Client

Nom, prénom : Rémi Fasol

Date de naissance : 18.04.1983

Téléphone : +4101020304

Adresse : Rue de Genève 1

Statut familiale : marié

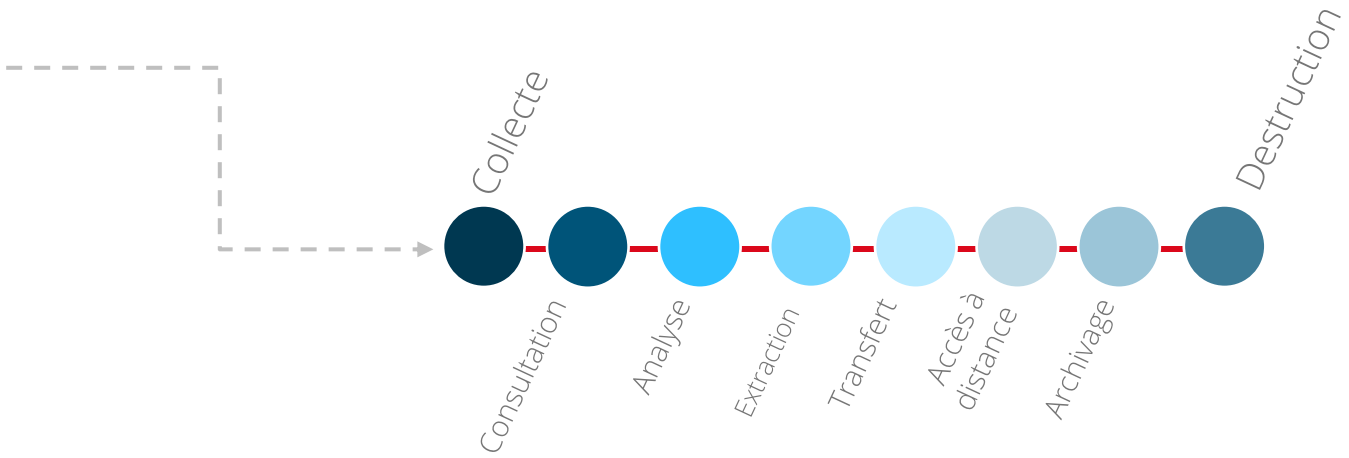
Profession : Comptable

IBAN: CHxxxxxxxxx

Un traitement de donnée personnelles est **toute opération effectuée sur les données personnelles** d'une personne concernée.

Ex:

- Formulaire d'inscription à une newsletter
- Consultation de la base de données clients
- Transfert de données à un prestataire



AGENDA

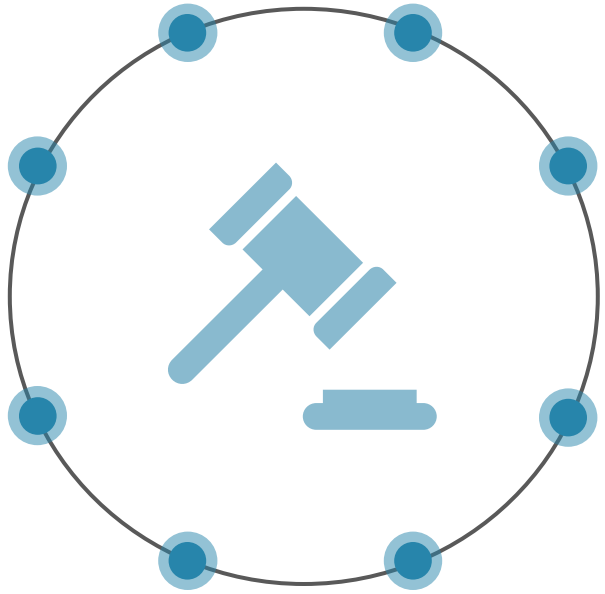
- Contexte
- Concepts et définitions
- **Quelques principes**
- Mener son projet de mise en conformité
- Etat des lieux interne
- Commencer par ce qui est visible depuis l'extérieur
- Respecter les droits des personnes
- Gérer les violations
- Outils de mise en conformité
- Questions

PRINCIPES

Sécurité
Garantir la sécurité, la confidentialité et la protection des données personnelles contre tout accès non autorisé ou toute utilisation abusive.

