KPMG

Praktische Compliance: GeschGehG

GI SECMGT Workshop 8. September 2022
Prof. Dr. Dirk Loomans

Agenda

KPMG

1. Gesetz und Abgrenzung

Neuordnung des Geschäftsgeheimnisschutzes

- Bisher galt: wer sein Know-how schützen wollte, konnte dieses ohne großen Aufwand zum Geschäftsgeheimnis erklären (subjektiver Geheimhaltungswille)

Neue Regelung:

Der Geheimnisinhaber **muss** zukünftig, um vom Schutz des GeschGehG zu profitieren, darlegen können, dass er sein Know-how durch nach außen hin erkennbare (objektive) angemessene Geheimhaltungsmaßnahmen geschützt hat. Hierzu zählen:

- **angemessene Schutzmaßnahmen** treffen,
- die zudem **ausreichend dokumentiert** werden müssen und eine
- **Compliance-Strategie zum Geheimnisschutz** erforderlich machen.

- **Unternehmen benötigen ein Geheimnisschutz-Management, um Haftungsfallen zu entgehen.**
- **Insbesondere müssen alle Unternehmensbereiche auf Geschäftsgeheimnisse hin untersucht und entsprechende Geheimhaltungsmaßnahmen ergriffen werden.**

Geheimnisschutz auf europäischer Ebene

Anlass für Harmonisierung:

- Geheimnisschutz war auf europäischer Ebene infolge seiner unterschiedlichen nationalen Regelungen bisher fragmentiert.
- Konsequenz: Hindernis für grenzüberschreitende Kooperation.
- Ferner bestand erhebliches Durchsetzungsdefizit dahingehend, dass Vertraulichkeit eines Geschäftsgeheimnisses im Verlauf von Gerichtsverfahren oft nicht gewahrt blieb.

EU-Recht:

- Erlass der **Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung** am 8. Juni 2016

Umsetzung nationales Recht:

- Gesetzesbeschluss des Bundestages am 18.04.2019 und **Inkrafttreten am 26.04.2019**

Überblick

01	Relevanz	Nach Schätzungen des BDI belaufen sich allein in Deutschland Schäden durch Datendiebstahl, Industriespionage und Sabotage auf jährlich über 50 Mrd. EUR. Zum besseren Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung (§ 1 GeschGehG) ist das neue Geschäftsgeheimnisgesetz in Kraft getreten.
02	Ziel	Ziel des Gesetzes ist ein zivilrechtlicher Schutz der Geschäftsgeheimnisse und die Harmonisierung des Geheimnisschutzes in der EU, welcher bislang erhebliche Unterschiede aufwies. Mit dem Gesetz zum Schutz von Geschäftsgeheimnissen wird definiert, was unter einem Geschäftsgeheimnis verstanden wird. (§ 2 GeschGehG)
03	Rechtliche Pflichten	Im Rahmen der Pflicht des Geschäftsführers gemäß § 43 Abs. 1 GmbH und des Vorstandes nach § 93 (1) & (2) AktG, Schaden von der Gesellschaft abzuhalten, ist die Geschäftsleitung verpflichtet, für einen ausreichenden Schutz der Geschäftsgeheimnisse zu sorgen. Sie hat auch dafür Sorge zu tragen, dass sie nicht fahrlässig Geschäftsgeheimnisse Dritter nutzt, die sie von anderen aus einer unerlaubten Handlung erlangt hat.
04	Das Geschäftsgeheimnis	Der rechtliche Schutz von Geschäftsgeheimnissen hängt allein von der tatsächlichen Geheimhaltung der betreffenden Information ab und nicht von anderen Voraussetzungen wie einer besonderen Schöpfungshöhe oder einer Eintragung in ein Register. Dies ist eine objektive Voraussetzung, die der Geheimnisinhaber im Streitfall beweisen muss.
05	Rechtliche Konsequenzen	Fehlt es beispielsweise an angemessenen rechtlichen, technischen und organisatorischen Geheimhaltungsmaßnahmen, gilt eine nicht ausreichend geschützte Information unabhängig von ihrem tatsächlichen Wert für ein Unternehmen **nicht** als Geschäftsgeheimnis. Zudem hat der Inhaber eines Geschäftsgeheimnisses im Schadensfall keinen Anspruch auf Schadenersatz (Beweislastumkehr). (§ 2 GeschGehG)
06	Geheimnisschutz-Compliance	Um im Schadensfall vom Gesetz zum Schutz von Geschäftsgeheimnissen zu profitieren und eine persönliche Haftung zu vermeiden, muss der Inhaber des Geschäftsgeheimnisses angemessene rechtliche, technische und organisatorische Geheimhaltungsmaßnahmen ergreifen. Dies kann der Geheimnisinhaber durch ausreichende Dokumentation der Informationssicherheits- und Compliance-Strategie und durch die Aufstellung eines Geheimnisschutz-Managements sicherstellen.

