Informatica

Livre blanc

Recommandations permettant de gérer l'aspect « données » du GDPR

À PROPOS D'INFORMATICA

La transformation digitale fait évoluer les attentes : service amélioré, livraisons plus rapides, à moindre coût.

Informatica se concentre à 100 % sur les données, car ce sont les données qui font tourner le monde. Les entreprises ont besoin de solutions de données pour le Cloud, les projets Big Data, le temps réel et les flux de données en continu. Informatica est le premier fournisseur mondial de solutions de gestion de données, que ce soit dans le Cloud, sur site ou dans les environnements hybrides.

Plus de 7 000 entreprises du monde entier font appel aux solutions de données d'Informatica.

Table des matières

1. Synthèse

À compter de mai 2018, le Règlement de confidentialité des données générales (GDPR) de l'Union européenne entrera en vigueur, améliorant ainsi la protection des données personnelles. Le GDPR s'applique à toute organisation basée dans l'UE et à toute organisation (partout dans le monde) qui traite les données personnelles des personnes concernées qui y résident, lorsqu'elle fournit des produits ou des services, ou qu'elle surveille ou suit leurs activités. Ce règlement pourrait avoir des répercussions importantes pour diverses organisations et la manière dont elles gèrent les données relatives aux clients, consommateurs, partenaires, salariés et autres « sujets de données », si ledit « sujet de données » est un particulier. Le GDPR affecte l'accès aux données d'un particulier, ainsi que leur stockage, traitement, transfert et communication. Il suppose également l'application de sanctions très lourdes en cas de violation.

Conformément au GDPR, un grand nombre d'organisations devront comprendre parfaitement la manière dont elles utilisent les informations actuelles et futures pour intégrer ces nouvelles exigences de confidentialité des données et améliorer la protection des droits à la confidentialité des citoyens. Pour beaucoup, les changements liés aux pratiques de gestion de l'information exigeront une évaluation approfondie des fonctionnalités de données actuelles et futures. Ce document explique comment analyser ces exigences permet de mieux comprendre les problèmes liés aux données. En outre, les organisations de direction pourront prendre leurs initiatives GDPR respectives.

Pour faciliter cette compréhension, ce document aborde une partie des questions les plus fréquentes que diverses organisations posent lors de la transition vers la conformité au GDPR. Nous qualifions ces questions de « questions de point d'entrée ». Pour aider à répondre à chaque question de point d'entrée, nous avons défini des exigences de fonctionnalité que nous considérons comme importantes. Selon chaque aptitude, un cas d'utilisation de solution technologique est fourni pour expliquer comment cette aptitude peut être développée. Le tableau suivant illustre le lien entre tous ces éléments.

Question de point d'entrée	Exigence de fonctionnalité	Cas d'utilisation de solution technologique
Où nos données potentielles dans le champ se trouvent-elles ?	Détection des données sensibles et analyse des risques	Détection et protection des données
Comment nos données personnelles sont-elles utilisées ?	Interprétation de la stratégie	Gouvernance des données d'entreprise
Comment gérer les sujets de données ?	Gestion des données personnelles	Comparaison des données et cas d'utilisation en matière de liaison
Comment sécuriser les données et éviter les tentatives d'accès non autorisées ?	Application de mesures de contrôle de la sécurité des données	Détection et protection des données

Dans certains cas, les exigences, comme la gestion et l'obtention du consentement, peuvent couvrir plusieurs exigences de fonctionnalité et cas d'utilisation de solution technologique. Ainsi, les organisations doivent bien connaître les difficultés éventuellement rencontrées.

Alors qu'il pose un grand nombre de problèmes, le GDPR offre un vaste champ de possibilités concernant l'utilisation des données. Ce document décrit les approches potentielles d'étude de cas d'utilisation et s'appuie sur notre vaste expérience en gestion de données pour permettre aux organisations de résoudre ces problèmes et d'intégrer des fonctionnalités innovantes de gestion, de gouvernance et de sécurité des données pour optimiser leurs programmes de conformité respectifs. Informatica fournit des solutions logicielles intégrées innovantes pour automatiser, sécuriser et contrôler les données. Ces solutions peuvent rapidement aider les organisations à mettre en œuvre leurs initiatives GDPR.

