AmbiCio
L'AMBITION CENTRÉE CLIENT

DPOview V2

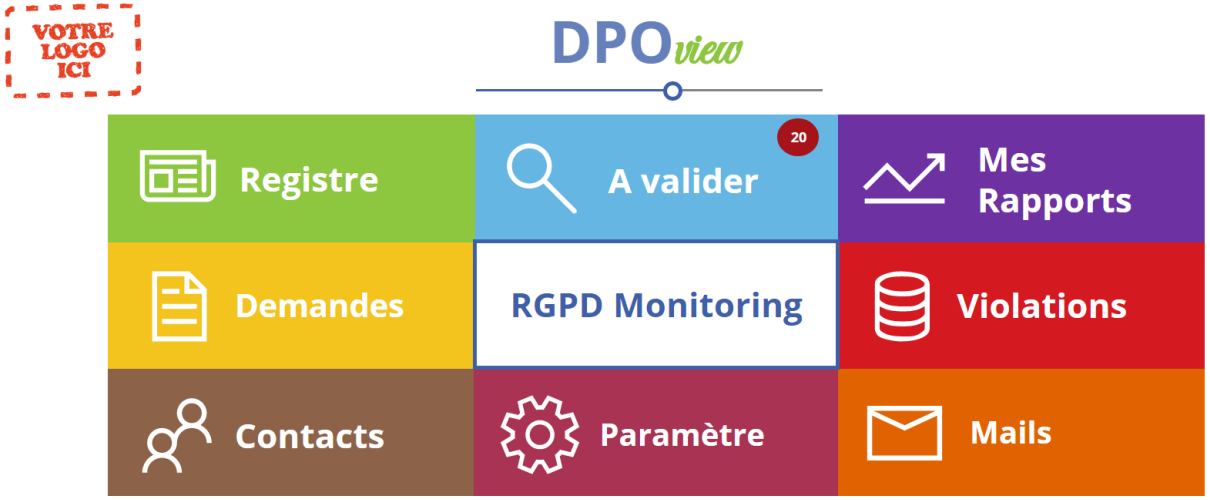
Document V1.6
sept 2019

François BOURGOGNON – Associé
fbourgognon@ambicio.fr
06 86 37 82 38

AmbiCio
140 bis rue de Rennes
75006 PARIS

Couverture fonctionnelle existante V2

Un outil pour DPO pensé par des experts du SI et des avocats



1- Gestion du Registre des traitements	2- Scorecard sensibilité et avancement de la conformité	3- Gestion des droits des personnes
4- Workflow de validation	5- Reporting	6- Top priorités des traitements
7- Personnalisable Multilingue	8- Gestion des fichiers joints	9- Gestion des acteurs/contacts (basique)
10- Gestion des violations de données	11- Gestion des demandes	12 – Accompagnement PIA et plan d'actions
13 – Accompagnement PIA et plan d'actions	14 – Historisation et Audit des modifications	15 – Gestion du dictionnaire des données

Présentation des fonctionnalités

1- Gestion du Registre des Traitements
Saisie, modification et représentation graphique des données relatives aux personnes et encadrées par le RGPD
Pilotage des droits des personnes pour chaque traitement
Avancement de la conformité du traitement (7 étoiles correspond à la validation technique et juridique complète du traitement)
Niveau de sensibilité de chaque traitement (Cf. RG Scorecard Sensibilité)
Attachement de Fichiers externes
Déclaration des contacts et de leur rôle (Hors UE inclus)
Outil d'analyse des risques
2- Scorecard Sensibilité et Avancement de la Conformité
<u>Exposition au risque de l'entreprise</u> : Niveau de 0 à 100 Données sensibles : 20pts Sous-traitants : 5pts par sous traitants (seuil à 20) Exposition extérieure (site-web, source de plaintes…) 20pts Licéité : 20pts Importance de la sécurité à mettre en place : 20pts
<u>Avancement de la conformité</u> : Niveau de 0 à 100 Droits : 25pts Licéité : 25pts Sécurité (IT/PSS) : 25pts Contrats (partenaires/sous-traitants) : 25pts