Das „neue" Geschäftsgeheimnis

Ein **Geschäftsgeheimnis** ist gemäß § 2 Nr. 1 GeschGehG eine Information, die

- **weder** insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, **allgemein bekannt oder** ohne weiteres **zugänglich** ist **und daher von wirtschaftlichem Wert** ist und

- Gegenstand von den Umständen nach **angemessenen Geheimhaltungsmaßnahmen** durch ihren rechtmäßigen Inhaber ist und

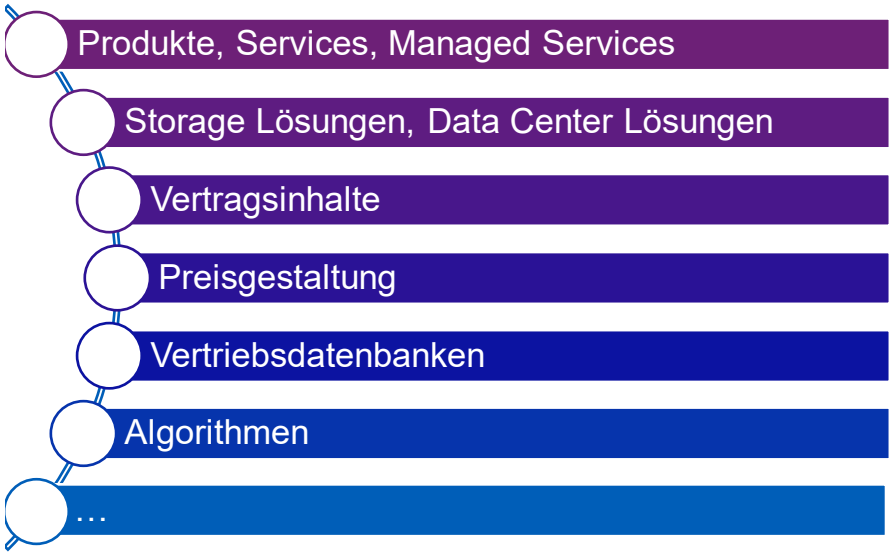
- bei der ein **berechtigtes Interesse an der Geheimhaltung** besteht.

  - ➢ Die vorstehenden Voraussetzungen müssen **kumulativ** vorliegen.

  - ➢ Fehlt es beispielsweise an angemessenen Geheimhaltungsmaßnahmen, gilt eine nicht geschützte Information unabhängig von ihrem tatsächlichen Wert für ein Unternehmen **nicht** als Geschäftsgeheimnis.

Das „neue" Geschäftsgeheimnis

- Es kann sich **sowohl** um **technisches als auch** um **kaufmännisches Wissen** handeln:
  - Die Unterscheidung zwischen Geschäfts- und Betriebsgeheimnissen wird aufgegeben.
  - Auch Kundendaten und Berechnungsmodelle oder Algorithmen können Geschäftsgeheimnisse sein.



- Nunmehr ist **stets auch eine „angemessene Geheimhaltungsmaßnahme"** erforderlich.

- Folge ist die **Änderung der Beweislast**: Geheimnisinhaber muss darlegen und beweisen, dass und vor allem welche konkreten, angemessenen Schutzmaßnahmen er getroffen hat.

„Nur wer sich selbst schützt, wird geschützt!"

Das „neue" Geschäftsgeheimnis

Unterschied zum Immaterialgüterrecht

- Der Schutz von Geschäftsgeheimnissen macht **keine besondere Qualität der betreffenden Informationen** für den rechtlichen Schutz erforderlich.

- Der rechtliche Schutz von Geschäftsgeheimnissen hängt **allein** von der **tatsächlichen Geheimhaltung** der betreffenden Information ab und **nicht von anderen Voraussetzungen** wie einer besonderen Schöpfungshöhe oder einer Eintragung in ein Register (BReg, Begründung GeschGehG-E, BT-DS 19/4724).

  - Dies ist eine **objektive Voraussetzung**, die der **Geheimnisinhaber** im Streitfall **beweisen** muss.

Das „neue" Geschäftsgeheimnis

Unterschied zu anderen Rechtsgebieten

- Patent- und Geheimnisschutz schließen sich nicht aus
- Wesentlicher Unterschied ist, dass bei Patenten, Marken oder Geschmacksmustern der Schutz durch Eintragung in das entsprechende Register entsteht.
- Anzahl der Patente ist deutlich geringer als die Anzahl an Geschäftsgeheimnissen
- Der rechtliche Schutz von Geschäftsgeheimnissen hängt allein von der tatsächlichen Geheimhaltung der betreffenden Information ab und nicht von anderen Voraussetzungen (besondere Schöpfungshöhe/Eintragung in ein Register)
- Patent: schützt gegen Nachahmung, kann gegen jeden durchgesetzt werden (absolut wirkendes Recht)
  GeschGeh: keine Möglichkeit gegen rechtmäßig erworbenes Wissen vorzugehen

Der Hauptunterschied des Informationsschutzes durch Geschäfts-geheimnisse gegenüber dem auch durch die Offenlegung der Information gekennzeichneten Patentschutz lässt sich plastisch mit dem **Bild eines Eisbergs** darstellen:

Während die verhältnismäßig **wenigen patentrechtlich geschützten** und offengelegten **Informationen als Spitze des Eisberges** aus dem Meer ragen, befindet sich dessen, um ein **Vielfaches größerer Rumpf**, **– die Geschäftsgeheimnisse – unsichtbar unter Wasser.**

Rechtsschutz

Ansprüche und Risiken aus unerlaubten Handlungen

01	Beseitigung und Unterlassung	Anspruch auf Beseitigung der Beeinträchtigung und bei Wiederholungsgefahr auch Anspruch auf Unterlassung.
02	Vernichtung und Herausgabe	Anspruch auf Vernichtung oder Herausgabe von im Besitz des Rechtsverletzers befindlichen Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die Geschäftsgeheimnisse enthalten oder verkörpern.
03	Rückruf, Entfernung und Rücknahme	Anspruch auf Rückruf des rechtsverletzenden Produkts, dessen dauerhafte Entfernung aus Vertriebswegen, auf Vernichtung rechtsverletzender Produkte und deren Rücknahme vom Markt, soweit das Geschäftsgeheimnis hierdurch nicht beeinträchtigt wird.
04	Auskunft und Schadensersatz	Anspruch auf Auskunft zu gesetzlich bestimmten Informationen wie zu Herstellern, Lieferanten, Mengen, Kaufpreise, das Geheimnis verkörpernde oder beinhaltende Gegenstände u.ä. sowie auf Schadensersatz bei Auskunftsverweigerung.
05	Schadensersatz	Anspruch auf Ersatz des aus der vorsätzlich oder fahrlässig begangenen unerlaubten Handlung entstehenden Schadens unter Berücksichtigung u.a. auch des Gewinns aus der Rechtsverletzung.

Folgen eines fehlenden Geheimnisschutzes

Beispiel: Rechtspraxis im Ausland – Italien mit dem GeschGehG entsprechenden Normen

Hintergrund:

- Ein Mitarbeiter eines Unternehmens hat technische Zeichnungen auf seinem privaten, passwortgeschütztem Laptop mit Wissen des Arbeitgebers gespeichert.

EU-Recht:

- Ehemaliger Arbeitgeber machte nach Ausscheiden des Mitarbeiters und gegen dessen neuen Arbeitgeber als Wettbewerber Ansprüche geltend.

Urteil des Gerichts/ Begründung:

- Verneinung des Vorliegens eines Geschäftsgeheimnisses durch das Gericht wegen fehlender Schutzmaßnahmen des ehemaligen Arbeitgebers.
  - Es hätte nicht zulässig sein dürfen, die technischen Zeichnungen auf dem privaten Laptop des Arbeitnehmers zu speichern.
  - Sie hätten ausschließlich in den Datenbanken des ehemaligen Arbeitgebers gespeichert werden dürfen.

  (Tribunal die Bologna, Urteil vom 27.07.2015, Nr. 2340/2015 – Az. 1658/2012)

KPMG

2. Klassifizierung / Schutzstufen modell

3. Klassifizierung/ Schutzstufenmodell

Geheimnisschutz-Management (1/3)

- Pflicht zum Geschäftsgeheimnis-Management-System
- Anforderungsdreiklang für angemessenes Geheimnisschutz-Management:

identifizieren  bewerten  schützen 

Erforderliche Schritte

- Identifizieren von Geschäftsgeheimnissen
- Wirtschaftliche Bewertung der Information, um „angemessenen“ Schutzumfang festzulegen
- Ergreifen von Schutzmaßnamen durch zuständige, vorher zu benennende Stellen

Bestandsaufnahme 1

- Schutzwürdig und schutzfähig?
- Dokumentation

Zuordnung sichern 2

- Rechtmäßige Kontrolle

Maßnahmen treffen 3

- Organisatorische Maßnahmen
- Technische Maßnahmen
- Rechtliche Maßnahmen

Compliance sichern 4

- Schulen und informieren
- Zuständigkeit („Geheimnisschutz-beauftragter“)
- Überwachen

Geheimnisschutz-Management (2/3)

Technische, organisatorische und rechtliche Maßnahmen sind miteinander zu verzahnen

Zumindest folgende Aspekte sollten berücksichtigt und geregelt werden:

- **Klassifizierung** unternehmenskritischer Informationen (Geheimhaltungsgrade unter Berücksichtigung der Folgen einer Offenlegung und Eintrittswahrscheinlichkeit),

- Festlegung der jeweiligen Klassifizierung **entsprechenden Schutzmaßnahmen (technisch und organisatorisch)** unter Berücksichtigung von:
  - Vorgaben für **IT-Systeme**, in denen Geschäftsgeheimnisse (geschützte Informationen) verarbeitet werden;
  - Fristen zur **Kontrolle der Klassifizierung** (Schutzbedarfe können sich ändern);
  - **Kennzeichnung** der Informationen gemäß dem jeweiligen Schutzbedarf;
  - **Vervielfältigung** von geschützten Informationen;
  - **Aufbewahrung und Vernichtung** geschützter Informationen (Papier, elektronisch etc.);
  - **Weitergabe** geschützter Informationen, insb. an Stellen im Ausland;
  - **Mitnahme** geschützter Informationen (Homeoffice, Auslandsreisen etc.);

