TaylorWessing

HISCOX BUSINESS ACADEMY

# DSGVO-CHECKLISTE

Seit Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO). Sie soll ein (weitestgehend) einheitliches Datenschutzniveau in allen EU-Mitgliedsstaaten herstellen und ist für alle Unternehmen in Deutschland neben lokalen Datenschutzvorschriften wie dem Bundesdatenschutzgesetz (BDSG) unmittelbar geltendes Recht. Dieses Dokument soll einen Überblick darüber geben, welche Maßnahmen Unternehmen umsetzen sollten, die sich bislang noch nicht oder nur teilweise mit der DSGVO befasst haben. Dabei ist wichtig zu verstehen, dass die DSGVO grundsätzlich auf alle Unternehmen unabhängig von Branche oder Unternehmensgröße Anwendung findet, sobald personenbezogene Daten verarbeitet werden – sei es von Kunden, Geschäftspartnern oder Mitarbeitern, im B2C- wie im B2B-Sektor. Je nach z. B. Größe des Unternehmens sowie Branchenzugehörigkeit und Sensitivität der in Rede stehenden Datenverarbeitungsprozesse sind bei der Umsetzung der Vorgaben der DSGVO andere Schwerpunkte und Prioritäten zu setzen, wofür die folgende Übersicht eine gewisse Hilfestellung bieten soll.

Diese Checkliste wurde exklusiv für die Hiscox Business Academy gemeinsam mit Taylor Wessing Partnerschaftsgesellschaft erarbeitet. Bei den nachfolgenden Ausführungen handelt es sich um unverbindliche Hinweise, die insbesondere keine Rechtsberatung darstellen und diese nicht ersetzen sollen und können. Sollten Sie weitere Fragen haben und hierzu eine Beratung wünschen, sprechen Sie uns und das Team von Taylor Wessing gerne an.

TaylorWessing

HISCOX BUSINESS ACADEMY

## DIESE FRAGEN WERDEN IM FOLGENDEN BEANTWORTET

### 1. DSGVO – Habe ich an alles gedacht?

Ungeachtet der Branche gilt es für alle Unternehmen, einen „DSGVO-Basisschutz“ zu implementieren. Anhand einer übersichtlichen Checkliste können Sie prüfen, ob Ihr Unternehmen die wesentlichsten Maßnahmen bereits implementiert hat.

### 2. Cyber-Attacken – Welche DSGVO-Anforderungen sollten Unternehmen in jedem Fall umsetzen?

In diesem Abschnitt erhalten Sie detailliertere Informationen zu den einzelnen Maßnahmen der DSGVO-Checkliste mit hilfreichen Verweisen auf weiterführende Informationen.

### 3. Cyber-Attacken – Was tun, wenn’s brennt?

Auch die beste Vorbereitung kann keinen hundertprozentigen Schutz vor Cyber-Attacken bieten. Wie Sie im Ernstfall richtig reagieren, erfahren Sie in dieser Anleitung.

## WAS SIE BEACHTEN MÜSSEN

Um Ihnen die Einschätzung Ihrer „DSGVO-Fitness“ zu erleichtern, haben wir Ihnen eine übersichtliche Checkliste besonders wichtiger Umsetzungsmaßnahmen zusammengestellt. Die Darstellung der Maßnahmen erfolgt in drei Schritten („Arbeitspaketen“). Mit der Einordnung soll keine „Wertung“ der einzelnen Maßnahmen im Hinblick auf ihre Relevanz unter der DSGVO vorgenommen werden. Alle datenschutzrechtlichen Pflichten sind wichtig und umzusetzen – ohne Wenn und Aber. Die Beratungspraxis zeigt jedoch, dass sich das Fehlen bestimmter Maßnahmen im Fall eines Cyberangriffs als besonders „schwierig“ herausstellt. Die nachfolgende Darstellung orientiert sich an diesen Erfahrungen und legt den Fokus darauf, welche Umsetzungsmaßnahmen von Aufsichtsbehörden, Kunden und Betroffenen z. B. im Zusammenhang mit der Meldung eines Datenschutzvorfalls vordringlich abgefragt bzw. beanstandet werden (könnten) und wo Fehler in der Umsetzung besonders visibel sind. Dies entbindet – wie gesagt – nicht von der (zeitgleichen) Umsetzung aller Maßnahmen, kann aber dort helfen, wo die Zeit knapp wird! Die nachfolgend beschriebenen Maßnahmen sind insoweit im Sinne eines „Erste-Hilfe-Kastens“ zu verstehen und erheben nicht den Anspruch, dass hiermit eine systematische und vollständige Umsetzung aller datenschutzrechtlichen Anforderungen in kurzer Zeit gewährleistet werden kann.

