DPO FORUM

DASTRA

Conformité RGPD et Legaltech : l'optimisation par la technologie ?

21 Octobre 2021

Introduction

Paul-Emmanuel BIDAULT
Co-fondateur de Dastra

Editeur

Banque

Conseil

DASTRA

Table des matières

RGPD : les autorités s'impatientent face aux retards de conformité alors que des moyens importants ont pourtant déjà été mobilisés

1,3 Mds €

Montant cumulé des sanctions pour toute sorte de manquements liés au RGPD au mois de septembre 2021(1)

128

Pays sur 194 ont désormais en place une législation sur les données personnelles(2)

39%

Seulement des entreprises ont déclarés avoir réalisé leur plan d'action à plus de 75%. (3)

1,3 M€

Dépenses moyennes des entreprises dans les initiatives de préparation au RGPD (4)

200 k$

Dépenses moyennes par mois des entreprises pour se conformer uniquement aux demandes d'exercices de droit (5)

(1) : enforcementtracker.com
(2) Conférence des Nations Unies sur le Commerce et le Développement (UNCTAD)
(3) Baromètre KPMG
(4) Source: PwC
(5) Source : IDC

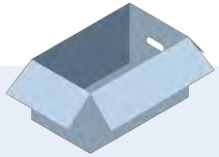
Les professionnels de la protection des données sont isolés, surchargés et font face à des défis complexes

L'**étude qualitative** réalisée par Dastra en 2020 sur 60 **Data Protection Officers** (DPO) révèle leur **isolement** et leur **manque de soutien**

Mauvaise collaboration avec les métiers

68%

Des recommandations des Data Protection Officers (DPO) ne sont pas suivies par leurs Métiers



Manque de ressource et de temps

66%

Estiment avoir une surcharge de travail nécessaire aux actions à mener

62%

des DPO réalisent encore leurs registres de traitements à l'aide d'Excel

Besoin de pilotage et de suivi

35%

des DPO déclarent manquer d'outils de gestion, de suivi et de contrôle de la conformité

Source : étude menée par le ministère du travail en 2020 sur le métier du DPO et des interviews qualitatives réalisés par Dastra sur 60 Data Protection Officers en France en 2020

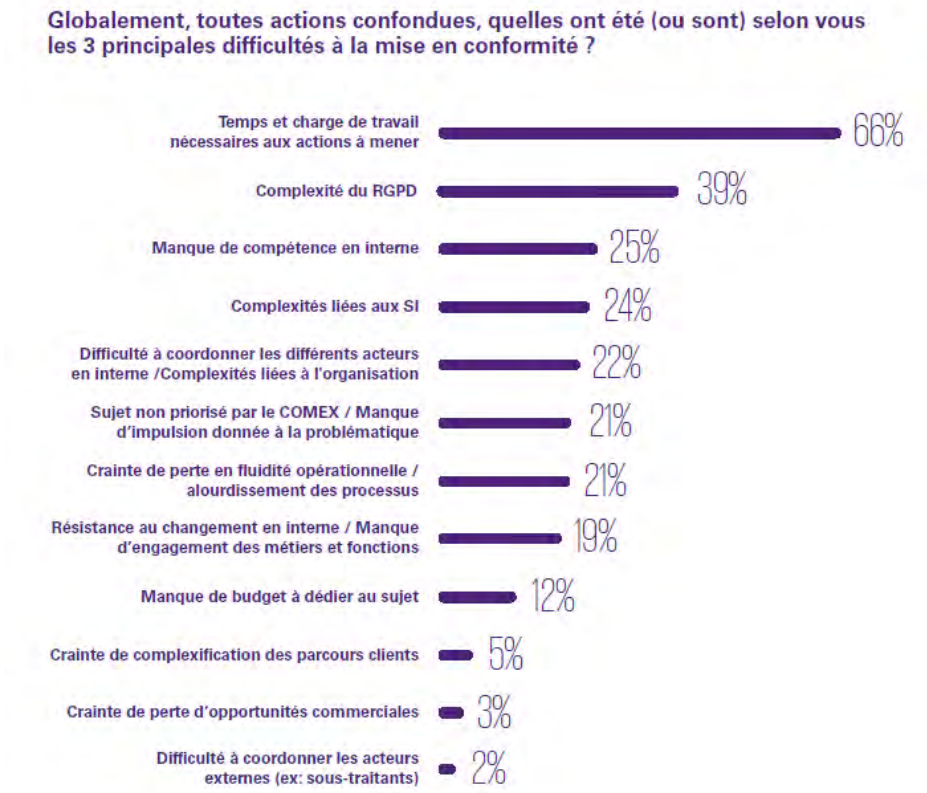
L'implication des opérationnels dans les processus RGPD : une étape cruciale vers l'accountability

