MEGA
SEE THE BIGGER PICTURE

GDPR : Accélérez votre mise en conformité au nouveau Règlement Général sur la Protection des Données

Une approche en 6 étapes

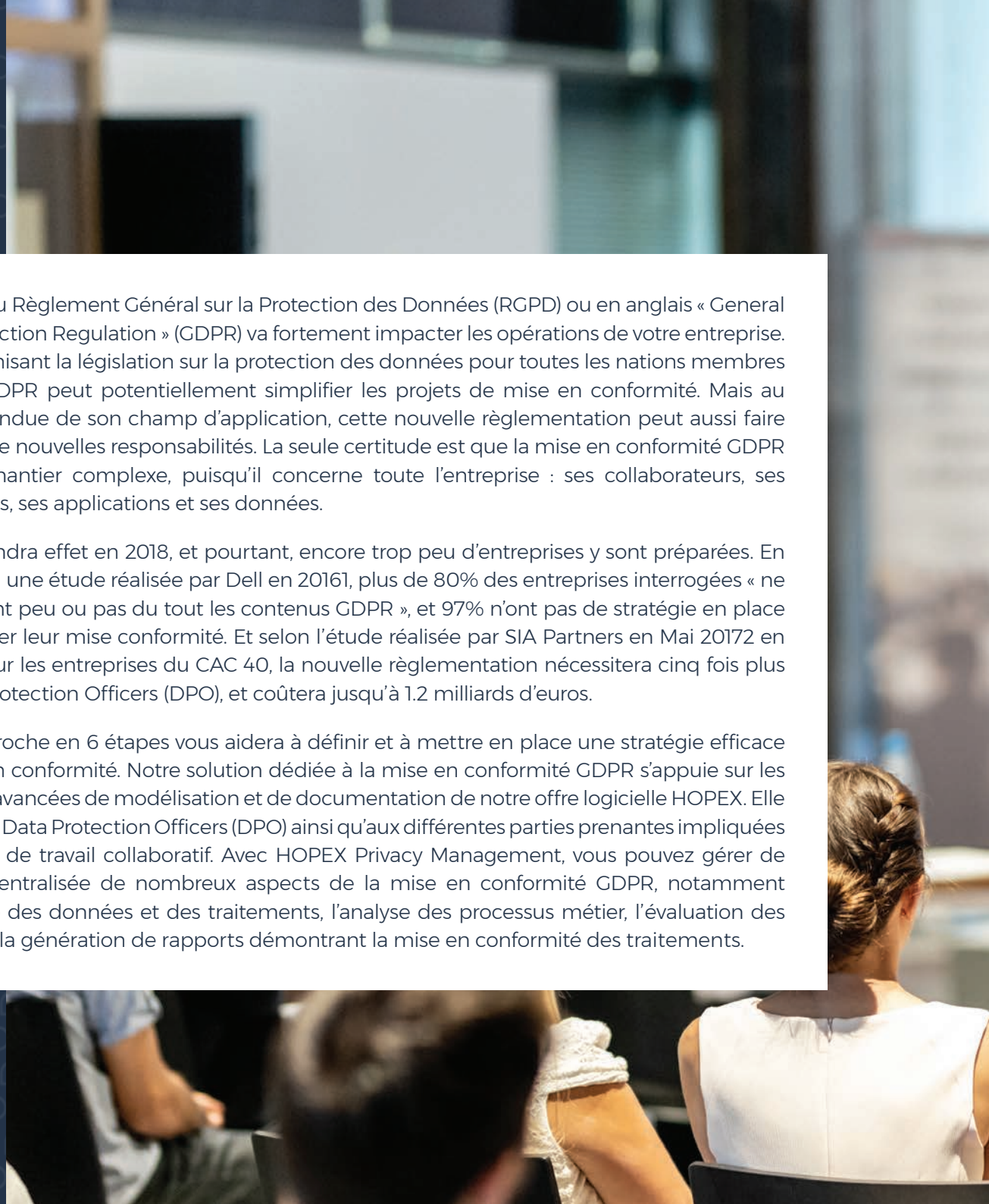
Livre blanc

Introduction

Le nouveau Règlement Général sur la Protection des Données (RGPD) ou en anglais « General Data Protection Regulation » (GDPR) va fortement impacter les opérations de votre entreprise. En harmonisant la législation sur la protection des données pour toutes les nations membres de l'UE, GDPR peut potentiellement simplifier les projets de mise en conformité. Mais au vu de l'étendue de son champ d'application, cette nouvelle règlementation peut aussi faire émerger de nouvelles responsabilités. La seule certitude est que la mise en conformité GDPR sera un chantier complexe, puisqu'il concerne toute l'entreprise : ses collaborateurs, ses traitements, ses applications et ses données.

