« RGPD : La maîtrise du risque juridique / réglementaire »

10 avril 2018

@BonnetFlorence
florence.bonnet@tnpconsultants.com

TNP
ACCÉLÉRATEUR DE PERFORMANCE

CIL CONSULTING by TNP
Conseil en protection des données

Etat d’avancement des entreprises à J-44

Etat d'avancement des entreprises à **J-44**

- **Le niveau de maturité varie en fonction de la taille**
  - **Acteurs de taille moyenne :** du diagnostic au plan d'action
  - **Gros acteurs tous secteurs confondus** : Phase mise en conformité et choix d'outils

Marché français (IDDC/Syntec Numérique)

- **42 %** des entreprises prennent tout juste conscience des implications du RGPD.
- **9%** considèrent être déjà en conformité avec ces nouvelles règles.
- **50% assurent qu'elles le seront d'ici à la fin de l'année ou en 2018.**

Marché EMEA (Deloitte)

- **45%** des organisations interrogées ont mené un diagnostic de conformité GDPR
- **40% disent envisager l'utilisation d'outils de cartographie des traitements**

De manière générale, il y a eu une sous-estimation de la complexité du GDPR et de ses impacts

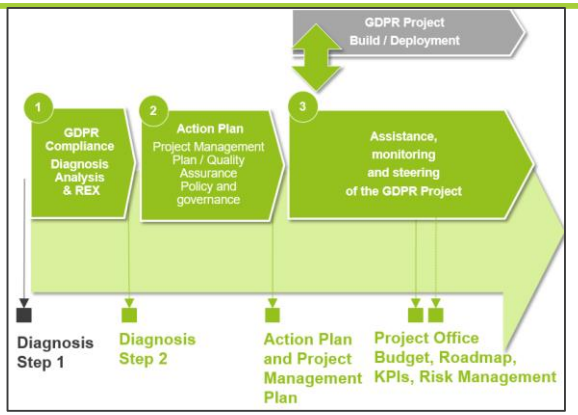
Comment se mettre en conformité avec le GDPR

Comment se mettre en conformité avec le GDPR

DEMARCHE PROPOSEE PAR LA CNIL

Etape 1:
Désigner un DPO comme pilote de la mise en conformité.

Etape 1:
- Désigner un sponsor
- Désigner un référent ou un DPO
- Sensibiliser
- Piloter le projet de mise en conformité



Etape 2:
Cartographier les traitements de données personnelles

Etape 2:
- Etablir et documenter une liste des traitements par finalités

Etape 3:
Prioriser les actions

Etape 3: :
- Evaluation des écarts de conformité
- Analyse des risques liés aux traitements sur les libertés et les droits fondamentaux (gravité + vraisemblance)

Stream	Mesures	Disponibilité des ressources	Date cible	Difficulté	Charge estimée j/h	Avancement
Stream 2 : Information des personnes	Mesure 1: Terminer la mise à jour des mentions d'informations clients et prospects sur les supports en ligne: Registration card,Questionnaire préférences, IBE, sites CB, W, LP (version longue et courte) et sur les formulaires papier (formulaires SPA, questionnaire préférence CB)	Oui	Le 25 mai 2018	Negligeable	5	☺
	Mesure 2: Vérifier l'information des clients en présence de caméras de vidéosurveillance	Oui	Sans délai	Negligeable	2	😐
Stream 3 : Contrats tiers et sous-traitants y compris transferts hors UE pour les contrats en cours	Mesure 1: Mettre à jour les contrats des fournisseurs en priorisant ceux à fort enjeux pour la protection des données	Oui avec difficultés	Le 25 mai 2018	Elevée	7	☹
	Mesure 2: Mettre à jour les contrats des TA/TO	Externe indispensable	Le 25 mai 2018	Elevée	10	☹
	Mesure 3: Vérifier les garanties de sécurité proposées par les prestataires	Externe indispensable	Le 25 mai 2018	Elevée	15	☹

CIL CONSULTING by TNP

Comment se mettre en conformité avec le GDPR

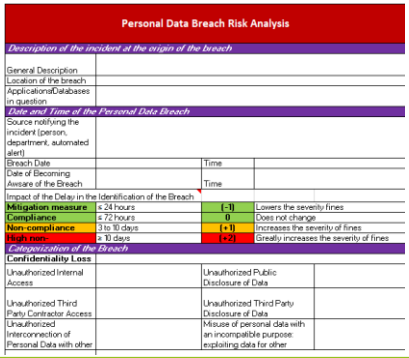
DEMARCHE PROPOSEE PAR LA CNIL

Etape 4:
Gérer les risques sur les droits et libertés des personnes (non-conformité et sécurité)