Présentation des fonctionnalités

3- Gestion des droits des personnes pour chaque traitement
Droit de rectification : Si des données sont erronées, la personne concernée peut les faire corriger dans les meilleurs délais
Droit à la limitation du traitement : les données sont « gelées » pendant un temps nécessaire (ex: si les données sont inexactes, le temps que la correction soit appliquée)
Droit à la portabilité : disposer des données dans un format structuré afin de les communiquer à une autre enseigne
Droit à l'effacement (droit à l'oubli) : effacement des données et déréférencement des données sur un moteur de recherche (ex : consentement retiré, traitement illicite…)
Droit à l'information : informer les personnes lorsqu'il y a un traitement (Articles 13 et 14)
Droit d'opposition : s'opposer à un traitement des données personnelles (motif légitime). Droit d'opposition au profilage (PIA préalable obligatoire).
4- Workflow de validation
3 profils par défaut : DPO / Juridique / SI (Informatique)
Le DPO a tous les droits
Le profil Juridique est chargé de valider les "blocs" juridiques et le profil SI de la même manière doit valider les "blocs SI".
Liste de tâches créés par le DPO avant de demander la validation du traitement

Présentation des fonctionnalités

5- Reporting - Affichage des KPIs (Maison Mère et Filiales)
Nb de traitement Validé par entité
Nb de traitement Validé au global
Taux d'avancement de la mise en conformité par entité
Taux d'avancement de la mise en conformité au global
Visualisation graphique du niveau de risque d'une entité
Visualisation graphique du niveau de risque au global
Matrice d’analyse des risques
6- Top priorités des traitements
Les 3 traitements à traiter qui représentent la plus grande sensibilité (cliquable)
7- Personnalisation Multilingue
Version fournie avec les langues français / anglais.
Ajout d’une nouvelle langue possible sur demande
8- Gestion des fichiers joints
Tout type de fichier (PDF, Excel, Word…..) peut être ajouté à la fiche de traitement

Présentation des fonctionnalités

9- Administration et Gestion des acteurs / contacts (version Basique)
Création des utilisateurs (rattachement à une filiale)
Annuaire des utilisateurs de toutes les entités disponibles
Annuaire des utilisateurs par entités disponibles
5 profils utilisateurs prévus par défaut
Accès par l'administrateur avec 1 seul login/password pour accéder aux différentes entités
Accès par l'utilisateur avec 1 seul login/password pour accéder aux différentes entités auxquelles il est autorisé à accéder
Possibilité de Création d'activité/Service par l'administrateur (DPO par exemple) sans intervention externe
10- Gestion des violations de données
Préparation et validation en interne du formulaire de déclaration de violation à la CNIL
Accompagnement de l'utilisateur dans les démarches en ligne
11- Gestion des demandes
Réception de mail dans l'application, identification des potentiels demande & validation de la création d'une demande
Le DPO pourra gérer les demandes provenant du RSSI et du juridique (éventuellement équipe MOA)

Présentation des fonctionnalités

12- Accompagnement PIA et plan d'actions
70 % du process est fusionné avec la déclaration du traitement
En saisie optionnelle, l'onglet « Risque » permet de finaliser le PIA lié à un traitement.
Workflow de génération du plan d'actions soumis au comité de gouvernance pour validation et/ou demande de détails.
13- Historisation et Audit des modifications
Toutes les modifications intervenant sur les registres sont enregistrées et protégées contre l'effacement.
L'administrateur/DPO peut suivre toutes les modifications réalisées au niveau groupe/filiales.
14- Gestion des demandes
DPOview échange avec le compte Microsoft DPO en temps réel afin de remonter les actions à réaliser
er Transformation d'unn mail en Demande dans l'application
15- Gestion du dictionnaire des données
Mise à disposition dans DPOview de données et support "type" (Exemple : Nom, prénom, fiche de salaire…), intégrant des règles de gestion spécifiques (temps de conservation conseillé avant archivage/purge, alerte de sensibilité,…)
L'utilisateur peut relier son dictionnaire de données manuellement ou automatiquement.
Création d'un champ Custom par le client (droit donné à l'administrateur).