GDPR prendra effet en 2018, et pourtant, encore trop peu d'entreprises y sont préparées. En effet, selon une étude réalisée par Dell en 20161, plus de 80% des entreprises interrogées « ne connaissent peu ou pas du tout les contenus GDPR », et 97% n'ont pas de stratégie en place pour assurer leur mise conformité. Et selon l'étude réalisée par SIA Partners en Mai 20172 en France pour les entreprises du CAC 40, la nouvelle règlementation nécessitera cinq fois plus de Data Protection Officers (DPO), et coûtera jusqu'à 1.2 milliards d'euros.

Notre approche en 6 étapes vous aidera à définir et à mettre en place une stratégie efficace de mise en conformité. Notre solution dédiée à la mise en conformité GDPR s'appuie sur les capacités avancées de modélisation et de documentation de notre offre logicielle HOPEX. Elle fournit aux Data Protection Officers (DPO) ainsi qu'aux différentes parties prenantes impliquées un espace de travail collaboratif. Avec HOPEX Privacy Management, vous pouvez gérer de manière centralisée de nombreux aspects de la mise en conformité GDPR, notamment l'inventaire des données et des traitements, l'analyse des processus métier, l'évaluation des risques, et la génération de rapports démontrant la mise en conformité des traitements.



Comprendre GDPR

Le nouveau règlement européen sur la protection des données personnelles entrera en application le 25 mai 2018. Il prévoit de renforcer le droit des personnes et s'impose à toute organisation - même située hors de l'UE - contrôlant ou traitant de données qui peuvent, directement ou indirectement, identifier une personne. Ces droits comprennent notamment :

Le droit d'accès (Article 15)

Le droit d'une personne concernée d'avoir confirmation que ses informations à caractère personnel sont traitées ou non et lorsqu'elles le sont, d'avoir accès à ces données ainsi qu'à de nombreuses autres information, telles que la finalité du traitement ou la durée de conservation envisagée.

Le droit à l'oubli (Article 17)

Le droit d'une personne concernée de stopper la diffusion et le traitement de ses données à caractère personnel et, le cas échéant, leur effacement. Les conditions d'effacement peuvent concerner des données conservées à des fins qui ne sont plus légitimes ou le retrait du consentement de la personne concernée.

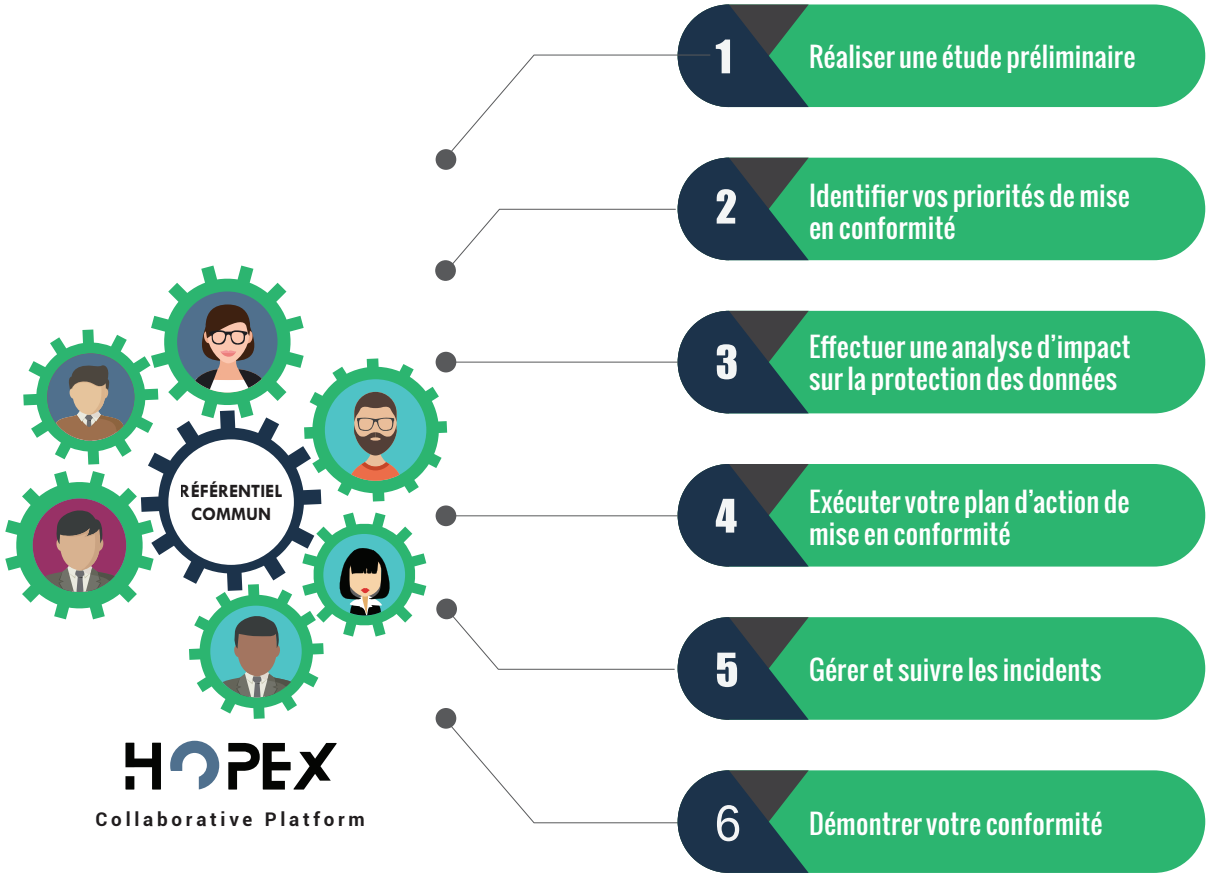
Le droit à la portabilité des données (Article 20)

Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle.

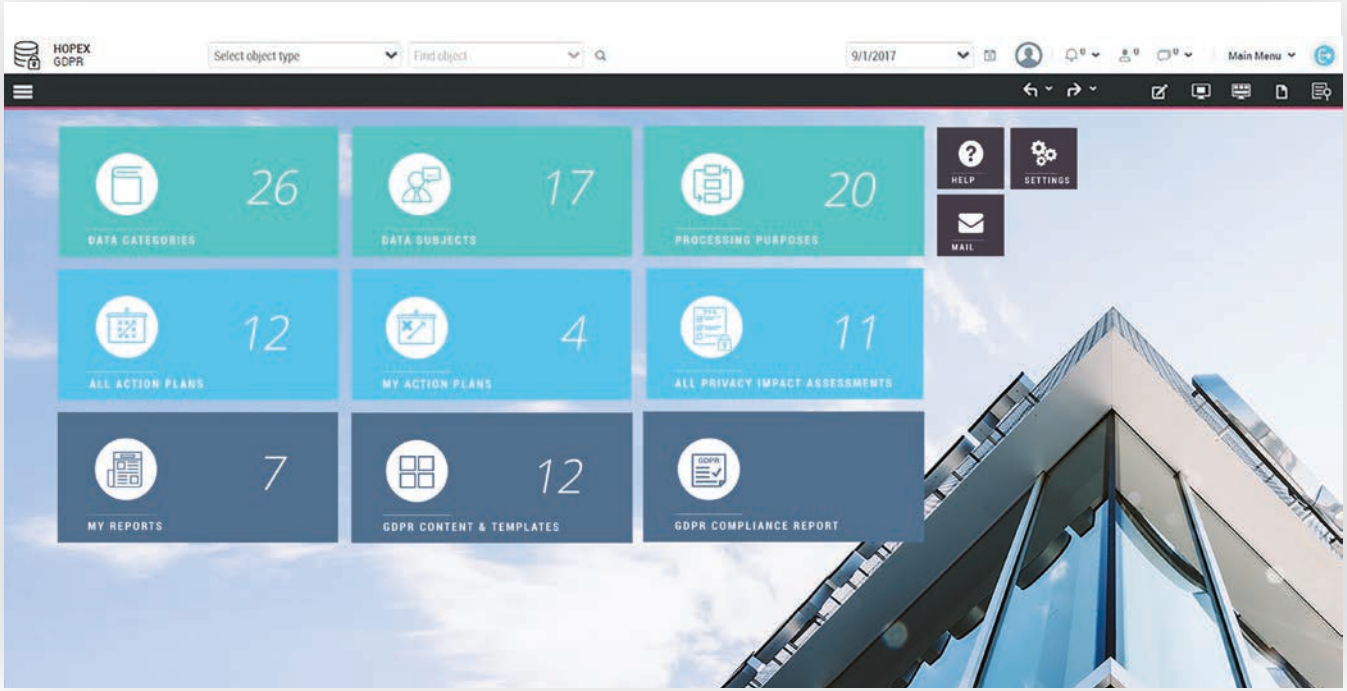
L'étendue de cette législation fait de GDPR la première règlementation globale sur la protection des données. Parmi les autres éléments clés de GDPR on trouve aussi : l'analyse d'impact relative à la protection des données, la tenue d'un registre des activités de traitement, l'obligation de déclarer toute violation de données dans les 72 heures qui suivent leur identification, et dans certains cas, l'obligation de désigner un DPO, Data Protection Officer. Ce règlement impose également l'obligation du respect de la vie privée dès la conception du système de traitement des données et leur protection par défaut (en anglais Privacy by design), ainsi que la capacité à démontrer la mise en conformité.
Le non-respect de GDPR peut entrainer des amendes qui vont de 10 à 20 millions d'euros, ou de 2 à 4 % du chiffre d'affaires total, selon le montant le plus élevé des deux.