Etape 4:
- Prioriser les actions en fonction des risques
- Traiter les risques identifiés et les réduire à un niveau acceptable,
  - Mesures juridiques
  - Mesures organisationnelles
  - Mesures techniques
  - Mesures de sécurité

Etape 5:
Organiser les processus internes

Etape 5:
- Information des personnes
- Gestion du consentement
- Gestion des droits des personnes
- Gestion des violations de données



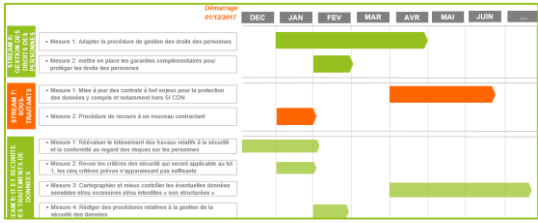
Personal Data Breach Risk Analysis

Description of the incident at the origin of the breach

General Description			
Location of the breach			
Applications/Databases in question			
Date and Time of the Personal Data Breach			
Source notifying the incident (person, department, automated alert)			
Breach Date		Time	
Date of Becoming Aware of the Breach		Time	
Impact of the Delay in the Identification of the Breach			
Mitigation measure	≤ 24 hours	(-1)	Lowers the severity fines
Compliance	≤ 72 hours	0	Does not change
Non-compliance	3 to 10 days	(+1)	Increases the severity of fines
High non-	≥ 10 days	(+2)	Greatly increases the severity of fines
Categorization of the Breach			
Confidentiality Loss			
Unauthorized Internal Access		Unauthorized Public Disclosure of Data	
Unauthorized Third Party Contractor Access		Unauthorized Third Party Disclosure of Data	
Unauthorized Interconnection of Personal Data with other		Misuse of personal data with an incompatible purpose: exploiting data for other	

Etape 6:
Documenter la conformité

Etape 6:
- Définir la gouvernance de la protection des données
- Constituer et regrouper la documentation nécessaire à garantir le maintien en conformité et à en apporter la preuve: politiques, procédures, analyse d'impact, code de conduite, certification…
- KPI conformité et risques



Comment se mettre en conformité avec le GDPR

LES ÉTAPES DU DIAGNOSTIC GDPR

- Cadrage
- Cartographie des traitements et des applications
- Evaluation des écarts de conformité et des principaux risques
- Recommandations et plan d'actions

PILOTAGE DE LA MISE EN CONFORMITÉ & ASSISTANCE

- Définition De la gouvernance du projet
- Définition du plan projet
- Assistance, pilotage, suivi
- Vérification de la mise en place des actions

CIL CONSULTING by TNP

Faut-il utiliser un outil logiciel pour être en conformité avec le GDPR?

Faut-il utiliser des outils logiciels pour se mettre en conformité?

LISTE DES TRAITEMENTS RH

Réf. du Trait.	Finalités	Personnes concernées	Données traitées	Destinataires	Transferts vers un état tiers	Durée de conservation	Commentaire
TRM-01	Identification de l'employé	Salariés	- identité : nom, prénom, photographie, sexe, date et lieu de naissance, nationalité, coordonnées professionnelles, coordonnées personnelles, matricule interne, références du passeport (uniquement pour les personnels amenés à se déplacer à l'étranger) ; - type, numéro d'ordre et copie du titre	- les personnes habilitées chargées de la gestion du personnel ; - les supérieurs hiérarchiques des employés concernés, à l'exclusion des données relatives à l'action sociale directement mise en oeuvre par l'employeur ; - les instances représentatives du personnel : après recueil de l'accord exprès des intéressés, coordonnées professionnelles des employés et données strictement		Temps de la période d'emploi de la personne concernée (sauf dispositions législatives ou réglementaires contraires). Au-delà, archivage possible sur support	

LOGO

4 - RISK ASSESSMENT AND DPIA

The **Risk assessment and DPIA** tab is the tool with which the IT Project Manager will make risk analysis and the DPIA if decided in the Data Privacy Focus (option) tab. One risks are assessed, countermeasures must be selected to reduceavoidtransfer the risks (reude impact or likelihood). It's an iterative approach. Measures must be added until residual risk is acceptable. This sheet is divided into two main parts :

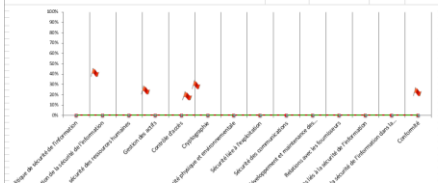
1. **Top risks (cyber and privacy)**
The IP Project Manager gives a list of top risks and associated threat scenarios, description and scoring of the potential impacts from a coporate point of view and from the subjects point of view (for DPIA), assess likelihood and calculates risk score.
2. **Security controls**
The Project Manager has to list all the countermeasures : those already implemented (transversal) and the specific measures to reduce the risks identified above.