Licéité
Tout traitement de données doit être licite et pour cela il doit respecter les règles destinées à protéger la personnalité.

Limitation des finalités
Ne collecter que pour des finalités déterminées et reconnaissables pour la personne concernée et les traiter ultérieurement de manière compatible avec ces finalités.



Transparence
Informer les personnes dont les données sont collectées sur les raisons du traitement et sur la manière dont leurs données seront utilisées.

Proportionnalité
Ne pas procéder à un usage abusif des données personnelles. Ne doivent être collectées que les données nécessaires à l'objectif poursuivi.

Bonne foi
Le traitement de données doit être effectué selon le principe de la bonne foi (i.e. ne pas tromper la personne concernée sur le but et le traitement de ses données).

Exactitude
S'assurer que les données sont exactes et tenues à jour.

Protection des données dès la conception et par défaut
Intégrer les enjeux de protection des données personnelles dès la conception des opérations de traitement et par défaut s'assurer de leur traitement selon le niveau le plus élevé de protection.

AGENDA

- Contexte
- Concepts et définitions
- Quelques principes
- **Mener son projet de mise en conformité**
- Etat des lieux interne
- Commencer par ce qui est visible depuis l'extérieur
- Respecter les droits des personnes
- Gérer les violations
- Outils de mise en conformité
- Questions

MENER SON PROJET DE MISE EN CONFORMITÉ

LPD

01
Définir et mettre en œuvre des procédures sur la protection des données

Elaborer une documentation de référence pour organiser la mise en œuvre des principes de protection des données

02
Piloter la gouvernance de la protection des données

Définir et désigner les rôles et responsabilités en matière de protection des données.

03
Recenser et tenir à jour la liste des traitements

Avoir une vue d'ensemble sur les traitements de données personnelles effectués.

04
Assurer la conformité juridique des traitements

Identifier et encadrer les échanges de données avec ses fournisseurs.

05
Former et sensibiliser

Former et sensibiliser les collaborateurs à la protection des données personnelles.

06
Traiter les demandes des usagers internes et externes

Anticiper et formaliser les modalités de gestion des demandes d'exercice des droits.

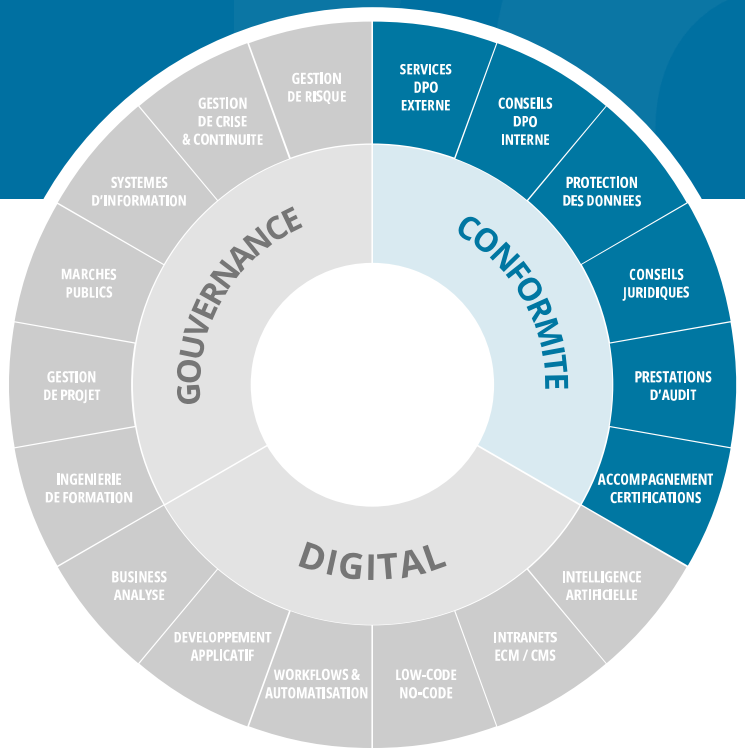
07
Gérer les risques de sécurité

Renforcer les mesures permettant d'assurer la sécurité des données.