Couverture fonctionnelle à venir V3

Disponibilité fin Q4 2019

16- Gestion des acteurs/contacts (Avancée)

17- Gestion des services (IT et Juridique)

18- Aide contextuelle en ligne

19- Création d'un plan d'actions (suite à une violation de données)

Présentation des fonctionnalités

16- Gestion des acteurs/contacts (Avancée)
Catégorisation des contacts sur 2 niveaux (Exemple : Prestataire RH/Sté de chasseur de tête)
Ajout des services internes de l'entreprise dans la liste des acteurs d'un traitement.

17 – Gestion des services (IT et Juridique)
Support sollicité via l'envoi des messages (ou d'appels téléphoniques) à travers les logos (Ex : AmbiCio – SI et Cabinet d'avocats – Juridique)
En option, "DPOview for lawyer" permet d'inclure un support juridique dans votre DPOview.

18- Aide contextuelle en ligne
Aide disponible sur les différentes fonctions du Logiciel : "i"
Disponibilité des textes "RGPD" liés à la tâche sur laquelle on est situé

19- Création d'un plan d'actions
Suite à une déclaration de violation de données

Architecture de l’application - Mode Saas

- **L’application** DPOview est une application de type « PowerApps », intégrée à l’environnement Office 365 de Microsoft.
  - Une instance dédiée de l’application sera mise en place.
  - Les utilisateurs de DPOview seront intégrés à l’ActiveDirectory d’AmbiCio.
  - AmbiCio se porte garant de la sécurité mise en œuvre, une authentification forte étant mise en place étant donné la sensibilité potentielle des informations pouvant êtres saisies.
- **La base de données** utilisée est également fournie par Microsoft, il s’agit du Common Data Service (CDS)
  - La gestion des accès est directement liée à la politique de gestion des accès d’AmbiCio.
  - Un backup des données est opéré tous les jours (la nuit), et est conservé pendant une durée de 30 jours.
  - Vous êtes seul propriétaire de ces données, AmbiCio s’engage à ne pas en exploiter le contenu et à mettre en œuvre tous les moyens permettant de garantir la confidentialité celles-ci.