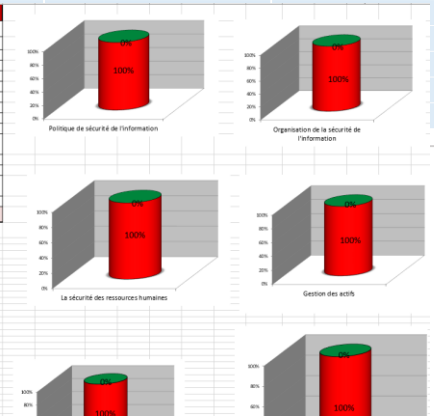
TOP RISKS (CYBER AND PRIVACY)

Risk id	Risk description	Due to... Threat scenarios	Type of risk	Impact description of cyber risk (company's perspective if applicable)	Impact level (1: none or low, 2:medium, 3:high, 4:very high)	*To be filled if DPIA required* Impact description of privacy risk (subjects' privacy perspective if applicable)	Impact level (1: none or low, 2:medium, 3:high, 4:very high)	Likelihood (1: very low, 2:low, 3:medium, 4:high)	Global risk value (1 to 16)	Global risk level (severity: LOW, MEDIUM or HIGH)	Residual risk accepted
R1									0	LOW	
R2									0	LOW	
R3									0	LOW	
R4									0	LOW	
R5									0	LOW	
									0	LOW	
									0	LOW	
									0	LOW	
									0	LOW	

2017

Site 1	Niveau d'application	Niveau à atteindre	Ecart	Niveau Acquis	Reste à couvrir
Politique de sécurité de l'information	0%	0%	0%	0%	100%
Organisation de la sécurité de l'information	0%	0%	0%	0%	100%
La sécurité des ressources humaines	0%	0%	0%	0%	100%
Gestion des actifs	0%	0%	0%	0%	100%
Contrôle d'accès	0%	0%	0%	0%	100%
Cryptographie	0%	0%	0%	0%	100%
Sécurité physique et environnementale	0%	0%	0%	0%	100%
Sécurité liée à l'exploitation	0%	0%	0%	0%	100%
Sécurité des communications	0%	0%	0%	0%	100%
Acquisition, développement et maintenance des systèmes d'information	0%	0%	0%	0%	100%
Relations avec les fournisseurs	0%	0%	0%	0%	100%
Gestion des incidents liés à la sécurité de l'information	0%	0%	0%	0%	100%
Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	0%	0%	0%	0%	100%
Conformité	0%	0%	0%	0%	100%
Niveau d'exigence de sécurité globale	0,00%	0,00%	0,00%	0,00%	100,00%





Des outils, oui… mais jusqu'à présent, surtout des outils excel

Faut-il utiliser des outils logiciels pour se mettre en conformité?

NOS PRINCIPAUX CONSTATS

- **Avant d'investir dans un outil, analyser le besoin de votre organisation suivant sa taille, la complexité de ses traitements, les ressources disponibles**

- **Etat du marché des outils :**
  - explosion du nombre d'outils « GDPR » ,
  - éclosion de nombreuses solutions Saas à destination des TPE/PME,
  - amélioration du niveau de maturité des solutions de registre,
  - alliances entre acteurs offrant des solutions complémentaires

- **La mise en conformité GDPR présente des enjeux en terme de:**
  - Conduite du changement
  - Gestion de projet
  - Gestion des risques
  - Pilotage du maintien en conformité
  - Sécurité

  } **Quels outils?**

- **Un outil, pour quoi faire?**
  - Outils de documentation des traitements: registre et DPIA
  - Outils de cartographie des données
  - Outils de workflow et de GRC
  - Outils de gestion des consentements
  - Outils de pseudonymisation et d'anonymisation
  - Outils de sécurité ….« GDPR »
  - Outils de sensibilisation et formation

CIL CONSULTING by TNP

Faut-il utiliser des outils logiciels pour se mettre en conformité?

