
ORACLE®

Die EU-Datenschutzgrundverordnung und wie Oracle Sie unterstützen kann

DOAG Regio München April 2018

Wolfgang Thiem
Email: wolfgang.thiem@oracle.com
ORACLE Deutschland B.V.&Co KG

ORACLE

GDPR Überblick
Oracle Database Security

Safe Harbor-Erklärung

Diese Präsentation dient lediglich dazu, unsere allgemeine Produktausrichtung zu skizzieren. Sie dient ausschließlich zu Informationszwecken und wird nicht Vertragsbestandteil. Sie stellt keinerlei Verpflichtung zur Lieferung von Materialien, Quellcode oder Funktionalität dar und es sollte bei einer Kaufentscheidung nicht auf sie vertraut werden. Die Entwicklung und die Freigabe von Features oder etwaiger Funktionalitäten verbleibt, auch in zeitlicher Hinsicht, im alleinigen Ermessen von Oracle. Nicht alle der genannten Technologien sind für alle Cloud Services verfügbar.

Haftungsausschluss

Die Informationen in dieser Präsentation dürfen nicht als rechtliche Beratung zu Inhalt, Auslegung oder Anwendung von Gesetzen, Verordnungen oder Richtlinien angesehen oder verwendet werden. Kunden und Interessenten sind gehalten, eigenständig entsprechenden Rechtsrat einzuholen, um die Anwendbarkeit von Gesetzen oder Bestimmungen auf die Verarbeitung personenbezogener Daten zu verstehen, einschließlich bei der Nutzung von Produkten oder Dienstleistungen eines Anbieters.

Einführung

Die EU Datenschutzgrundverordnung ist eine neue und wichtige Regelung zu Datenschutz und Datensicherheit.

Neben ihr existiert eine Reihe von Verordnungen und Gesetzen, um Unternehmen anzuhalten, Datenschutz in einer kommerziell digitalisierten Welt zu verbessern.

- Vorfälle im Bereich Internetsicherheit sind augenscheinlich in internationalen Berichten und in der Presse zu finden.

- Es gibt viele weitere wichtige europäische Gesetze, etwa:
  - Sicherheitsrichtlinie zu «Security of Network and Information Systems » (NIS)
  - Verordnung zu «electronic Identification And trust Services» (eIDAS)
  - Richtlinie zu «Payment Services in the Internal Market » (PSD2)
  - Vorschläge zu einer neuen ePrivacy Verordnung

Ursache ➡ Wirkung

Was haben diese Gesetze und Verordnungen gemeinsam?

- Sie erfordern ein interdisziplinäres Vorgehen (im Zusammenspiel von Recht und Technik).
- Sie sollten ganzheitlich angegangen werden, nicht einzeln.
- Die Verantwortlichkeit von Unternehmen und Einzelpersonen (Vorstände und Geschäftsführer) ist wichtig.
- Sie benötigen eine gute IT und gute Datensicherheit.
- Immer häufiger beziehen sie sich auf internationale «Best Practices» und Konzepte.

DS-GVO

Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Die EU Datenschutz-Grundverordnung (DS-GVO)

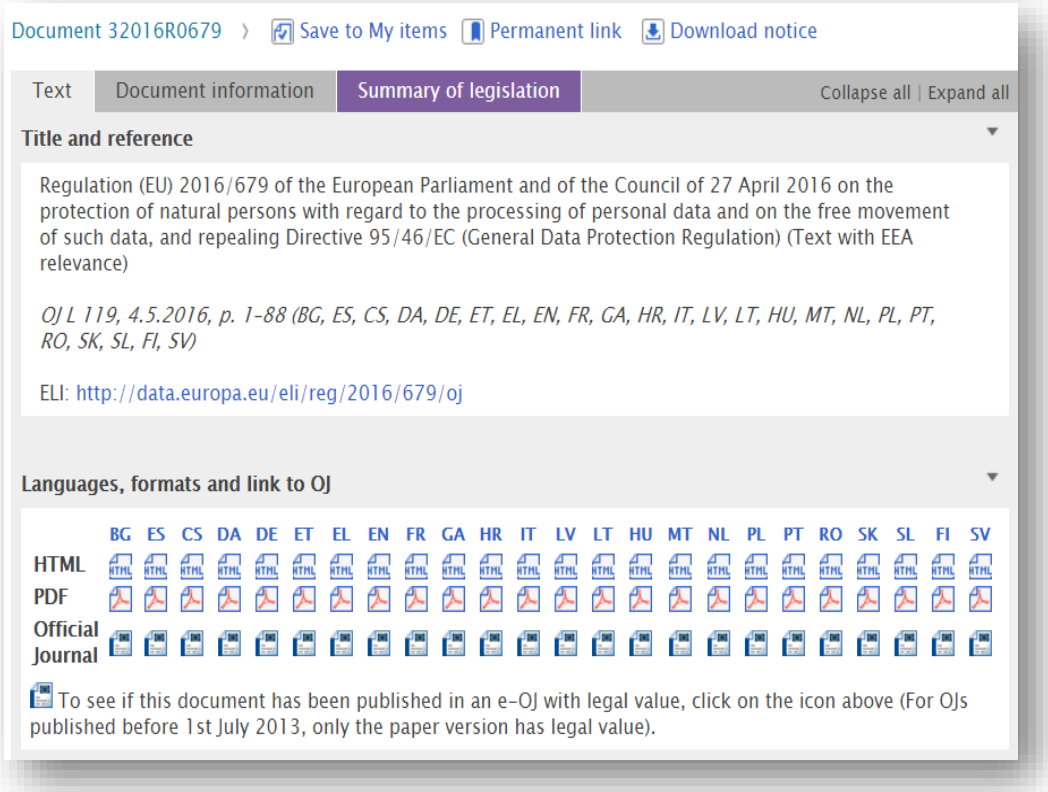
1. Die DS-GVO ist da.
2. Sie erfordert Ihr Tätigwerden.
3. Wir können Sie dabei unterstützen, compliance-relevante Punkte zu adressieren.

