Accélérez votre projet de conformité RGPD (règlement général sur la protection des données)

En utilisant les produits Oracle Database Security

LIVRE BLANC ORACLE | JANVIER 2017

AUTEUR : DINESH RAJASEKHARAN | RESPONSABLE PRODUIT PRINCIPAL | DATABASE SECURITY

Avertissement : l'objectif de ce document est d'aider les entreprises à comprendre comment la technologie Oracle Database Security permet d'assurer la conformité avec certaines exigences du règlement général sur la protection des données de l'Union européenne. Certaines des technologies Oracle Database Security peuvent ne pas être pertinentes en fonction de l'environnement spécifique d'une entreprise. Oracle recommande systématiquement de tester les solutions de sécurité au sein de votre environnement spécifique afin de vous assurer que les performances, la disponibilité et l'intégrité sont au niveau requis.

Les informations contenues dans ce document ne doivent pas être interprétées ni utilisées comme un avis juridique sur le contenu, l'interprétation ou l'application de toute législation, réglementation ou directive réglementaire. Les clients existants et potentiels doivent s'adresser à leur propre conseiller juridique pour comprendre l'applicabilité de toute loi ou réglementation relative à leur traitement de données personnelles, y compris par l'intermédiaire des produits ou services de tout fournisseur.

Introduction

Alors que les entreprises se préparent à l'application du nouveau règlement général sur la protection des données (RGPD) de l'Union européenne (UE) en envisageant d'apporter des modifications à leurs processus, à leur personnel et à leurs contrôles techniques, il est important pour elles de prendre connaissance de la façon dont les produits Oracle peuvent les aider à accélérer l'adoption des contrôles d'évaluation, de prévention et de détection du RGPD. Ces solutions constituent des outils de contrôle simples nécessaires à la mise en œuvre de bon nombre des principes de sécurité des données préconisés par le RGPD.

Ce livre blanc identifie plusieurs exigences clés du RGPD et les relie aux fonctionnalités Oracle Data Security correspondantes. Si le RGPD rend obligatoires de nombreux principes et exigences en matière de gouvernance et de protection des données (notamment pour les transferts internationaux de données), ce livre blanc traite uniquement des principes de sécurité clés du RGPD relatifs à la protection des données qui sont susceptibles d'être mis en œuvre grâce aux fonctionnalités Oracle Data Security.

Genèse du règlement général sur la protection des données (RGPD)

L'Union européenne (UE) a imposé sa norme de protection des données il y a 20 ans par le biais de la directive générale sur la protection des données 95/46/CE. Étant donné qu'une directive européenne donne aux États membres une certaine marge de manœuvre pour sa transposition dans le droit national, l'Europe a hérité d'une mosaïque de différentes lois sur la protection de la vie privée. En outre, l'augmentation des violations de sécurité, la vitesse des développements technologiques et la mondialisation sur ces 20 dernières années ont apporté leur lot de nouveaux défis en matière de protection des données à caractère personnel. Afin de résoudre cette situation, l'Union européenne a développé le règlement général sur la protection des données (RGPD).

Objectifs de sécurité clés du RGPD

Les objectifs de sécurité clés du RGPD sont les suivants.

Objectif	Description
Faire de la confidentialité des données un droit fondamental	Le RGPD considère que la protection des données est un droit de l'homme fondamental des personnes physiques, ce qui inclut un « droit à la protection » de leurs données à caractère personnel. Toute personne physique établie dans l'Union européenne, ou manipulant ou ciblant les données à caractère personnel d'individus localisés dans l'Union européenne, doit disposer des processus, de la technologie et de l'automatisation nécessaires à la protection efficace de ces données.

Clarifier les responsabilités pour la protection des données de l'Union européenne	Le RGPD s'applique à un responsable du traitement ou un sous-traitant localisé ou établi dans l'Union européenne, ou à une entreprise localisée hors de l'Union européenne mais qui propose des biens ou des services hors des frontières de l'Union européenne à une personne concernée localisée dans l'Union européenne, ou qui surveille le comportement de personnes concernées localisées dans l'Union européenne.
Définir une base de référence pour la protection des données	Afin d'éviter la fragmentation et l'ambiguïté, le RGPD a défini une base de référence pour la protection des données en exigeant que toute personne traitant les données à caractère personnel d'un individu localisé dans l'Union européenne respecte les directives établies dans le RGPD.
Étoffer les principes de la protection des données	Le RGPD considère uniquement le chiffrement comme l'un des composants d'une stratégie de sécurité globale et préconise que les entreprises envisagent des contrôles d'évaluation, de prévention et de détection en fonction du niveau de sensibilité de leurs données à caractère personnel.
Renforcer le pouvoir exécutif	L'Union européenne vise à assurer la conformité avec le RGPD en appliquant des amendes considérables allant jusqu'à 4 % du chiffre d'affaires annuel en cas de non-respect de la directive.

Acteurs principaux du RGPD

Le RGPD définit divers acteurs afin d'expliquer les concepts de protection des données et les rôles qui leur sont associés :

Acteur	Description
Personne concernée	Personne physique qui peut être identifiée, directement ou indirectement, par l'intermédiaire d'un numéro d'identification. Il peut notamment s'agir d'un identifiant national, d'un numéro de carte bancaire, d'un nom d'utilisateur ou d'un cookie.
Données à caractère personnel	Toute donnée à caractère personnel, y compris à caractère sensible, se rapportant à une personne concernée. Par exemple, son adresse, sa date de naissance, son nom, sa localisation et sa nationalité.
Responsable du traitement	La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Par exemple, le responsable du traitement peut être un organisme ou un directeur informatique (DSI).
Délégué à la protection des données	Personne travaillant pour un organisme responsable du traitement ou un sous-traitant, ayant une connaissance approfondie des lois et des normes relatives à la confidentialité des données. Le délégué à la protection des données est chargé d'aviser le responsable du traitement ou le sous-traitant de ses obligations envers le RGPD et de contrôler la mise en œuvre de ce dernier. Le délégué à la protection des données assure la liaison entre le responsable du traitement/sous-traitant et l'autorité de contrôle. Par exemple, un délégué à la protection des données peut être un responsable ou un administrateur de la sécurité.

Sous-traitant	La personne physique ou morale, le service ou tout autre organisme qui traite les données à caractère personnel pour le compte du responsable du traitement. Par exemple, un développeur, un testeur ou un analyste. Un sous-traitant peut également être un prestataire de service Cloud ou une entreprise d'externalisation.
Destinataire	La personne physique ou morale, le service ou tout autre organisme qui reçoit des données à caractère personnel. Par exemple, une personne, un conseiller fiscal, un agent ou une compagnie d'assurance.
Entreprise	Toute personne physique ou morale exerçant une activité économique. Cela inclut tous les organismes, du secteur privé comme du secteur public, établis au sein ou hors de l'Union européenne.
Tiers	Toute personne physique ou morale, service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données, par exemple, des partenaires ou des sous-traitants.
Autorité de contrôle	Autorité publique indépendante établie par un État membre (appelée « autorité nationale chargée de la protection des données » dans la directive européenne actuelle relative à la protection des données), par exemple une agence de contrôle.

Exemple hypothétique

Afin de comprendre les divers acteurs, leurs rôles et leurs interactions, imaginons une entreprise fictive de fabrication de gadgets appelée XYZ et établie en France. Les clients de XYZ passent leurs commandes en ligne via le portail Web de l'entreprise. Dans le cadre de son modèle économique multinational, XYZ stocke et traite les données à caractère personnel concernant les individus (« personnes concernées »). Cette entreprise localisée dans l'Union européenne détermine les objectifs et les moyens employés pour traiter les données à caractère personnel (« responsable du traitement »). Les tâches de développement, de test, de service clientèle et de facturation sont externalisées auprès de sous-traitants externes localisés au Brésil et en Inde (« sous-traitants »), où les employés copient souvent les données des clients (« données à caractère personnel ») sur leurs systèmes locaux à des fins de développement, de test et de traitement, respectivement. XYZ entretient également un partenariat avec des entreprises de paiement et de livraisons (« tiers ») établies dans divers pays, et leur fournit les données d'une personne (« données à caractère personnel ») en vue du traitement d'une commande. Une autorité publique indépendante surveille l'application du RGPD (« autorité de contrôle »).

L'illustration suivante montre la répartition géographique des acteurs mentionnés précédemment.