- **Dans les organisations complexes ou avec de nombreux traitements évolutifs, il semble difficile de garantir le maintien, la documentation et le contrôle de la conformité dans le temps sans l'aide d'outils logiciels.**

- **Selon les cas, le développement de solutions en interne ou l'adaptation d'une solution déjà utilisée sera un choix plus pertinent que le recours à un outil supplémentaire.**

- **L'outil ne sera d'aucune utilité si personne ne sait ou ne veut l'utiliser :** les modalités de formation au nouvel outil sont un élément essentiel à prendre en considération.

- **Il n'existe pas d'outil miracle garantissant à lui seul la conformité des traitements de données au GDPR**

- **Lancer le déploiement de l'outil sur un périmètre cible , dans un délai déterminé et avancer par étape avant de prendre toutes les options.**

- **Le GDPR n'est que la face immergée de l'iceberg**

Etat des lieux des outils DPO/GDPR…

Etat des lieux des outils DPO/GDPR…

Objectifs:

- Analyser l'offre à destination des
- entreprises et des DPO;
- Aider les entreprises à y voir plus clair,
- Séparer le bon grain de l'ivraie…

► **Au regard de l'état d'avancement du marché, focus sur les outils de registre ++++**

- Pas d'évaluation d'outils répondant à une seule problématique spécifique
- Ou répondant à une problématique non spécifique au GDPR: ex. GRC

► **Mais il existe aussi:**

- Les outils de **gestion du consentement**
- Les **outils sécurité**:
  - Anonymisation/pseudonymisation/masquage de données,
  - Analyse des risques sécurité,
  - Contrôles d'évènements et suivi de comptes à privilèges
  - Détection et prévention des failles

Etat des lieux des outils DPO/GDPR…

Nos critères d'évaluation:

Critères liés à la nature de l'outil:

- **Ergonomie** : facilité d'utilisation de l'outil et lisibilité des représentations
- **Multi-langue** : outil / solution disponible en plusieurs langues
- **Multi-utilisateurs / multi-entité** : gestion des accès, des droits et des habilitations
- **Déploiement** (On-premise ou SaaS ou les deux)
- **Confidentialité**
- **Evolution de l'outil**

Critères liés aux fonctionnalités de l'outil

	Exigences GDPR	Outil de registre	Analyse des risques et DPIA	Identification des données	Workflow	Sensibilisation/ Formation	Gestion des droits des personnes	Gestion du consentement
Accountability (Art. 24)	Mise en place des mesures pour s'assurer et être en mesure de démontrer que le traitement est conforme (Art. 24)	✓	✓	✓	✓	✓	✓	✓
	Contrôler le respect du règlement et de toutes règles de protection des données applicables (Art. 39)			✓	✓	✓		
	Tenir un registre des activités de traitement (Art. 30)	✓		✓				
	Evaluer les risques et mener une analyse d'impact (Art. 25, 32, 35, 39)		✓					
	Gérer le consentement et les demandes d'exercice des droits des personnes concernées (Art. 7,12 à 21)						✓	✓