GDPR : 6 étapes pour accélérer votre mise en conformité

Prenez les commandes de votre mise en conformité GDPR en suivant nos 6 étapes : identifiez les stratégies efficaces pour évaluer vos besoins, en vous concentrant sur l'identification et la priorisation du traitement des données à caractère personnel ; découvrez comment remédier à la non-conformité, en vous appuyant sur la modélisation des processus métier; et démontrez votre conformité à l'autorité de contrôle ainsi qu'à vos dirigeants, grâce à une documentation détaillée et aux différents rapports générés automatiquement.



Page d'accueil de HOPEX Privacy Management



1. Réaliser une étude préliminaire

Les exigences de GDPR étant vastes, elles nécessitent une collaboration étendue et transverse à tous les départements de l'entreprise : du marketing au commercial, en passant par le juridique et les ressources humaines, jusqu'à la sécurité et l'informatique. Ainsi réunies, toutes les parties prenantes sont en charge de la planification et de l'exécution des activités règlementaires. Et pour être complètement efficaces sur cette mission, elles doivent non seulement s'engager à coopérer, mais aussi diffuser une culture d'entreprise selon laquelle la confidentialité des données doit toujours passer en premier.

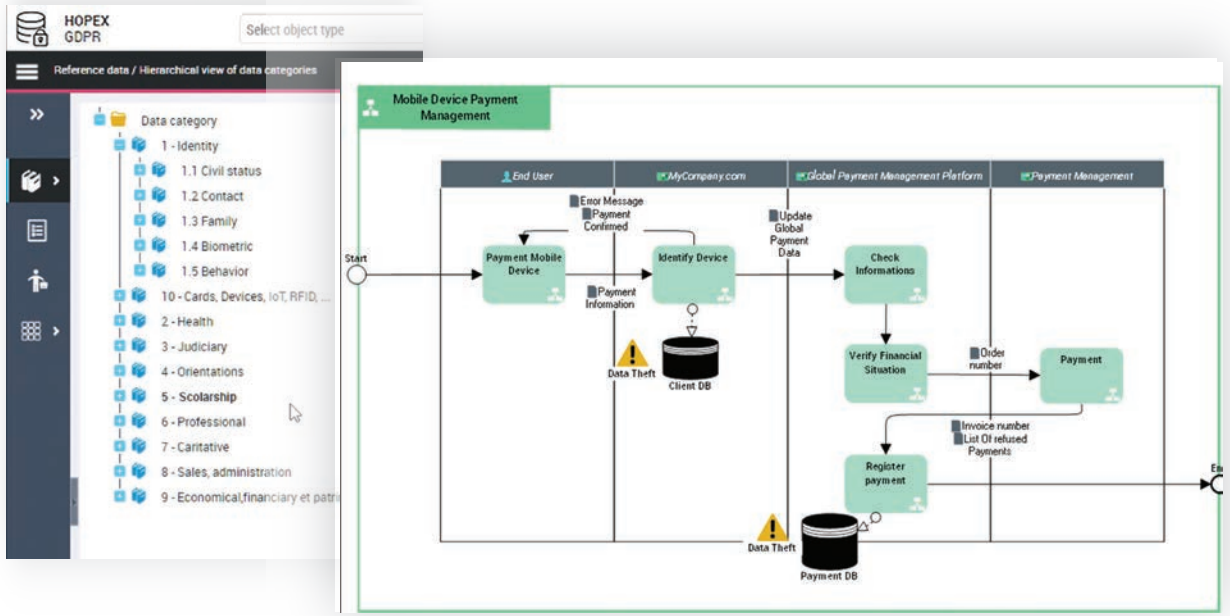
Le rôle du DPO, dont GDPR, crée la fonction et définit les responsabilités, est d'accompagner les différentes parties prenantes et de superviser les activités liées à la protection des données personnelles. Organiser des formations d'entreprise permettra aussi de garantir l'efficacité de ces activités. Le DPO devra par ailleurs prendre en charge de nombreuses autres responsabilités, qui, le cas échéant et en fonction des complexités liées à chaque entreprise, nécessiteront le recrutement de ressources dédiées. Par exemple, pour les entreprises traitant des catégories de données personnelles relatives à des condamnations pénales, les exigences réglementaires nécessiteront un recrutement dédié.

La première mission du DPO et des autres parties prenantes consistera à effectuer en amont une étude préalable d'impact de GDPR. Il s'agit d'identifier :

- les données, les applications et les services de stockages qui y sont associés,
- les données à caractère personnel qui identifient directement ou indirectement une personne concernée,
- le Responsable de Traitement et ses sous-traitants ou co-traitants,
- les processus métier utilisant les données à caractère personnel,
- les personnes interagissant avec ces données.

Par ailleurs, cette étude préliminaire doit consister en un inventaire de données catégorisé et priorisé. Cela permettra d'identifier les données à caractère personnel critiques liés aux processus métier, et de comprendre les interactions entre les données et les personnes.