- Oracle ist bei der Bereitstellung von Cloud Services ein “Auftragsverarbeiter” (und speichert im Auftrag der Kunden personenbezogene Daten).
- Kunden sind im Sinne der DS-GVO Verantwortliche in Bezug auf Verarbeitung personenbezogener Daten, die sie Oracle anvertrauen.
- Oracle unterstützt Kunden als Technologieanbieter mit Hilfe von Lösungen (Produkten und Services) dabei, ihre Complianceanforderungen umzusetzen.

“Verantwortliche und Auftragsverarbeiter” sind die Schlüsselrollen in der EU-Datenschutzgrundverordnung

Die Datenschutzgrundverordnung

- Die DS-GVO ersetzt die über 15 Jahre alte EU Datenschutz-Richtlinie.
- Sie wurde am 4. Mai 2016 veröffentlicht und wird ab dem 25. Mai 2018 wirksam.
- Sie besteht aus 99 Artikeln und 173 erläuternden Erwägungsgründen.



http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1462886509332&uri=CELEX:32016R0679

Unternehmen in Europa und weltweit nehmen die Anforderungen der DS-GVO ernst:

Denn:

- Es können hohe Strafen fällig werden (bis zu 4 % des weltweiten Jahres-umsatzes oder 20 Mio. Euro) (Art. 83),
- Datenschutzverstöße müssen innerhalb von 72 Stunden der Aufsichtsbehörde gemeldet werden (Art. 33),
- Die Betroffenen müssen bei Daten-schutzverstößen ohne schuldhaftes Zögern benachrichtigt werden. (Art. 34).

Sie sollten zusätzlich berücksichtigen:

- dass Aufsichtsbehörden zur Verhängung von temporären oder endgültigen Beschränkungen oder Einstellung von Verarbeitungstätigkeiten befugt sind (Art. 58),
- dass Betroffene Beschwerde bei den zuständigen Datenschutzaufsichtsbehörden einlegen können (Art. 77),
- das Recht auf Einlegung eines Rechtsbehelfs gegen den Verantwortlichen oder Auftragsverarbeiter besteht (Art. 79),
- Anspruch auf Ersatz materieller und nicht-materieller Schäden besteht (Art. 82),
- Vertretungsrechte bestehen (Art. 80) um Schaden-ersatzansprüche gemäß Art. 82 in Anspruch zu nehmen.

Die DS-GVO verstehen: gute IT und gute Sicherheit

Der Schutz natürlicher Personen hinsichtlich der Verarbeitung ihrer personenbezogener Daten ist ein Grundrecht, das notwendigerweise in enger Beziehung zur Informationstechnologie (IT) steht.

In modernen Gesellschaften ist IT unumgänglich, wobei viele Anforderungen der Verordnung eine **gut aufgestellte IT** und **gute Sicherheit** implizieren**.**

Die DS-GVO verstehen: die DS-GVO und IT

- Der Schutz von Daten setzt Wissen voraus
  - über den Speicherort von Daten,
  - über die Bestimmung von Risiken.
- Manche Verpflichtungen können/müssen erfüllt werden im Hinblick
  - auf Veränderungen von Anwendungen,
  - bei der Gestaltung der IT-Architektur.

1. Verfahrensverzeichnisse

DATENBESTAND

Wissen über die Verarbeitung von Daten ist notwendig für deren Verarbeitung

Jeder Verantwortliche bzw. jeder in der Sphäre des Verantwortlichen Handelnde im Sinne der Verordnung, muss ein “Verzeichnis aller Verarbeitungstätigkeiten” für seinen Verantwortungsbereich führen (Art.30).

- Liste der Verarbeitungstätigkeiten:
  - Zwecke der Verarbeitung (z.B. Personalbeurteilung),
  - Benennung der Betroffenen (z.B. Beschäftigte),
  - Datenkategorien (z.B. Beurteilungen),
  - Informationen im Hinblick auf Übermittlung in Drittländer und internationale Organisationen (z.B. USA-Oracle Talent cloud services),
  - Wahrung von Aufbewahrungs- und Löschfristen (z.B. nach Ausscheiden aus dem Unternehmen + 1 Monat),
  - Beschreibung der Sicherheitsvorkehrungen (z.B. Level 3 Maßnahmen in MyGroup XY, +CASP).

- Die Führung von Verfahrensverzeichnissen ist der Ausgangspunkt für IT-Sicherheit im Rahmen der DS-GVO Compliance.
- Verfahrensverzeichnisse sollten auch zur Erreichung und Kontrolle von Complianceanforderungen verwendet werden.
- Verfahrensverzeichnisse können zum Nachweis von Compliance und Verantwortlichkeit verwendet werden.
- Verfahrensverzeichnisse können nach und nach mit weiteren Informationen befüllt werden.

2. Datenschutz-Folgeabschätzung

Risiko als Schlüsselwort kommt in der Verordnung 75 x vor: Verantwortlicher (Controller) und Auftragsverarbeiter müssen das Risiko für den Betroffenen kennen und abschätzen:

- Wenn in der Verarbeitung absehbar hohe Risiken für die Rechte und Freiheiten natürlicher Personen zu erwarten sind, muss vorab eine Datenschutz-Folgeabschätzung (Art. 35) seitens des Unternehmens erfolgen:
  - um die anwendbaren Datensicherheits-maßnahmen identifizieren zu können,
  - um beurteilen zu können, ob die Aufsichts-behörden in die Freigabe der Datenverarbeitung einbezogen werden müssen.