Architecture de l'application – On Premise

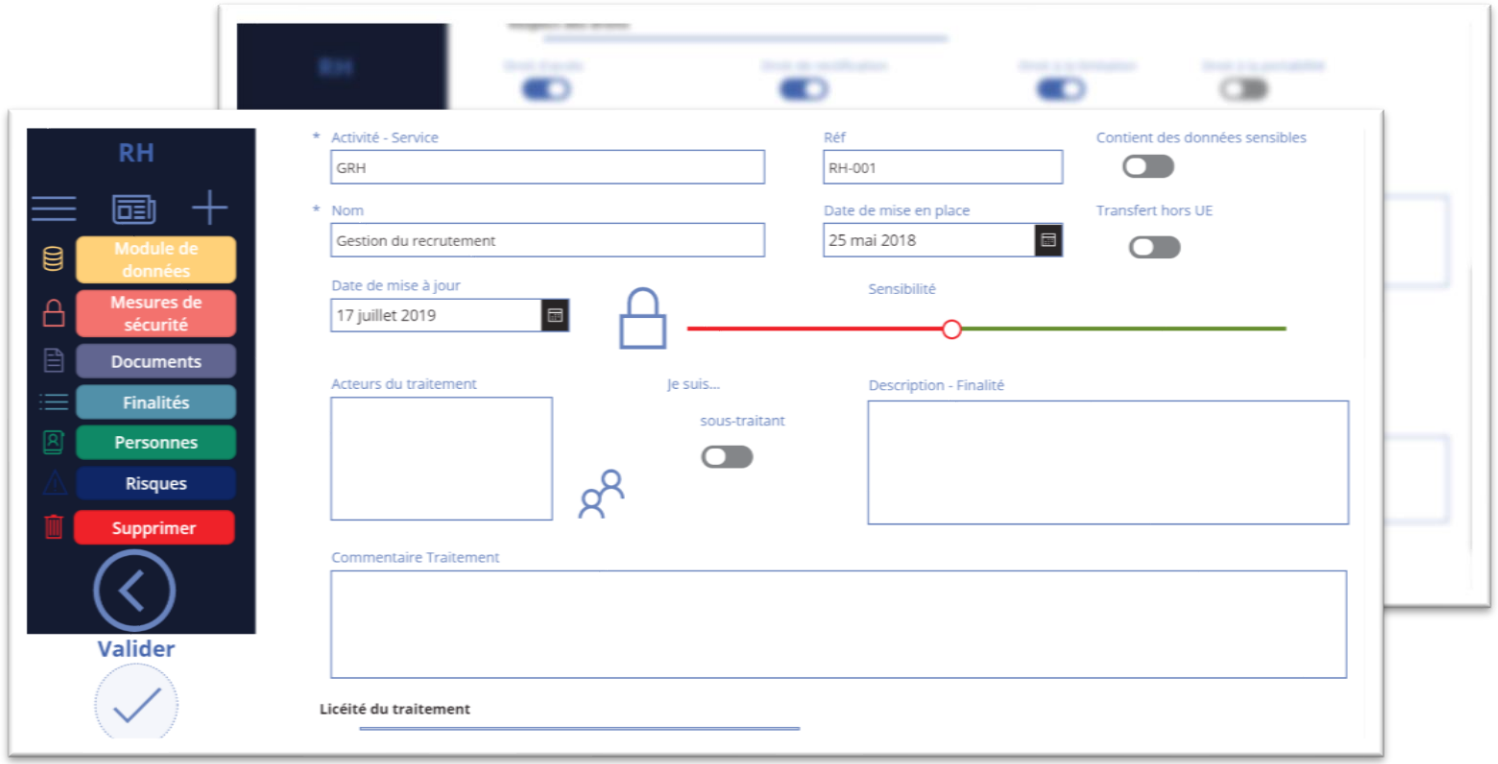
- **L'application** DPOview est une application de type « PowerApps », intégrée à l'environnement Office 365 de Microsoft.
  - Une instance hébergée par l'entreprise cliente et dédiée à l'application sera utilisée
  - Des licences PowerApps Plan 1 peuvent être nécessaires, en fonction du plan office souscrit par l'entreprise cliente
  - La gestion des accès sera gérée directement par l'entreprise cliente, via Active Directory
- **La base de donnée** utilisée est également fournie par Microsoft, il s'agit du Common Data Service (CDS)
  - La gestion des accès et des données est directement liée à la politique de gestion des accès de l'entreprise.
    - Ex : Réalisation d'un backup des données tous les jours (la nuit), et conservation pendant une durée de 30jours.
  - Une licence PowerApps Plan 2 peut être nécessaire, en fonction du plan office souscrit par l'entreprise cliente.

Gestion du Registre des traitements DPOview

Classement personnalisé selon votre Organisation

Navigation intuitive

Interface adaptée à un usage tactile



Une vision détaillée du traitement et de son état de conformité

Reporting DPOview

Un maximum d'informations sur un seul écran, directement présentable en comités

Compatibilités DPOview

Restez mobile sans contraintes matérielles !

IOS

MacOs

Android

Windows

Windows Phone

Navigateurs Web

Gouvernance - Privacy by design recommandé par AmbiCio

Cette démarche répond à la notion de « privacy by design » du RGPD. Elle est toutefois, également conseillée dans le cadre de la gouvernance du SI de l'organisation. Cela permettra une meilleure maitrise des coûts, des risques et de la stratégie d'entreprise.

