

ORACLE®

EU DS-GVO. Beitrag von Oracle Lösungen zur Datensicherheit

Ernst Lorenz

BDM Security Tech North

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.

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

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

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

Denn:

- Es können hohe **Strafen** fällig werden (bis zu 4 % des weltweiten Jahresumsatzes oder 20 Mio. Euro) (Art. 83),
- Datenschutzverstöße müssen innerhalb von 72 Stunden der Aufsichtsbehörde **gemeldet** werden (Art. 33),
- Die Betroffenen müssen bei Datenschutzverstößen 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 Schadenersatzansprüche gemäß Art. 82 in Anspruch zu nehmen.

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.





DATENBESTAND

Wissen über die Verarbeitung von Daten ist notwendig für deren Verarbeitung

1. Verfahrensverzeichnisse

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, +CASB).
- 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 Datensicherheitsmaßnahmen identifizieren zu können,
 - um beurteilen zu können, ob die Aufsichtsbehörden 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 assessment – Guidelines”

3. Bestimmungen im Zusammenhang mit Betroffenenrechten

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 personenbezogener 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 Datensicherheitsbestimmungen konkretisiert:

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

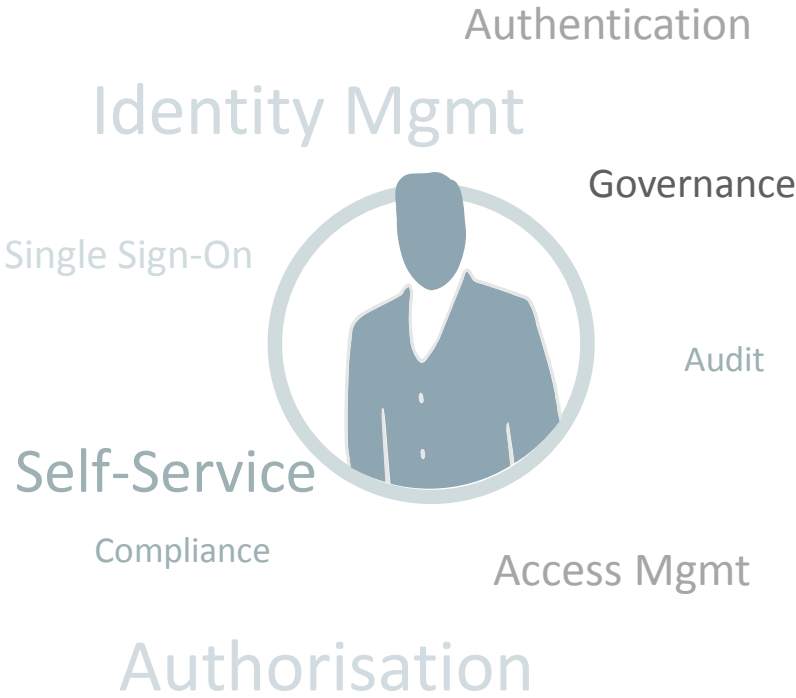
Einige Sicherheitskonzepte, die mehr und mehr an Bedeutung gewinnen:

- 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

Oracle SECURITY PRODUKTSEGMENTE

Oracle SECURITY Produktsegmente

Personensicherheit



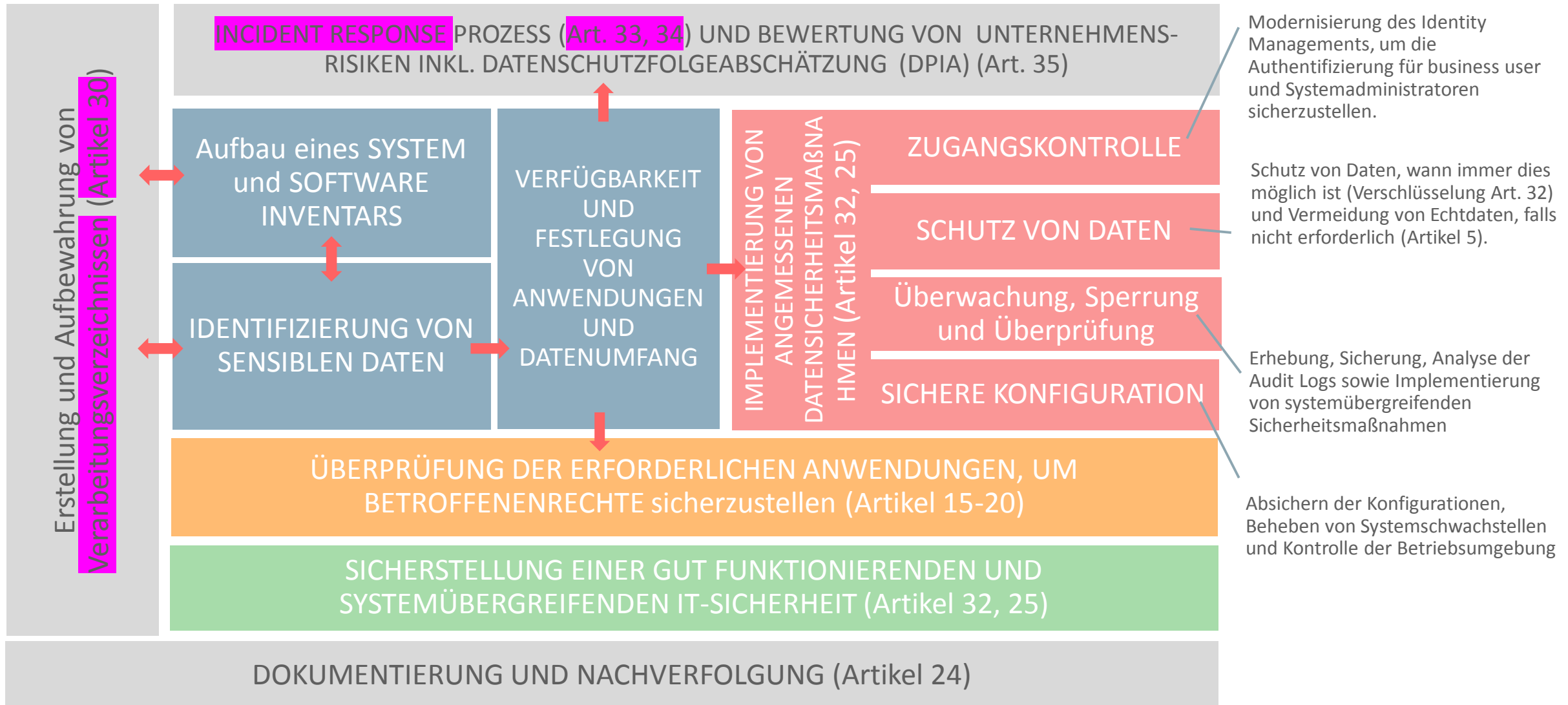
Sicherheit in der Software



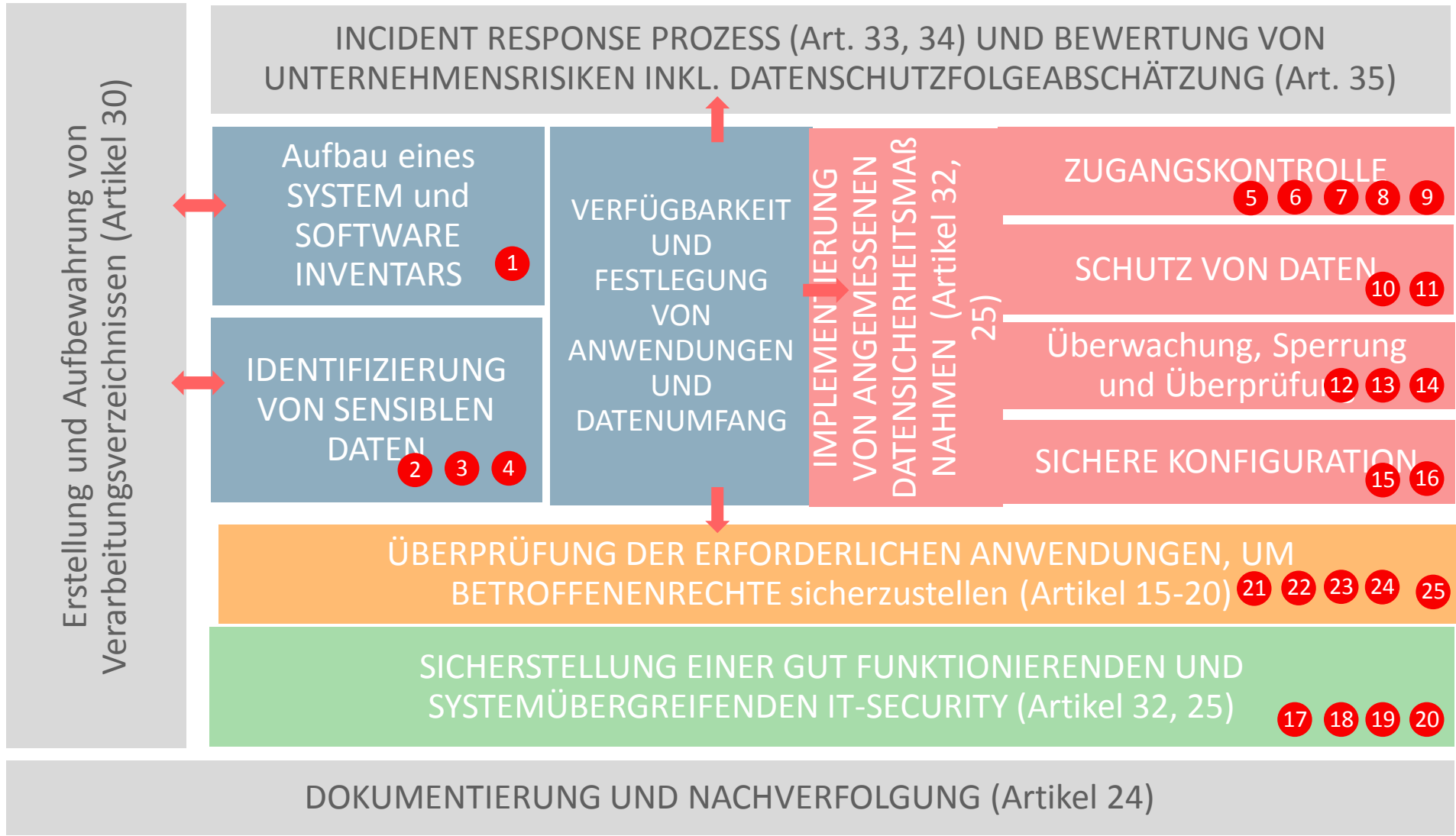
Datensicherheit



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



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



wie geht's weiter?

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



Live Webcast

Accelerate EU GDPR Compliance with Database Security, June 27, 2017

A photograph showing three business professionals in an office setting. Two men and one woman are gathered around a laptop, looking at the screen with interest.

On-demand Webcast

How Selected Oracle Data Security Solutions May Assist with Your GDPR Compliance

A photograph of a man in a checkered shirt, looking thoughtful with his hand on his chin.

Whitepaper

Accelerate Your Response to the EU General Data Protection Regulation (GDPR)

Accelerate Your Response to the EU General Data Protection Regulation (GDPR)
Using Oracle Database Security Products

The cover of a whitepaper document, featuring a red and white design.

Integrated Cloud

Applications & Platform Services

ORACLE®