08
Gérer les violations de données

Savoir reconnaître et traiter les violations de données personnelles.

DÉMARCHE



Etape 1

Analyse de l'existant et évaluation des besoins

Gestion de projet

Etape 2

Création /développement de contenu et référentiels internes

Métier

Technique

Juridique

Etape 3

Communication, sensibilisation et formation

Formation continue

Etape 4

Accompagnement phase de mise en œuvre

Autonomie

Etape 5

Audit de suivi et adaptations

Rapport d'analyse d'écart	Registre des traitements	Formation	Rapport d'audit
	Documents internes	Déclaration de confidentialité	DPAdvisor / DPOaas

MENER SON PROJET DE MISE EN CONFORMITÉ

Documenter

- ❑ Ai-je besoin d'un CPD (conseiller à la protection des données) ou un référent est-il suffisant ?
- ❑ Suis-je dans l'obligation d'élaborer un registre des traitements ?
- ❑ Documenter les modalités de gestion des demandes de droits.
- ❑ Documenter les modalités de gestion des violations de données.

S'outiller

- ❑ Mettre en place un système de stockage des consentements.
- ❑ A minima des fiches Excel / Word grâce aux modèles fournit par les autorités de contrôle.
- ❑ Choisir un logiciel du marché.

Se faire aider

- ❑ Mandater un DPO externe
- ❑ Faire appel à des spécialistes (juristes, avocats, experts en sécurité)
- ❑ Formateurs

