
ORACLE®

Le Règlement Général sur la Protection des Données de l'Union européenne

Comment les solutions de sécurité Oracle peuvent aider

Jérôme CHAGNOUX
Business Development Manager Sécurité – GDPR Champion
Oracle France
13 mars 2018

Déclaration de mise en garde

Ce qui suit est destiné à décrire l'orientation générale pour nos produits. Il est conçu uniquement à des fins d'information et ne peut-être incorporé dans un contrat. Il ne s'agit pas d'un engagement à fournir du matériel, du code ou des fonctionnalités, et ne ne doit pas être utilisé pour prendre des décisions d'achat. Le développement, la publication et le calendrier des caractéristiques ou fonctionnalités décrites pour les produits Oracle reste à la seule discrétion de Oracle. Les technologies identifiées ne sont pas disponibles pour tous les services Cloud.

Avertissement

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.

Présentation du règlement

- Le Règlement Général sur la Protection des Données (« RGPD ») remplace une Directive européen de Protection des Données vieille de plus de 15 ans.
- Nouvelles exigences légales pour les responsables du traitement (ou contrôleurs) et les sous-traitants (ou processeurs).
- Les exigences comprennent un nouveau régime de responsabilités et de sanctions.
- Dates clefs :
  - Publication : 4 mai 2016
  - Application : 25 mai 2018[1]

Journal officiel **L 119**

de l'Union européenne

Édition de langue française — Législation — 59e année, 4 mai 2016

Sommaire — *I Actes législatifs* — page

RÈGLEMENTS

* **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ([1])** 1

DIRECTIVES

* **Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil** 89

* **Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière** 132

([1]) Texte présentant de l'intérêt pour l'EEE

FR

Les actes dont les titres sont imprimés en caractères maigres sont des actes de gestion courante pris dans le cadre de la politique agricole et ayant généralement une durée de validité limitée.

Les actes dont les titres sont imprimés en caractères gras et précédés d'un astérisque sont tous les autres actes.

[1] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

Certains aspects clés du Règlement

Harmonisation des lois sur la confidentialité des données	Le patchwork de 28 lois existantes se transforme en un règlement global (à quelques exceptions)
Applicabilité globale	Les organisations établies dans l'UE ainsi que les organisations extérieures à l'UE offrant des biens et des services à des personnes basées dans l'UE
Droits renforcés pour les individus	Droit de retrait/d'effacement/à l'oubli – que l'utilisateur peut demander à tout moment
Consentement explicite	Usage des données personnelles conformément à l'accord obtenu explicitement, sans engagement par défaut, avec la personne concernée (propriétaire des données)
Transferts de données	Les droits de confidentialité sont attachés aux données et suivent globalement les données dans leur transfert
Besoin de protection des données	Exigence explicite de protection des données, par conception et par défaut, ainsi que la sécurisation des traitements
Notification obligatoire des failles	Dans les 72 heures aux autorités de contrôle, « sans délai » aux personnes concernées
Responsabilité conjointe	Entre responsables de traitement et sous-traitants
Mise en application commune	Les autorités de contrôle appliqueront le règlement en se consultant entre elles
Amendes augmentées	Jusqu'à 4% du chiffre d'affaires global ou 20 000 000€, selon la valeur la plus élevée
Recours collectifs	Ouvre la possibilité de poursuites collectives de la part des individus

La date fatidique approche…

1. Le RGPD est là
2. Vous devez faire quelque chose
3. Nous pouvons vous aider à vous mettre en conformité

- Oracle est un « sous-traitant » lorsqu'elle fournit à ses clients des services Cloud (et héberge des données personnelles pour le compte de ses clients)
- Les clients sont « responsables de traitement » en ce qui concerne les données personnelles à confier à Oracle
- Oracle est un fournisseur de technologie lorsqu'il fournit des solutions (produits et services) à ses clients pour les aider à se mettre en conformité

Articles

Article 32

Sécurité du traitement

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés

Protection des données dès la conce

Article 25

Protection des données dès la conception et protection des données par défaut

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, 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, qui sont 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.

2. 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. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

3. Un mécanisme de certification approuvé en vertu de l'article 42 peut servir d'élément pour démontrer le respect des exigences énoncées aux paragraphes 1 et 2 du présent article.

3. Un mécanisme de certification approuvé en vertu
des exigences énoncées aux paragraphes 1 et 2 du présen
agissant sous l'autorité du responsable du traitement ou
personnel, ne les traite pas, excepté sur instruction du re
l'Union ou le droit d'un État membre.
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

Sécurité du traitement

1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, 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:

a) la pseudonymisation et le chiffrement des données à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier 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.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

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, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.
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

Pourquoi se pre… par défaut (arti…

…onception et …2)

Article 34

Communication à la personne concernée d'une violation de données à caractère personnel

1. 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.