Maßnahmen im „Arbeitspaket 1“ beschreiben Maßnahmen, die besonders „visibel“ sind und deren Fehlen im Fall eines Datenschutzvorfalls besonders ins Auge fällt. „Arbeitspaket 2“ beschreibt Maßnahmen, die unerlässlich sind, um die Rechenschaftspflichten nach der DSGVO zu erfüllen. Maßnahmen des „Arbeitspakets 3“ zielen darauf ab, das Datenschutzmanagement auszudifferenzieren und geeignete zukunftsfähige Prozesse zu implementieren.

Je nach Unternehmenskultur, Kritikalität der Datenverarbeitungsprozesse, Branche oder Stand der Umsetzung können ein anderes Vorgehen oder die Umsetzung deutlich umfangreicherer Maßnahmen geboten sein. In jedem Fall empfiehlt sich, möglichst früh Ihren Datenschutzbeauftragten in die Umsetzung einzubinden.

Bei der Prüfung und Umsetzung der nachfolgend beschriebenen Maßnahmen sollte in keinem Fall auf entsprechende rechtliche Beratung verzichtet werden. Zur Umsetzung der geltenden Anforderungen sollten betroffene Unternehmen auf datenschutzrechtliche Fragestellungen spezialisierte Rechtsberatung in Anspruch nehmen, um – nicht zuletzt aufgrund der hohen Komplexität der einschlägigen Fragestellungen – Fehler bei der Umsetzung zu vermeiden, die zu Gesetzesverstößen und Sanktionen führen können.

TaylorWessing

HISCOX BUSINESS ACADEMY

# 1. DSGVO – HABE ICH AN ALLES GEDACHT?

## Arbeitspaket 1: Die „datenschutzrechtliche Visitenkarte“

### Basis-Dokumentation IT-Sicherheit

- ☐ Erstellung eines Datensicherheitskonzepts inkl. Berechtigungskonzepten für wesentliche Systeme einschließlich Dokumentation entsprechender Handlungsanweisungen zur Datensicherheit wie Passwortrichtlinien, Zutrittssicherheit in Gebäuden etc.

### Maßnahmen mit Außenwirkung

- ☐ Benennung eines Datenschutzbeauftragten und Mitteilung seiner Kontaktdaten an die zuständige Behörde
- ☐ Erstellung Datenschutzhinweise für (i) die Website des Unternehmens, (ii) für unternehmenseigene Apps/Software sowie (iii) für Mitarbeiter und Bewerber
- ☐ Korrekte Implementierung von Analyse- und Werbetools auf den Webseiten und in den Diensten des Unternehmens
- ☐ Umsetzung erforderlicher Maßnahmen zur Cookie-Compliance und Nutzung von Webseiten-Daten (z. B. durch sog. Cookie-Consent)
- ☐ Verschlüsselung von Online-Formularen und Kommunikation über die Website