2. Contexte

2.1 Contexte général et implications potentielles

La digitalisation de la société actuelle évolue de manière rapide : environ chaque organisation exploite la puissance des données pour mieux prendre des décisions, s'engager auprès de ses clients et partenaires, et développer des processus métiers transformationnels. Selon la Commission européenne, la plupart des données créées, recueillies, traitées et stockées sont en réalité des données personnelles, lesquelles peuvent fournir des informations complètes sur les personnes concernées dans l'UE.

Les normes actuelles sur la protection des données ne réduisent pas forcément les zones d'incertitude concernant la protection et la sécurité des données personnelles. La diversité des normes sur la protection des données dans les États membres de l'UE est telle qu'elle en devient frustrante pour les personnes concernées. Pour 90 %, le même règlement de protection des données devrait être appliqué dans l'ensemble de l'UE, quel que soit l'emplacement de stockage ou de traitement de leurs données respectives.*

Ainsi, le GDPR a été adopté pour mieux protéger les droits fondamentaux à la confidentialité des citoyens à l'ère du numérique et tenir compte des préoccupations liées à la diversité des lois sur la protection des données.

Conformément au GDPR, un grand nombre d'organisations devront début mai 2018 gérer et protéger plus efficacement les données relatives aux clients, citoyens, salariés et autres personnes. Ce règlement s'applique aux personnes concernées dans l'UE, quels que soient leur nationalité ou lieu de résidence, pour leur fournir des principes et des normes sur la protection des données personnelles.

Le GDPR étant un règlement basé sur des « principes », on suppose que les organisations doivent tenir compte des obligations qu'elles sont ou non en mesure de respecter, compte tenu de leur situation particulière et de l'utilisation des données. Ainsi, un grand nombre d'organisations devront interpréter ces principes d'une certaine façon pour guider et gérer la mise en œuvre de leurs initiatives GDPR.

Conformément au GDPR, elles devront mieux savoir comment utiliser leurs informations actuelles et futures pour respecter ces nouveaux principes de confidentialité des données. Cela aura un impact sur les salariés, les processus, les technologies et les pratiques et politiques de gestion de données d'un grand nombre d'organisations.

Tout manquement au règlement de leur part pourra entraîner l'application de lourdes pénalités financières, selon le type et l'ampleur de la violation. Des amendes pouvant atteindre jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel global de l'organisation dans le monde entier pourront être infligées, le chiffre d'affaires annuel le plus important étant retenu.

* http://ec.europa.eu/justice/data-protection/reform/index_en.htm

2.2 À qui le GDPR s'applique-t-il ?

La conformité au GDPR couvre plusieurs dimensions ; elle ne se limite pas à la géographie physique. Les organisations, qu'elles soient basées en Amérique du Nord, en Asie ou dans d'autres régions du monde, doivent respecter ce règlement si elles enregistrent et traitent les données de sujets de l'UE. Aujourd'hui, les organisations qui traitent directement avec les consommateurs (B2C), les organisations qui traitent avec d'autres organisations (B2B), ainsi que les sociétés de traitement de données dédiées assurent la gestion des données personnelles. Les organisations qui traitent les données des personnes concernées dans l'UE devront connaître parfaitement les exigences de conformité, quel que soit le pays où leurs centres de données sont implantés ou où elles réalisent des opérations.

2.3 Qu'est-ce qui complique l'application du GDPR en termes de données ?

Pour de nombreuses organisations, différents problèmes liés aux données concernant le GDPR existent. La conformité au GDPR suppose le contrôle et la gouvernance des données personnelles dans une organisation. Toutefois, la prolifération des données au sein des organisations et de leurs écosystèmes peut compliquer la gestion des données. Certaines tendances majeures, comme la diversité accrue des données et la transition vers l'informatique basé sur le Cloud, compliquent davantage la gestion et la sécurité des données en créant un environnement informatique très dynamique. Afin d'illustrer ces problèmes, nous avons posé quelques questions auxquelles un bon nombre d'organisations ont du mal à répondre par rapport au GDPR :