Les **principaux facteurs** ralentissant la mise en conformité sont :

- La **charge de travail** pour les DPOs (66%)
- La **complexité** du Règlement (39%)

Parmi les étapes les **moins avancées** figurent :

- les **analyses d'impact** relatives à la protection des données (42%)
- la mise en place des **durées de conservation** (30%)
- le **privacy by design** (21%).



Mettre en place et maintenir la conformité RGPD impose donc **de mettre en place des processus outillés** permettant à **toutes les personnes impliquées** dans la protection des données **d'agir** de concert, sous l'orchestration du DPO

Source: KPMG – Baromètre RGPD : 3 ans après où en êtes-vous ?

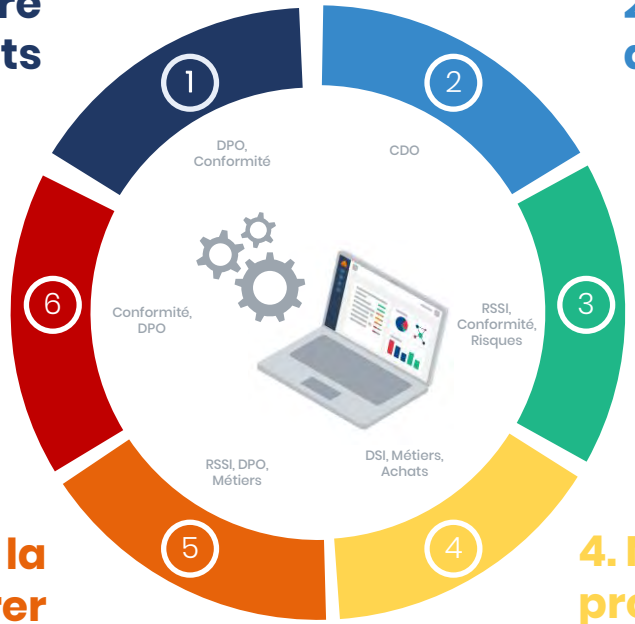
Table des matières

La gestion du RGPD : plus qu'un projet, un processus continu nécessitant l'implication de toute l'entreprise

Le **Data Protection Officer (DPO)** est le référent responsable au sein des organismes de la bonne mise en œuvre du RGPD. Qu'il soit nommé ou non, les organisations doivent :