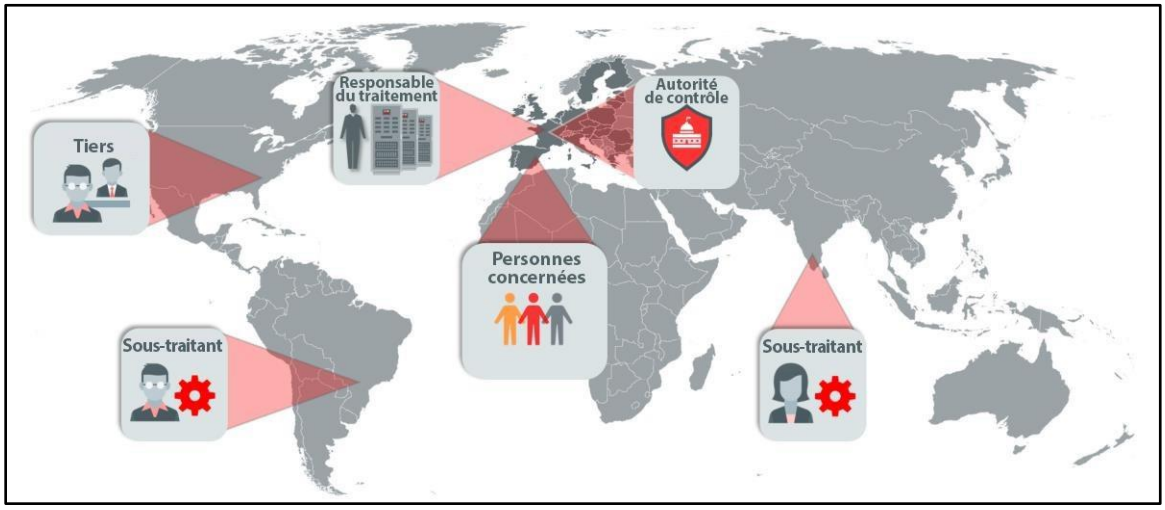

Figure 1 : Acteurs du RGPD avec l'entreprise et le responsable du traitement établis au sein de l'Union européenne

Le RGPD s'applique aux responsables du traitement, sous-traitants et tiers qui sont établis hors de l'Union européenne mais qui manipulent les données des personnes concernées localisées dans l'Union européenne. Par exemple :

- Une société australienne proposant des biens et des services aux résidents de l'Union européenne et exploitant un site Web à vocation mondiale à partir des États-Unis.
- Une société indienne effectuant le suivi des profils de résidents de l'Union européenne (par exemple, un site de réseau social ou des sites Web établis hors de l'Union européenne).
- Un fournisseur (interne ou externe) établi au Canada sans présence physique ni serveurs au sein de l'Union européenne, et proposant des services de Cloud Computing aux ressortissants de l'Union européenne.
- Une campagne marketing pilotée à partir d'une société établie en Chine, ciblant les ressortissants de l'Union européenne (entre autres) et proposant divers services.
- Des fournisseurs de services Cloud établis hors de l'Union européenne, qui sont en mesure d'héberger, directement ou indirectement (via leurs clients et partenaires), des données à caractère personnel appartenant à des résidents de l'Union européenne.
- Une chaîne d'hôtels ou une compagnie aérienne établie aux États-Unis qui stocke des données de ressortissants de l'Union européenne voyageant aux États-Unis.

Le RGPD s'applique également aux entreprises établies hors de l'Union européenne et qui propose des biens et des services ou qui surveillent le comportement d'individus localisés dans l'Union européenne. Son application n'est pas strictement réservée aux entreprises établies dans l'Union européenne.

Dans l'illustration suivante, le responsable du traitement est établi hors de l'Union européenne, mais est tout de même assujetti au RGPD.

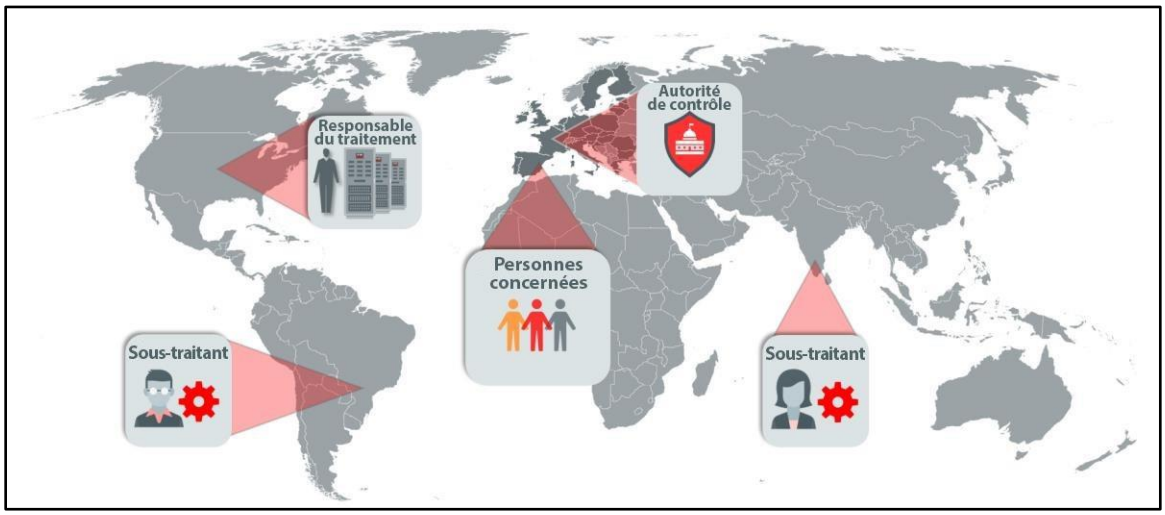

Figure 2 : Acteurs du RGPD avec une entreprise et un responsable du traitement établis hors de l'Union européenne

Exigences clés pour la sécurité des données dans le cadre du RGPD

Les exigences clés pour la sécurité des données dans le cadre du RGPD peuvent être classées en trois grandes catégories : évaluation, prévention et surveillance/détection. Le RGPD exige également la conformité aux principes de protection des données afin d'améliorer la qualité et la rigueur de la protection des données. La présente section résume les exigences clés en termes de sécurité des données mentionnées dans le RGPD.

Évaluation des risques de sécurité

Le RGPD exige que les responsables du traitement effectuent des analyses d'impact sur la protection des données lorsque certains types de traitements de données à caractère personnel sont susceptibles de représenter un « risque élevé » pour la personne concernée. L'évaluation doit inclure une estimation systématique et complète des processus et des acteurs de l'organisme, et de la façon dont ces outils protègent les données à caractère personnel.

> *… Le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires…* *-- Article 35 du RGPD*

Les analyses d'impact sur la protection des données posent les bases de la prévention des violations potentielles en identifiant les failles et les risques.

Prévention des attaques

L'importance de la prévention des violations de la sécurité est mentionnée dans différents points du RGPD.
Ce dernier recommande ainsi plusieurs techniques permettant de prévenir une attaque :

» Chiffrement

Le RGPD considère le chiffrement comme l'une des techniques de base permettant de rendre les données inintelligibles à toute personne ne disposant pas des autorisations d'accès aux données à caractère personnel.

> *… le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : la pseudonymisation et le chiffrement des données à caractère personnel ;*
>
> *-- Article 32 du RGPD*

Conformément aux recommandations du RGPD, en cas de violation des données, le responsable du traitement ne notifie pas les personnes concernées si les données sont chiffrées et rendues inintelligibles à toute personne y accédant, ce qui élimine les coûts de notification pour les organismes.

> *La communication à la personne concernée… n'est pas nécessaire si... le responsable du traitement a mis en œuvre les mesures de protection techniques... appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation en particulier... le chiffrement…*
>
> *-- Article 34 du RGPD*

» Anonymisation et pseudonymisation

L'anonymisation est une technique qui consiste à brouiller ou obscurcir entièrement les données, alors que la pseudonymisation revient à réduire le degré de corrélation d'un jeu de données avec l'identité originale d'une personne concernée. Le RGPD indique que les techniques d'anonymisation et de pseudonymisation peuvent réduire les risques de divulgation accidentelle ou intentionnelle en rendant les informations non identifiables par une personne ou une entité.

> *... La pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données.*
>
> *-- Considérant 28 du RGPD*

Au sujet de l'exclusion des données à caractère personnel rendues anonymes du champ d'application :

> *... Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche.*
>
> *-- Considérant 26 du RGPD*

» Contrôle de l'accès des utilisateurs à privilèges

Le RGPD requiert le contrôle des utilisateurs à privilèges ayant accès aux données à caractère personnel afin d'éviter les attaques provenant de l'intérieur et la compromission de comptes utilisateurs.

> *… Le sous-traitant et toute personne..., ayant accès à des données à caractère personnel, ne peut pas traiter ces données, excepté sur instruction du responsable du traitement…* *-- Article 29 du RGPD*

» Contrôle d'accès au niveau le plus fin

Outre le contrôle des utilisateurs à privilèges, le RGPD préconise l'adoption d'une méthodologie de contrôle d'accès au niveau le plus fin afin de veiller à ce que l'accès aux données à caractère personnel s'effectue de façon sélective et uniquement dans un but défini. Ce type de contrôle d'accès permet aux organismes de réduire autant que possible les accès non autorisés aux données à caractère personnel.