- Où toutes les données pertinentes et dans le champ auxquelles le GDPR pourrait s'appliquer se trouvent-elles dans l'organisation et son écosystème ? Ces données sont-elles menacées ?
- Comment les organisations en assurent-elles le suivi dans leurs écosystèmes opérationnels respectifs ?
- Comment une organisation peut-elle définir et gérer l'ensemble de ses données pertinentes pour veiller à mettre en œuvre et appliquer toutes les politiques et procédures nécessaires ?
- Où toutes les données pertinentes et dans le champ auxquelles le GDPR pourrait s'appliquer sont-elles stockées dans l'organisation ? Comment peut-on les identifier et les lier ?
- Comment une organisation obtient-elle et gère-t-elle le consentement d'un sujet de données ? Comment une organisation peut-elle gérer les modifications du choix du consentement du sujet de données ou gérer la définition du consentement ?
- Comment une organisation peut-elle répondre efficacement aux demandes d'accès de sujets ou d'application du droit d'effacement ou de portabilité dans les délais requis ?
- Comment l'organisation contrôle-t-elle l'accès aux données pertinentes ? Les données confidentielles sont-elles supprimées lorsqu'elles ne sont pas requises pour le fonctionnement ou l'activité de l'organisation ?

2.4 Types de données potentiellement dans le champ

Un autre problème éventuel consiste à savoir comment les organisations réagissent aux types de données qu'elles détiennent. En l'occurrence, nous définissons des types de deux manières :

1. Un type d'entité de données
2. Un type de technologie gérant le type d'entité de données

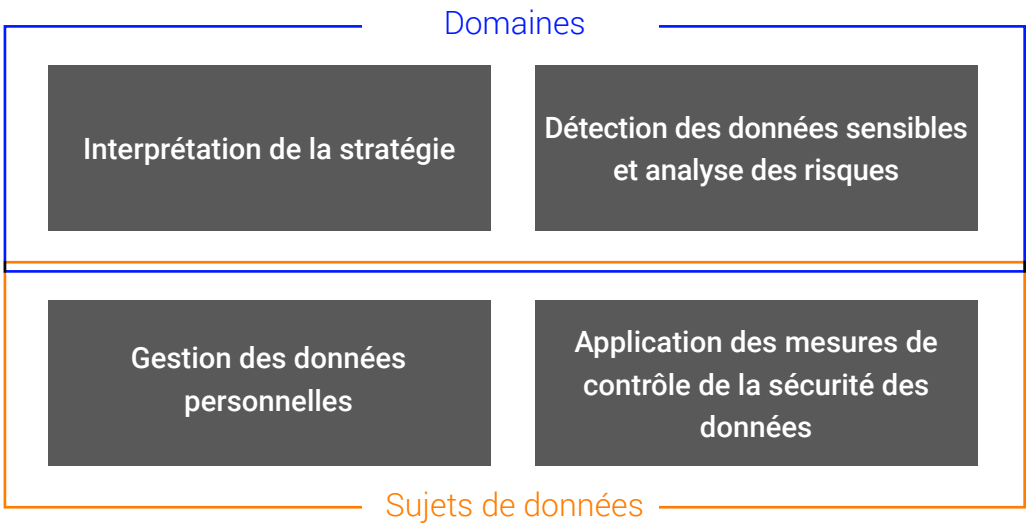
La plupart des informations relatives à des sujets de données correspondent à un ou plusieurs types d'entités de données, ainsi qu'à un ou plusieurs types de technologies. Le diagramme ci-dessous présente des exemples de types potentiels de données et de technologies, qui peuvent s'appliquer aux données GDPR dans le champ :

ENTITÉ DE DONNÉES	TECHNOLOGIE				
• Utilisateur • Client • Titulaire d'un contrat d'assurance • Bénéficiaire • Contact • Salarié • Sous-traitant • Bénévole • Visiteur • Autre	• Structurée • Semi-structurée • Non structurée	• En ligne • De proximité • Hors ligne • Sauvegarde	• Digitale • Physique • Combinée	• Explicite • Implicite • Combinée	• Interne • Externe

Ces différents types peuvent obliger les organisations à envisager d'utiliser des approches, méthodes et technologies très différentes pour capturer et gérer les données GDPR dans le champ.