2. La communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d).

3. La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement;

b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser;

c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

4. Si le responsable du traitement n'a pas déjà communiqué à la personne concernée la violation de données à caractère personnel la concernant, l'autorité de contrôle peut, après avoir examiné si cette violation de données à caractère personnel est susceptible d'engendrer un risque élevé, exiger du responsable du traitement qu'il procède à cette communication ou décider que l'une ou l'autre des conditions visées au paragraphe 3 est remplie.

Article 83

Conditions générales pour imposer des amendes administratives

1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

2. Selon les caractéristiques propres à chaque cas, les amendes adminis… place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). P… …nende administrative, …

…ompte tenu de la natu… …icernées affectées et le …

…nt ou par négligence;

…ement ou le sous-trait…

…itement ou du sous-tra… …vertu des articles 25 et …

…nt par le responsable d…

…le contrôle en vue de…

…oncernées par la violati…

…naissance de la violati… …otifié la violation;

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédem… du traitement ou du sous-traitant concerné pour le même objet, le respe…

j) l'application de codes de conduite approuvés en application de l'ar… approuvés en application de l'article 42; et

k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

Article 83

Conditions générales pour imposer des amendes administratives

1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives.

2. Selon les caractéristiques propres à chaque cas, les amendes administratives sont imposées en complément ou à la place des mesures visées à l'article 58, paragraphe 2, points a) à h), et j). Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants:

a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi;

b) le fait que la violation a été commise délibérément ou par négligence;

c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées;

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32;

e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant;

f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;

g) les catégories de données à caractère personnel concernées par la violation;

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation;

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures;

j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42; et

k) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation.

Les outils de Sécurité Oracle qui peuvent être utiles pour le RGPD

Sécurité des Identités

Authentification

Gestion des identités

Gouvernance

Single Sign-On

Audit

Self-Service

Conformité

Gestion des accès

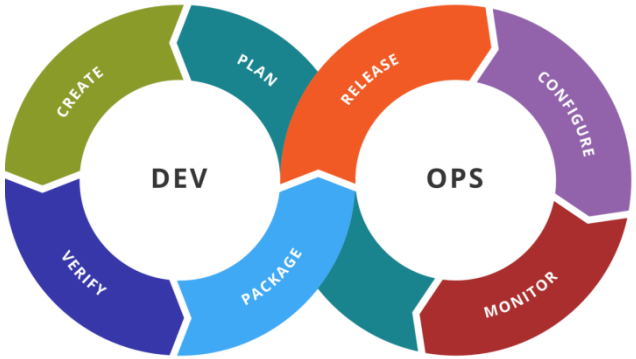
Habilitations

Sécurité des API

Sécurité des Applications

Configuration des applications et des services

Conformité IT



Sécurité des API

Performance des applications et des services

Patching

Audit

Sécurité des Données

Contrôles préventifs

Chiffrement

Séparation des pouvoirs

Data Masking

Gestion des clefs

Contrôles d'administration

Contrôles par investigation

Audit

Surveillance des menaces, Analyse des logs et des utilisateurs, Réponse aux incidents