Etat des lieux des outils DPO/GDPR…

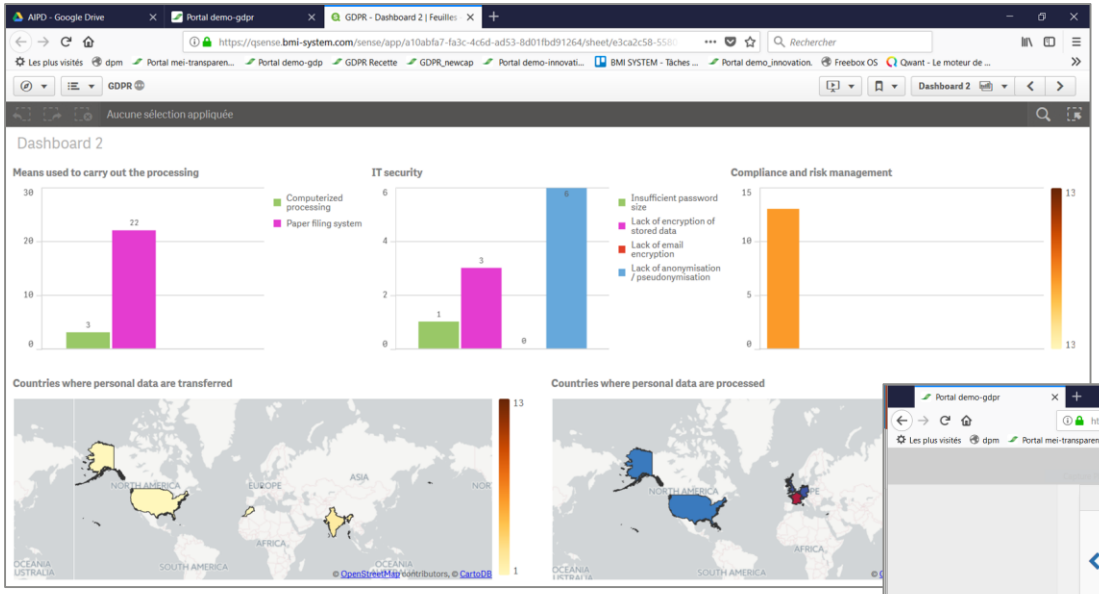
- Outil de registre
  - DPM by Lexagone
  - Captain DPO
- Outil de registre amélioré avec génération de rapports: DPIA, gestion des violations de données..
  - DPO ORGANIZER
  - PRIVACIL
  - TRUST ARC
- Outil de GRC et de workflow: gestion de la phase de diagnostic, d'implémentation (projet) et de maintien en conformité (plan d'actions, attribution et suivi des tâches): ex. gestion des éléments déclencheurs d'analyse d'impact, documentation des audits, envoi de questionnaires aux sous-traitants, gestion des incidents de sécurité..
  - SERVICE NOW
  - TESSI
  - Outils de GRC intelligents
    - KENZU
- Outils d'exploration, d'identification et de classification des données structurées et non structurées pour y associer ensuite des actions de limitation, de suppression, d'anonymisation…
  - Suite logicielle IBM
  - VARONIS
  - INFORMATICA
  - VERITAS
  - D.Day Labs,
  - EXONAR
  - INDICA
  - INTEGRIS
  - PRIFENDER
- Outil d'analyse détaillée du code source des applications et formatage des informations extraites dans des outils d'aide à la décision
  - CAST SOFTWARE