> *… Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.* *-- Article 25 du RGPD*

» Minimisation des données

Le RGPD recommande autant que possible la minimisation de la collecte et de la conservation de données à caractère personnel afin de réduire la limite de conformité. Lors de la collecte, du traitement ou du partage des données d'une personne concernée, les responsables du traitement et les sous-traitants doivent être économes et limiter la quantité d'informations aux nécessités d'une activité spécifique.

> *Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données).*
> *-- Article 5 du RGPD*

Surveillance et détection des failles de sécurité

Bien que les mesures de sécurité préventives aident les organismes à minimiser le risque d'attaque, elles ne permettent pas d'éliminer totalement la possibilité d'une violation des données. Afin de détecter de telles violations, le RGPD recommande l'application des mécanismes suivants de surveillance et d'alerte :

» Données d'audit

Le RGPD recommande non seulement l'archivage ou l'audit des activités effectuées sur les données à caractère personnel, mais également que ces archives soient conservées et centralisées sous la responsabilité du responsable du traitement. En d'autres termes, les sous-traitants et les tiers ne doivent pas être en mesure d'altérer ni de détruire les enregistrements d'audit. Les mécanismes d'audit sont utiles à des fins d'enregistrement, mais également en cas d'enquête suite à une fuite de données.

> *Chaque responsable du traitement et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement.*
> *-- Article 30 du RGPD*

» Surveillance et alertes dans les meilleurs délais

La surveillance constante des activités effectuées sur les données à caractère personnel est essentielle à la détection d'anomalies. Outre une surveillance étroite, le RGPD exige également des notifications dans les meilleurs délais en cas de violation.

> *En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente..., dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance…* *-- Article 33 du RGPD*

Les trois grandes catégories de directives de sécurité (évaluation, prévention et détection) permettent aux organismes de traiter les menaces sous des angles différents et de protéger les données contre tout accès non autorisé.

Qualité de la protection

Pour les organismes de grande comme de petite taille, la mise en œuvre et l'administration de la sécurité des données sans planification appropriée est susceptible d'entraver les opérations informatiques quotidiennes et d'entraîner d'importants surcoûts d'administration. Si ce manque de planification et cette augmentation des coûts ont pu, par le passé, donner des raisons à certaines entreprises de ne pas mettre en œuvre un système de sécurité, avec un règlement tel que le RGPD, la sécurité n'est plus une option mais une obligation. Afin de relever certains de ces défis, le RGPD stipule les lignes directrices suivantes pour réduire les coûts d'administration et améliorer la qualité de la protection :

» Sécurité des données par défaut dès la conception

Le RGPD exige de placer la protection des données au cœur du système. L'intégration de la sécurité lors de la phase initiale de conception du cycle de vie d'une technologie améliore la sécurité intrinsèque du système et garantit que les contrôles techniques de sécurité s'effectueront comme prévu.

> ***Protection des données dès la conception et protection des données par défaut***
>
> *… Le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.* *-- Article 25 du RGPD*

» Centralisation

Le RGPD recommande une administration centralisée lors du traitement de la sécurité de plusieurs applications et systèmes, car cela permet de prendre des mesures immédiates en cas de violation. Les contrôles centralisés imposent également l'uniformisation des méthodes de travail, réduisent les risques d'erreur isolée et exploitent les meilleures pratiques à tous les niveaux de l'entreprise.

> *L'établissement principal d'un responsable du traitement dans l'Union devrait être le lieu de son administration centrale dans l'Union... et devrait supposer l'exercice effectif et réel d'activités de gestion déterminant les décisions principales quant aux finalités et aux moyens du traitement...*
>
> *-- Considérant 36 du RGPD*

» Sécurité de bout en bout

Les menaces et les attaques peuvent provenir de plusieurs sources, et les organismes doivent être préparés à faire face à toutes les situations. Le RGPD exige la protection des données à caractère personnel à toutes les étapes du cycle de vie des données, notamment pour les données stockées et les données en transit.

> *Lors de l'évaluation du niveau de sécurité approprié, il est particulièrement tenu compte des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.*
>
> *-- Article 32 du RGPD*

Oracle Database Security et le RGPD

Les entreprises disposent de plusieurs niveaux de sécurité s'articulant autour de la base de données comme des pare-feux, des systèmes de détection d'intrusion et un cloisonnement réseau adéquat, dans l'optique de protéger la base de données contre des attaques ciblées. Toutefois, les frontières traditionnelles du réseau interne étant de plus en plus floues et le nombre de personnes (administrateurs, développeurs, équipes de tests et partenaires) bénéficiant d'un accès direct à la base de données étant de plus en plus important, il devient essentiel de sécuriser en profondeur les bases de données. Dans l'optique de réduire l'exposition aux attaques et le nombre de biais par lesquels les cybercriminels peuvent atteindre la base de données, il est extrêmement important de renforcer la sécurité au plus près possible des données.

L'un des défis qui se présentent lors de l'évaluation de la nature des risques consiste à déterminer ce qui doit être évalué. En effet, les applications possèdent généralement plusieurs points d'entrée situés au niveau des réseaux, des systèmes d'exploitation, des bases de données et de l'application elle-même. Des intrus malveillants peuvent exploiter les faiblesses de n'importe quel point d'entrée. En outre, les intrus peuvent cibler les employés et les prestataires responsables de l'utilisation, de la gestion, des tests et de la maintenance du système. Les entreprises doivent également prendre en considération la façon dont leurs systèmes sont déployés, notamment si ce déploiement est effectué sur le Cloud, s'il inclut des applications anciennes dont le code source n'est pas forcément disponible et s'il y a une dépendance envers les équipes de test et de développement tierces, qu'elles soient établies au sein ou hors de l'Union européenne.

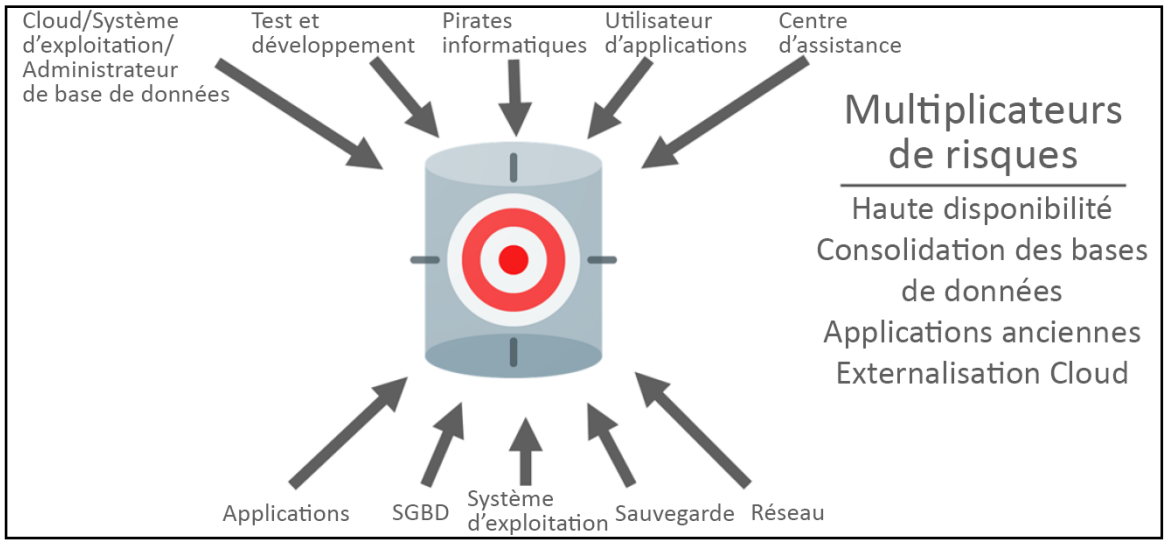

Figure 3 : Vecteurs et cibles d'attaque pour les bases de données

Depuis plusieurs dizaines d'années, Oracle est le leader incontesté dans le domaine de la sécurité des données et développe des produits novateurs dédiés à la sécurité des données afin d'aider les organismes à se prémunir contre les attaques provenant de différents vecteurs de menace. Oracle a été la première entreprise à introduire des modules de contrôle tels que la sécurité au niveau des lignes, l'audit granulaire, le chiffrement transparent des données, la restriction d'accès des utilisateurs à privilèges aux données sensibles, l'analyse des rôles et privilèges ainsi que le pare-feu de base de données.

Les technologies et produits Oracle Database Security peuvent aider les entreprises à accélérer leur projet de conformité avec le RGPD en adressant chaque point grâce à une suite de technologies et de produits automatisés, transparents et performants. Cette section explique comment les modules de contrôle Oracle Database Security aident à synthétiser les exigences du RGPD pour l'évaluation, la prévention et la détection en matière de sécurité.