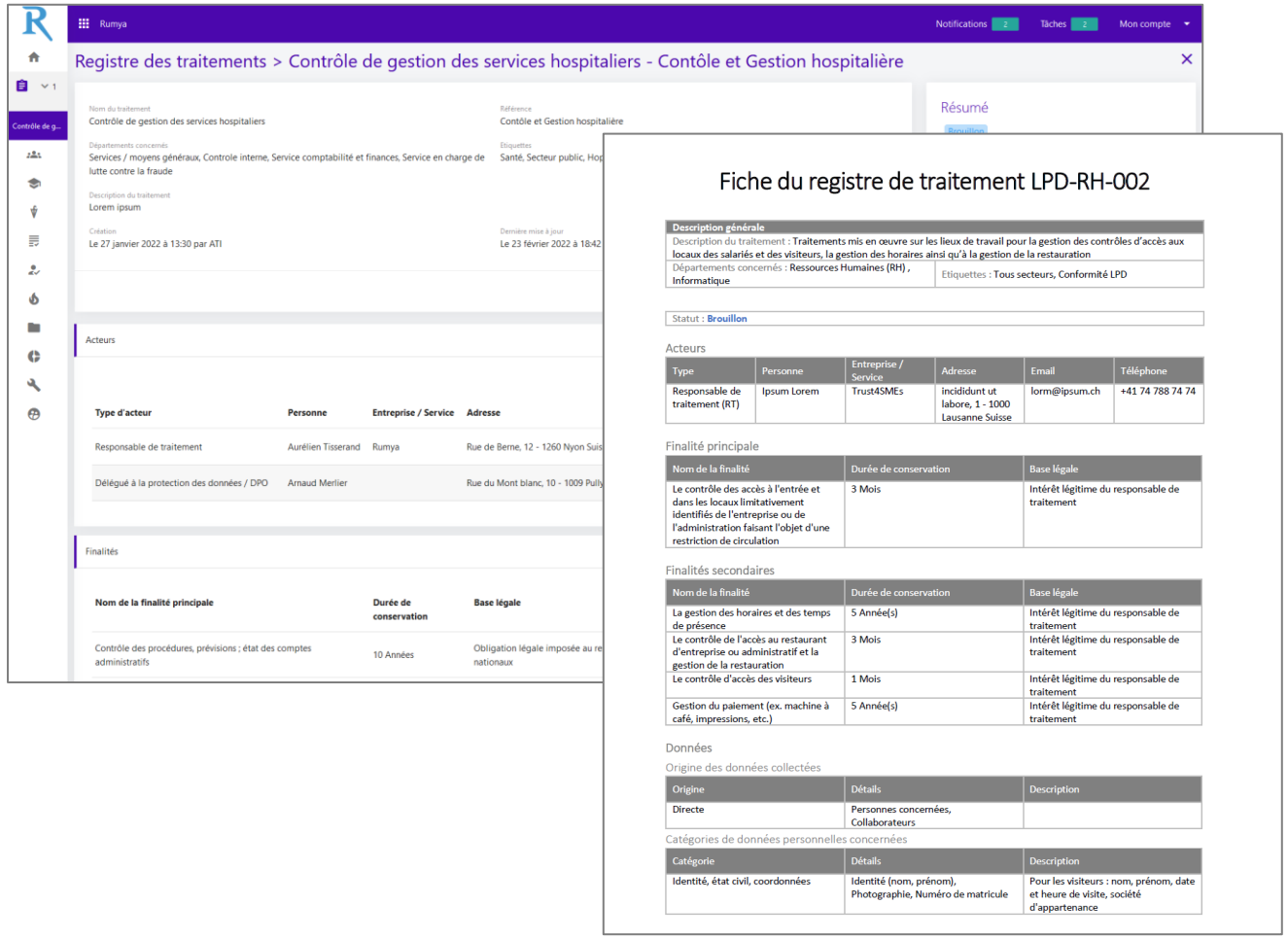
AGENDA

- Contexte
- Concepts et définitions
- Quelques principes
- Mener son projet de mise en conformité
- **Etat des lieux interne**
- Commencer par ce qui est visible depuis l'extérieur
- Respecter les droits des personnes
- Gérer les violations
- Outils de mise en conformité
- Questions

ETAT DES LIEUX INTERNE

REGISTRE DES TRAITEMENTS

- ❑ Lister les traitements de données qui utilisent des données personnelles
- ❑ Quels sont les acteurs ?
- ❑ Quelles sont les finalités des traitements, les bases légales et les durées de conservation ?
- ❑ Des données sensibles sont-elles concernées ? Quelles sont les catégories de personnes concernées ?
- ❑ Quelles données sont collectées ?
- ❑ Quelle est l'origine des données ? Transmettez-vous les données à des tiers ?
- ❑ Existe-t-il des transferts internationaux ? Licéité du transfert ?
- ❑ Quelles sont les mesures de sécurité en place (juridiques, physiques, logiques) ?



ETAT DES LIEUX INTERNE

REGISTRE DES TRAITEMENTS

- ❑ 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 des conversations téléphoniques
- IT : Mise à disposition des outils informatiques
- IT : Gestion du Wi-Fi
- SEC : Vidéosurveillance

ETAT DES LIEUX INTERNE

REGISTRE DES TRAITEMENTS

- Quels sont les acteurs ?

Type	Contact	Entreprise	Adresse	Email	Téléphone
Responsable de traitement	Thanner Michael	Mon Entreprise SA	Chemin de Lausanne 1 1009 Pully	thanner@entreprise.ch	078 241 41 41
Délégué à la protection des données	Miguel Amélie	DPO Externe Conseil	Route de Fleurbois 16 1009 Pully	a.miguel@dpo.ch	021 142 14 14
Sous-traitant	Joly Etienne	Bagdes Père et Fils SARL	Avenue de Vevey 8 1009 Pully	j.etienne@bpf.ch	079 847 44 14