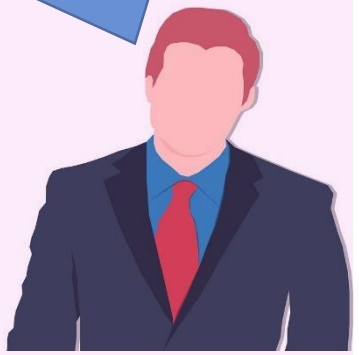
Comité RGPD (2 fois/mois)

Comité durant lequel, des chefs de projets, manager… pourront soumettre leur demande de mise en place de nouveaux traitements sur les DCP.

DPO : S'assure de la conformité RGPD
RSSI : Garant de la sécurité du SI
Qualité : Gouvernance, référentiel ISO
PMO : Vision globale des chantiers
Juridique : Référentiel légal à respecter

Cette démarche devra être amorcée par le DPO.

Je souhaite mettre en place un nouveau traitement, mais il me semble que je touche à de la DCP



PIA light

Nécessite de fournir un PIA ?

NON

La mise en place du traitement peut continuer, mon PIA light a permis au comité de référencer mon traitement.

OUI

Alors je dois construire un PIA avec le soutien du comité

Présentation synthétique de DPOView

- L'application DPOView a pour objet principal de recenser les différents traitements de données personnelles de l'entreprise et les classer par filiales, directions et services. Un traitement est le nom qui est donné à un processus d'entreprise en ayant une approche plutôt juridique. La première étape dans l'utilisation de DPOView est donc la déclaration des différents traitements dans l'application. Une fois cette phase terminée DPOview devient un outil de pilotage qui permet de mettre en œuvre et suivre la mise en conformité de l'organisation face au RGPD.
- L'outil DPOview est basé sur le module PowerApps de Microsoft. C'est une technologie qui a pour avantage de faciliter la création d'application Cross Platform en reposant sur le principe de container d'application. Ce qui a pour but de rendre DPOview disponible sur Android, IOS et navigateur internet, en minimisant les efforts de développement. La plateforme PowerApps a également été choisie grâce à la facilité de production d'une application professionnel rapide.
- De plus, notre partenariat avec Microsoft et l'inscription de DPOView à leur Market Place va permettre de relayer notre offre vers les clients et prospects Microsoft.

Les fonctions clés de DPOView

- La gestion des registres et des fiches de traitement
- La pré-catégorisation des risques sur la Protection des Données
- La génération automatique de rapports et de dashboard,
- Le pilotage global de la mise en conformité au RGPD
- La Cartographie et le suivi des mesures juridiques et techniques
- La gestion des demandes d'exercice des droits des personnes
- La gestion des violations de données conformément aux exigences du RGPD
- L'adaptation de l'outil aux structures complexes en permettant de répondre aux besoins suivants:
  - Bénéficier d'une gestion collaborative basée sur un workflow capable d'engager quand cela est nécessaire les rôles qui ont des responsabilités
  - Mener des analyses (DPIA) sur la base de la méthodologie CNIL
- La gestion de l'approche et des processus relatifs à la Privacy by Design et la Privacy by Default
- La mise en place d'une gestion et d'une gouvernance des sous-traitants, de la qualification du sous-traitant jusqu'à l'audit des mesures de conformité et de sécurité.