Geheimnisschutz-Management (3/3)

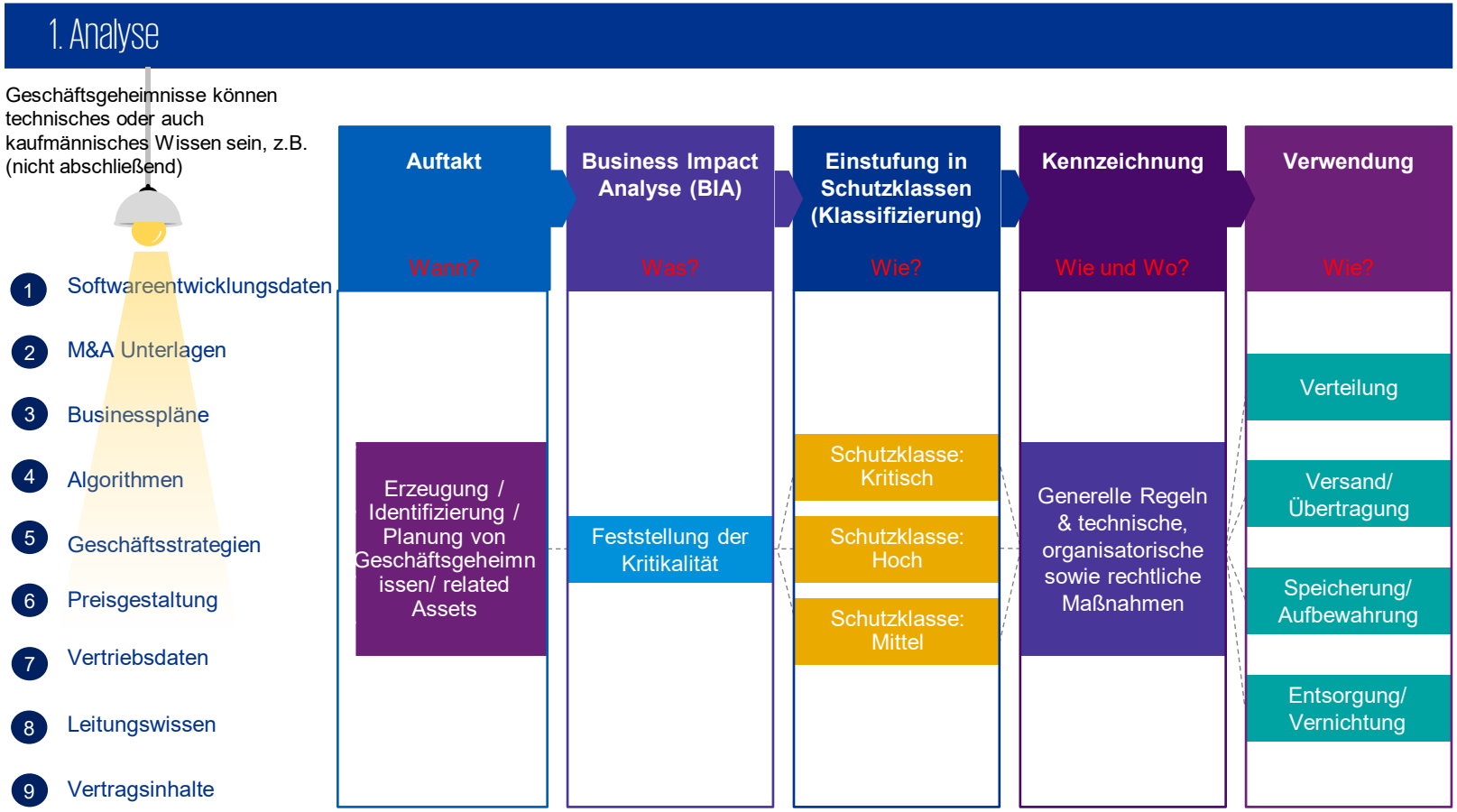
Technische, organisatorische und rechtliche Maßnahmen sind miteinander zu verzahnen

Zumindest folgende Aspekte sollten berücksichtigt und geregelt werden:

- Einbindung des IT-Sicherheits-Managements (ISMS);
- ggf. die Bestellung eines Geheimnisschutzbeauftragten und Festlegung seiner Aufgaben und
- Erstellung einer Geheimnisschutzdokumentation mit den wesentlichen Inhalten.