HOPEX Privacy Management comprend un espace de travail centralisé, entièrement dédié à la mise en conformité GDPR. Conçu pour les DPO et les différentes parties prenantes, cet espace de travail favorise la collaboration entre les départements. Il facilite la catégorisation et priorisation des données, la consultation des flux de données, et la génération de rapports. Un référentiel centralisé de votre inventaire de données – qui inclut aussi leurs liens avec les applications et avec les processus métier – favorise la collaboration et peut servir de base à de nombreuses autres activités de mise en conformité.



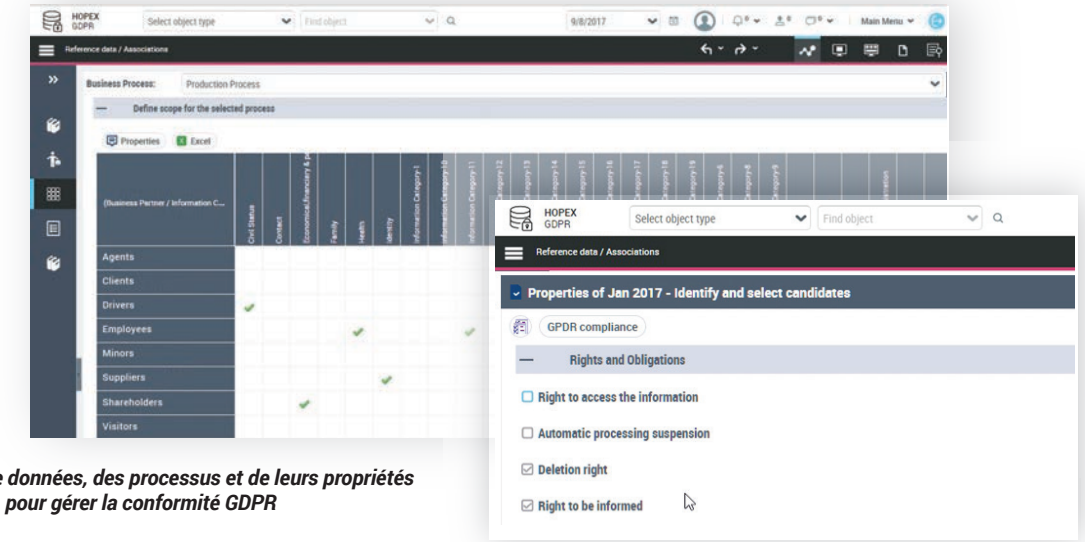
Catégoriser les données, relier ces données aux processus métier et revoir chaque processus en détail depuis le référentiel commun

2. Identifier vos priorités de mise en conformité

GDPR a pour objectif de réguler le cycle de vie des données à caractère personnel. Ce qui implique pour les entreprises de connaître non seulement la nature des données qu'elles possèdent, mais aussi les finalités du traitement et comment elles les protègent. Un inventaire de données doit alors proposer plus qu'une liste des données contrôlées et/ou traitées par votre entreprise ou partenaires. Il doit aussi rendre compte du type de traitement et de sa finalité. Catégoriser les données à caractère personnel, en les associant aux traitements et aux applications permet d'évaluer la finalité de leur utilisation et de les prioriser selon leur niveau de sensibilité.

Les catégories de données regroupent de façon logique les données individuelles. Chacune de ces catégories permet d'approfondir l'étude et d'évaluer la sensibilité des données. Lorsque ces catégories sont associées avec les processus métier, il devient aisé de faire le lien entre des groupes de données, et d'identifier les actions de conformité à réaliser en priorité.
Notez que toute donnée pouvant, directement ou indirectement, être utilisée pour identifier une personne physique, est soumise à la règlementation. Ce qui signifie qu'une donnée prise seule, qui n'identifie pas de personne concernée, mais qui peut permettre de l'identifier lorsqu'elle est groupée avec d'autres données, est considérée comme une donnée à caractère personnel. C'est pour cette raison qu'il est indispensable de modéliser les liens entre les catégories de données, de traitement et les personnes. En visualisant les liens entre les catégories de données, de traitement et de personnes, vous pouvez comprendre les zones de l'organisation à considérer en priorité.

HOPEX Privacy Management permet de recouper aisément les catégories de données avec les processus métier, rendant ainsi observables les processus gérant des données personnelles sensibles. Les utilisateurs peuvent aussi zoomer sur les détails de ces intersections, pour décider des actions de conformité à mettre en place, de leur priorisation, et pour les partager avec leurs équipes.