- Die “Data Protection Working Party” (WP29) hat Richtlinien für das “Data Protection Impact Assessment” (DPIA) veröffentlicht.
- Das DPIA eröffnet die Möglichkeit, mit Risiken für Betroffene umzugehen und stellt speziell auf die Sicht des Betroffenen ab, während hingegen das Risikomanagement an anderen Stellen auf die Organisation als Ganzes abzielt (z.B. Datensicherheit).
- Die DPIA Richtlinien referenzieren auf international “Best Practices” wie z.B. ISO 31000:2009 Riskomanagement und Grundlagen, ISO/IEC 29134 (Projekt), “Information technology – Security techniques – Privacy impact assess.ment – Guidelines”

3. Bestimmungen im Zusammenhang mit Betroffenenrechten

ANWENDUNGEN

Diese Verpflichtungen erfordern oftmals Anpassungen von Anwendungen.

Kapitel III der Verordnung „Rechte der betroffenen Person“ listet die Verpflichtungen für den Verantwortlichen (Controller) auf:

- Zugangsrechte der betroffenen Person (Art. 15),
- Recht auf Berichtigung (Art. 16),
- Recht auf Löschung (“Recht auf Vergessenwerden”) (Art .17),
- Recht auf Einschränkung der Verarbeitung (Art.18),
- Mitteilungspflichten im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung (Art. 19),
- Recht auf Datenübertragbarkeit (Art. 20).

- Diese Bestimmungen erfordern oftmals manuelles Eingreifen und/oder Anpassungen von Anwendungen, wie z.B folgende:
- Löschungen sind zu prüfen, wobei andere Betroffenenrechte zu berücksichtigen sind wie z.B. offene Zahlungsverpflichtungen (manuelles Eingreifen),
- Datenportabilität benötigt eine spezielle Funktion, wonach ein Datenexport in ein maschinenlesbares Format möglich ist, falls dies vom Betroffenen gewünscht ist (Anpassung der Anwendung).

4. Datensicherheitsbestimmungen

Einige Bestimmungen der DS-GVO referenzieren auf die Verpflichtung, geeignete technische und organisatorische Maßnahmen zu implementieren:

- Grundsätze für die Verarbeitung personen-bezogener Daten (Art. 5),
- Verantwortung des Verantwortlichen (Art. 24),
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („data privacy by design and by default”) (Art. 25),
- Auftragsverarbeiter (Art. 28),
- Sicherheit der Verarbeitung (Art.32),
- Benachrichtigungen bei Datenschutzverstößen (Art. 34)

Am aussagekräftigsten ist Artikel 32 «Sicherheit der Verarbeitung», weil er die Datensicherheits-bestimmungen konkretisiert:

- den Kontext und die Ziele benennt,
- ein Beispiel für eine Datensicherheits-maßnahme benennt (Verschlüsselung),
- die Zielstellung erläutert,
- Elemente, die dem Aufzeigen vom Compliance dienen können.

Welche Datensicherheitsmaßnahmen sind zu implementieren?

Da:

- das Gesetz offenlässt, welche spezifischen Datensicherheitsmaßnahmen zu ergreifen und der Verantwortliche sowie der Auftragsverarbeiter gleichermaßen verantwortlich sind,
- Zertifizierungen, CoC, Aufsichtsbehörden, Richter und Sachverständige sich am allgemeinen Rechtsempfinden und an internationalen «Best Practices» orientieren.

Müssen Sie:

1. wissen, welche personenbezogenen Daten verarbeitet werden und wo sich diese im System befinden,
2. die Risiken für die Betroffenen kennen,
3. die grundlegenden Datensicherheitsmaßnahmen implementieren,
4. zusätzliche Sicherheit schaffen und eine funktionierende IT sicherstellen.

Risikoanalyse und häufige Fehler

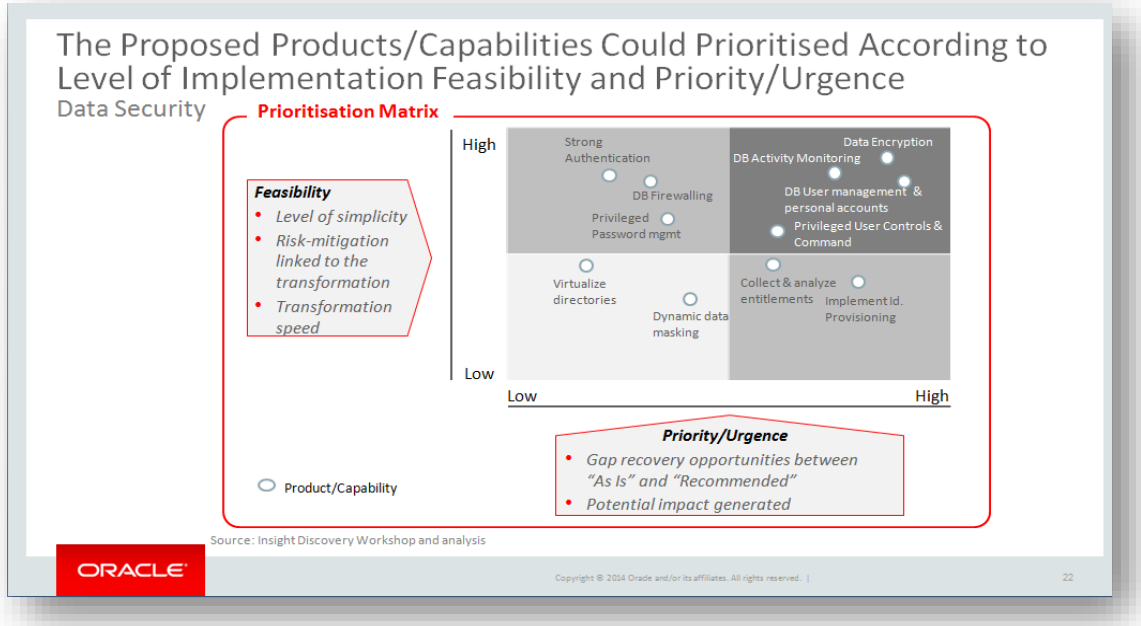
Einige Sicherheitskonzepte, die mehr und mehr an Bedeutung gewinnen:

- Starke/mehrschichtige/föderierte Authentifizierung
- Adaptierte/feinkörnige Zugangskontrolle
- «Segregation of Duties» Prinzip
- «Need-to know & least privilege Prinzip»
- Festlegung von Verantwortlichkeiten /Login Management (+ Protokollierung)
- Verschlüsselung
- Anonymisierung + Pseudonymisierung
- «Segregation of Environment» Prinzip
- Sicheres Konfigurationsmanagement / «Härtung» des Systems
- Backup, «High-Availability» und Disaster Recovery

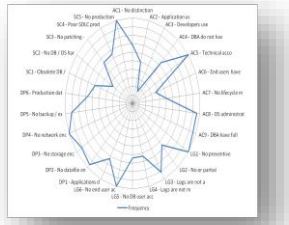
Häufige Defizite im elementaren Sicherheitsbereich

Oracle unterstützt seine Kunden seit Jahren bei der Identifizierung von Sicherheitslücken mit Hilfe des sog. «Security Assessments» oder einer

«Security Maturity Evaluation»



- Die häufigsten Defizite:
  - Mehrfachnutzung von Passwörtern
  - Fehlendes Logging
  - Unzureichende Installation von Patches
  - Keine Verschlüsselung
  - Zu weitreichende Privilegienvergabe



- Die Einhaltung von Compliance funktioniert nicht ohne ausreichende Basissicherheit.

Ask a Security Assessment
Check this video for the DBSecurity http://bit.ly/29GIYF3
Ask the Most Common Mistake white paper

ORACLE

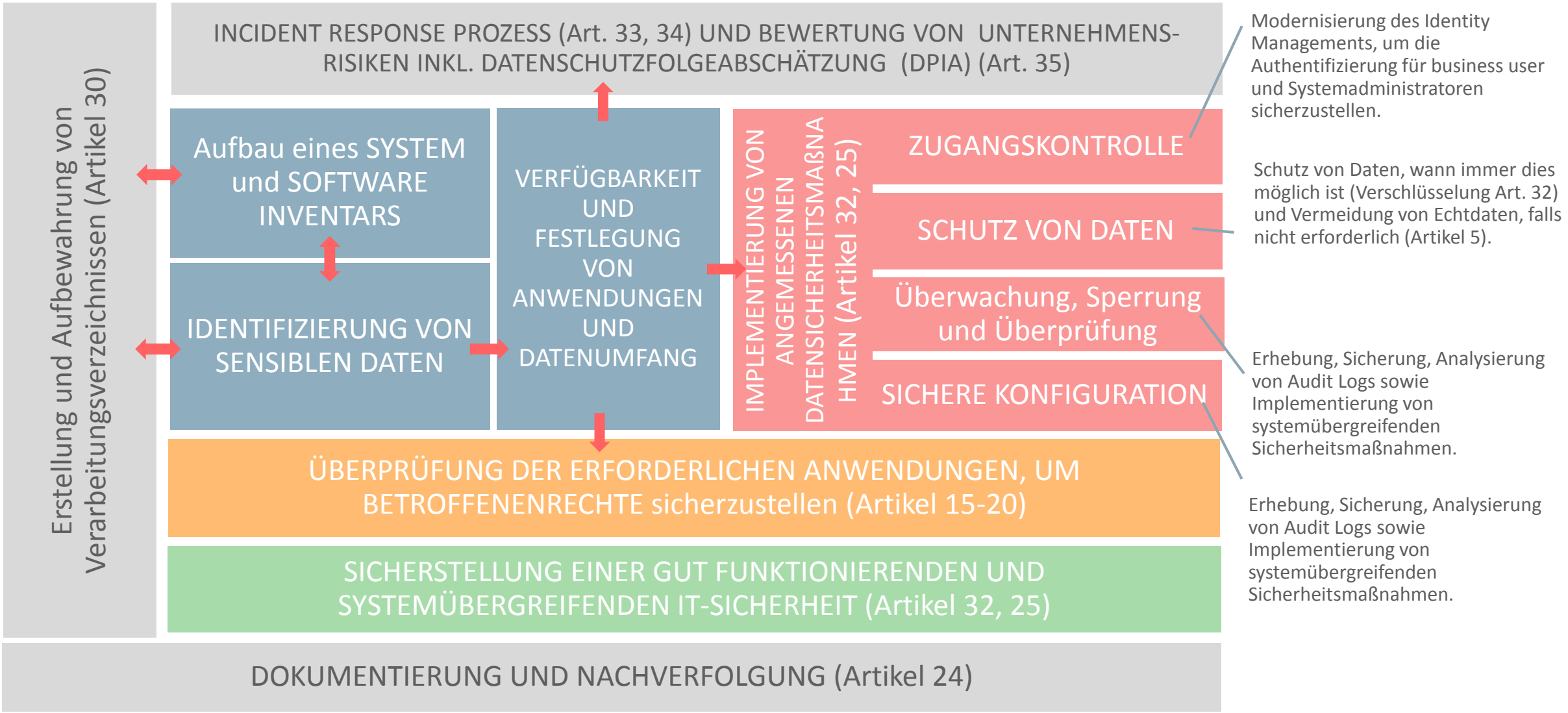
Oracle als Technologieanbieter

DS-GVO & Oracle

- Compliance benötigt das Zusammen-wirken von abgestimmten Handlungen durch unterschiedliche Abteilungen in einem Unternehmen:
- Folgende Aspekte müssen berücksichtigt werden:
  - Organisatorische Belange
  - Rechtliche und vertragliche Belange
  - Informationstechnologie
- Eine gut aufgestellte IT kann bei der Einhaltung von Compliance unterstützen.