ETAT DES LIEUX INTERNE

REGISTRE DES TRAITEMENTS

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

Finalité principale	Durée de conservation	Base légale
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

Finalités secondaires	Durée de conservation	Base légale
La gestion des horaires et des temps de présence	3 ans	Obligation légale imposée au 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 années	Intérêt légitime du responsable de traitement

ETAT DES LIEUX INTERNE

REGISTRE DES TRAITEMENTS

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

Données sensibles	Détails	Commentaires
Données biométriques	Empreinte digitale	Couplée au système de badge pour les accès nécessitant le plus haut niveau d'accréditation. Ex. Datacenter

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

ETAT DES LIEUX INTERNE

REGISTRE DES TRAITEMENTS

- Quelles données sont collectées ?

Catégories	Détails	Commentaires
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	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 RH
Données d'ordre économique	Paiements	
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.

ETAT DES LIEUX INTERNE

REGISTRE DES TRAITEMENTS

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

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

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

ETAT DES LIEUX INTERNE

REGISTRE DES TRAITEMENTS

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

Destinataire	Pays	Zone	Garantie	Documentation	Commentaires
Stempeluhr AG	Allemagne	Adéquat (Pays de l'UE)	-	-	Logiciel des badgeuses
Amazon	USA	Non adéquat	Clauses Contractuelles Types	Contrat Amazon.pdf	Système de backup
Deep Spirit Inc.	Inde	Non adéquat	Aucune	CGU.html	Analyse de risque lié aux badges assisté par IA

ETAT DES LIEUX INTERNE

REGISTRE DES TRAITEMENTS

- Quelles sont les mesures de sécurité en place (juridiques, physiques, logiques) ?

Mesures juridiques	Détails	Justificatifs
Convention de partenariat ou contrat de sous-traitance avec les clauses spécifiques de protection des données à caractère personnel	Avec hébergeur de données	Convention.pdf
Politique de protection des données		Privacy_policy.pdf
Charte informatique	Avec collaborateurs	Charte.pdf

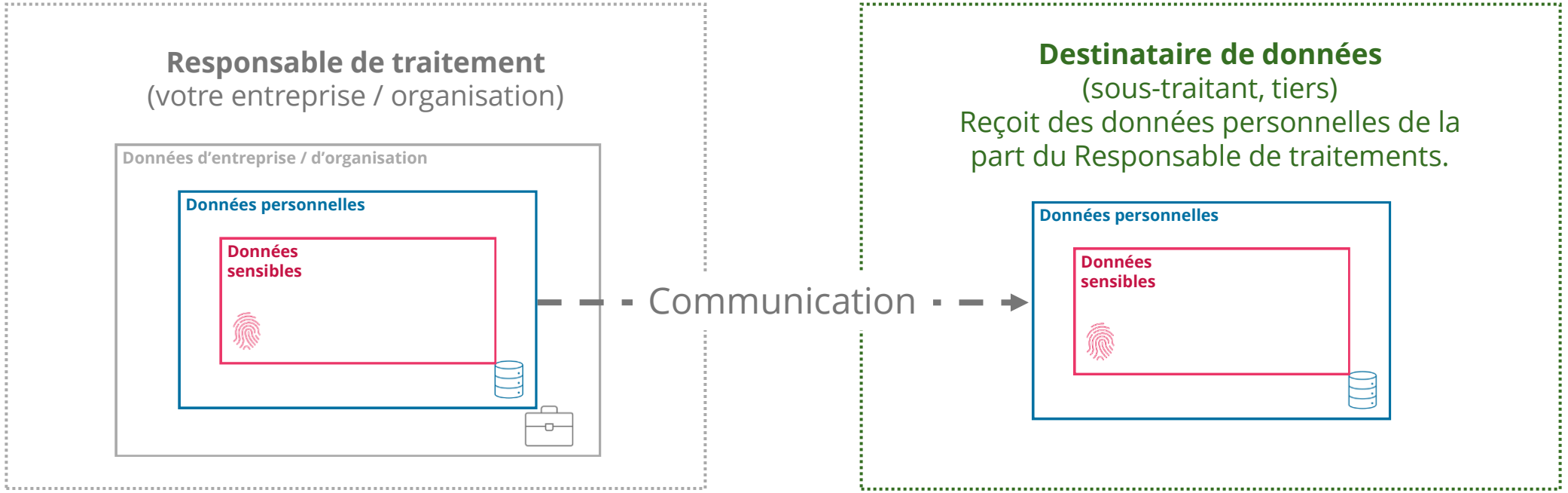
Mesures physiques	Détails	Justificatifs
Stockage des données chez hébergeur	-	Audit_2024.pdf
Serveur local avec protection incendie / inondation	Local fermé à clef	-