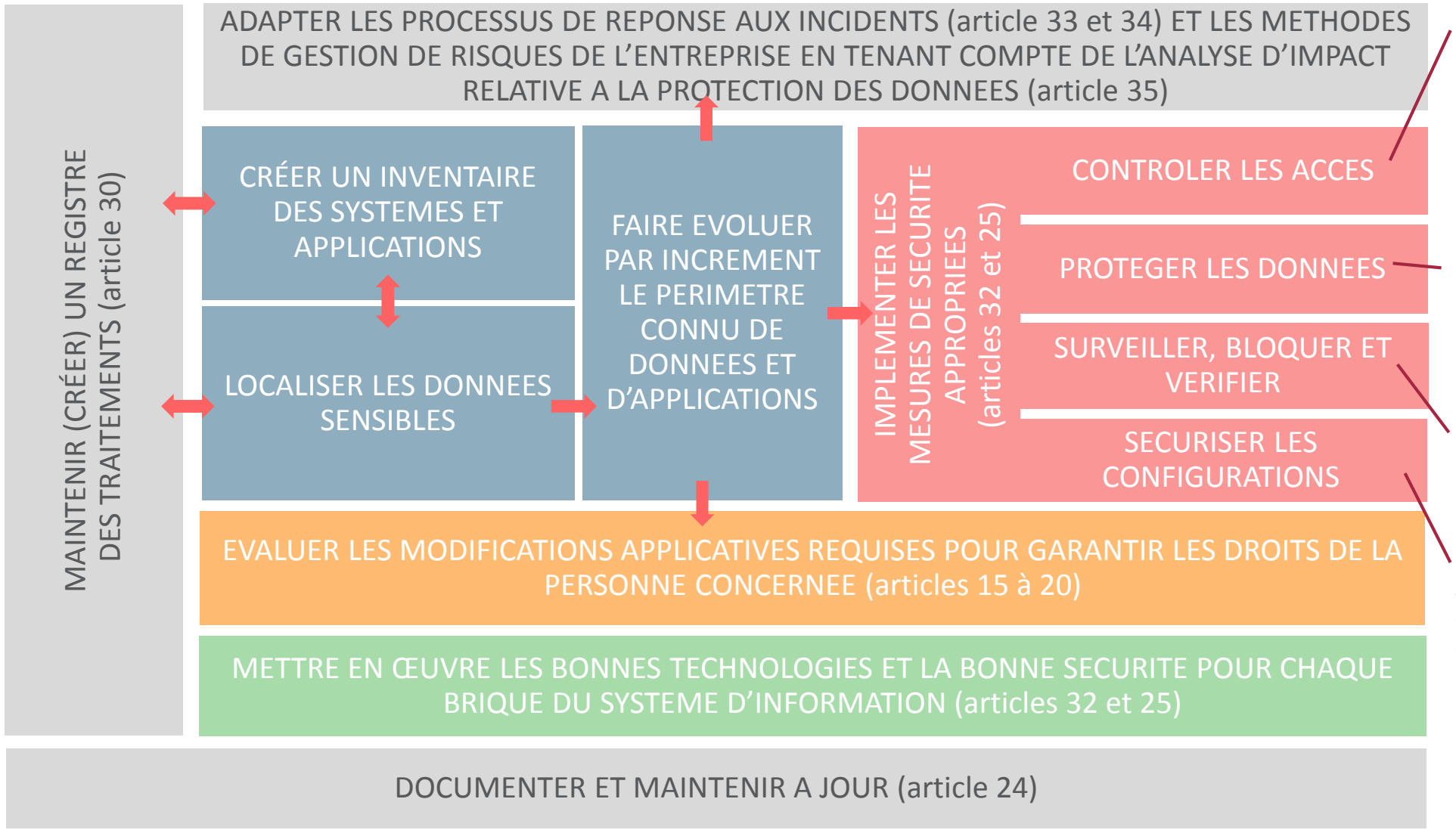
Synthèse des capacités des produits Oracle Security

- **Sécurité de la base de données**
  - Oracle Advanced Security
    - Chiffrement des données au repos
    - Réécriture de données à la volée
  - Oracle Key Vault
    - Gestion des clés de chiffrement (création, renouvellement, répudiation…)
  - Oracle Database Vault
    - Protection contre les utilisateurs à privilèges (par exemple DBA)
  - Oracle Audit Vault & Database Firewall
    - Entrepôt pour la centralisation des traces d'activités pour les bases de données de différents éditeurs ou d'autres produits
    - Protection contre les attaques par injection SQL (pour les bases de données de différents éditeurs)
  - Oracle Label Security
    - Protection supplémentaire pour les lignes d'enregistrement très importantes
  - Data Masking
    - Masquage (ou pseudonymisation) des données sensibles pour les environnement hors production

- **Gestion des Identités et des Accès**
  - Oracle Identity Governance
    - Gestion du cycle de vie des utilisateurs (arrivées, mutations, départs)
  - Oracle Access Management
    - Single Sign On, authentification double-facteurs
  - Oracle Directory Services
    - Offre d'annuaires LDAP (incluant la virtualisation d'annuaire)

- **Services Cloud de Sécurité**
  - DB Cloud peut utiliser les fonctionnalités/options de sécurité de la base de données
    - Certaines options peuvent se déployer sur site (on-premise)
  - Oracle Identity Cloud Service
  - Oracle Cloud Access Security Broker (CASB) Cloud Service
  - Oracle Security Monitoring and Analytics Cloud Service
  - Oracle Compliance Cloud Service
  - Oracle API Platform Cloud Service