3. Points d'entrée, exigences de fonctionnalité et cas d'utilisation de solution technologique

Pour développer la connaissance, la sensibilisation et la planification des activités d'aide, Informatica a identifié plusieurs questions de point d'entrée soulignant une partie des problèmes les plus courants liés aux données GDPR. En général, ces points d'entrée s'inspirent de questions simples pouvant demander aux organisations de bien vouloir tenir compte des salariés, processus et technologies nécessaires afin d'y répondre. Pour aider à répondre à ces questions, nous décrivons les fonctionnalités potentielles requises, ainsi que certains cas d'utilisation de solution technologique fournissant ces fonctionnalités. Les fonctionnalités requises sont classées par groupes ; le diagramme ci-dessous illustre les principes de ces groupes et la pertinence de chacun.



Ces fonctionnalités portent sur deux points : les domaines et les sujets de données.

Les **domaines** renvoient aux domaines des données des personnes concernées. Ils renseignent sur la détection et la gestion des domaines. Ces informations permettent également de définir le champ, ainsi qu'une vue organisationnelle des données.

Les **sujets de données** renvoient aux données réelles de la personne concernée au niveau transactionnel. Ils renseignent sur la gestion des données personnelles. En outre, ces informations permettent de fournir des réponses et des informations au niveau du sujet.

3.1 Question de point d'entrée : où nos données potentielles dans le champ se trouvent-elles ?
Contexte : En général, les données sont réparties sur divers systèmes, applications et sources d'une entreprise. C'est notamment vrai pour les grandes organisations et celles qui ont prospéré suite à un rachat. En raison des différents rôles que les personnes concernées dans l'UE peuvent jouer dans une organisation (client, fournisseur, partenaire, salarié, etc.), il est peu probable que les données personnelles se limitent à un service ou système unique. Les organisations utilisant des systèmes informatiques plus diversifiés doivent non seulement tenir compte des données des applications de base, mais également des feuilles de calcul, des bases de données locales et des solutions Big Data.

Fonctionnalités requises : la fonctionnalité de détection des données sensibles et d'analyse des risques permet de détecter des données sur une vaste gamme de solutions technologiques et, ainsi, en s'aidant d'autres sources d'information, telles que les quantités de données réelles et la prolifération des données, d'évaluer les risques en matière de données. Grâce à cette évaluation des risques, les organisations arrivent à savoir où les données présentant un risque majeur sont stockées, afin de pouvoir hiérarchiser les exigences d'application d'éventuelles mesures correctives ou de contrôle de la sécurité en fonction du risque. Observer cette évaluation des risques à terme permet de déterminer si les mesures correctives ou de contrôle prises améliorent la position de risque des données. On peut exiger le consentement du sujet pour soutenir des objectifs légitimes afin que certaines fonctionnalités, comme le lignage de données, permettent aux organisations d'identifier de nouveaux magasins de données personnelles dans le but de comprendre les changements potentiels en cours.

Cas d'utilisation de solution technologique : on peut considérer la détection des données sensibles et l'analyse des risques comme un cas d'utilisation à des fins de détection et de protection, l'accent étant mis sur la détection. Ces fonctionnalités de base permettent de connaître l'emplacement des données sensibles dans le champ et la zone de prolifération correspondante ; les risques liés aux données sont analysés. Les fonctionnalités types pouvant s'appliquer à ce cas d'utilisation sont notamment :

- **La définition d'une stratégie de gestion des données :** définitions des termes commerciaux et informatiques, données floues, conflit stratégique
- **La détection automatique des données :** recherche des données sensibles et dans le champ pertinentes, premier passage et surveillance permanente, classification des données, soutien de l'intégration système
- **La prolifération des données :** où les données se situent-elles ? Où sont-elles acheminées ? Existe-t-il d'autres sources ?
- **L'évaluation des risques liés aux données :** processus basé sur le transfert des données + prolifération + accès + volume, hiérarchisation et planification, historique et suivi à terme de l'évaluation
- **La protection des données :** déterminez les points où l'accès aux données doit être restreint, les données à pseudonymiser, la nécessité de crypter les données et l'affichage des données selon l'heure, l'emplacement et le rôle

Les solutions technologiques : Informatica Secure@Source permet de détecter les différents emplacements des données dans le champ, de classer les données, de surveiller la prolifération des données et d'évaluer les risques. Le suivi à terme indique la manière dont les changements opérés affectent de manière positive ou négative les mesures de conformité prises.

Bénéfice : ces outils permettent de connaître l'emplacement des données et de les évaluer en fonction du risque.