DPO

1. Documenter le registre des traitements



2. Cartographier les données personnelles

6. Piloter la conformité, suivre la progression & contrôler

3. Auditer, analyser les risques & réaliser les PIA

5. Planifier la remédiation & orchestrer la conformité

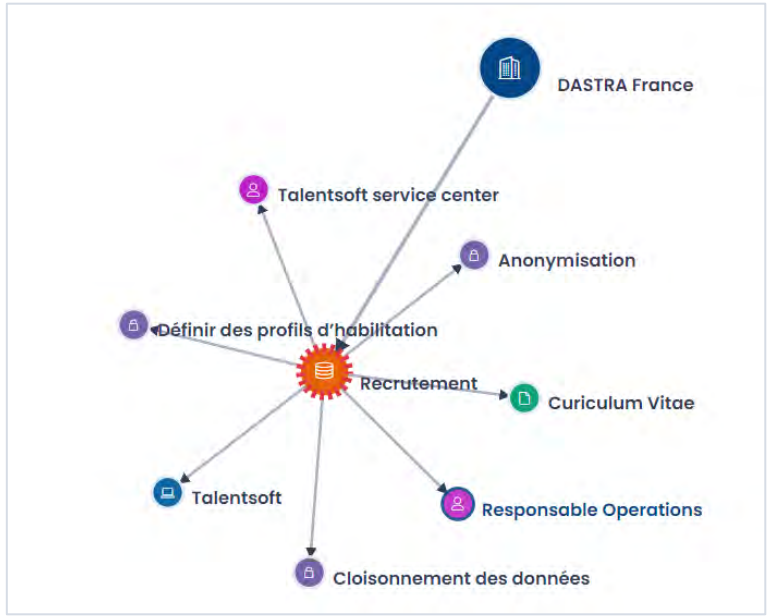
4. Mettre en œuvre les processus obligatoire
(exercices de droit, violation de données, privacy by design...)

Un registre des traitements « augmenté » intégrant la cartographie des données

L'article 30 du RGPD impose à chaque responsable du traitement de **tenir un registre des activités de traitement** dont il porte la responsabilité, et qu'il met en œuvre en tant que sous-traitant. Il permet de **recenser les traitements** de données et de disposer **d'une vue d'ensemble** de ce qui est fait avec les données personnelles.

Apports d'un outil de registre augmenté

1. Dépasser la simple conformité à l'article 30 (qui ne suffit pas pour être conforme)
2. Travailler efficacement sur la conformité via la collaboration avec les métiers / opérationnels
3. Piloter l'activité de conformité, constituer une piste d'audit et suivre les KPIs / KCIs
4. Réutiliser le travail déjà réalisé, mettre en œuvre la gouvernance des données personnelles et insuffler une culture data



Exemple de visualisation graphique d'un traitement de données « Recrutement» issu du registre de traitement de données de l'entité « Dastra France »

Les PIA & audits automatisés

L'analyse des **risques** sur la vie privée, **de non-conformité** vis-à-vis du RGPD, **sous-traitant** ou d'**image** nécessite de s'y retrouver dans le flux constant des données personnelles, d'appliquer efficacement les plans de contrôle, ainsi que de suggérer automatiquement des plans d'actions de remédiation.

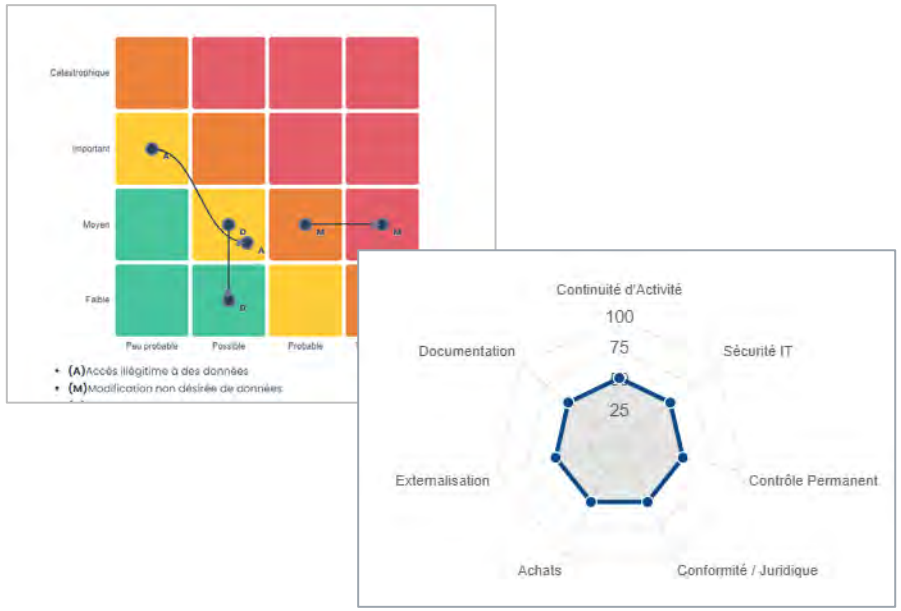
Apports d'un outil de PIA & audit automatisé

1 Réviser les PIAs et audits régulièrement et à tout moment, dès lors qu'une modification intervient.

2 Importer automatiquement les traitements & attacher les PIAs aux référentiels.

3 Travailler efficacement sur les analyses via la collaboration et le guidage de toutes les parties prenantes.

4 Traçer et historiser l'ensemble des actions. Centraliser et documenter en cas de contrôle ou dans le cadre de l'instruction d'une plainte.