Mesures logiques	Détails	Justificatifs
Chiffrement des transmissions	Y compris accès SAAS et backup	Rapport Qualys 2024.pdf
Double authentification	Accès SAAS	-

ETAT DES LIEUX INTERNE

FOURNISSEURS / CLIENTS

- ❑ Liste des fournisseurs / clients
- ❑ Définir la relation : sous-traitant, responsable conjoint, responsable du traitement
- ❑ Identification des fournisseurs ayant un accès potentiel aux données
- ❑ Revue des contrats



ETAT DES LIEUX INTERNE

COLLABORATEURS

Informer

- ❑ Diffuser la Charte d'utilisation des outils informatiques, la Politique interne de protection des données.
- ❑ Gérer les utilisateurs (nouvelle embauche, habilitations, fin de contrat).
- ❑ Mettre à disposition de l'information efficace : aide-mémoire, guidelines, do's and dont's, etc.

Former

Deux publics cibles :

- ❑ Le département IT de l'entreprise
- ❑ L'ensemble des employés

But : dispenser l'information à tous les échelons de l'entreprise, afin que tous les employés soient rendus attentifs aux questions de cybersécurité et de protection des données.

Les employés devraient bénéficier d'une formation tant à leur arrivée que de façon continue, tout au long de leur emploi.

AGENDA

- Contexte
- Concepts et définitions
- Quelques principes
- Mener son projet de mise en conformité
- Etat des lieux interne
- **Commencer par ce qui est visible depuis l'extérieur**
- Respecter les droits des personnes
- Gérer les violations
- Outils de mise en conformité
- Questions

COMMENCER PAR CE QUI EST VISIBLE DEPUIS L'EXTÉRIEUR

Site internet

- ❑ Avez-vous des mentions légales ? Sont-elles à jour ?
- ❑ Avez-vous une politique de confidentialité ?
- ❑ Mettre en place une adresse email de contact pour les questions de protection des données.

Newsletter

- ❑ Quelles données sont collectées et dans quel but ? Qui en a la gestion ?
- ❑ D'où proviennent les adresses ? Avez-vous le consentement ? Le gérez-vous ?
- ❑ Le bouton de désinscription est-il présent ? Fonctionne-t-il ? Où est stockée la liste d'oppositions ?

Extranet

- ❑ Avez-vous une politique de confidentialité / d'utilisation ?
- ❑ L'utilisateur peut-il mettre à jour ses données ?
- ❑ Statut de la sécurité ?
- ❑ Qui gère le site Extranet ?

AGENDA

- Contexte
- Concepts et définitions
- Quelques principes
- Mener son projet de mise en conformité
- Etat des lieux interne
- Commencer par ce qui est visible depuis l'extérieur
- **Respecter les droits des personnes**
- Gérer les violations
- Outils de mise en conformité
- Questions

RESPECTER LES DROITS DES PERSONNES

CONNAÎTRE LES DROITS

Chaque personne concernée dispose de droits afin de garder la maîtrise de ses données personnelles.

Droit d'être informé

Être informé au préalable de toute collecte ou traitement de données qui concerne l'utilisation de ses données personnelles.

Droit de rectification

Faire corriger ses données lorsqu'elles sont inexactes ou incomplètes.