3.2 Question de point d'entrée : comment nos données personnelles sont-elles utilisées ?
Contexte : la société subit actuellement une transformation digitale qui touche tous les secteurs. La quantité croissante de données générées, recueillies et analysées est clairement une tendance mondiale. En outre, un pourcentage important de ces données est imputable aux données personnelles de particuliers. Parce qu'elles prolifèrent dans l'organisation, la propriété, le contrôle et la gestion de ces données sont de plus en plus difficiles. À l'instar de nombreux types de règlements de conformité, on va optimiser le respect du GDPR en adoptant une approche à l'échelle de l'entreprise en matière de gouvernance de données.

Fonctionnalités requises : la fonctionnalité d'interprétation stratégique permet de bien comprendre les stratégies, les responsabilités, les processus, les termes de données et les modèles logiques et physiques d'un point de vue commercial et technologique. Autre point important : elle lie la connaissance de l'environnement technique à celle de l'environnement commercial. Ce lien fournit aux organisations un aperçu global des informations concernant leurs domaines de données dans le champ. En outre, il fait partie intégrante d'une approche utilisée pour gérer leurs données.

Cas d'utilisation de solution technologique : on peut considérer l'interprétation stratégique de cas d'utilisation en matière de gouvernance de données d'entreprise. Ces fonctionnalités de base permettent de donner un point de vue ascendant et descendant sur la gestion organisationnelle des données et de lier les points de vue commerciaux et informatiques sur les données. Les exigences types pouvant s'appliquer à ce cas d'utilisation sont notamment :

- **La définition de la stratégie :** définitions des termes commerciaux et informatiques, documentation à tous les niveaux opérationnels des données commerciales, logiques et physiques, et des modèles de processus
- **Les responsabilités :** qui détient les données ? Qui les utilise ? Quelles fonctions sont responsables de la qualité et de la sécurité ?
- **La définition des termes et processus :** processus métiers, entités de données clés, caractéristiques, systèmes, qualité et contrôles qualité, normalisation, définitions commerciales du consentement
- **Le processus de changement :** gestion du processus concernant les définitions, gestion du processus de changement, gouvernance des processus
- **Le lien avec des objets :** lien entre les objets logiques et physiques, lignage des données commerciales et techniques, intégration de la qualité des données

Les solutions technologiques : utilisez des solutions de gouvernance de données d'entreprise permettant aux professionnels de la vente et de l'informatique de collaborer pour réaliser un objectif commun de gouvernance de données. Certaines solutions, telles que **la solution de gouvernance de données Informatica Axon**, ont spécialement été conçues pour harmoniser les points de vue commerciaux et informatiques sur les données, et lier les données logiques et physiques.

Bénéfice : contribution plus simple et rapide de tous les experts en la matière pour définir les processus, les politiques et les entités de données dont l'organisation dispose pour créer une fonction de gouvernance globale de données dans le champ.

3.3 Question de point d'entrée : comment gérer les données des personnes concernées ?
Contexte : conséquence directe de l'utilisation diversifiée des données dans des environnements informatiques complexes, il est difficile de donner un point de vue unique sur l'ensemble des informations pour chaque sujet de données. Ce problème est lié au fait que plusieurs systèmes utilisent des mécanismes très différents pour stocker et indexer les données. Il est difficile de respecter le GDPR sans avoir un aperçu complet des données de chaque personne concernée et de la manière dont elles sont stockées, gérées ou traitées dans une organisation, notamment pour ce qui est des droits de cette personne.

Fonctionnalités requises : la fonctionnalité de gestion des données personnelles permet d'identifier les données d'un sujet dans toutes les sources identifiées, de comparer et de lier des données pour chaque personne concernée, et de créer un référentiel Entity 360. Ce référentiel fournit une source de données de haute qualité concernant les données réelles actuelles contenues dans les sources de données dans le champ et la manière dont chaque donnée est liée à la personne concernée. Le référentiel Entity 360 peut être utilisé comme source de données faisant autorité lorsque les organisations répondent aux demandes d'accès de sujets ou d'application du droit d'effacement ou du droit de portabilité. D'un point de vue commercial, Entity 360 peut aider les organisations à gérer le consentement à l'utilisation des données personnelles, puis le consentement proprement dit : à quel moment ce consentement a-t-il été donné/révoqué ? Par quel biais ? Quelles conditions particulières ont été convenues ?