Référencement croisé des catégories de données, des processus et de leurs propriétés telle que leur sensibilité, pour gérer la conformité GDPR

3. Effectuer une analyse d'impact sur la protection des données (DPIA)

L'analyse d'impact relative à la protection des données (DPIA) est un des composants clés de GDPR. Elle est nécessaire lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques. Le responsable des traitements doit, avant d'effectuer le traitement, analyser l'impact des opérations envisagées sur la protection des données à caractère personnel. Dans la plupart des cas, ce document obligatoire sera exigé par le régulateur. Il doit comporter la liste des activités de traitement des données qui peuvent potentiellement impacter les droits et libertés des personnes concernées. Un rapport DPIA doit comporter les éléments suivants :

- Description des opérations de traitement envisagées et de leur finalité
- Analyse d'impact des risques pour les droits et libertés des personnes concernées
- Les mesures prises pour limiter ces risques et les mécanismes de sécurité visant à protéger les données

L'approche recommandée par MEGA - qui peut et doit être adaptée aux besoins spécifiques de votre entreprise - pour effectuer une DPIA est la suivante :

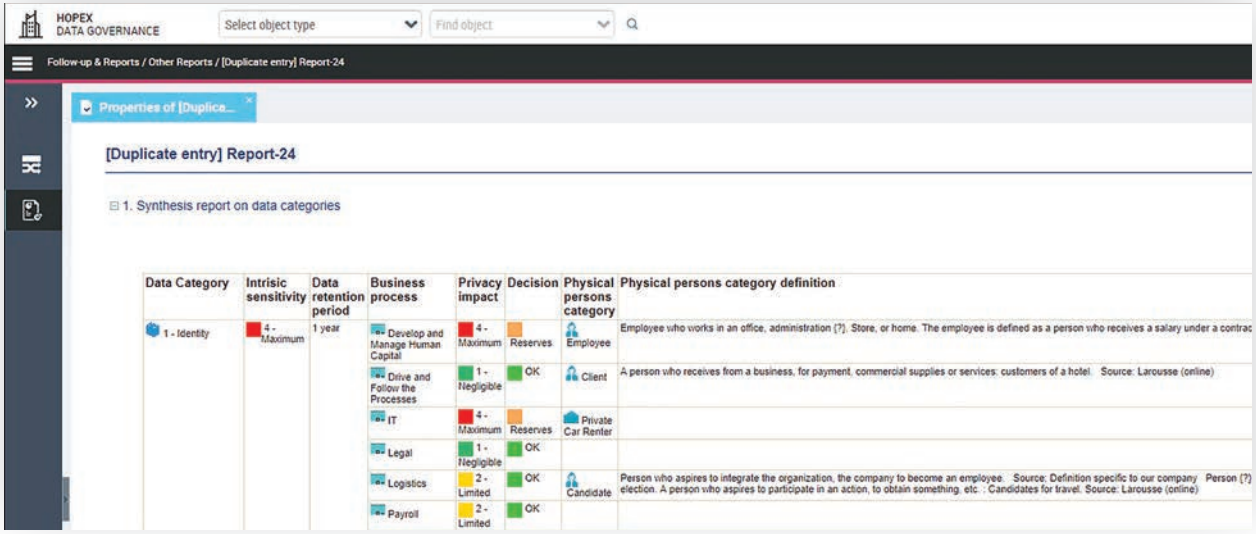
Décrivez les opérations de traitement représentant un risque élevé pour les droits et libertés des personnes privées
Expliquez quelle est la nature des traitements envisagés, leur portée, leur contexte et leur finalité. Evaluez la proportionnalité des traitements au regard des finalités. Utilisez les cartographies des processus métier pour présenter les activités de traitement des données envisagées.

Réalisez une analyse d'impact
Évaluez les risques que ces traitements représentent pour les droits et libertés des personnes concernées. Reliez ces traitements aux technologies qui les sous-tendent.

Décrivez les mesures prises pour limiter les risques
Les mesures pour limiter les risques peuvent comporter : la mise en place de technologies de sécurisation des données (comme le chiffrement), des modifications apportées aux processus métier, ou encore des formations dispensées aux employés sur le traitement efficace des données.

Définissez des modèles opérationnels complètement sécurisés
Communiquez sur la manière dont votre entreprise prévoit de s'ajuster dans le temps pour assurer sa complète conformité sur un domaine spécifique.

Les cartographies des processus métier - décrivant les flux de données et où elles interagissent avec les applications et les personnes - constituent des éléments fondateurs de la mise en conformité GDPR, et font partie intégrante des éléments qui composent une DPIA. La solution de MEGA fournit des fonctionnalités supplémentaires de modélisation des processus, qui vous permettent d'analyser les modifications avant leur mise en œuvre, pour évaluer leurs impacts sur votre entreprise et sur votre mise en conformité. Vous pouvez aussi utiliser ces fonctionnalités de modélisation pour définir des opérations complètement sécurisées, ce qui renforce d'autant plus votre conformité.