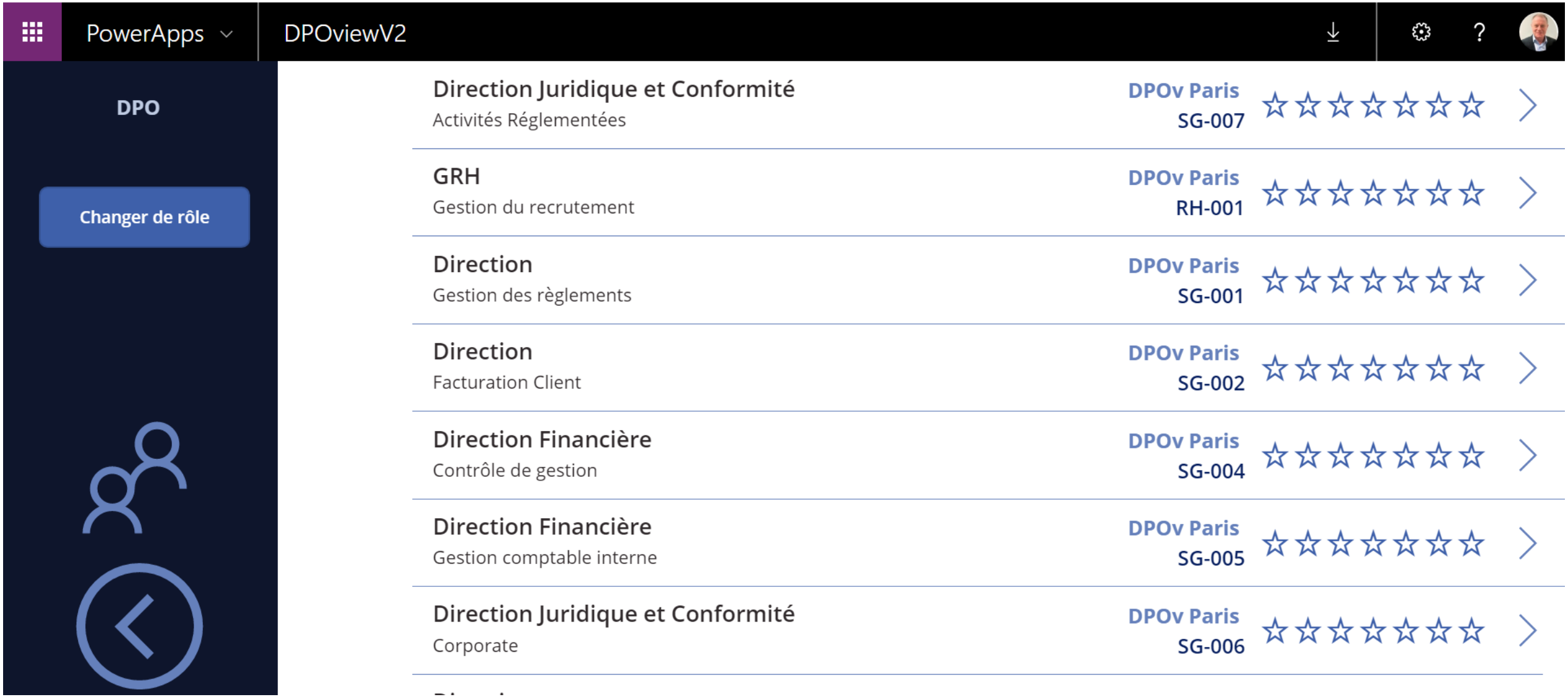
DPOView soumis aux critères d'évaluation suivants :

- Ergonomie ★★★
- Multilingue ★★ + Langue supplémentaire à la demande
- Multi-utilisateurs / Multi-entité ★★★★
- Déploiement (On Premise ou/et Saas) ★★★★
- Confidentialité ★★★★ PowerApps hébergé par Microsoft
- Evolution de l'outil ★★★★
- Registre des activités de traitement ★★★
- DPIA / PIA ★★★★
- Cartographie des données ★★
- Workflow et Reporting ★★★★
- Gestion des droits des personnes ★★
- Gestion du consentement ★★