- Oracle stellt Technologie zur Verfügung, um u.a.
  - Vertraulichkeit, Integrität und Verfügbarkeit zu verbessern
  - Systemstabilität zu erhöhen,
  - sensible Daten in den Systemen zu identifizieren,
  - die Auswirkungen von Vorfällen abzumildern.
- Oracle kann dabei unterstützen, Techno-logie in den richtigen Rahmen zu setzen.

Schrittweise Annäherung an die EU DS-GVO – Aufgaben und Lösungen



Modernisierung des Identity Managements, um die Authentifizierung für business user und Systemadministratoren sicherzustellen.

Schutz von Daten, wann immer dies möglich ist (Verschlüsselung Art. 32) und Vermeidung von Echtdaten, falls nicht erforderlich (Artikel 5).

Erhebung, Sicherung, Analysierung von Audit Logs sowie Implementierung von systemübergreifenden Sicherheitsmaßnahmen.

Erhebung, Sicherung, Analysierung von Audit Logs sowie Implementierung von systemübergreifenden Sicherheitsmaßnahmen.

Schrittweise Annäherung an die DS-GVO

VERFÜGBARKEIT UND FESTLEGUNG VON ANWENDUNGEN UND DATENUMFANG

IMPLEMENTIERUNG VON ANGEMESSENEN DATENSICHERHEITSMAßNAHMEN (Artikel 32, 25)

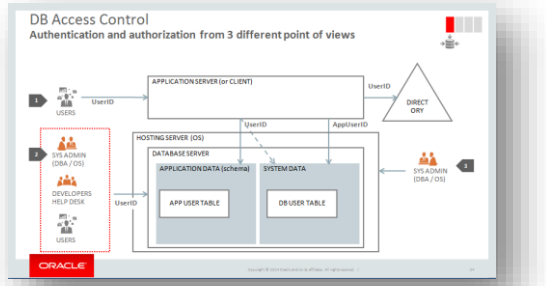
- ZUGANGSKONTROLLE
- SCHUTZ VON DATEN
- Überwachung, Sperrung und Überprüfung
- SICHERE KONFIGURATION

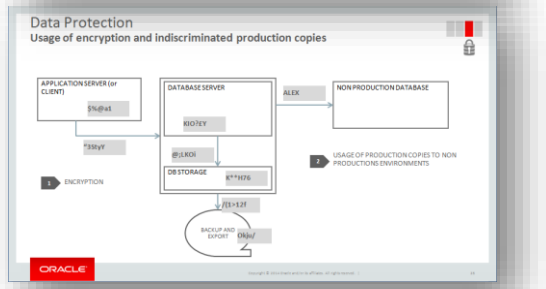
Modernisierung des Identity Managements, um die Authentifizierung für business user und Systemadministratoren sicherzustellen.

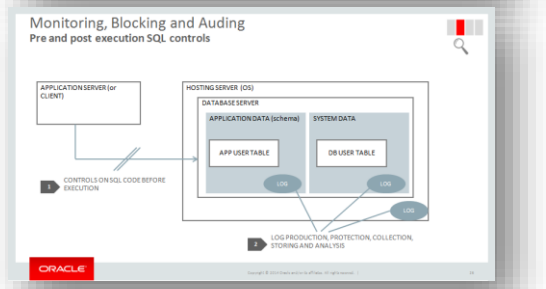
Schutz von Daten, wann immer dies möglich ist (Verschlüsselung Art. 32) und Vermeidung von Echtdaten, falls nicht erforderlich (Artikel 5).

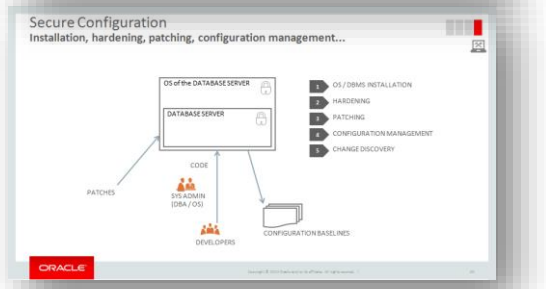
Erhebung, Sicherung von Analysierung von von Audit Logs sowie Implementierung von systemübergreifenden Sicherheitsmaßnahmen.

Erhebung, Sicherung von Analysierung von von Audit Logs sowie Implementierung von systemübergreifenden Sicherheitsmaßnahmen.