Trajectoire pour la conformité RGDP – Tâches et activités



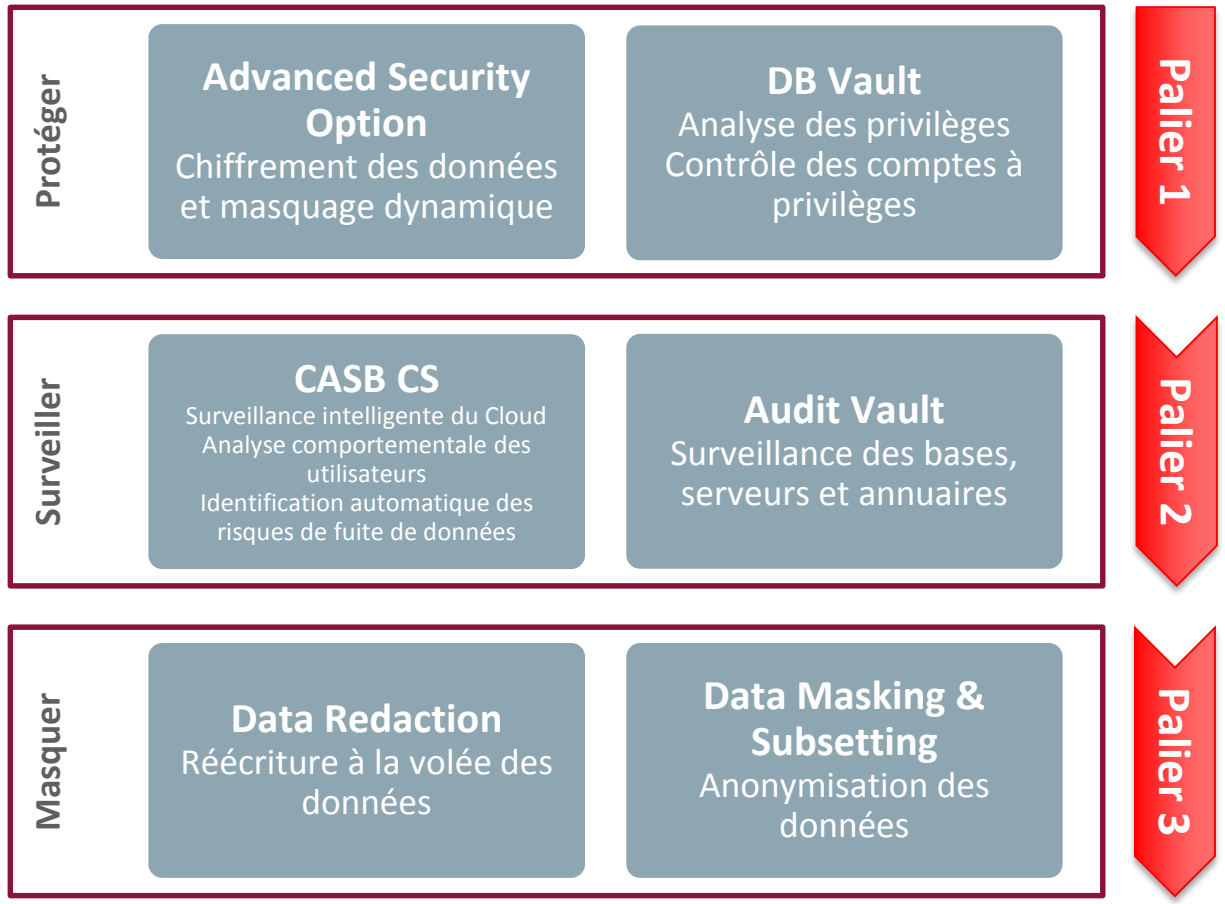
Moderniser la gestion des identités pour garantir l'authentification et la gestion des habilitations à la fois pour les utilisateurs de l'entreprise et le personnel informatique

Protéger les données où qu'elles soient (chiffrement, article 32) et éviter d'utiliser des données de production si elles ne sont pas nécessaires (article 5 et considérant 26)

Collecter, sécuriser et analyser les journaux d'audit et mettre en place des protections périmétriques

Sécuriser les configurations, corriger les vulnérabilités et contrôler les pratiques de production informatique

Une trajectoire sécurité pour le SI de l'entreprise



Gains pour l'entreprise

- **Métiers**
  - Approche générique pour l'accélération du projet de mise en conformité GDPR
  - Supervision intelligente du SI
- **IT**
  - Stratégie de déploiement calée par type d'intervenants
  - Répondre avec efficacité à la surcharge de travail induite par la mise en conformité GDPR
- **Conformité réglementaire**
  - Mise en œuvre rapide des points de conformité au RGPD (cités aux articles 25, 32, 34)
  - Respect des principes de « Sécurité par défaut » et « Sécurité à la conception »

Alors, que faire maintenant ?

- Evaluer votre maturité Sécurité avec Oracle
- Visualiser nos webcasts Sécurité, en particulier sur GDPR
- Vous informer grâce à nos lettres d'information et nos ebooks
- Visiter le site http://www.oracle.com/goto/GDPR

Integrated Cloud

Applications & Platform Services


ORACLE®