### Basis-Verantwortlichkeiten & Sensibilisierung von Mitarbeitern

- ☐ Bestimmung eines Verantwortlichen bzw. Ansprechpartners für Datenschutzanfragen und Kommunikation im Unternehmen
- ☐ Erstellung eines Konzepts für den Umgang mit Datenschutzanfragen
- ☐ Verpflichtung der Mitarbeiter zur Vertraulichkeit und Dokumentation
- ☐ Schulung der Mitarbeiter zu IT-Sicherheit (z. B. unter Einsatz eines externen Dienstleisters/Programms)

## Arbeitspaket 2: Rechenschaftspflicht

### Dokumentation der Umsetzung des Datenschutzes

- ☐ Ermittlung und Dokumentation aller relevanten Verarbeitungen und Erstellen und Führen eines Verfahrensverzeichnisses (als Verantwortlicher od. Auftragsverarbeiter)
- ☐ Erstellen erforderlicher Datenschutzfolgenabschätzung(en)
- ☐ Erstellung eines Löschkonzepts und Löschen nicht mehr benötigter Daten
- ☐ Dokumentation konkreter Prozesse zum Umgang mit Betroffenenrechten (u. a. durch Definition von Standardprozessen und Verantwortlichkeiten), Umgang mit Datenschutzverletzungen (u. a. durch Beschreibung von Prozessabläufen) und zu „Privacy by Design“ (z. B. durch Entwicklung einer Richtlinie zum Datenschutz durch Technikgestaltung)

### Verträge mit Dienstleistern und Kooperationspartnern

- ☐ Abschluss notwendiger Vereinbarungen zur Auftragsverarbeitung mit Dienstleistern, wenn Dienste Dritter genutzt werden
- ☐ Für Dienstleister: Abschluss notwendiger Vereinbarungen zur Auftragsverarbeitung mit Kunden
- ☐ Abschluss erforderlicher Datenschutzverträge innerhalb der Unternehmensgruppe (u. a. gemäß Art. 26 DSGVO zur gemeinsamen Verantwortlichkeit)

## Arbeitspaket 3: Aufbau eines Datenschutzmanagementsystems und Maintenance

### Verfeinerung von Prozessen und Erstellung interner Regelungen

- ☐ Aufbau eines integrierten Datenschutzmanagementsystems, das mit anderen Prozessen (Compliance-Management, Incident-Management) eng verknüpft ist
- ☐ Erstellung eines „Incident Response Plan“ und Simulation des Ernstfalls

### Keeping up to date

- ☐ Etablierung von Prozessen für die regelmäßige Prüfung und Qualitätssicherung des Datenschutzmanagementsystems und Fortentwicklung auf Basis rechtlicher Neuerung (Rechtsfeldbeobachtung)

# 2. CYBERATTACKEN – WELCHE DSGVO-ANFORDERUNGEN SOLLTEN UNTERNEHMEN IN JEDEM FALL UMSETZEN?

## Cyberattacken: die „richtige“ rechtliche Vorbereitung

Cyberattacken können nicht nur einen erheblichen finanziellen Schaden und den gefürchteten Damage to Goodwill (Schaden am Firmenwert) anrichten. Je nach Hergang offenbaren sie unter Umständen auch Schwachstellen im Schutz der IT-Infrastruktur der betroffenen Unternehmen sowie Versäumnisse beim Aufbau einer funktionierenden Datenschutzorganisation im Einklang mit den Vorgaben der DSGVO, was nicht selten zu aufsichtsbehördlichen Verfahren und empfindlichen Bußgeldern führen kann.

Ein Datenschutzvorfall wie z. B. eine Hackerattacke, die den Behörden gemäß Art. 33 DSGVO zu melden ist, wird oftmals zum Ausgangspunkt entsprechender aufsichtsbehördlicher Ermittlungen, bei denen neben der Ermittlung des konkreten Vorfalls die behördlichen Maßnahmen schnell auch auf weitere (potenzielle) Verstöße des betroffenen Unternehmens ausgeweitet werden können.