Cas d'utilisation de solution technologique : on peut considérer la gestion des données personnelles comme un cas d'utilisation en matière de comparaison et de liaison de données. Ces fonctionnalités de base permettent d'identifier les données de sujets sur plusieurs systèmes. En outre, elles fournissent un aperçu intersystème des données en comparant les données similaires et en les liant. Les fonctionnalités types pouvant s'appliquer à ce cas d'utilisation sont notamment :

- **L'accès aux données pertinentes :** données de profil des personnes concernées, extraction des données pertinentes à partir des systèmes sources, application des processus d'analyse aux demi-contenus et aux contenus non structurés
- **Le traitement de la qualité des données :** évaluation de la qualité des données, application manuelle/automatique des mesures correctives, contrôle des processus en cas de mesure corrective manuelle, rapports métriques
- **Source de données unique fiable sur les personnes concernées, y compris le consentement et la manière dont il est obtenu et géré :** comprend les différents points de vue et perspectives de la personne concernée en fonction de son consentement
- **Comparaison et liaison :** définition des règles de comparaison basées sur les définitions de processus métiers, comparaison des données, liaison des données similaires et de l'évaluation, consentement associé
- **La persistance des données :** persistance des données liées/non liées, des analyses et des rapports

Les solutions technologiques : utilisez des solutions permettant de détecter à l'aide d'algorithmes avancés les données des personnes concernées dans tous les domaines de données pour comparer toutes les données liées à la même personne concernée, quel que soit leur emplacement de stockage. **Informatica Relate 360** utilise des algorithmes avancés pour identifier les données associées à la même personne concernée. En outre, la gestion des données de référence fournit un cadre permettant de maintenir et gérer une vue commune des données sur les personnes concernées.

Bénéfices : le point de vue unique de particuliers présente des avantages pour l'entreprise au-delà du GDPR. C'est notamment vrai si la personne en question est un client qui souhaite de plus en plus vivre des expériences personnelles sur mesure. D'un point de vue du GDPR, la possibilité de lier toutes les données pour chaque personne concernée permettra d'alléger le fardeau de l'exercice des droits de cette personne : le droit de connaître la manière dont les données sont utilisées, le droit à l'oubli et la vérification de l'application appropriée du consentement.

3.4 Question de point d'entrée : comment sécuriser les données et éviter les tentatives d'accès non autorisées ?

Contexte : les contrôles de protection des données constituent une approche à utiliser pour imposer les exigences de consentement du GDPR et contribuer à protéger les données personnelles. Les professionnels de l'informatique peuvent demander la suppression, le masquage ou la pseudonymisation des données de production utilisées à des fins de test pour les transferts de données externes. Le contrôle de l'accès aux données personnelles au niveau utilisateur dans les applications doit être examiné à des fins de conformité.

Fonctionnalités requises : la fonctionnalité de **détection et protection des données** permet de contrôler l'accès aux informations sur les personnes concernées et de les protéger. En général, ces informations sont visibles par un grand nombre de personnes différentes au sein d'une organisation et de son écosystème. Les mesures de contrôle de la sécurité des données permettent de supprimer ou masquer les informations que les personnes non autorisées ne doivent pas voir, alors qu'elles les rendent accessibles aux personnes autorisées à les voir.

Cas d'utilisation de solution technologique : on peut considérer l'activation du contrôle du consentement comme un cas d'utilisation en matière de détection et de protection de données. Ces fonctionnalités de base permettent de protéger et sécuriser l'accès aux données, en utilisant des contrôles axés sur les données, comme les contrôles de masquage, de cryptage et d'accès, et de gérer le cycle de vie des données, notamment l'archivage et la suppression des données, ainsi que l'application. Les fonctionnalités types pouvant s'appliquer à ce cas d'utilisation sont notamment :

- **La saisie des données d'analyse des risques :** application de l'évaluation des risques aux méthodes de contrôle direct des données
- **L'orchestration :** possibilité de planifier et coordonner les tâches de protection des données sur la base des risques identifiés et le contrôle de l'accès ou des cas dangereux
- **Les contrôles de sécurité des données :** masquage dynamique ou statique, pseudonymisation, accès basé sur les rôles, cryptage ou tokénisation.
- **L'historique des modifications/mises à jour :** application sur les systèmes sources, masquage des données ou archivage des résultats par rapport aux données de consentement, génération de pistes de vérification à titre de preuves
- **L'archivage :** extraction des données depuis les systèmes de production, activité de journalisation visant à fournir des preuves et mise hors ligne pour éviter tout accès ou usage accidentel