3. Klassifizierung/ Schutzstufenmodell

Vorgehensweise - Analyse

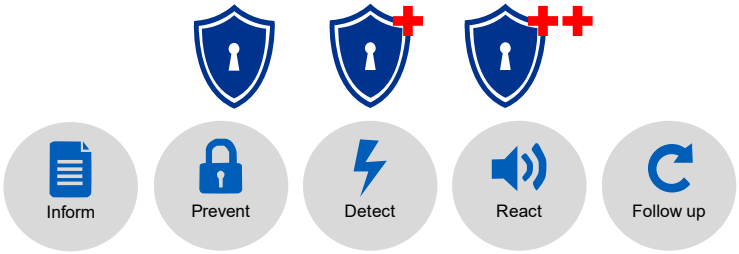


Vorgehensweise - Implementierung

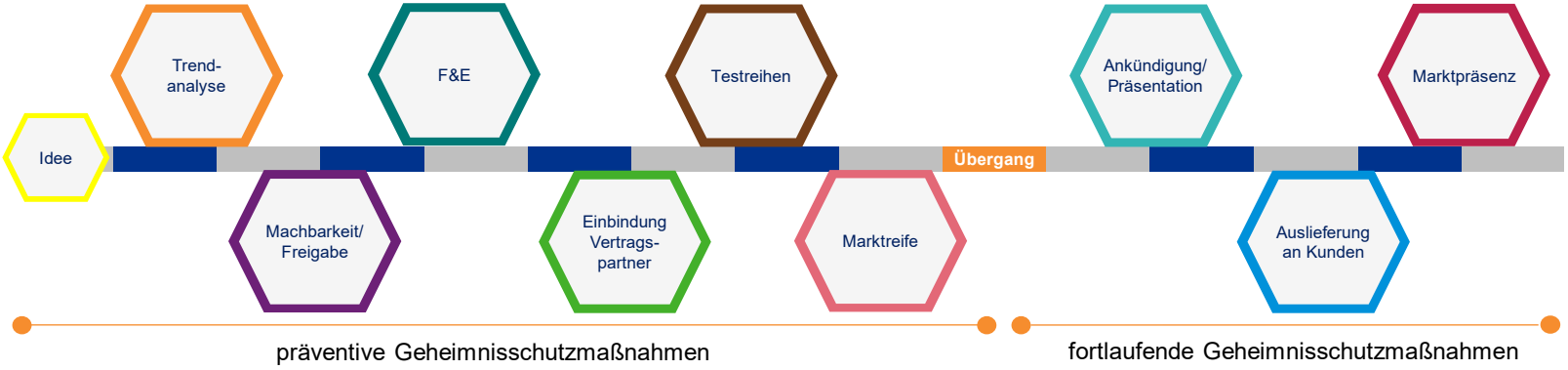
3. Implementierung entlang des Product-Lifecycle-Prozesses von der Idee bis zur Marktpräsenz

Maßnahmen zum Schutz von Geschäftsgeheimnissen ergreifen

- Implementierung adäquater technischer, organisatorischer und rechtlicher Maßnahmen
- Durchführung von Sensibilisierungsschulungen für alle Stakeholder, die am Product-Lifecycle beteiligt sind
- **Achtung:** Es dürfen keine Geschäftsgeheimnisse Dritter in diesen Prozess gelangen



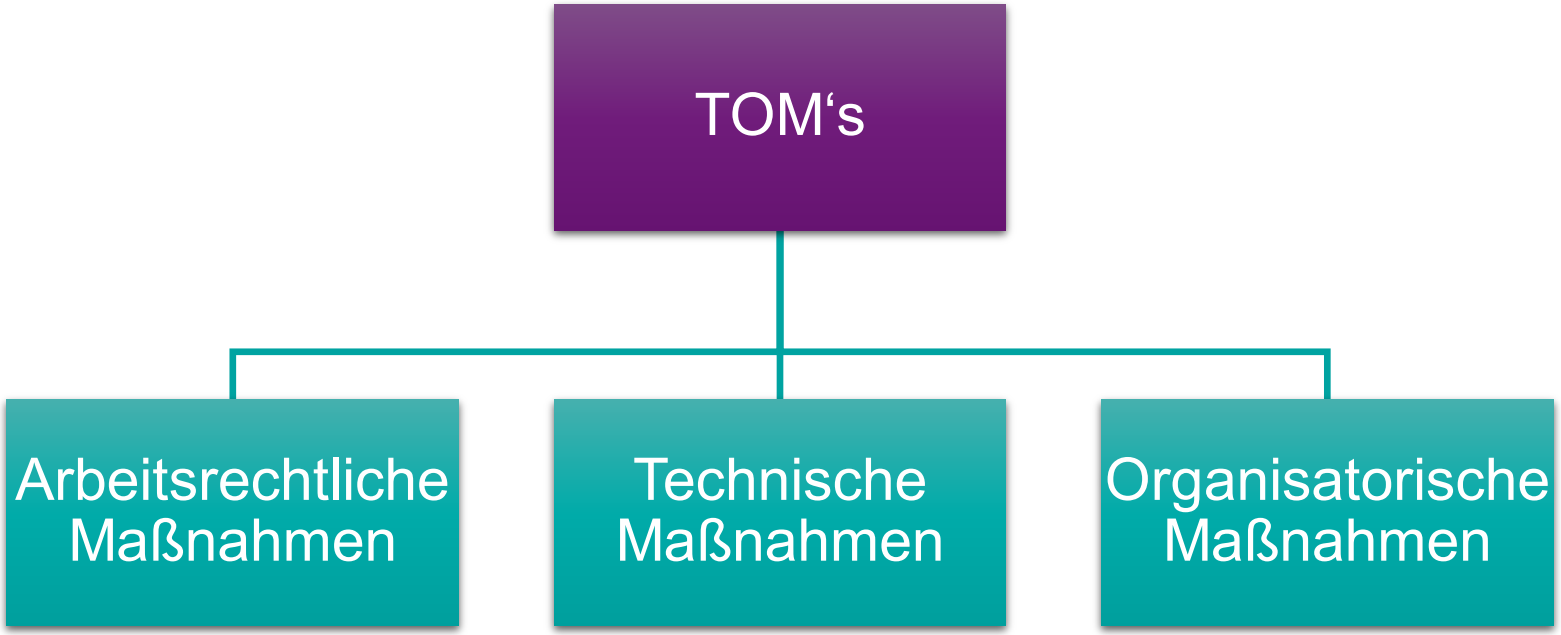
Die technischen, organisatorischen und rechtlichen Maßnahmen sind miteinander zu verzahnen.
Sie richten sich nach den in jedem Prozessschritt involvierten Personen und/oder Abteilungen im Product-Lifecycle-Prozess. Die Prozessbetrachtung ermöglicht eine risikoorientierte Implementierung der Schutzmaßnahmen.