ÉVALUATION	PRÉVENTION	DÉTECTION
Processus, profils, sensibilité des données, risques	Chiffrement, pseudonymisation, anonymisation, contrôle d'accès au niveau le plus fin, contrôle de l'accès des utilisateurs à privilèges, séparation des tâches	Audits, surveillance de l'activité, alertes, reporting

Figure 4 : Principes d'évaluation, de prévention et de détection du RGPD

Évaluation des risques de sécurité

L'article 35 préconise une analyse d'impact sur la protection des données pour certains types de traitement de données. L'un des défis qui se présentent lors de l'évaluation de la nature des risques consiste à déterminer ce qui doit être évalué. En effet, les applications possèdent généralement plusieurs points d'entrée et les données à caractère personnel sont réparties sur plusieurs colonnes et tables avec un contrôle d'accès souvent défini de façon imprécise.

La technologie et les produits Oracle Database Security permettent de relever ce défi en fournissant les outils nécessaires à l'évaluation de plusieurs aspects des données de l'application :

- Recherche des tables et des colonnes contenant des « données à caractère personnel »
- Configuration des bases de données pour déterminer le profil global de sécurité
- Analyse des rôles et des privilèges sur la base de données pour déterminer comment les responsables du traitement, les sous-traitants, les tiers, les personnes concernées et les destinataires peuvent accéder aux données à caractère personnel

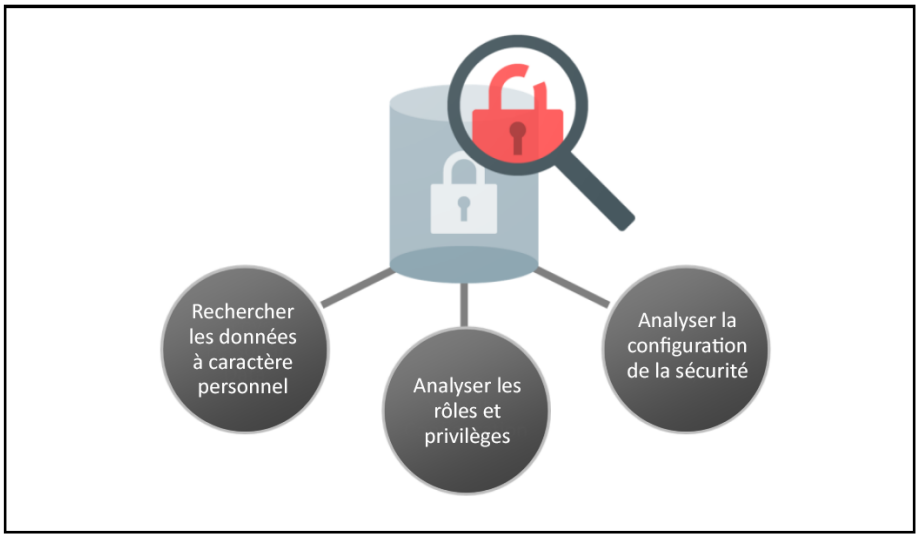

Figure 5 : Évaluation des risques de sécurité

» Évaluation de l'ensemble des données sensibles à l'aide d'Oracle Application Data Modeling

La recherche de données à caractère personnel est une tâche ardue dans les applications complexes actuelles, car diverses informations d'identification peuvent être intégrées à plusieurs tables réparties sur plusieurs schémas de base. Oracle Application Data Modeling automatise la recherche des colonnes contenant des données à caractère personnel et les relations parent-enfant correspondantes définies dans la base. Le processus de recherche utilise des modèles de reconnaissance préconçus et personnalisables, tels que des numéros de carte bancaire et des identifiants nationaux, pour échantillonner les données et identifier les colonnes sensibles. Une fois les données à caractère personnel identifiées, il devient possible d'appliquer les contrôles pertinents, qu'ils relèvent de la prévention ou de la détection. Le modèle de données d'application qui en résulte fournit l'ensemble complet des colonnes sensibles ainsi que leurs relations, ce qui garantit l'intégrité de l'application par des contrôles adaptés pour la protection des données.

» Évaluation du juste niveau de privilège à l'aide d'Oracle Database Vault Privilege Analysis

Une fois les données à caractère personnel identifiées, il devient important d'identifier les utilisateurs (personnes concernées, tiers, autorités de contrôle et destinataires), y compris les utilisateurs à privilèges et les administrateurs (responsables du traitement, sous-traitants), qui sont non seulement en mesure d'y accéder, mais aussi de les traiter. Lors du processus de conception et de maintenance de l'application, des privilèges supplémentaires peuvent être accordés par inadvertance aux utilisateurs. Oracle Database Vault Privilege Analysis permet d'améliorer la sécurité des applications en identifiant les privilèges réellement utilisés lors de l'exécution. Les privilèges identifiés comme inutilisés peuvent être étudiés et éventuellement révoqués, ce qui permet d'obtenir un modèle de moindre privilège.

» **Évaluation de la configuration des bases de données par l'intermédiaire d'Oracle Database Lifecycle Management Pack**

Toutes les bases de données sont dotées de paramètres de configuration ajustables qui couvrent un large éventail d'exigences en matière de sécurité. Il est important de s'assurer que la configuration est toujours sécurisée, n'a pas dérivé avec le temps et respecte les bonnes pratiques du moment. Les entreprises ont besoin d'analyser les bases de données pour y rechercher de nombreux paramètres relatifs à la sécurité, y compris les mots de passe des comptes génériques, l'état des comptes et des profils de compte. Database Lifecycle Management Pack d'Oracle Enterprise Manager permet d'exécuter plus de 100 contrôles standard, d'identifier des tendances et de surveiller la dérive par rapport à la configuration de référence. Des contrôles de configuration personnalisés peuvent également être définis pour compléter ceux fournis en standard par Oracle.

» **Évaluation du profil de sécurité des base de données à l'aide de l'outil Oracle Database Security Assessment**

Conformément à l'article 36 du RGPD, en fonction du degré de sensibilité des données, il est possible que les entreprises soient obligées d'obtenir l'approbation d'une autorité de contrôle avant de traiter certaines données à caractère personnel. Le défi consiste à générer rapidement un rapport présentable sur l'évaluation de la sécurité et de la confidentialité à soumettre à l'autorité de contrôle. L'outil Oracle Database Security Assessment analyse non seulement la configuration, mais également la façon dont certaines des politiques de sécurité sont mises en œuvre. Il présente alors ses résultats dans un format structuré lisible par l'utilisateur, que vous pouvez ensuite présenter à l'autorité de contrôle. Il n'est pas nécessaire pour une entreprise de consacrer de nombreuses heures ni d'affecter de nombreuses ressources à la collecte et à l'analyse des résultats d'une évaluation de sécurité des bases Oracle. Ces informations peuvent aider considérablement dans la génération d'une analyse d'impact relative à la protection des données.

Prévention des attaques

Nous avons évoqué précédemment les diverses techniques de prévention recommandées par le RGPD, comme le chiffrement, la pseudonymisation, l'anonymisation, le contrôle des utilisateurs à privilèges, entre autres. L'un des défis présentés par tout contrôle préventif de protection des données tient dans la surcharge que cela génère pour les applications et les opérations informatiques quotidiennes. Cette surcharge peut prendre la forme de changement de processus, de modifications requises du code source de l'application, de tests, de problèmes de performance et d'évolutivité. Confrontés à ces défis, certaines entreprises peuvent hésiter à déployer des mesures de sécurité préventives pour les applications existantes.

Si certaines de ces inquiétudes pouvaient être valides il y a une dizaine d'années, Oracle Database Security les adresse grâce à des contrôles préventifs qui sont transparents pour la plupart des applications et qui ont un impact extrêmement minime sur les performances et les opérations courantes. Oracle fournit une suite de contrôles préventifs faciles à mettre en œuvre, qui permet aux entreprises de déployer les techniques de prévention clés recommandées par le RGPD, notamment le chiffrement, la pseudonymisation, l'anonymisation, le contrôle des utilisateurs à privilèges, le contrôle d'accès au niveau le plus fin et le masquage des données.