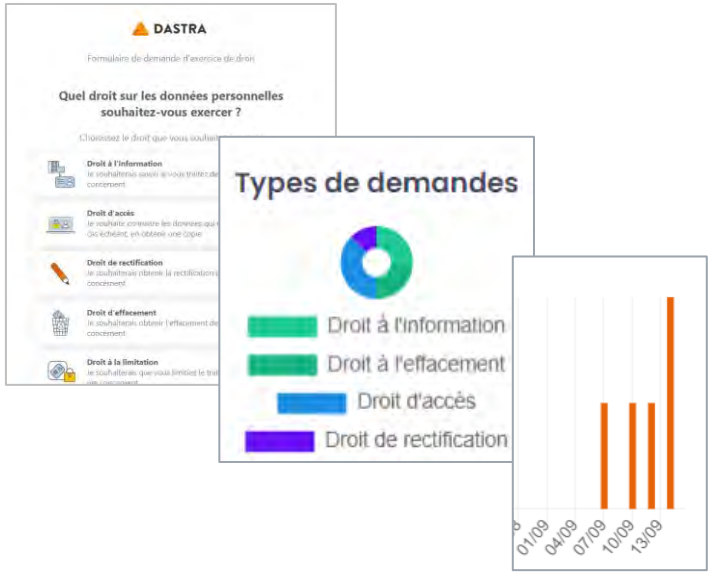
Exemple de PIA & analyse de risque sous-traitant

Automatisation des processus (exercices de droits, violations, consentement, privacy by design…)

Le RGPD impose aux organisations de mettre en œuvre des **processus** tels que la **gestion des demandes d'exercices de droit** d'accès, d'information, de suppression… Pour assurer leur efficacité à grande échelle et mobiliser de manière transverse les acteurs concernés, les organisations ont besoin de les industrialiser et de garder les preuves.

Apports d'un outil d'industrialisation des processus RGPD

1. Collecter et qualifier automatiquement les demandes d'exercices de droit, puis les exécuter de manière sécurisé
2. Aide à la décision dans la qualification des demandes (simples ou complexes, légitime, points de contacts…)
3. Communication et transmission des données via un canal sécurisé (plutôt que par mail)
4. Traçer et historiser l'ensemble des actions. Centraliser et documenter en cas de contrôle ou dans le cadre de l'instruction d'une plainte.



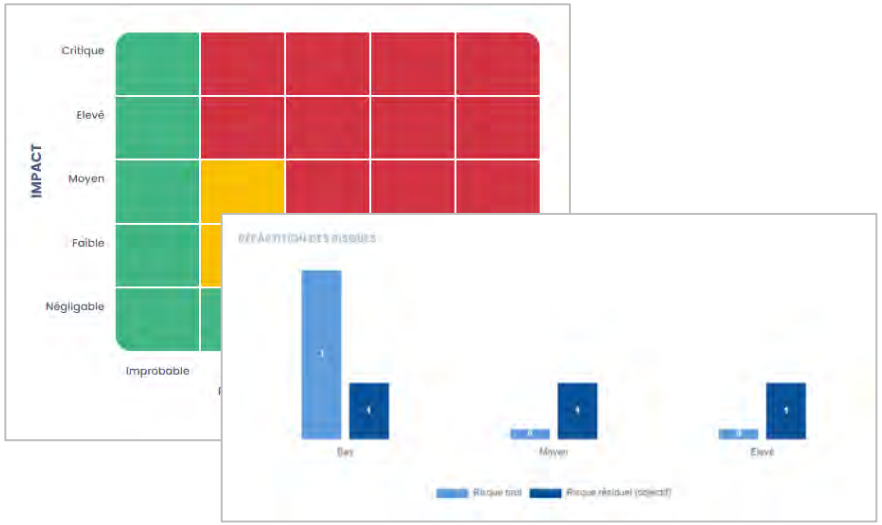
Exemple de processus industriel de gestion des demandes d'exercices de droit