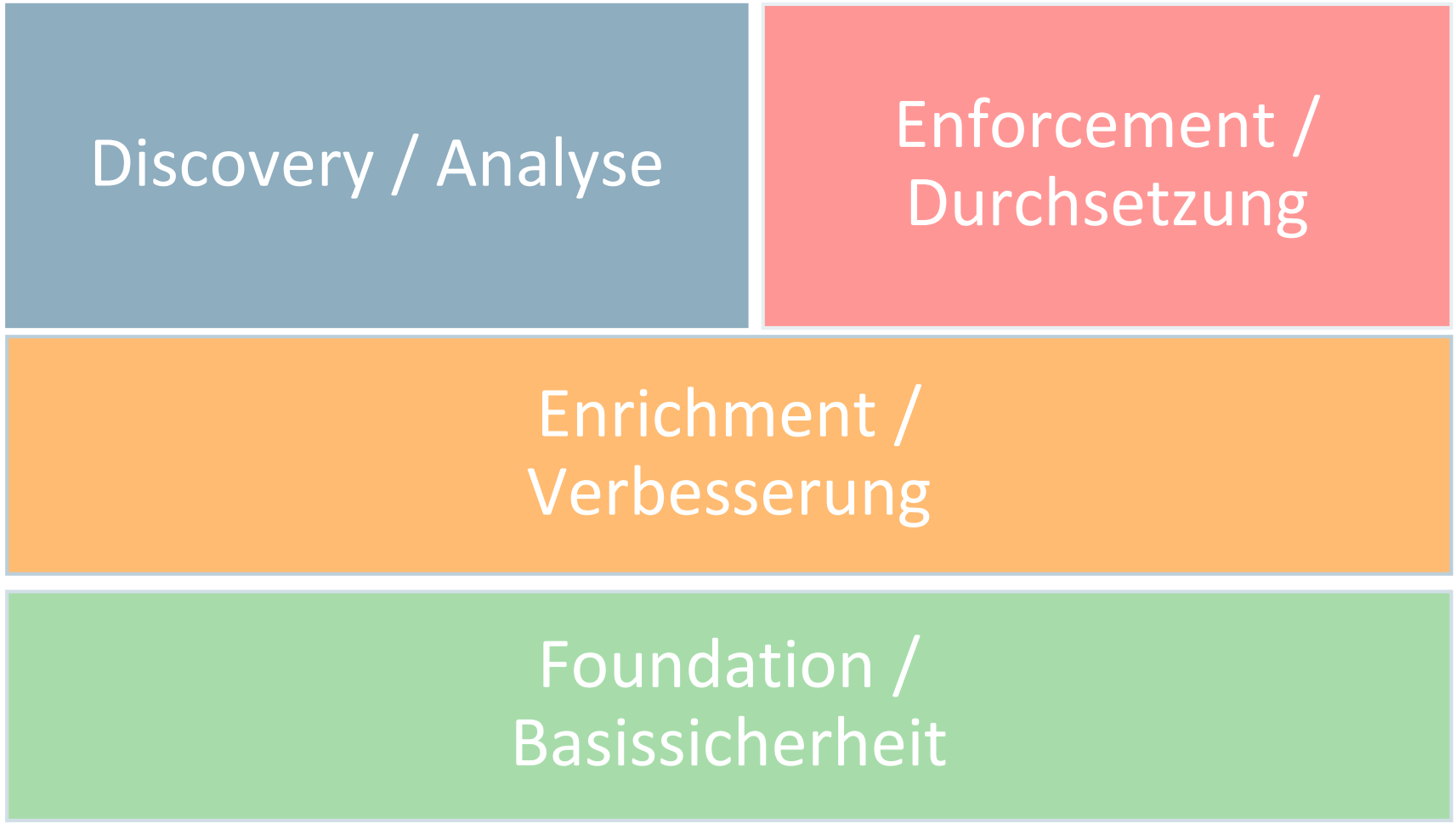


Sie müssen Ihre IT Sicherheit überprüfen und Ihre Verbesserungsprojekte priorisieren.

Hierzu können Sie das Oracle Security Assessment einsetzen und die Implementierung Ihrer Oracle Technologie überprüfen.