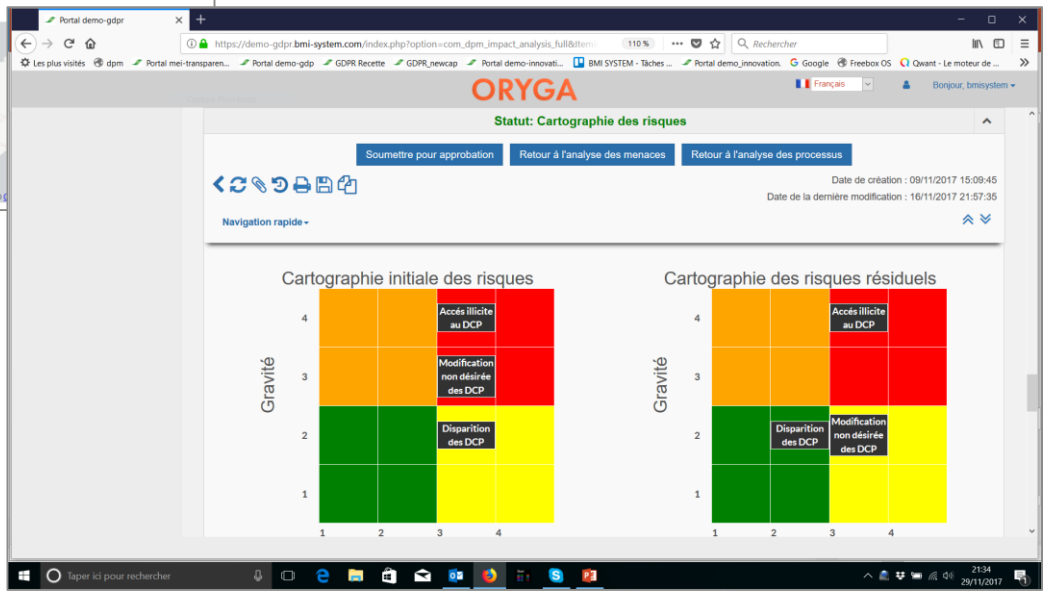
- ONE TRUST,
- NIMITY
- EGERIE

- ORYGA/BMI

Etat des lieux des outils DPO/GDPR…

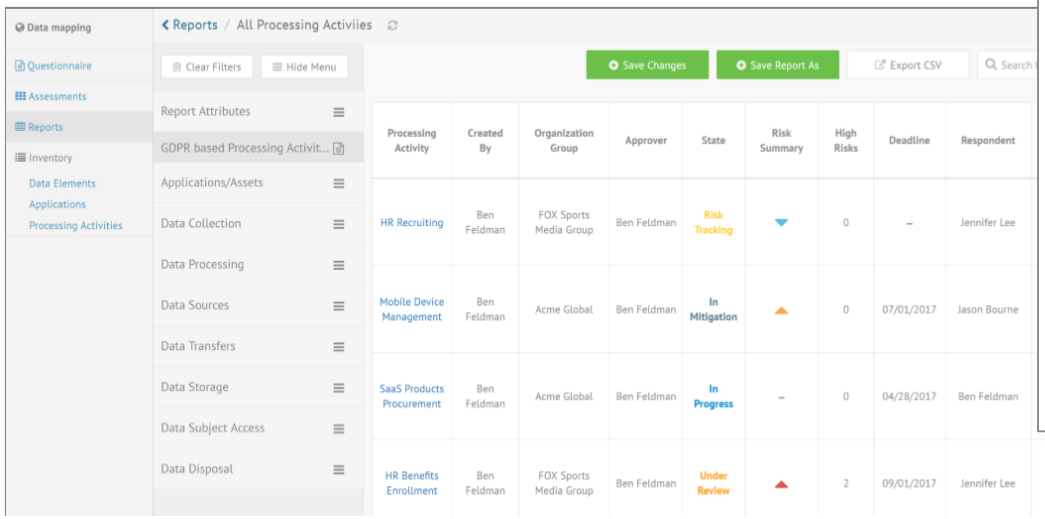
- Extraits ORYGA – BMI System’