Droit d'opposition

S'opposer à la réalisation d'un traitement précis de ses données personnelles.

Droit d'accès et de portabilité

Accéder à ses données et pouvoir en obtenir une copie.
Recevoir ses données sous format structuré.

Droit à l'effacement

Demander l'effacement de ses données.

Droit à la limitation

Dans l'attente d'une réponse à l'exercice du droit de rectification ou d'opposition, le traitement peut être suspendu.

RESPECTER LES DROITS DES PERSONNES

PROCESSUS DE TRAITEMENT

- ❑ Mettre en place une procédure

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 / planifier l'usage à une extension du délai
- Attention au mode de réponse (papier / digital)

RESPECTER LES DROITS DES PERSONNES

PROCESSUS DE TRAITEMENT

- ❑ Mettre en place la 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
    - Identification de la personne
    - Validation ou refus de la prise en charge
5. Collecte des informations / transmission de la demande de suppression / etc.
6. Vérification des informations collectées / analyse de la suppression / etc.
7. Transmission des informations / quittance de traitement / etc.
8. Conservation des informations transmises, réponse et métadonnée avec durée de conservation adéquates

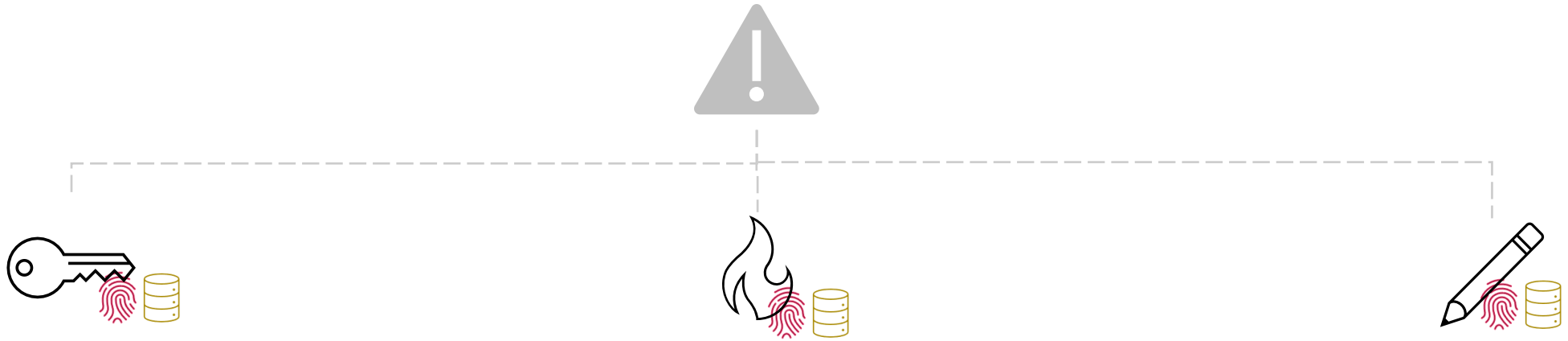
AGENDA

- Contexte
- Concepts et définitions
- Quelques principes
- Mener son projet de mise en conformité
- Etat des lieux interne
- Commencer par ce qui est visible depuis l'extérieur
- Respecter les droits des personnes
- **Gérer les violations**
- Outils de mise en conformité
- Questions

GÉRER LES VIOLATIONS

DÉTECTER

Toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données personnelles, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données.