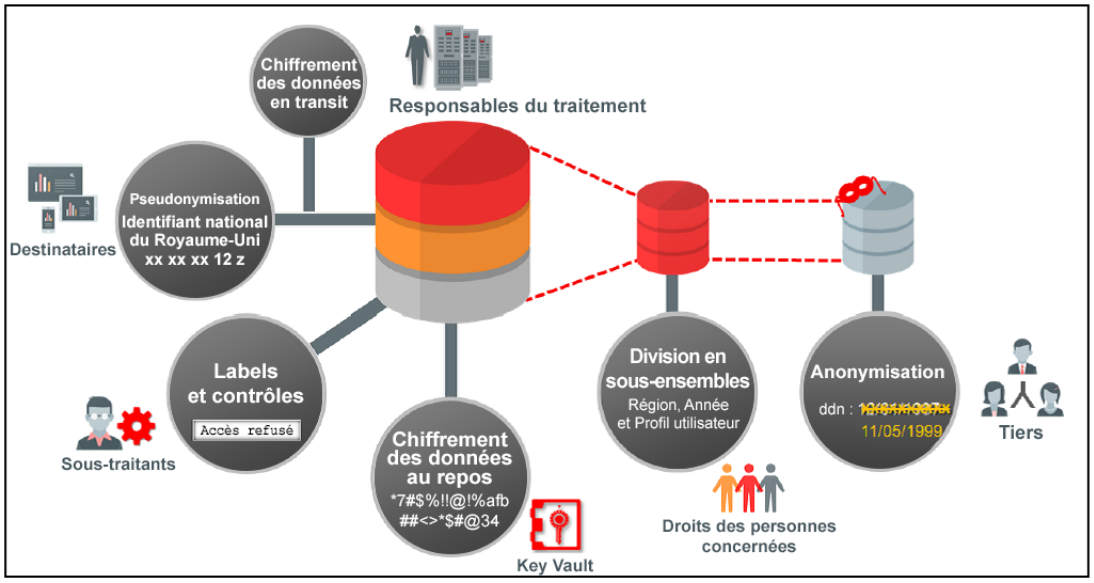

Figure 6 : Contrôles préventifs de sécurité Oracle Database

» Chiffrement des données au repos par l'intermédiaire de l'outil Transparent Data Encryption

L'article 32 et le considérant 83 du RGPD recommandent fortement le chiffrement comme l'une des techniques de protection des données. L'un des défis auxquels les entreprises sont confrontées lors de la mise en œuvre du chiffrement des données est de s'assurer que non seulement les données à caractère personnel sont chiffrées dans les tables, mais également dans les sauvegardes, les transferts de données et les fichiers de logs.
La recherche et le chiffrement des données provenant de toutes ces sources est une tâche consommatrice de ressources. Oracle Advanced Security - Transparent Data Encryption (TDE) relève ce défi en chiffrant toutes les données directement à la source (couche base de données). L'outil TDE chiffre automatiquement les données lorsqu'elles sont écrites vers un support de stockage, y compris les sauvegardes, les exports de transferts de données et les fichiers de logs. Parallèlement, les données chiffrées sont déchiffrées automatiquement lorsqu'elles sont lues à partir du support de stockage. Cette capacité automatique de chiffrement-déchiffrement au niveau de la base rend la solution transparente pour les applications. Les contrôles d'accès appliqués aux niveaux de la base de données et de l'application demeurent en vigueur. Les requêtes SQL ne sont pas altérées et aucune modification du code ni de la configuration de l'application n'est donc nécessaire. L'outil TDE est pré-installé sur Oracle Database et peut être facilement activé.

Un autre problème rencontré lors du chiffrement des données est l'impact sur les performances de la base de données et des applications. Le processus de chiffrement et de déchiffrement est extrêmement rapide car TDE exploite les optimisations de mise en cache d'Oracle Database et utilise l'accélération matérielle des chipsets Intel (AES-NI) et Oracle SPARC.

» Gestion centralisée des clés de chiffrement grâce à Oracle Key Vault

La centralisation aide les responsables du traitement à appliquer les contrôles de sécurité partout et à prendre des mesures rapides en cas de faille de sécurité. Oracle Key Vault (OKV) fournit un contrôle centralisé sur les données chiffrées grâce au processus de chiffrement transparent des données TDE (Transparent Data Encryption). TDE offre une gestion des clés de chiffrement à deux niveaux, avec des clés de chiffrement de données et des clés de chiffrement principales. Ces dernières peuvent être contrôlées et gérées de façon centralisée en utilisant Oracle

Key Vault (OKV). OKV permet de suspendre l'accès à la clé principale et de rendre les données chiffrées inintelligibles en cas de violation des données ou d'activité suspecte.

Oracle Key Vault est un logiciel qui permet de déployer rapidement le chiffrement et d'autres solutions de sécurité en gérant de façon centralisée leurs clés de chiffrement, les portefeuilles (« wallets ») Oracle, les magasins de clés Java (Keystores) et les fichiers de crédentiels.

» Chiffrer les données en transit par l'intermédiaire d'Oracle Database Network Encryption and Data Integrity

Afin de satisfaire aux exigences de l'article 32 du RGPD pour la protection des données à caractère personnel lors de leur transmission, Oracle Database Network Encryption and Data Integrity permet aux entreprises et aux responsables du traitement de chiffrer les données en transit et de prévenir les écoutes illicites, la perte de données, le rejeu de trame et les attaques dites de « l'homme du milieu ».

Oracle fournit un chiffrement natif du réseau, ainsi que l'utilisation du protocole TLS (Transport Layer Security) pour les entreprises dotées d'une infrastructure à clés publiques (PKI). L'outil Network Encryption and Data Integrity est intégré à Oracle Database et installé par défaut. Oracle assure le support des algorithmes de chiffrement globaux tels qu'AES.

» Pseudonymisation des données à l'aide de Data Redaction et Database Vault

L'article 32 et le considérant 28 du RGPD recommandent la pseudonymisation. Par exemple, il est possible qu'un attribut d'une colonne de table représentant une personne concernée soit occulté ou qu'une table contenant plusieurs attributs pouvant permettre d'établir un lien avec la personne concernée initiale soit protégée de telle manière qu'elle soit impossible à joindre, réduisant ainsi le degré de corrélation du jeu de données avec la personne concernée.

La pseudonymisation permet de remédier aux attaques en prévenant l'affichage accidentel ou intentionnel des données sensibles sur les écrans des applications. Ce type de filtre peut être utilisé par les responsables du traitement et les tiers du support applicatif ou dans un centre d'appels qui peut être situé hors des frontières de l'Union européenne. L'un des défis que présente la mise en œuvre de la pseudonymisation tient dans la façon d'intercepter les requêtes d'application vers la base de données et de transformer les données sans affecter l'application ni la base de données principale.

La fonctionnalité Data Redaction d'Oracle Advanced Security permet de faire face à ce problème en proposant une occultation sélective, à la volée, des données à caractère personnel dans les résultats de requêtes SQL avant de les renvoyer vers l'application, de sorte que les utilisateurs non autorisés ne puissent pas afficher ces données. Cette fonctionnalité permet une occultation cohérente des colonnes de base de données sur les modules applicatifs accédant aux mêmes informations. La fonctionnalité Oracle Data Redaction minimise les modifications apportées à l'application car elle n'altère pas les données réelles dans les mémoires tampon, les caches ni les supports de stockage internes aux bases de données, tout en préservant le type d'origine des données et en effectuant un formatage lorsque les données transformées sont renvoyées à l'application. Oracle Data Redaction n'a aucun impact sur les opérations de maintenance sur la base de données, telles que la sauvegarde et la restauration, la mise à niveau et le patch, et le clustering pour la haute disponibilité, car les données persistantes ne sont pas modifiées. Contrairement aux approches traditionnelles qui exigeaient d'apporter des modifications aux applications ou d'intercepter les accès à la base de données par le biais d'un proxy, les règles d'Oracle Data Redaction sont appliquées directement dans le noyau de la base de données, ce qui permet d'obtenir une sécurité accrue et une amélioration des performances. Oracle Data Redaction permet également au responsable du traitement de spécifier les conditions selon lesquelles les données réelles doivent être renvoyées aux destinataires autorisés. La fonctionnalité Data Redaction est pré-installée sur Oracle Database et peut être facilement activée.

Oracle Database Vault peut aider à protéger les attributs sensibles qui sont stockés dans plusieurs tables en créant des domaines qui protègent l'accès aux données en le limitant au personnel autorisé et à des conditions données. Par exemple, l'utilisateur de l'application peut être autorisé à lire tous les attributs (dans plusieurs tables) de la personne concernée alors que les administrateurs de base de données ou d'autres utilisateurs peuvent uniquement consulter les attributs principaux de la table parent, ce qui empêche d'établir un lien avec la personne concernée.

» Anonymisation et minimisation par l'intermédiaire d'Oracle Data Masking and Subsetting

L'anonymisation permet d'empêcher l'identification de la personne concernée par ses données à caractère personnel et de prévenir l'exposition de ces données à caractère personnel dans des environnements moins protégés, comme les environnements de test et développement. Par exemple, l'anonymisation permet de transformer un numéro de carte bancaire à 16 chiffres en un numéro factice à 16 chiffres tel que 5678-0987-4512-1111. L'un des défis présentés par l'anonymisation est que si elle n'est pas effectuée correctement, les données brouillées ou transformées pour ne plus être identifiables risquent d'être inexploitables par les testeurs et les développeurs. De plus, cette méthode est susceptible d'endommager l'intégrité des données au niveau des applications et des bases de données.