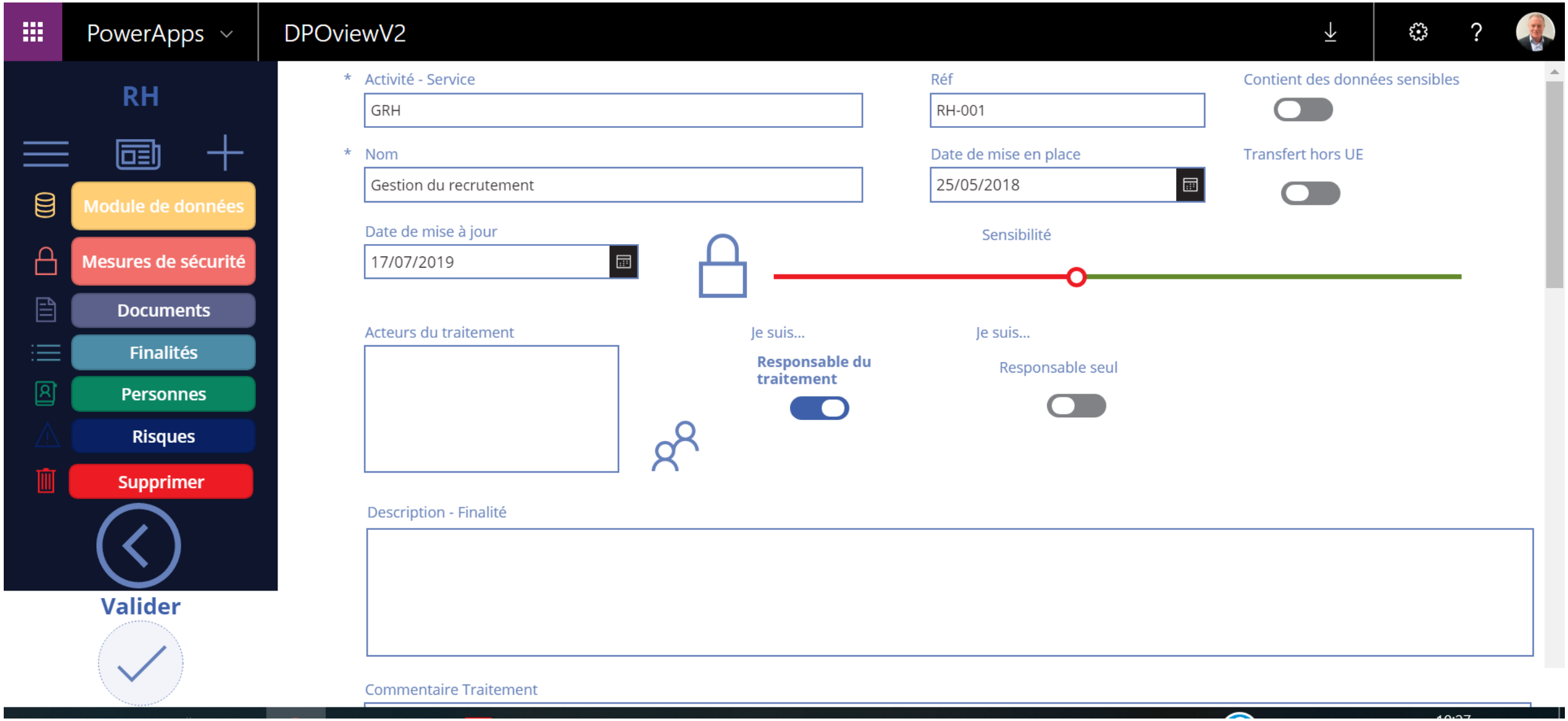
Les éléments différenciants de DPOView

- Solution Franco-française basée sur l'expérience acquise en missions d'audit (Références : RAJA avec 18 filiales européennes, Cyrus Conseil….) avec des Avocats spécialisés
- Héritage et bénéfice de l'infrastructure Microsoft (base de donnée, sécurisation des accès via Active Directory, authentification forte, libre exploitation des données dans Power BI de Microsoft)
- Formation très rapide : 2h par utilisateur et 3h par DPO dans le cas de filiales
- Gestion de plusieurs filiales d'un groupe
- Intégration de la collaboration avec un service Juridique
- Tous les référentiels de l'outil sont personnalisables
- AmbiCio met à disposition des clients un dictionnaire de données prérempli
- DPOView est complémentaire avec les outils de gouvernance des données tels que Meta Analysis de Synergy, MEGA et autres. Il peut être utilisée en mode stand alone.
- Coût mensuel par utilisateur à estimer au cas par cas. Hors prestation de setup.