ORACLE

Schrittweise Annäherung an die DS-GVO – Produktbereiche

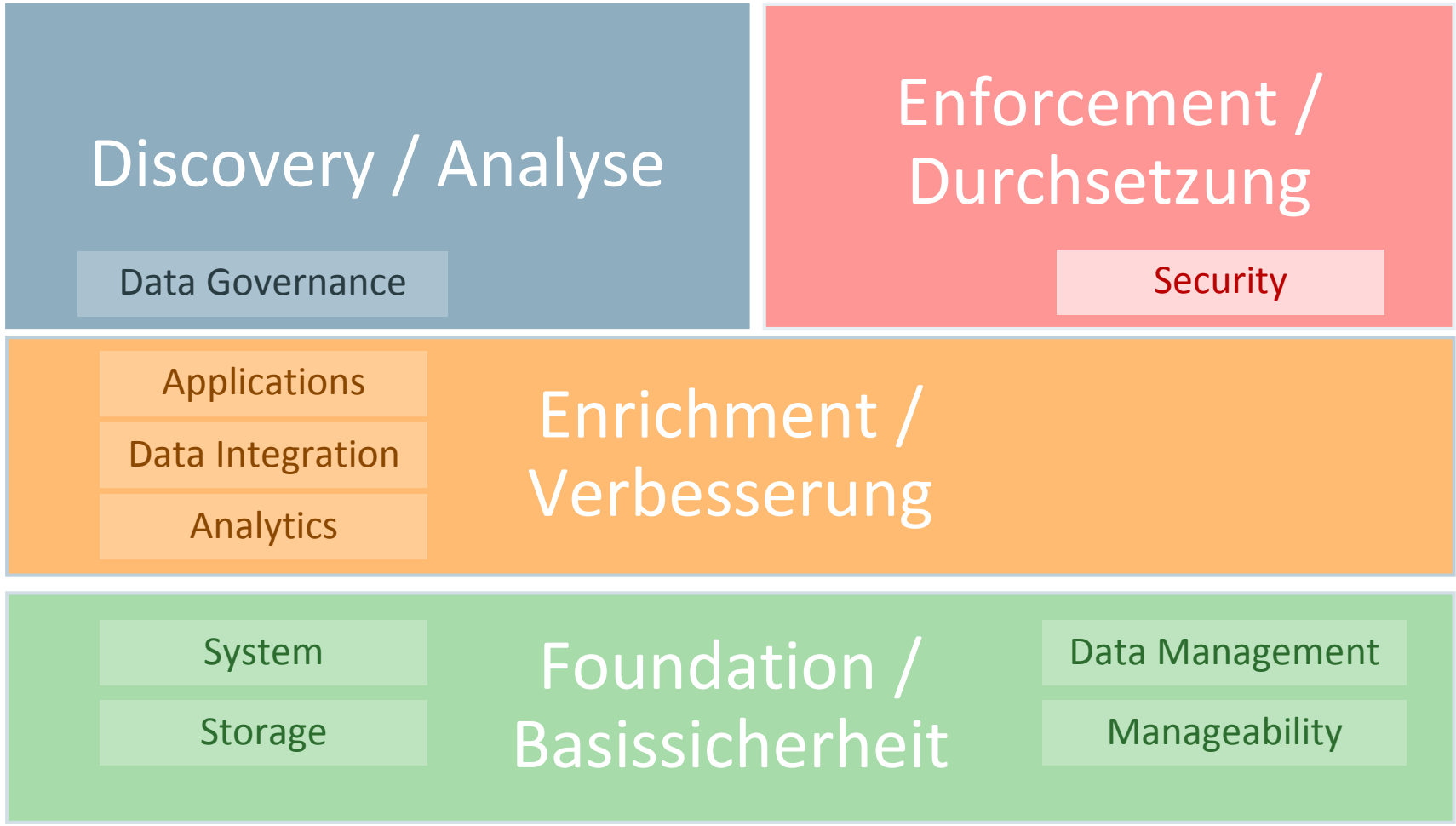


Oracle Produkte oder Security Cloud Services können bei der Sicherstellung von Compliance mit der EU DS-GVO unterstützen.

Wir können bei folgenden Themenbereichen unterstützen:

1. **Identifikation** von sensiblen Daten mit Data Governance Lösungen.
2. **Durchsetzung** strenger Daten-, Software- und Benutzersicherheit.
3. **Anreicherung** von Anwendungs-funktionen, um Betroffenen-rechte zu gewährleisten.
4. **Unterstützung** von gut funktionierenden “IT Practices” im Hinblick auf Hochverfügbarkeit und Systemsstabilität.

Schrittweise Annäherung an die DS-GVO – «tech domains»

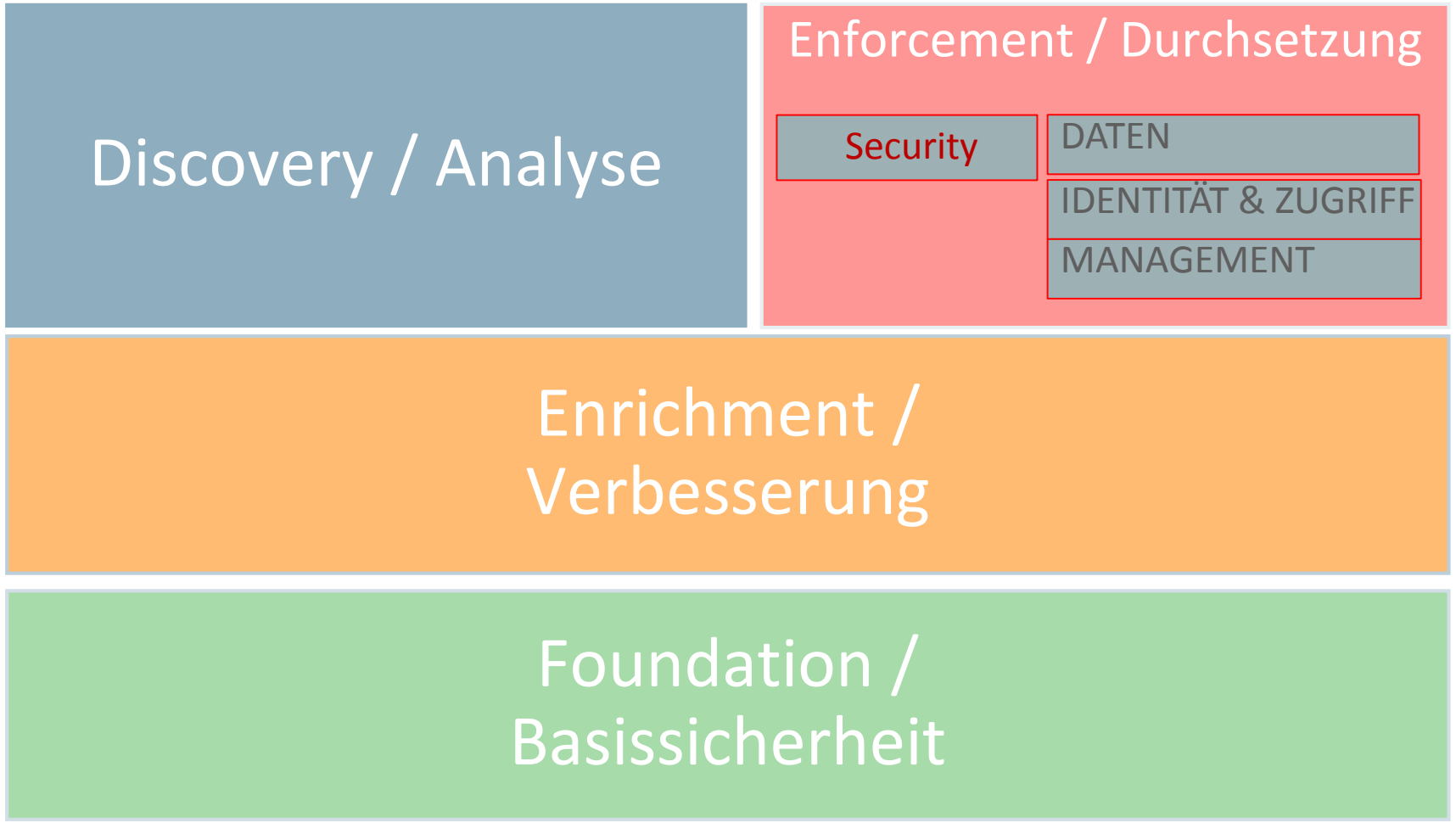


Oracle Produkte oder Security Cloud Services können bei der Sicherstellung von Compliance mit der EU DS-GVO unterstützen.

Wir können bei folgenden Themenbereichen unterstützen:

1. **Identifikation** von sensiblen Daten mit Data Governance Lösungen.
2. **Durchsetzung** strenger Daten-, Software- und Benutzersicherheit.
3. **Anreicherung** von Anwendungs-funktionen, um Betroffenen-rechte zu gewährleisten.
4. **Unterstützung** von gut funktionierenden “IT Practices” im Hinblick auf Hochverfügbarkeit und Systemsstabilität.