Oracle Data Masking and Subsetting permet d'adresser ces problèmes en fournissant une bibliothèque complète et extensible de formats d'anonymisation et de masquage, de fonctions/transformations et de modèles d'application. Les données à caractère personnel et d'autres données sensibles, telles que les numéros de carte bancaire, les identifiants nationaux et d'autres données d'identification personnelles peuvent être facilement masquées grâce à une bibliothèque prête à l'emploi de formats d'anonymisation et de masquage.

L'article 5 du RGPD préconise la minimisation des données afin de réduire la quantité de données à caractère personnel recueillies, traitées, partagées et conservées. Toutefois, la plupart des entreprises globales combinent les données provenant de plusieurs pays ou régions dans une seule table. De ce fait, il est difficile d'appliquer des politiques différentes à différentes parties de la table. Cela devient particulièrement problématique lorsque les entreprises doivent fournir une copie des données (y compris les données à caractère personnel) à des tiers ou à des sous-traitants, tels que des partenaires établis dans un pays hors de l'Union européenne. Si toutes les exigences du RGPD ne peuvent être satisfaites, la meilleure solution consiste sans doute à supprimer les données relatives à l'Union européenne de l'ensemble, tout en conservant les autres pour des besoins commerciaux spécifiques. Oracle Data Masking and Subsetting permet de remédier à ce problème grâce à une division en sous-ensembles facile à définir et basée sur un objectif ou une condition, par exemple, une division en sous-ensembles basée sur les identifiants nationaux. La division en sous-ensembles des données est une fonctionnalité automatisée pour identifier, supprimer ou extraire un sous-ensemble de données à partir d'un jeu de données de taille importante. La division en sous-ensembles des données permet également de traiter automatiquement les relations et les dépendances entre les données, ainsi que les dépendances lors de la suppression ou de l'extraction, préservant ainsi l'intégrité du jeu de données.

Oracle Data Masking and Subsetting extrait des copies ou des sous-ensembles entiers de données d'application à partir de la base de données, anonymise et minimise les données à caractère personnel de sorte qu'elles puissent être partagées en toute sécurité avec les sous-traitants et les tiers, comme le personnel chargé des tests et du développement et les partenaires. L'intégrité de la base de données est préservée, assurant ainsi la continuité de fonctionnement des applications.

Oracle Data Masking and Subsetting est pré-installé dans Oracle Enterprise Manager. Il fournit une interface graphique Web unique permettant de masquer et de diviser en sous-ensembles les bases de données on-premise et sur Oracle Cloud.

Le considérant 26 stipule également qu'il n'y a pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes si les données à caractère personnel sont rendues anonymes de telle manière que la personne concernée ne soit plus identifiable. Le masquage des données dans des applications hors production peuvent aider à garder les environnements de développement, de tests et autres hors du champ d'application du RGPD où les données à caractère personnel ne sont pas véritablement requises.

» Contrôle des utilisateurs à privilèges et séparation des tâches avec Oracle Database Vault

L'article 32 du RGPD recommande de limiter l'accès d'un sous-traitant car les comptes à privilèges représentent l'une des voies les plus utilisées pour accéder aux données sensibles directement dans la base de données. Si leur donner des accès étendus et sans restriction facilite la maintenance de la base de données, cela crée par là même un point d'attaque permettant d'accéder à des quantités importantes de données.

Il a toujours été difficile de restreindre l'accès des utilisateurs à privilèges (par exemple, les administrateurs de bases de données) aux données à caractère personnel. De telles restrictions peuvent affecter les opérations quotidiennes, comme l'application de correctifs ou la maintenance. Oracle Database Vault intègre le contrôle d'accès des utilisateurs à privilèges au sein d'Oracle Database afin de limiter l'accès aux données à caractère personnel par les utilisateurs à privilèges, tout en autorisant les administrateurs de bases de données à effectuer leurs activités habituelles, comme l'application de correctifs, l'import ou l'export de données et les sauvegardes, sans leur accorder l'accès aux données à caractère personnel. Oracle Database Vault permet de définir le périmètre des données à caractère personnel qui doit être protégé non seulement contre les utilisateurs à privilèges, mais également par l'intermédiaire de lignes de commandes. Cet outil contrôle les mécanismes et les moyens susceptibles d'être utilisés par les responsables du traitement, les sous-traitants et les tiers (utilisateurs autorisés) pour accéder aux données à caractère personnel.

» Masquage sélectif des données par l'intermédiaire d'Oracle Virtual Private Database

Le RGPD introduit des techniques préventives permettant de gérer des problèmes ponctuels, par exemple rendre temporairement inaccessibles les données à caractère personnel sélectionnées. Pour autant, le véritable défi consiste à filtrer et masquer facilement un sous-ensemble d'un jeu de données de taille importante. Par exemple, une entreprise peut avoir besoin de masquer temporairement toutes les données correspondant aux résidents d'Italie, suite à la détection d'activités suspectes. Les opérations permettant de filtrer et de masquer uniquement les identifiants nationaux des ressortissants italiens enregistrés dans une colonne contenant un très grand nombre d'identifiants nationaux de différents pays exigeraient normalement un important travail de programmation.

Oracle Virtual Private Database (VPD) adresse ce problème grâce à ses politiques de sécurité simples à positionner au niveau des lignes. L'outil calcule un prédicat ou une clause WHERE qui est automatiquement ajouté aux instructions SQL entrantes, restreignant ainsi l'accès aux lignes et aux colonnes de la table. VPD est installé avec Oracle Database par défaut et protège la base de données des accès non autorisés, non seulement en cas de problèmes ponctuels, mais également tout au long des opérations courantes. Cela permet de minimiser la surface d'attaque si une erreur de programmation permettait aux utilisateurs d'afficher leurs propres données ainsi que celles des autres utilisateurs.

» Contrôle des accès grâce à Oracle Label Security

Le RGPD recommande que les entreprises et les responsables du traitement veillent à ce que les sous-traitants puissent accéder aux données à caractère personnel de façon sélective et dans un but défini. Oracle Label Security (OLS) aide les entreprises à classifier les données à caractère personnel en leur attribuant des étiquettes en fonction du niveau de confidentialité (par exemple, public, sensible ou strictement confidentiel) ou des régions (par exemple, Amérique du Nord, Europe ou Asie-Pacifique). OLS fournit des contrôles d'accès faciles à déclarer basés sur cette classification des données. Par exemple, les lignes contenant des éléments de données sensibles, tels que des numéros de cartes bancaires, peuvent être classifiées comme des données européennes extrêmement sensibles et être accessibles uniquement à certains sous-traitants ou utilisateurs.

Grâce à ses contrôles d'accès faciles à déclarer, OLS simplifie le modèle à plusieurs niveaux de sécurité (MLS, multi-level security), qui est généralement obligatoire pour de nombreux organismes gouvernementaux et de défense. Oracle Label Security est pré-installé dans Oracle Database et peut être facilement activé.

» Faciliter le contrôle des accès de bout en bout grâce à Oracle Real Application Security

Conformément au considérant 64 du RGPD, pour tout service en ligne, le responsable du traitement doit, avant d'accorder l'accès à des données à caractère personnel, vérifier l'identité de la personne effectuant la requête. Dans les applications modernes en architecture 3 tiers, cette vérification est un véritable défi car, en général, les applications et les serveurs d'application se connectent à la base de données en utilisant un compte technique, ce qui rend difficile l'identification de l'utilisateur à l'origine de la demande.

Oracle Real Application Security (RAS) adresse ce problème en fournissant un modèle d'autorisation basé sur des règles, qui reconnaît les utilisateurs, les privilèges et les rôles de l'application au sein même de la base de données. Grâce à un support natif de la propagation des sessions des utilisateurs de l'application, RAS permet de protéger les données par des règles de sécurité tenant compte des utilisateurs de l'application, de leurs rôles et de leurs contextes de sécurité. À l'aide de listes de contrôle d'accès, l'outil RAS, qui est pré-installé sur Oracle Database, peut contrôler qui peut accéder à Oracle Database.

Que ce soit en matière de chiffrement, de pseudonymisation ou de contrôle des accès à privilèges, Oracle Database Security permet de réduire la quantité de travail nécessaire à la mise en œuvre et à la maintenance des principes de protection des données recommandés par le RGPD grâce à son large éventail de solutions de contrôles préventifs.