Les solutions technologiques : utilisez des solutions permettant de gérer le cycle de vie des données et de leur appliquer certains contrôles. Les fonctionnalités de **masquage de données persistantes Informatica** et de **masquage de données dynamiques Informatica** peuvent aider à limiter automatiquement le nombre de personnes et de systèmes bénéficiant d'un accès illimité aux données personnelles. **Informatica Secure@Source** permet d'appliquer des mesures correctives liées à la sécurité des données en orchestrant les mises à jour des contrôles de sécurité.

Bénéfices : vous automatisez le masquage des données pour réduire le risque de violation de la confidentialité des données personnelles. La visibilité des données personnelles se limite aux personnes autorisées ; elles ne sont pas diffusées sans dispositif de protection adapté.

4. Partenaires

À l'instar des nombreux types de normes de conformité, seule la technologie ne garantit aucune conformité. Les organisations devront peut-être fournir un leadership mieux pensé pour la transition vers la conformité au GDPR, ainsi que la fourniture de solutions technologiques et de services classiques. Informatica collabore avec de nombreux partenaires hautement qualifiés et compétents pour vous soutenir dans la mise en œuvre de l'initiative GDPR plus importante. Ces partenaires ont été spécifiquement choisis en raison de leur connaissance approfondie de la gestion des données et la manière dont ils mettent la conformité au GDPR en avant.

Trouvez le bon partenaire ou contactez votre représentant Informatica local pour vous aider à trouver les meilleurs partenaires en fonction de vos besoins et exigences.

5. Conclusion

Ce document établit la nécessité pour les organisations d'examiner les implications du GDPR en matière d'applications. Ce nouveau règlement présente différents enjeux et opportunités pour un grand nombre d'organisations. Parce qu'il entrera prochainement en vigueur, elles seront beaucoup à devoir tenir compte de la manière dont leur interprétation des principes du GDPR affectera les procédures de gestion de données actuelles et futures.

Pour aider les organisations à passer rapidement à la mise en pratique de ces interprétations, Informatica a mis l'accent sur les questions de point d'entrée clés que les intervenants posent et proposé d'utiliser des fonctionnalités qui devront permettre d'y répondre. Ces questions et fonctionnalités ne se contentent pas de traiter une partie de l'ensemble des exigences du GDPR ; ils permettent plutôt de créer une gamme complète de fonctionnalités pour résoudre les nombreux problèmes liés aux données que ce règlement pose.

Un cas d'utilisation de solution technologique est fourni pour chaque fonctionnalité. Chaque cas d'utilisation décrit les différents types de technologies et solutions logicielles que l'on peut utiliser pour le fournir.

Informatica est le plus grand fournisseur de gestion de données depuis plus de 20 ans. Il a résolu les problèmes complexes de gestion de données de milliers d'organisations dans le monde entier. Le GDPR présentera divers problèmes complexes de gestion des données pour nombre d'entre elles. Informatica et son écosystème de partenaires associés sont bien placés pour aider ces organisations à mettre en œuvre leurs initiatives GDPR respectives.

6. Clause de non-responsabilité

La conformité au GDPR dépend de la situation particulière de l'entreprise, des opérations qu'elle réalise et de la manière dont elle utilise les données. Ce document donne des pistes de réflexion pouvant s'avérer utiles dans le cadre de la mise en conformité au GDPR de l'organisation. Il ne prétend pas constituer un avis, un conseil ou des recommandations juridiques. L'organisation doit consulter son conseiller juridique concernant les obligations qu'elle doit ou non respecter.

Informatica

Siège mondial, 2100 Seaport Blvd., Redwood City, CA 94063, États-Unis Téléphone : +33 1 42 04 89 00 (France)
Numéro gratuit aux États-Unis : 1.800.653.3871
www.informatica.com/fr www.informatica.com linkedin.com/company/informatica twitter.com/InformaticaFr

IN09_0218_03337