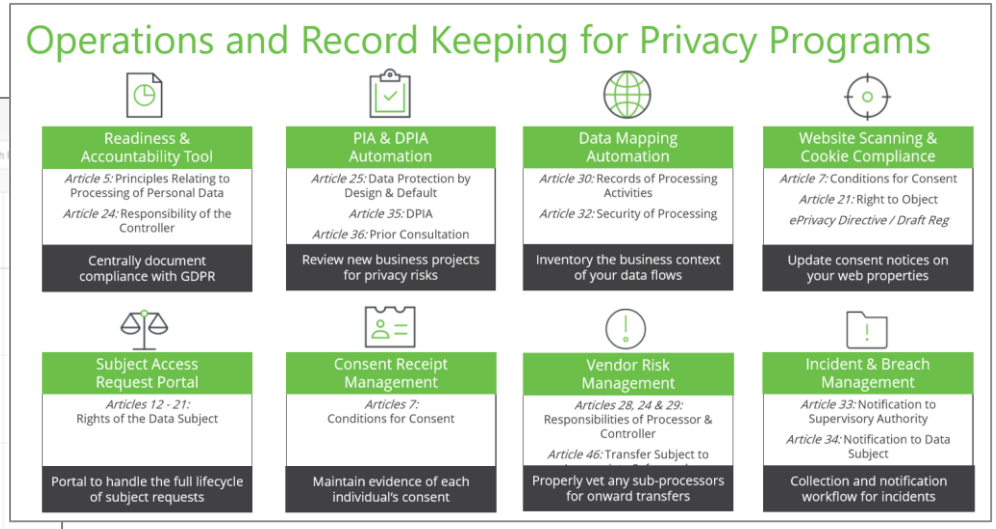


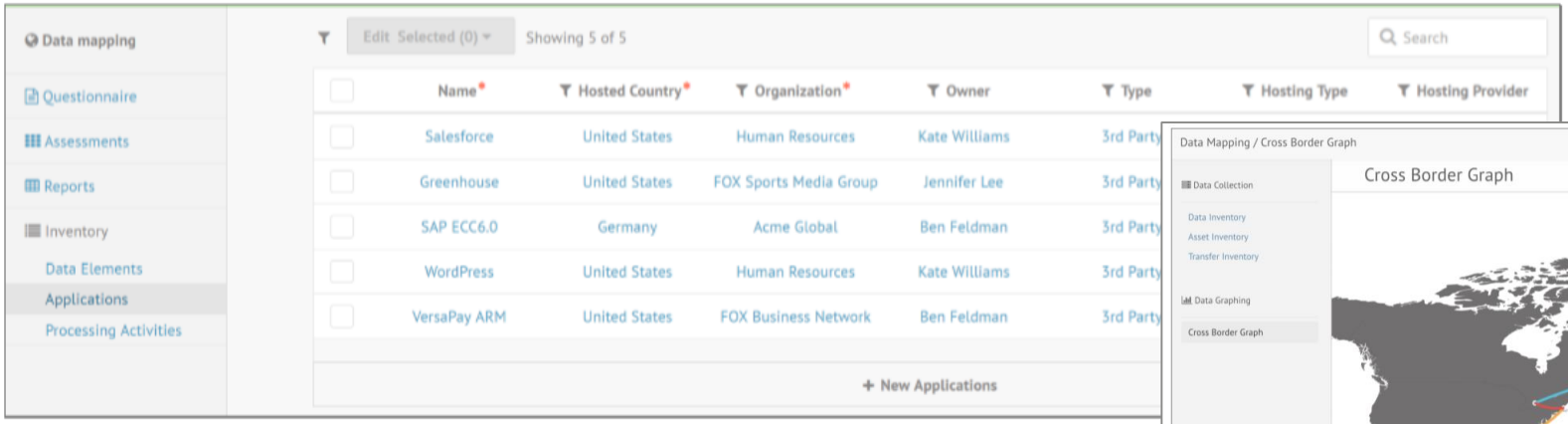


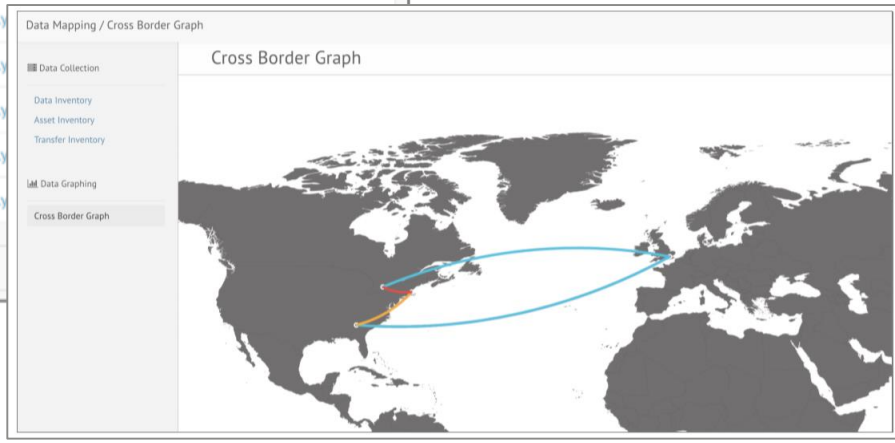
Etat des lieux des outils DPO/GDPR…

- Extraits ONE TRUST



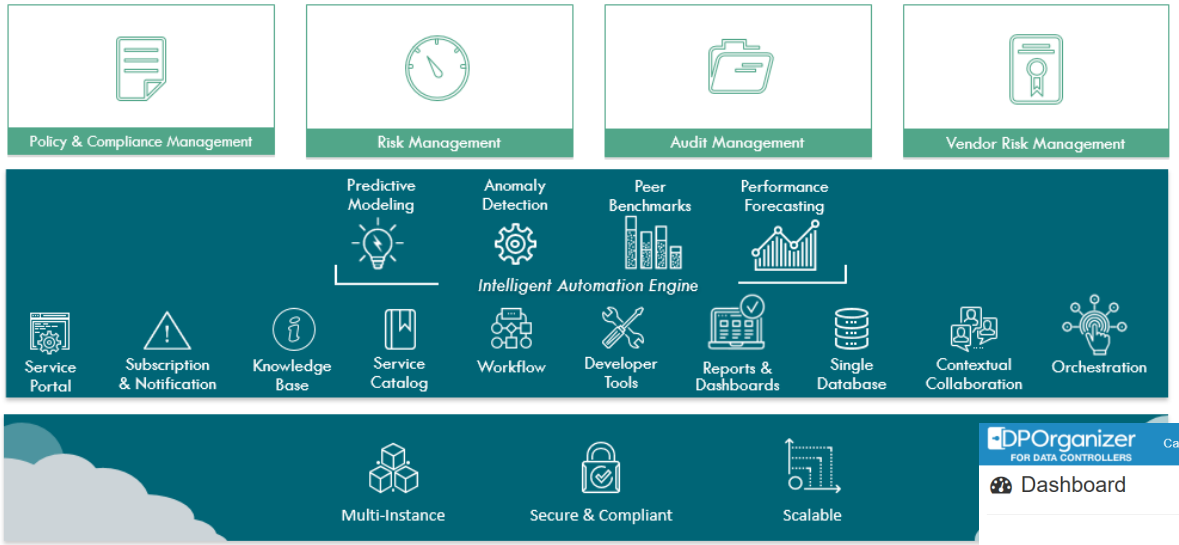




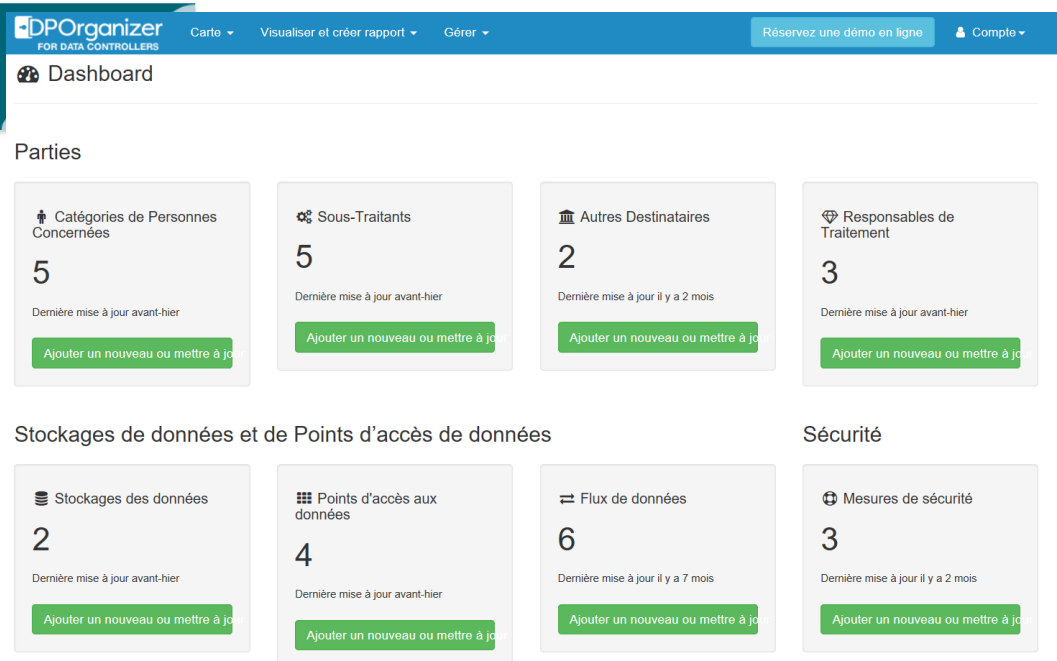


Etat des lieux des outils DPO/GDPR…