KPMG

3. Risiken und Maßnahmen zur Umsetzung von TOMs

Überblick der erforderlichen Maßnahmen



Arbeitsrechtliche Maßnahmen

Mit Inkrafttreten des GeschGehG ist **§ 17 UWG** entfallen

Die Geheimhaltungspflicht ist eine arbeitsvertragliche Nebenpflicht. Mit dem Arbeitnehmer ist aus Gründen der Rechtssicherheit eine ausdrückliche vertragliche Regelung im Arbeitsvertrag zu vereinbaren.

- Die vertragliche Regelung zur Geheimhaltungspflicht sollte **möglichst hinreichend bestimmt** sein und zumindest die **Art der Information** benennen, über die Stillschweigen zu bewahren ist.
- Sog. **"Catch-All"-Klauseln**, nach denen sämtliche dem Arbeitnehmer bekanntgewordenen Informationen als Betriebs- und Geschäftsgeheimnisse gewertet werden, **sind unwirksam**.
- Es besteht ein **gesetzliches Wettbewerbsverbot**, wonach der Arbeitnehmer während des Arbeitsverhältnisses nicht mit dem Arbeitgeber in Wettbewerb treten darf (§ 60 HGB).
- In Schutzrechteklauseln wird die Pflicht des Arbeitnehmers zur Übertragung von Nutzungs- und Verwertungsrechten an Erfindungen auf den Arbeitgeber ausdrücklich festgelegt.
- Nachvertragliches Wettbewerbsverbot (§§ 74 ff. HGB) und Vereinbarung über die Zahlung einer Karenzentschädigung

➢ **Arbeitsverträge mit Mitarbeitern, die Zugang zu kritischen Geschäftsgeheimnissen haben sind an die Erfordernisse des GeschGehG anzupassen.**

Technische Maßnahmen

Sobald eine Information als Geheimnis eingestuft wird, reicht es nicht sie nur so zu bezeichnen, sondern sie muss tatsächlich als Geheimnis behandelt werden.

Auf kollektiver Ebene können Maßnahmen getroffen werden, um generell zu verhindern, dass Geschäftsgeheimnisse weitergegeben werden können. Hier sind beispielhaft aber nicht abschließend folgende Maßnahmen zu nennen:

- Einführung von Zugangsbeschränkungen (bspw. Ausweise) der Zugang zu bestimmten Unternehmensbereichen und damit zu bestimmten Informationen gezielt gesteuert werden. Je geringer der Personenkreis ist, der mit den Geschäftsgeheimnissen in Berührung kommt, desto geringer ist auch der Personenkreis, der diese unberechtigterweise weitergeben kann.
- Staffelung von Informationen nach bestimmten "Geheimhaltungsstufen" und eine entsprechende Eingruppierung der Arbeitnehmer, um das Weitergaberisiko zu begrenzen.
- Geschäftsgeheimnisse sollten nur von unternehmenseigenen Geräten und Medien einsehbar sein (Ausschluss von Bring Your Own Device).
- Kontrolle/Beschränkung der Druck- und Kopierfunktion für bestimmte Dokumente erfolgen. Hilfreich ist insofern die Verwendung eines Dokumenten-Management-Systems.