Gérer les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, il est nécessaire de mener des analyses détaillées s'interfaçant avec les métiers risques

Apports d'un outil de gestion des risques

1. Evaluation fine de tous les risques (vie privée, opérationnels, non-conformité, stratégique etc...)
2. Plan de remédiation
3. Suivi & progression des points de contrôles
4. Traçer et historiser l'ensemble des actions. Centraliser et documenter en cas de contrôle ou dans le cadre de l'instruction d'une plainte.



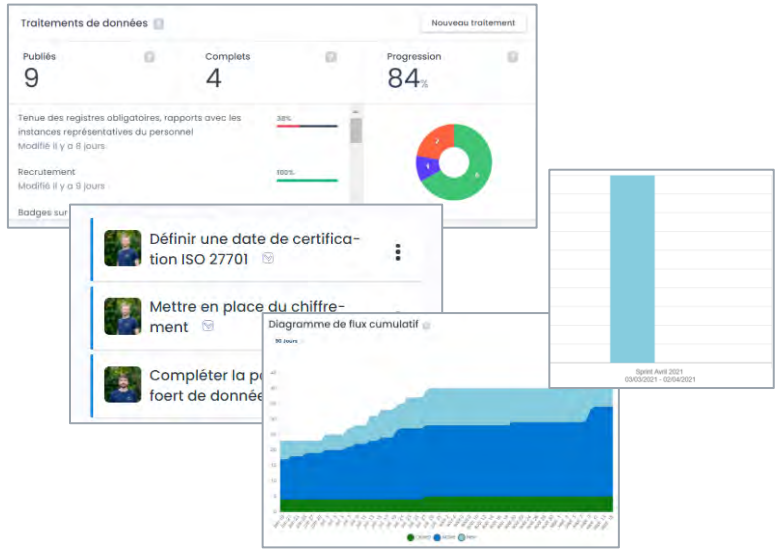
Exemple de visualisation des risques

Planifier la remédiation en équipe et piloter la conformité RGPD

Le principe d'Accountability du RGPD impose aux organisations de mettre en œuvre des mécanismes et des procédures internes permettant de **démontrer** le respect des règles relatives à la protection des données.

Apports d'un outil de planification et de pilotage de la conformité RGPD

1. Créer des tickets, allouer des tâches, travailler en équipe sur la protection des données en mode agile
2. Piloter les actions réalisées via des tableaux de bord globaux de la conformité RGPD
3. Intégrer les processus RGPD au sein du modèle opérationnel interne à l'organisation et diminuer les frictions
4. Traçer et historiser l'ensemble des actions. Centraliser et documenter en cas de contrôle ou dans le cadre de l'instruction d'une plainte.



Exemple d'indicateur de pilotage, de plan d'action et de statistiques

Les outils permettent d'améliorer la qualité de votre conformité RGPD et vous faire gagner du temps

28% de **fréquences d'erreurs en moins** liées aux données du registre des traitements, base de nombreux livrables RGPD

69% des DPOs passent **moins de temps** à localiser leurs données et créer leurs rapports avec un outil