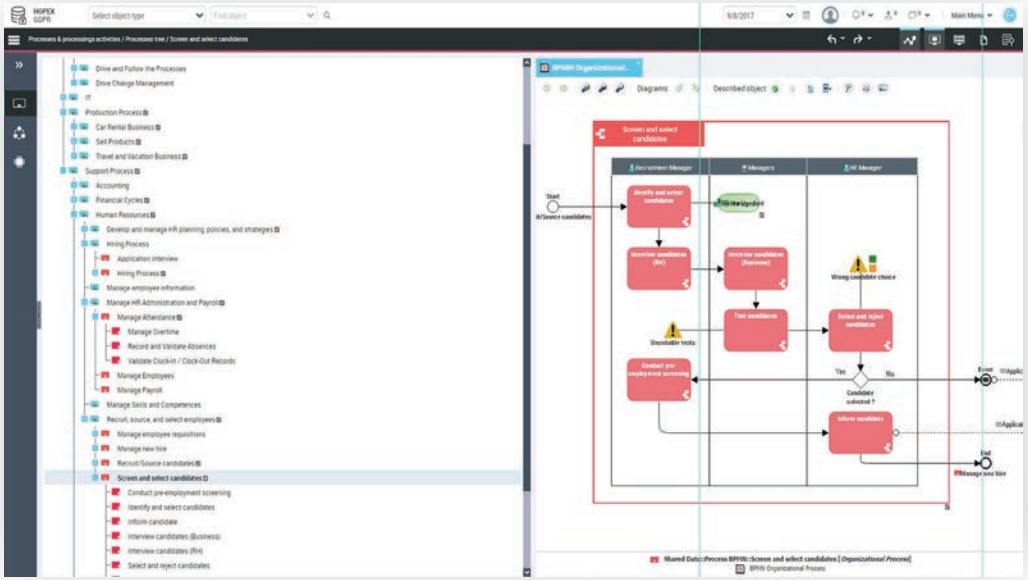
Partager les résultats des DPIA avec des rapports accessibles à l'ensemble des parties prenantes

4. Exécuter votre plan d'action de mise en conformité

Une fois les analyses d'impact sur la protection des données réalisées, vous devrez mettre en place les mesures que vous aurez définies pour limiter les risques sur la vie privée des personnes concernées. Ce plan d'action défini, vous pourrez commencer son exécution. L'un de ses éléments clé est l'analyse des processus métier, car nombre des processus que vous aurez identifiés comme contrôlant ou traitant des données à caractère personnel devront être sécurisés. Il est important que cette sécurisation soit réalisée sans impacter de manière négative votre entreprise. Par ailleurs, les mises à jour des cartographies de processus sont une manière efficace d'observer les dépendances et d'éviter des dépenses inutiles.

De plus, GDPR a pour objectif de sécuriser le cycle de vie des données à caractère personnel, mais aussi d'étendre les droits à la protection de la vie privée pour les personnes concernées. Les droits d'accès, à l'oubli et de portabilité, nécessitent, pour chacun d'entre eux, de créer de nouveaux processus métier ou de mettre à jour les processus existants.

Les logiciels comme HOPEX vous aident à concevoir, modéliser et partager ces nouveaux processus ou leurs mises à jour. Lorsque ces modifications concernent aussi les systèmes IT, votre entreprise peut organiser ses opérations de manière à proposer des produits et services parfaitement conformes, et ce sans sacrifier à l'agilité. À l'ère de la transformation digitale, pouvoir assurer des évolutions en continu sans entraver la conformité est devenu indispensable.



Modéliser les processus métier et les flux de données pour être conforme dès la conception

5. Gérer et suivre les incidents

L'article 33 de GDPR exige que le responsable du traitement notifie à l'autorité de contrôle une violation de données à caractère personnel dans les 72 heures suivant la découverte, à moins que la violation ne soit susceptible de porter atteinte aux droits et libertés des personnes concernées. Par conséquent, le suivi des activités de traitement des données et des incidents - lorsque l'incident peut entraîner un non-respect de la réglementation ou une violation des données - doit être un effort continu pour garantir la conformité de l'entreprise.

HOPEX Privacy Management fournit un portail permettant à toute personne de l'entreprise de signaler un incident. Le DPO et d'autres responsables de la conformité peuvent examiner de manière centralisée le rapport des incidents, en évaluer la gravité et définir si besoin les actions à entreprendre pour garantir la protection des données à caractère personnel. En ce qui concerne les violations de données, les capacités de reporting d'HOPEX Privacy Management peuvent permettre de réduire le temps écoulé entre la découverte d'un incident et sa prise en compte par l'organisation et faciliter ainsi le respect du délai de déclaration dans les 72 heures exigées dans les cas les plus graves.