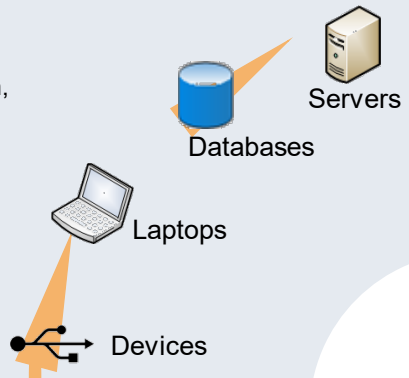
➢ **Es ist zu gewährleisten, dass technische Maßnahmen getroffen werden, die dem Stand der Technik entsprechen und einen Schutz der Informationen garantieren.**

Technische Maßnahmen - Beispiel

Technische Maßnahmen zum Schutz von Geschäftsgeheimnissen sind im Kontext einer DLP-Strategie abzuleiten. Dazu bietet sich folgendes Modell an:

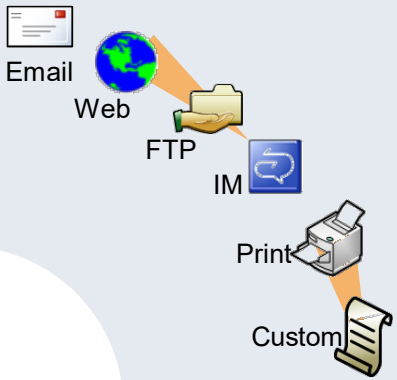
Data may originate from

- Sensitive information is typically distributed across the organization, and as such, may originate from multiple structured and unstructured information stores
- Depending upon an organization's access and data permission controls, both internal users and third-party may have access to sensitive information / data sets within the enterprise



What is the user doing with the data?

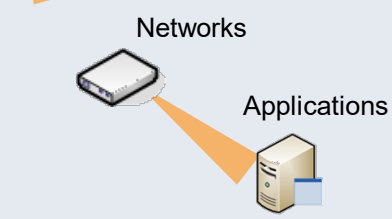
- A user may attempt to write, extract, print, move, burn, copy/paste, upload and/or attach sensitive information to various destination



Sensitive Information

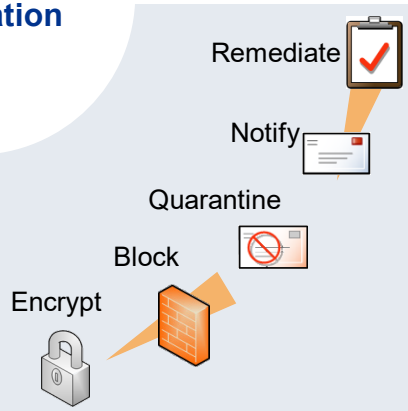
How is data being accessed and used?

- Leveraging DLP technology, data handling policies can be enforced and activity can be proactively monitored to prevent unauthorized data access at devices, within networks and applications.
- All sensitive information usage activities can be logged and tracked by DLP for auditing and forensic purposes



Policy and actions

- Based upon customized business rules and policies that are enforced on the network and endpoints using DLP, actions can be pre-defined to monitor, track, or block access to sensitive data.
- DLP controls can be both preventative or reactive and they can be configured in multiple variations depending on the available solution features



Kundenbeispiel - Risiken

External Threat Actors		Internal Threat Actors	
Hackers	Disgruntled Contractors	Employee Resistance to Change	Careless Insider
Contractor with Intellectual Property (i.e. developer)	General Public (i.e. PA citizen)	Compliancy Failure	Disgruntled Insider
Organized Crimes/Syndicates		Illegal Use of Corporate Assets	

- High Threat Risk
- High – Medium Threat Risk
- Medium Threat Risk

Kundenbeispiel - Risiken

High Risk
High-Medium Risk
Medium Risk

Data Loss Threat Vectors	Hacker	Employee Resistance to Change	Disgruntled Insider	Disgruntled Contractor	Contractor with I.P.	Compliancy Failure	Careless Insider	Illegal Use of Corporate Assets	Organized Crime / Syndicates	General Public (i.e., PA Citizen)
	Threat Actors									
Non-Company Devices	X	X	X	X	X	X	X		X	
Web Traffic	X	X	X	X	X	X	X	X	X	X
Webmail	X	X	X	X	X	X	X	X	X	
Company Devices	X	X	X	X	X	X	X	X	X	
Outbound Email	X	X	X	X	X	X	X	X	X	X
Internal Email		X	X	X		X	X	X		
Data Replication		X	X	X	X	X	X	X		
User Download			X	X	X	X	X	X		
Network Storage		X	X	X	X	X	X	X		X
Peer-to-Peer		X	X	X		X	X	X		

Beispiele - Maßnahmen

Data Origination	Unauthorized Upload Attempt
User Action(s)	User attempts to send sensitive information in an email from a personal web mail account, upload the information to an external web site or cloud service (e.g. forums, blogs, wikis, Dropbox, Google Drive, etc.), or extradite the information through alternative channels (e.g. FTP, VPN connection to office computer, peer-to-peer file sharing, etc).
DLP Response	DLP monitors and analyzes network egress points based on policies for predefined data elements and [Client] document tags. [Client] document tagging and user-defined fingerprinting allow DLP to monitor and/or prohibit the movement of sensitive information based on policies.
Available Action(s)	Monitor, record/block, and notify
Result	Sensitive information is tracked, and the transmission is prevented. User, manager, security, and/or HR notified of policy violation.