Schrittweise Annäherung an die EU DS-GVO – security product families

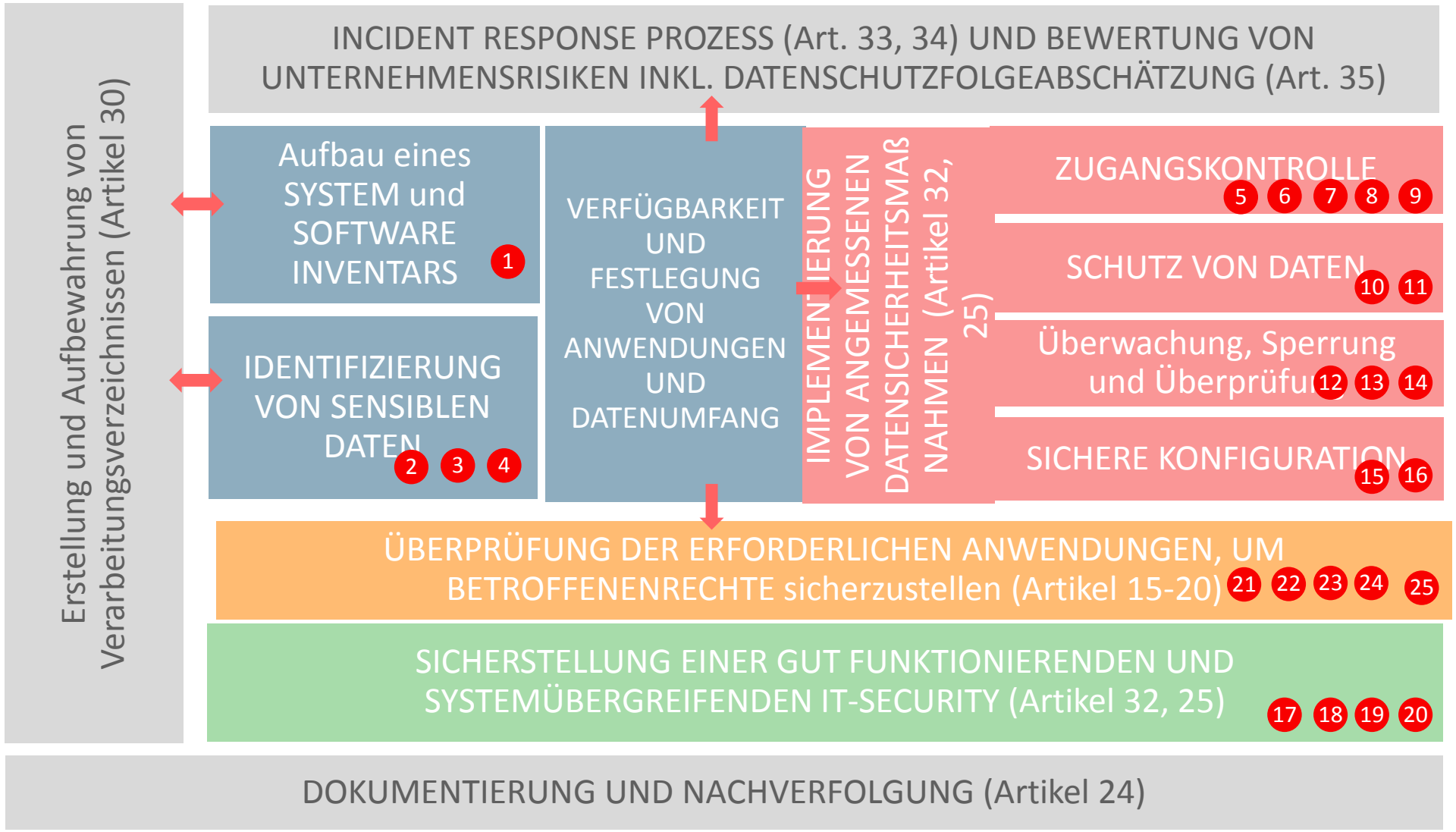


Oracle Security and Manangementlösungen können ein Unternehmen bei folgenden Themen-bereichen unterstützen:

1. **Datensicherung** im Ruhe-zustand und Überführung in Datenbanken.
2. **Organisation und Kontrolle** der Identifikation und des Zugangs von busienss usern und Systemadministratoren.
3. **Management** eines komplexen IT Systems

in zunehmenden hybriden CLOUD Infrastrukturen.

Schrittweise Annäherung an die EU DS-GVO – Details



Produkt / Suite

1 Enterprise Manager - Automatic Discovery
2 Enterprise Metadata Management
3 Enterprise Data Quality
4 Application Data Modeling - Sensitive Data Discovery
5 Identity Governance
6 Access Management
7 Centralized Directory
8 Identity Cloud Service
9 Database Vault
10 Advanced Security and Key Vault
11 Database Masking and Subsetting
12 Audit Vault & DB Firewall
13 Security Monitoring and Analytics
14 Cloud Access Security Broker
15 Enterprise Manager - Configuration and Compliance pack
16 Configuration and Compliance Cloud Service
17 Data Guard and Real Application Cluster
18 Exadata and Supercluster
19 Zero Data Loss Recovery Appliance & ZFS
20 SPARC / Solaris
21 Customer Data Management Cloud Service
22 Policy Automation
23 Analytics Cloud
24 BI Enterprise Edition
25 Data Integration

Nächste Schritte

Oracle UK > About Oracle > Features > General Data Protection Regulation

Oracle security solutions

GDPR is Coming. Are You Ready?

Learn how Oracle Security Solutions can help organizations implement controls that reduce the risk of non-compliance fines around GDPR.

oracle.com/goto/gdpr

Integrated Cloud

Applications & Platform Services


ORACLE®