- Extrait SERVICE NOW

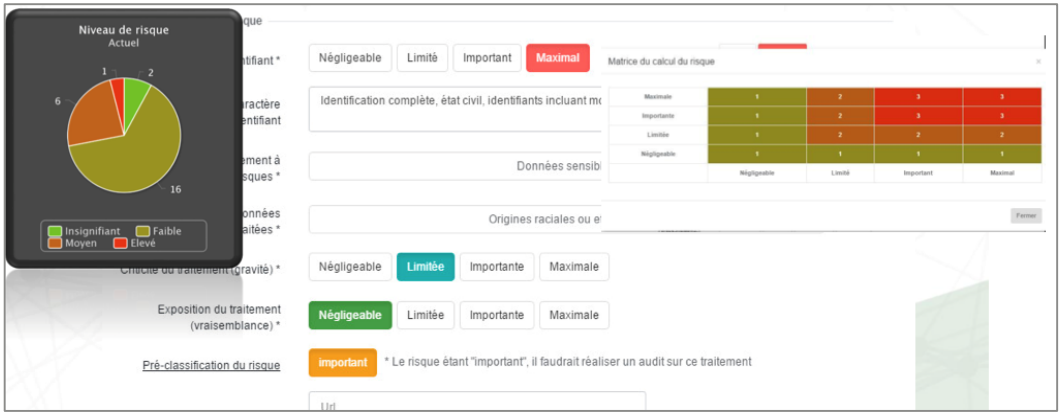


- Extrait DPO ORGANIZER



Etat des lieux des outils DPO/GDPR…

- Extraits EGERIE Privacy manager’



www.tnpconsultants.com

31 rue du Pont
92200 NEUILLY-SUR-SEINE

Tél. : +33 1 47 22 43 34 | Fax : +33 1 46 05 11 09

Contact GDPR : florence.bonnet@tnpconsultants.com