VIOLATION DE LA CONFIDENTIALITÉ

Divulgation ou accès non autorisé à des données personnelles

VIOLATION DE LA DISPONIBILITÉ

Perte d'accès ou destruction des données personnelles

VIOLATION D'INTÉGRITÉ

Modification non autorisée ou accidentelle des données personnelles

GÉRER LES VIOLATIONS

PROCESSUS DE GESTION

- ❑ Gérer et documenter la violation dès la détection ou la suspicion de survenance d'un incident

Comment faire :

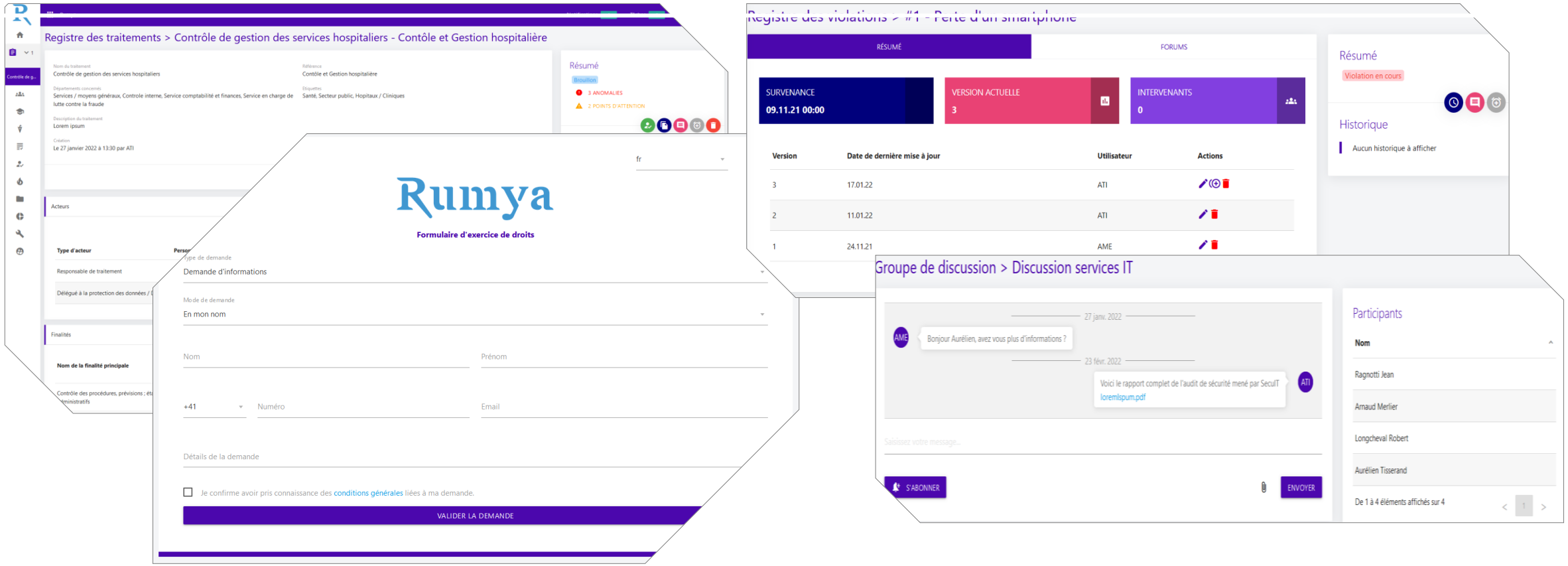
- Avoir définir au préalable une "task force" et des tiers de confiance
- Décrire l'incident
- Détailler la chronologie des évènements.
- Evaluer les traitements les données et les personnes concernées.
- Analyse des mesures en place.
- Evaluation du risque et des conséquences prévisibles.
- Mesures appliquées et actions à venir
- Notifications selon risque évalué
  - Autorités de contrôle
  - Personnes concernées
  - Organismes tiers
  - Responsable de traitement dans le cas d'un traitement en tant que sous-traitant

AGENDA

- Contexte
- Concepts et définitions
- Quelques principes
- Mener son projet de mise en conformité
- Etat des lieux interne
- Commencer par ce qui est visible depuis l'extérieur
- Respecter les droits des personnes
- Gérer les violations
- **Outils de mise en conformité**
- Questions

OUTIL DE MISE EN CONFORMITÉ LPD / RGPD

Registres | Exercice de droits | Consentements | Violations



QUESTIONS & CONCLUSION

Merci pour votre participation.
Avez-vous des questions ?