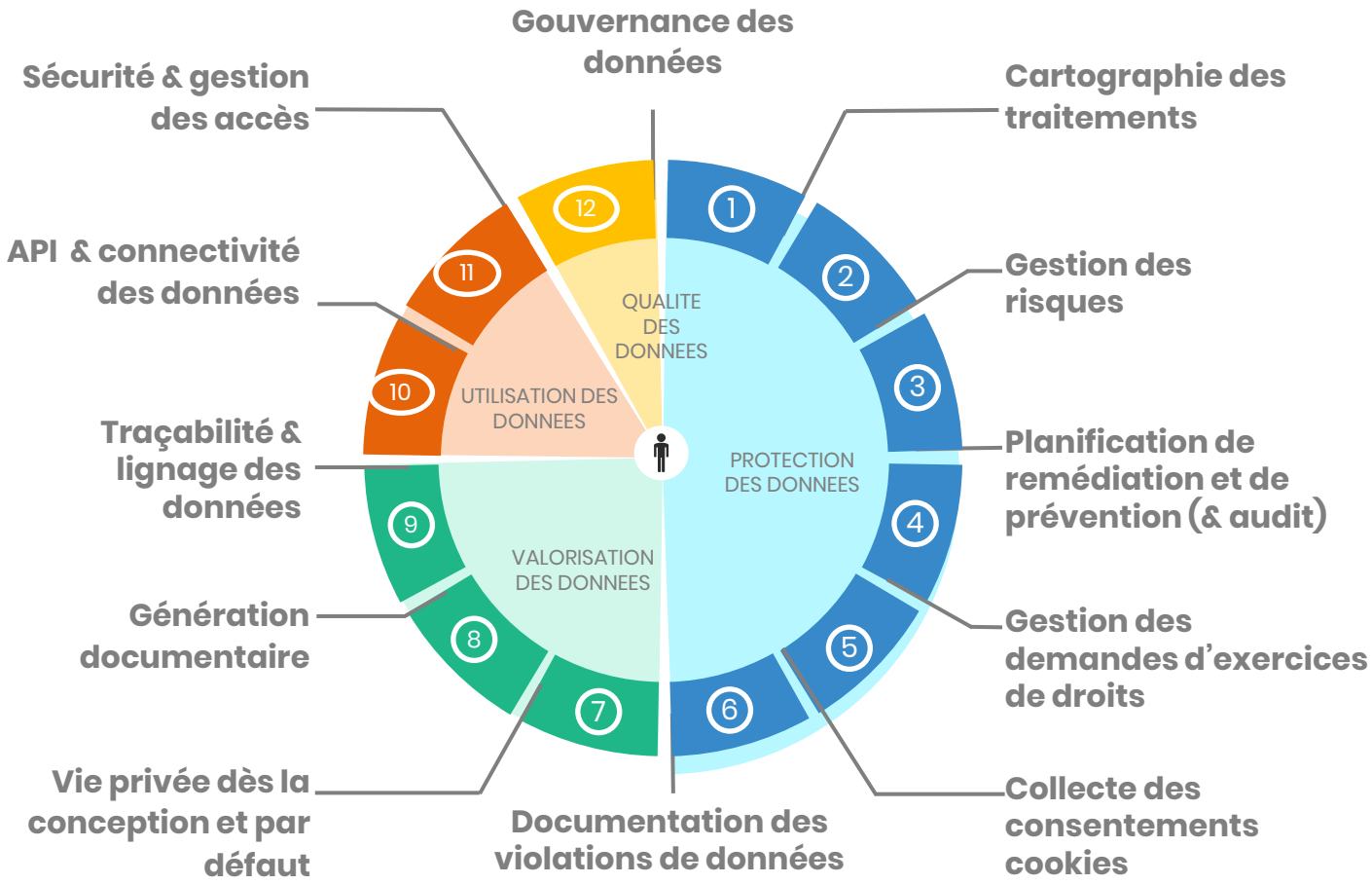
23% **D'augmentation de la productivité** brute des équipes en charge de réaliser des audits ou de gérer les demandes d'exercices de droit

Source : étude Dastra basée sur l'interview de 60 data protection officers en France (2020)

Table des matières

Vers une plateforme de gouvernance des données personnelles

Les 4 piliers de la stratégie de données…



appliqués à votre plateforme de gouvernance des données personnelles !

La solution Dastra : tous les cas d'usages RGPD intégrés dans une seule plateforme

Table des matières

DASTRA

Transformez vos contraintes RGPD en accélérateur avec la solution Dastra

Demandez une démo Essayez gratuitement