Captures d’écran DPOView : Les traitements en attente



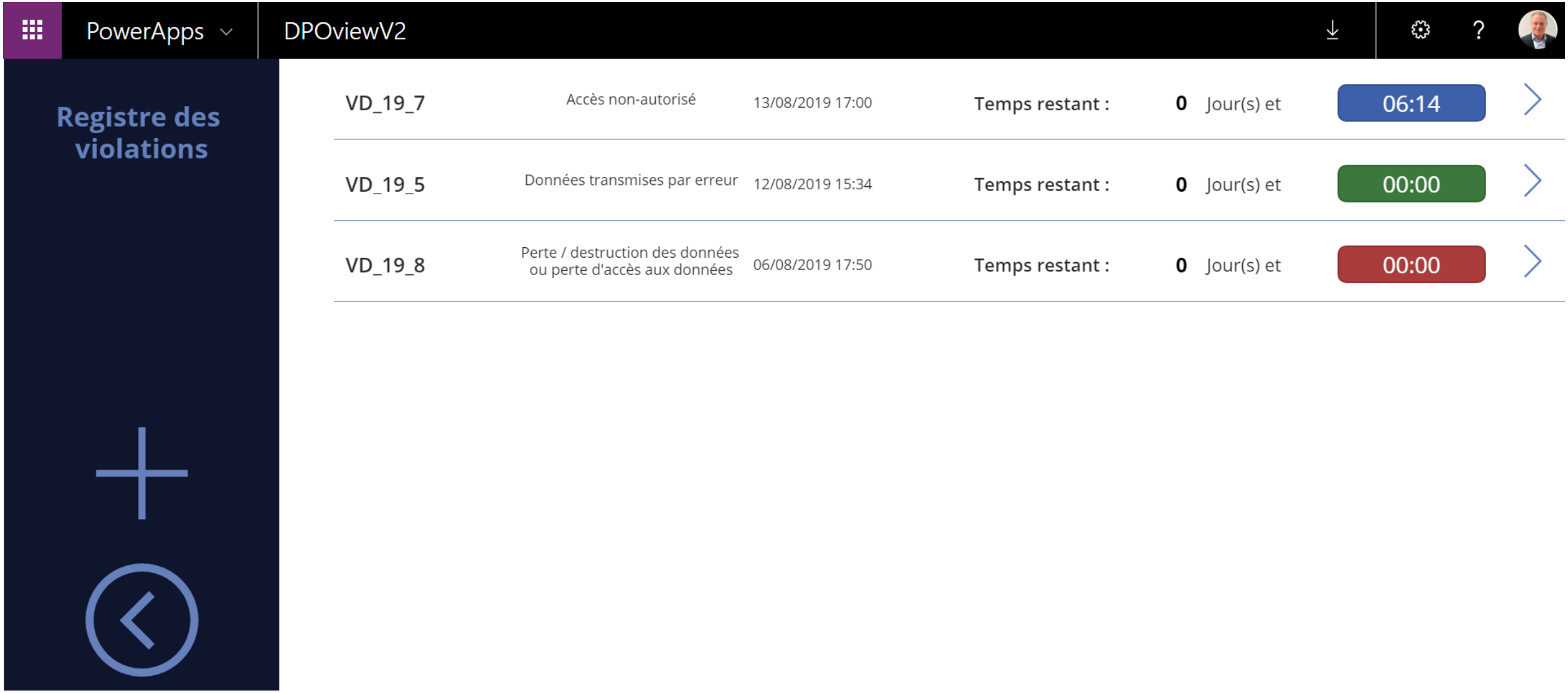
Captures d’écran DPOView : gestion d’un traitement



Captures d’écran DPOView : Sélection des critères pour un PIA

Captures d’écran DPOView : Cartographie des Risques

Captures d’écran DPOView : Gestion du registre des violations



Captures d’écran DPOView : Reporting des indicateurs