Surveillance et détection des failles de sécurité

Les pare-feux périmétriques classiques jouent un rôle important pour protéger les datacenters contre les accès externes non autorisés, mais les attaques ont évolué pour devenir de plus en plus sophistiquées. Elles peuvent désormais contourner la sécurité périmétrique, abuser de tiers de confiance, voire usurper l'identité d'utilisateurs internes disposant de privilèges élevés. Les enquêtes portant sur de nombreux incidents de sécurité ont démontré qu'un examen au bon moment des données d'audit aurait pu permettre la détection précoce d'une activité non autorisée et la réduction de l'impact financier qui en résulte. Les articles 30 et 33 du RGPD exigent des entreprises qu'elles tiennent un registre de leurs activités de traitement.

Pour ce faire, la seule solution consiste à surveiller et à contrôler constamment les activités effectuées sur les données à caractère personnel. Ces données peuvent ensuite être utilisées pour notifier rapidement les autorités en cas de violation. Outre les audits obligatoires et les alertes dans les meilleurs délais, le RGPD exige également des entreprises qu'elles conservent les enregistrements d'audit sous leur contrôle. Un contrôle centralisé des enregistrements d'audit empêche les pirates ou les utilisateurs malveillants de camoufler les traces de leur activité suspecte grâce à la suppression de traces locales.

Oracle Database Security fournit un mécanisme complet de création de rapports et de recueil de données d'audit afin de satisfaire aux exigences du RGPD en matière de surveillance. Oracle Audit Vault and Database Firewall (AVDF) fournit une plateforme nouvelle génération de contrôle et de protection centrée sur les données (DCAP) qui offre une surveillance complète et flexible grâce à la consolidation des données d'audit provenant de bases de données Oracle et de bases de données tierces, de systèmes d'exploitation, de systèmes de fichiers et de données d'audit propres aux applications. Parallèlement, Oracle Database Firewall peut jouer un rôle de premier rang dans la défense de l'infrastructure : il régule le comportement des applications de façon à éviter que l'injection SQL, le contournement d'application et d'autres activités malveillantes n'atteignent la base de données. Oracle Audit Vault and Database Firewall peut consolider les données d'audit provenant de plusieurs bases de données et, dans le même temps, surveiller le trafic SQL afin de rechercher, de signaler et d'empêcher toute instruction SQL non autorisée ou hors politique de sécurité. Les délégués à la protection des données et les responsables du traitement peuvent spécifier les conditions selon lesquelles les alertes peuvent être lancées en temps réel et tenter ainsi de repérer les intrus par des activités anormales. Des dizaines de rapports prêts à l'utilisation, associés à une interface de création de rapports personnalisés, fournissent une vue complète de l'activité des bases de données à travers toute l'entreprise, cette surveillance étant effectuée depuis le réseau ou les fichiers journaux d'audit. Oracle AVDF prend en charge les bases de données Oracle, Microsoft SQL Server, IBM DB2 pour LUW, SAP Sybase ASE et Oracle MySQL.

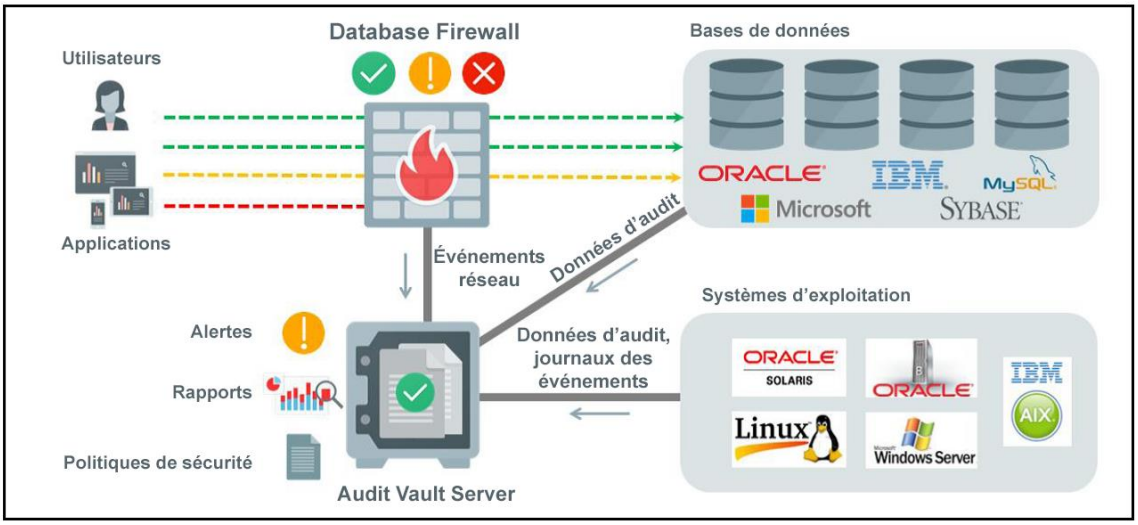

Figure 7 : Contrôles de surveillance Oracle Database Security

Protection maximum en respectant la transparence, la précision, les performances et l'évolutivité

L'article 25 du RGPD introduit le concept de protection des données par défaut dès la conception. Les applications actuelles contiennent plusieurs composants sous-jacents tels que des passerelles Web, des proxys Web, des serveurs Web, des serveurs d'application et des serveurs de base de données. La définition et la mise en œuvre de tous les contrôles de sécurité dans un environnement multicouche est une tâche ardue. La consolidation de l'intégralité de ces contrôles de sécurité et de technologies provenant de divers fournisseurs représente pour les entreprises un véritable défi en termes d'intégration et d'administration.

Oracle Database Security adresse ce problème en positionnant les contrôles au plus près des données et en appliquant la sécurité au sein de la base de données. La plupart des solutions de protection des données proposées par Oracle sont intégrées à la base de données. Non seulement la sécurisation des données à la source simplifie la conception et le déploiement, mais elle améliore également l'efficacité de la protection et permet de réduire la surface d'attaque.

Oracle Key Vault, Audit Vault et Database Firewall complètent la capacité de protéger les données à la source par la centralisation du contrôle et de l'administration. Qu'il s'agisse de milliers de clés de chiffrement, de millions d'enregistrements d'audit ou de types différents de politiques de sécurité, vous pouvez gérer ces composants de façon centralisée, ce qui simplifie nettement les tâches d'administration. Oracle Enterprise Manager (EM) fournit une interface graphique Web unique pour la gestion des composants Oracle Database Security.

Plus important, tous les produits Oracle Database Security s'intègrent parfaitement pour protéger les données à caractère personnel des menaces internes et externes. L'illustration suivante représente l'architecture Oracle « Maximum Data Security » et démontre comment les différents produits s'intègrent les uns aux autres pour la sécurisation des données à caractère personnel.

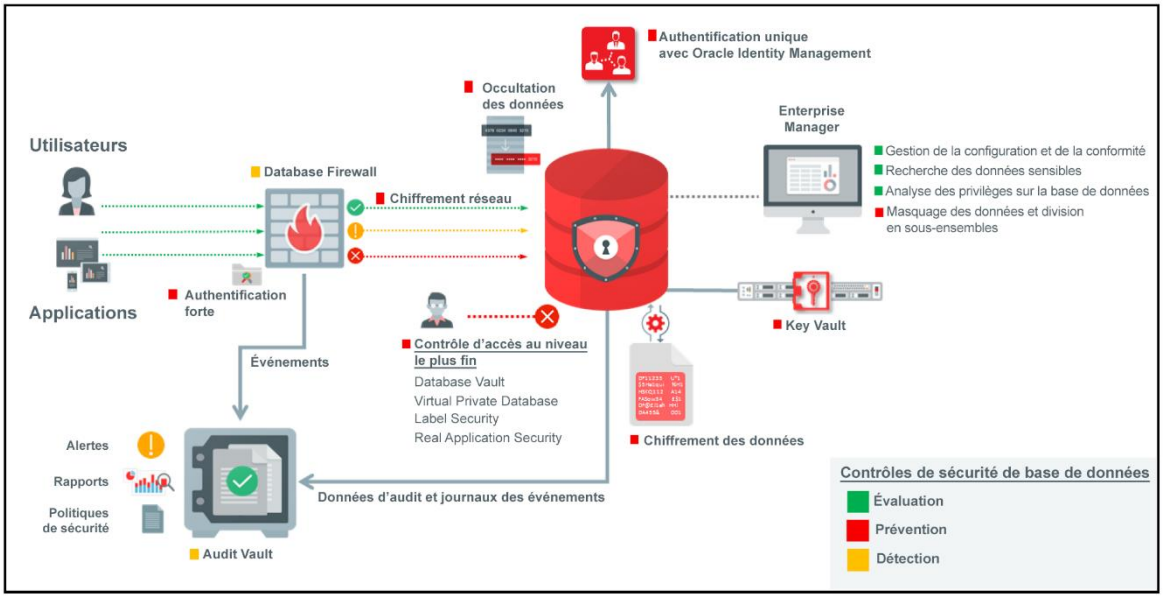

Figure 8 : Architecture Oracle « Maximum Data Security »

Exemple hypothétique

Maintenant que nous avons décrit les objectifs, les acteurs et les principes clés de protection des données du RGPD, voici comment la société fictive française XYZ, présentée plus tôt dans ce livre blanc, est susceptible d'exploiter les produits Oracle Database Security afin de respecter les exigences du RGPD.