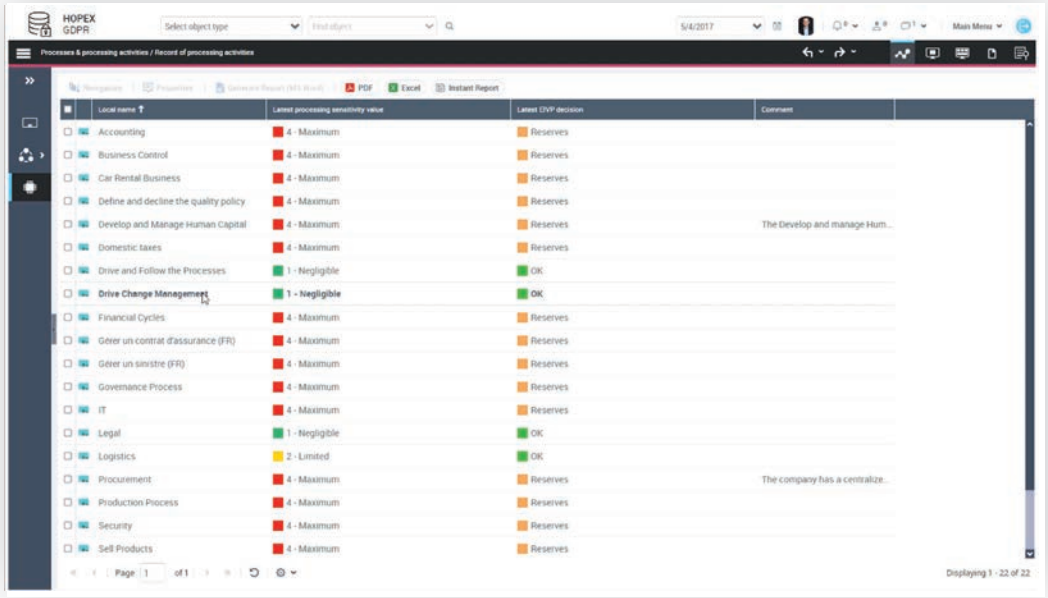
Une fois les incidents signalés et suivis, il est également important d'identifier leur origine. L'incident est-t-il le résultat d'un problème ponctuel ou bien d'un problème structurel ? Comprendre la portée de l'incident, sa nature, le type de données concernées, la catégorie de données et le risque pour les personnes concernées peuvent aider à redéfinir les priorités de conformité et à mettre en œuvre des mesures correctives. Le DPO ainsi que les autres parties prenantes peuvent grâce à HOPEX comprendre l'évolution des traitements liés aux données personnelles ainsi que des risques associés et mettre en œuvre cycle d'amélioration continue afin de garantir le maintien de la conformité dans le temps.

6. Démontrer votre conformité

GDPR met l'accent sur les preuves - démontrées de manière complète et détaillée - de respect de toutes les exigences en matière de protection des données personnelles. Car une autorité de contrôle peut demander au DPO de lui fournir des informations spécifiques, relatives aux preuves de conformité, dans des délais très courts. Cette information peut comprendre :

- Un registre des traitements
- Un compte rendu des violations de données
- Une DPIA des activités de traitements à hauts risques
- Les détails contractuels entre votre entreprise et un prestataire tiers traitant et/ou contrôlant des données pour votre compte

La fonctionnalité de reporting disponible dans HOPEX Privacy Management vous permet de générer un document unique qui décrit : vos processus pour gérer les données personnelles, les résultats de votre DPIA, les demandes des clients concernant les données personnelles, vos risques liés à la protection des données personnelles, incidents, et plans d'actions (ainsi que leurs évolutions). Ce document peut être partagé intégralement ou partiellement avec les autorités de contrôle, le cas échéant. Par ailleurs, le format et contenus des rapports requis sont facilement paramétrables. Et enfin, le référentiel HOPEX est collaboratif, il favorise l'alignement des parties prenantes, il facilite la coordination des actions au sein de l'entreprise, et permet de communiquer l'information appropriée à ceux qui n'y auraient pas accès grâce aux nombreux formats d'export disponibles.



Démontrer la conformité grâce aux rapports détaillés sur la gestion des données

Conclusion

GDPR est inévitable, quelle que soit la taille de votre organisation, son secteur ou son chiffre d'affaires. Vous manquez de temps pour effectuer votre mise en conformité ? Avez-vous identifié le périmètre du travail à étudier ? Savez-vous de combien d'informations vous disposez et ce qui vous reste à collecter et à évaluer ? Qu'en est-il de la gestion de vos risques ? Nous pouvons vous accompagner dans votre travail de mise en conformité, qu'il soit de court ou de long terme.

À propos de MEGA

Fondée en 1991, MEGA est un éditeur français d'envergure mondiale reconnu leader international sur le marché depuis plus de onze ans. Présente sur les 5 continents, l'entreprise travaille en partenariat avec ses clients et les accompagne dans leurs projets de gouvernance et de transformation. MEGA les aide à prendre les bonnes décisions pour optimiser leur mode de fonctionnement et accélérer la création de valeur. La plateforme HOPEX connecte et centralise l'ensemble des informations liées aux métiers, au système d'information, aux données et aux risques dans un référentiel commun tout en s'intégrant parfaitement dans l'écosystème existant de l'entreprise. Les équipes Services de MEGA accompagnent et guident les clients dans leurs projets en suivant une approche pragmatique qui garantit un retour sur investissement rapide.

www.mega.com/fr

MEGA
SEE THE BIGGER PICTURE