Data Origination	Inappropriate Internal Sensitive Information Transfer
User Action(s)	User attempts to communicate or transfer sensitive information to an unauthorized internal user through means other than email (e.g. FTP/peer-to-peer transfer, IM communication, VPN, etc).
DLP Response	DLP monitors workstation and mobile device activity for the use and/or transfer of sensitive information based on policies for predefined data elements and [Client] document tags. [Client] document tagging and user-defined fingerprinting allow DLP to monitor and/or prohibit the movement of sensitive information based on policies.
Available Action(s)	Monitor, record/block, and notify
Result	Sensitive information is tracked, and the transmission or communication is prevented. User, manager, security, and/or HR notified of policy violation.

Organisatorische Maßnahmen

Informationen sind als Geheimnis einzustufen, damit sie tatsächlich als Geheimnis behandelt werden können.

Es sind organisatorische Maßnahmen zu treffen, die Geschäftsgeheimnisse identifizieren, Kennzeichnen und den Umgang mit solchen genau beschreiben. Hier sind beispielhaft aber nicht abschließend einige Maßnahmen genannt:

- Erstellung einer Trade-Secret-Policy;
- Einstufung der Geschäftsgeheimnisse, abgestuft nach ihrer Bedeutung für das Unternehmen;
- Kennzeichnung der Geschäftsgeheimnisse;
- Regelung von Verantwortlichkeiten und Zugriffsrechten;
- Limitierung und Protokollierung des tatsächlichen Zugriffs (Need-to-know-Prinzip, die Protokollierung kann zudem zur schnelleren persönlichen Zuordnung bei unberechtigtem Datenabfluss beitragen);
- Schulung der Mitarbeiter über den Umgang mit Geschäftsgeheimnissen und über die Folgen bei Verstößen;
- Abschluss von Geheimhaltungsvereinbarungen mit Dienstleistern;
- Implementierung eines Change Management Prozesses.

➢ **Es ist zu gewährleisten, dass organisatorische Maßnahmen getroffen werden, die dem Umgang mit Geschäftsgeheimnissen als solche entsprechen und einen Schutz der Informationen garantieren.**

4. Umsetzungsplan

Vorgehensweise - Überblick

Analyse 1

- Identifikation von Geschäftsgeheimnissen
- Analyse des **Geschäftsumfeldes des Unternehmens**
- Analyse bestehender **Organisationsstrukturen** und Dokumentation zum Umgang mit Geschäftsgeheimnissen:
  - Verträge mit Geschäftspartnern
  - Arbeitsverträge
  - bestehende technische, organisatorische Maßnahmen
- Identifikation **risikobehafteter Abteilungen und Prozesse**
- Erarbeitung einer **Gap-Analyse** und Darstellung von Handlungsfeldern

Konzeptionierung 2

- Klassifizierung unternehmenskritischer Informationen und Festlegung von **Schutzzielen**
- **Rechtliche Bewertung** der Angemessenheit der getroffenen Schutzmaß-nahmen aufgrund der gesetzlich verankerten Beweislastumkehr
- Definition von **Verantwortlich-keiten** und Aufgaben
- Erstellung neuer/ Überarbeitung bestehender **Richtlinien, Vorgaben und Verträge**
- Konzeptionierung von **Prozessen und technischer, organisatorischer und rechtlicher Maßnahmen**

Implementierung 3

- Erstellung und Durchführung von **Schulungen**:
  - Sensibilisierungsschulungen für alle Mitarbeiter
  - fachliche Schulungen für relevante Mitarbeiter zur Umsetzung der Data Governance (bspw. HR, Forschung und Entwicklung)
- Unterstützung bei der **Implementierung** der erstellten Prozesse und technischer, organisatorischer und rechtlicher Maßnahmen

Prüfung 4

- **Readiness Check** vor der eigentlichen Prüfung
- **Prüfung** von umgesetzten Maßnahmen auf ihre Konzeption, Angemessenheit und Wirksamkeit
- Laufende **Überwachung** der Wirksamkeit

Umgang mit Vorfällen und Rechtsschutz

- Prüfung und Geltendmachung von Ansprüchen gegen Rechtsverletzer aus unerlaubten Handlungen zum Schutz eigener Geschäftsgeheimnisse.
- Aufarbeitung **wirtschaftskrimineller Vorfälle** mit Zielsetzung der Optimierung von Prozessen und Kontrollsystemen.
- Analyse von **Design und Funktionsfähigkeit** bei Prozessabläufen sowie interner Kontrollen im Hinblick auf wirtschaftskriminelle Handlungen.

Ihr Ansprechpartner

Prof. Dr. Dirk Loomans
Partner, Cyber Security
T +49 6131 370-248
dloomans@kpmg.com

KPMG AG
Wirtschaftsprüfungsgesellschaft
Erthalstraße 1
55118 Mainz

www.kpmg.de/socialmedia

www.kpmg.de