» Évaluation

Tout d'abord, le responsable de la sécurité (RSSI) de XYZ guide les groupes chargés de l'application (APP) et de la base de données (BDD) dans l'évaluation de l'état actuel de la sécurité des données. Le processus est résumé ci-dessous :

- Évaluer le profil de sécurité des bases de données en analysant la configuration par l'intermédiaire d'Oracle Database Lifecycle Management Pack ou de l'outil Oracle Database Security Assessment
- Rechercher les colonnes de base de données contenant des données sensibles sur les personnes concernées par l'intermédiaire d'Oracle Application Data Modeling
- Évaluer les moyens d'accès aux données sensibles en analysant les privilèges et les rôles des utilisateurs par l'intermédiaire d'Oracle Privilege Analysis
- Générer un rapport d'évaluation détaillé afin de présenter les résultats aux auditeurs et à l'autorité de contrôle

» Prévention

En fonction des résultats de l'évaluation, le RSSI accompagne les équipes BDD et APP dans la mise en œuvre de techniques préventives visant à isoler les applications des attaques externes comme internes. Le processus est résumé ci-dessous :

- Chiffrer la base de données contenant les données à caractère personnel de la personne concernée par l'intermédiaire d'Oracle Advanced Security - Transparent Data Encryption
- Gérer les clés de chiffrement de façon centralisée dans Oracle Key Vault
- Pseudonymiser les informations sensibles dans l'application de service client et de facturation par l'intermédiaire d'Oracle Advanced Security - Data Redaction et Oracle Database Vault
- Chiffrer le trafic réseau de la base de données par l'intermédiaire d'Oracle Database Network Encryption and Data Integrity
- Anonymiser les données à caractère personnel avant de les traiter dans un contexte de test et de développement par l'intermédiaire d'Oracle Data Masking and Subsetting
- Mettre en œuvre le contrôle d'accès des utilisateurs à privilèges et la séparation des tâches à l'aide d'Oracle Database Vault
- Mettre en œuvre des contrôles d'accès au niveau le plus fin dans l'application à l'aide d'Oracle Virtual Private Database, Oracle Label Security et Oracle Real Application Security

» Détection

Pour finir, le RSSI accompagne les équipes BDD et APP dans la mise en œuvre de techniques de détection visant à surveiller les applications et la base de données et à repérer les activités suspectes. Le processus est résumé ci-dessous :

- Mener un audit des activités sur les données des personnes concernées à l'aide des audits Oracle Database
- Recueillir et gérer de façon centralisée les enregistrements d'audit à l'aide d'Oracle Audit Vault
- Surveiller et bloquer les comportements suspects, lancer des alertes et générer des rapports à l'aide d'Oracle Database Firewall

Conclusion

Depuis plusieurs dizaines d'années, Oracle est le leader incontesté du domaine de la sécurité des données. Oracle développe depuis plusieurs années des produits novateurs dédiés à la sécurité de données afin d'aider les entreprises à se prémunir contre les attaques provenant de différents vecteurs de menace. Les entreprises du monde entier peuvent désormais accélérer leur projet de conformité aux exigences du RGPD en exploitant les contrôles d'évaluation, de prévention et de détection d'Oracle Database Security avec des coûts minimes, un haut degré de transparence et une faible complexité de déploiement.

Il est crucial de commencer à planifier dès maintenant la façon dont vous allez répondre aux exigences du RGPD. Grâce aux produits Oracle Database Security, toutes les organisations peuvent commencer très vite à mettre en œuvre leur projet de conformité, ainsi qu'à mettre en place une sécurité de haut niveau pour les données à caractère personnel et les données métier sensibles.

Références

Les sites Web suivants vous permettront de consulter davantage d'informations sur les produits Oracle Database Security et le RGPD de l'Union européenne.

- RGPD de l'Union européenne : http://ec.europa.eu/justice/data-protection/reform/index_en.htm
- Oracle Technology Network pour les fiches techniques, les livres blancs, les FAQ, la documentation, les références, les blogs, les forums et les démonstrations relatifs aux produits Oracle Database Security : http://www.oracle.com/technetwork/database/security/index.html
- Oracle Database Lifecycle Management Pack : http://www.oracle.com/technetwork/oem/lifecycle-mgmt/index.html
- Outil Oracle Database Security Assessment : http://go.oracle.com/LP=38340

Annexe : Mise en correspondance des produits Oracle Database Security avec le RGPD

	Référence	Directive RGPD	Recommandations spécifiques à Oracle Database
Évaluation	Article 35	Analyse d'impact relative à la protection des données : « ... le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».	» Utiliser Application Data Modeling d'Oracle Enterprise Manager pour évaluer l'ensemble des données sensibles en analysant les colonnes de base de données pour rechercher les informations sensibles » Utiliser la fonctionnalité Privilege Analysis d'Oracle Database Vault pour évaluer les moyens d'accès aux données sensibles en analysant les rôles et privilèges des utilisateurs dans Oracle Database » Utiliser Database Lifecycle Management Pack d'Oracle Enterprise Manager pour évaluer le profil de sécurité des bases de données Oracle en analysant leur configuration » Utiliser l'outil Oracle Database Security Assessment pour évaluer la configuration de sécurité de la base de données, les politiques de sécurité déployées, l'état des utilisateurs, des rôles et des privilèges accordés
	Considérant 84	« ... lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque. ... »	
Prévention	Article 6	« ... 4.) Lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée ... le responsable du traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres : 4.e.) de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation... »	» Utiliser Oracle Advanced Security - Transparent Data Encryption pour chiffrer les données » Utiliser Oracle Advanced Security - Data Redaction pour pseudonymiser les données en production » Utiliser Oracle Data Masking and Subsetting pour anonymiser les données dans les applications hors production
	Article 32	« ... le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins, la pseudonymisation et le chiffrement des données à caractère personnel... »	
	Considérant 28	« La pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données. »	

	Considérant 83	« Afin de garantir la sécurité et de prévenir tout traitement effectué en violation du présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. »	
	Considérant 26	« ... Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche. »	» Utiliser Oracle Data Masking and Subsetting pour masquer ou anonymiser les données dans les applications hors production
	Article 5	« Les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ; »	» Utiliser Oracle Data Masking and Subsetting pour diviser les données en sous-ensembles en supprimant les données ou en les extrayant et en les transférant vers un autre emplacement
	Article 29	« Le sous-traitant et toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement… »	» Utiliser Oracle Virtual Private Database pour assurer un contrôle d'accès au niveau le plus fin » Utiliser Oracle Label Security pour assigner des labels de classification des données aux données sensibles » Utiliser Oracle Label Security pour contrôler l'accès en fonction de la classification des données » Utiliser Oracle Database Vault pour contrôler l'accès aux utilisateurs à privilèges, tels que les sous-traitants
	Article 32	« ... 4) Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement.… »	
	Considérant 64	« ... Le responsable du traitement devrait prendre toutes les mesures raisonnables pour vérifier l'identité d'une personne concernée qui demande l'accès à des données, en particulier dans le cadre des services et identifiants en ligne. »	» Utiliser des techniques d'authentification forte telles que SSL ou Kerberos conjointement à Real Application Security (RAS) pour vérifier l'identité des utilisateurs de la base de données et de l'application accédant aux informations sensibles

Détection	Article 30	« Chaque responsable du traitement et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement. »	» Utiliser les audits Oracle Database pour activer et conserver les archives (enregistrements d'audit) du traitement » Utiliser Oracle Fine Grained Auditing pour enregistrer ou effectuer un audit d'activités spécifiques des utilisateurs, telles que l'opération SELECT sur les données sensibles » Utiliser Oracle Audit Vault and Database Firewall pour stocker et gérer de façon centralisée les traces du traitement » Utiliser Oracle Audit Vault and Database Firewall pour effectuer la surveillance et lancer des alertes dans les meilleurs délais en cas de comportements suspects
	Article 33	« En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance... »	
	Article 34	« Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais. »	
Protection maximum	Article 25	« ... Le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée. »	» Utiliser l'architecture de protection maximum d'Oracle Database Security pour protéger les données contre les menaces internes et externes en déployant des contrôles d'évaluation, de prévention et de détection
	Article 32	« Lors de l'évaluation du niveau de sécurité approprié, il est particulièrement tenu compte des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite. »	

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, États-Unis

Demandes mondiales
Téléphone : +1.650.506.7000
Fax : +1.650.506.7200

COMMUNIQUEZ AVEC NOUS

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

| Oracle s'engage à développer des pratiques et des produits contribuant au respect de l'environnement.