## Nach welchen DSGVO-Anforderungen fragen Aufsichtsbehörden besonders?

Für viele Unternehmen ist die Meldung eines Datenschutzvorfalls gemäß Art. 33 DSGVO der erste Kontakt zu einer Datenschutzaufsichtsbehörde. In diesem Zusammenhang können Unternehmen viele Dinge in der Kommunikation mit der Aufsichtsbehörde „richtig“, aber ebenso viele auch „falsch“ machen. Wie man sich in einer solchen Situation verhält, welche Maßnahmen zu treffen sind und wie das richtige Verhalten gegenüber einer Aufsichtsbehörde im Fall eines Datenschutzvorfalls aussehen kann, wird nachfolgend in der Checkliste „Cyberattacken – Was tun, wenn’s brennt?“ weiter erläutert.

Zunächst sollte sich ein jedes Unternehmen jedoch mit den Maßnahmen und Vorgaben der DSGVO beschäftigen, die typischerweise durch jede Aufsichtsbehörde im Fall der ersten Kontaktaufnahme geprüft werden und so schon ohne großes Zutun der Behörde erste Sanktionen nach sich ziehen können. Diese Maßnahmen finden Sie zusammengefasst unter „Arbeitspaket 1“. Sie sollten mit einer gewissen Dringlichkeit bearbeitet und umgesetzt werden, da Fehler in diesem Bereich im Fall einer aufsichtsbehördlichen Prüfung besonders schnell offenkundig werden („low hanging fruits“).

**Die unter „Arbeitspaket“ beschriebenen Maßnahmen sind als absolute Minimalanforderungen zu betrachten, die jedes Unternehmen – unabhängig von Größe, Branche oder Sensitivität der jeweiligen Datenverarbeitungsprozesse – umsetzen muss. Ausnahmen hierzu sind in der DSGVO oder dem BDSG nicht bzw. nur in absoluten Ausnahmefällen vorgesehen.**

Gleiches gilt selbstverständlich auch für die in der Folge in den Arbeitspaketen 2 und 3 beschriebenen Maßnahmen; dies jedoch mit der Maßgabe, dass diese Maßnahmen in Fällen, in denen im Unternehmen bislang keine bzw. nur rudimentäre Anstrengungen zur Umsetzung der DSGVO unternommen wurden und es „schnell“ gehen muss, soweit nicht anders möglich nach den Maßnahmen des Arbeitspakets 1 betrachtet werden.

# DIE MASSNAHMEN IM EINZELNEN

**Bitte beachten Sie:** Bei diesen Maßnahmen handelt es sich um absolute Minimal-Standards, die jedes Unternehmen umsetzen muss. Die Umsetzung entsprechender Maßnahmen entbindet nicht von der Implementierung eines effizienten Datenschutzmanagementsystems, das in der Regel deutlich weitergehende Prozesse und Dokumentationen erfordert (vgl. hierzu Arbeitspaket 3).

Hilfreich können verschiedene Handreichungen und Muster der deutschen und/oder europäischen Datenschutzaufsichtsbehörden und Gremien sein. Verschiedene Hilfestellungen, Anleitungen und Stellungnahmen in z. B. deutscher Sprache finden sich unter anderem auf den Websites des Bayerischen Landesamtes für Datenschutz und Informationsfreiheit unter www.lda.bayern.de/de/index.html unter „Veröffentlichungen“.

## Arbeitspaket 1: Die „datenschutzrechtliche Visitenkarte“

### 1. Basis-Dokumentation IT-Sicherheit

Erstellung eines Datensicherheitskonzepts inkl. Berechtigungskonzepten für wesentliche Systeme einschließlich Dokumentation entsprechender Handlungsanweisungen zur Datensicherheit wie Passwortrichtlinien, Zutrittssicherheit in Gebäuden etc.:

Art. 25, 32 DSGVO verpflichten zur Umsetzung ausreichender technisch-organisatorischer Maßnahmen (TOM) im Hinblick auf die Datensicherheit. Die getroffenen Maßnahmen sind zu dokumentieren. Zudem ist ein Prozess zu entwickeln und zu dokumentieren, mit dem die Wirksamkeit der getroffenen Maßnahmen regelmäßig überprüft und soweit erforderlich angepasst werden kann. Die Erstellung des Datensicherheitskonzepts erfolgt grundsätzlich in enger Zusammenarbeit mit der IT-Abteilung des Unternehmens sowie je nach Kritikalität und Bedarf mit externer Expertise. Diese Maßnahmen nehmen oftmals einen längeren Zeitraum in Anspruch. In der Zwischenzeit bietet es sich insoweit an, zunächst eine Basisdokumentation für technisch-organisatorische Maßnahmen (z. B. eine erste kürzere TOM-Liste) mit einem in der Regel niedrigeren Detailgrad zu schaffen, die unter anderem für den Abschluss von Verträgen zur Auftragsverarbeitung genutzt werden können.

In diesem Zuge müssen u. a. für die zentralen Datenverarbeitungssysteme im Unternehmen ausreichend detaillierte Berechtigungskonzepte erstellt werden, mit denen der Zugriff durch Mitarbeiter bzw. externe Dienstleister geregelt und dokumentiert wird. Dokumentationen entsprechender Handlungsanweisungen zur Datensicherheit wie Passwortrichtlinien, Zutrittssicherheit in Gebäuden etc. sind wesentlicher Bestandteil des Konzepts. Umzusetzen ist der „Stand der Technik“. Was das im Einzelfall bedeutet, wird in der DSGVO nicht definiert. Hilfestellung hierfür bilden Handreichungen von Verbänden wie dem Teletrust (vgl. https://www.teletrust.de/publikationen/broschueren/stand-der-technik/) oder der ENISA (vgl. https://www.enisa.europa.eu/securesme/downloads).

### 2. Maßnahmen mit Außenwirkung

Benennung eines Datenschutzbeauftragten und Mitteilung seiner Kontaktdaten an die zuständige Behörde: Gemäß Art. 37 DSGVO bzw. den korrespondierenden Regelungen im BDSG haben Unternehmen ab einer gewissen Größe (regelmäßig dann, wenn dauerhaft 20 Personen oder mehr mit der Verarbeitung personenbezogener Daten betraut sind) einen Datenschutzbeauftragten zu bestellen. Hierbei kann es sich um einen internen wie einen externen Datenschutzbeauftragten handeln. Für Unternehmen einer Unternehmensgruppe bietet sich zudem die Möglichkeit der Bestellung eines gemeinsamen Datenschutzbeauftragten für mehrere Gruppenunternehmen an. Der Datenschutzbeauftragte hat eine ausreichende Fachkunde und Zuverlässigkeit aufzuweisen und muss sein Amt frei von Weisungen und sonstigen Interessenkonflikten im Unternehmen ausüben können. Somit scheiden einzelne Funktionsträger wie z. B. Mitarbeiter mit Geschäftsführungs- oder Management-Verantwortung, Controlling-Verantwortung sowie Personen in anderen leitenden Positionen (z. B. der Leiter der Rechtsabteilung oder der IT-Abteilung) regelmäßig als Datenschutzbeauftragte aus. Der Datenschutzbeauftragte ist der jeweils zuständigen Landesdatenschutzaufsichtsbehörde zu melden, wobei die Meldung unter Beachtung formaler Kriterien zu erfolgen hat. Nähere Informationen finden sich auf den Websites der Aufsichtsbehörden. Im Fall der Kontaktaufnahme mit einer Aufsichtsbehörde im Rahmen eines Cybervorfalls prüft diese oftmals das Register auf Einträge für einen Datenschutzbeauftragten. Nicht selten stellen Aufsichtsbehörden im Rahmen der Kommunikation entsprechende Nachfragen, die wahrheitsgemäß zu beantworten sind. Sollte sich in diesem Zuge herausstellen, dass ein Datenschutzbeauftragter nicht oder nicht richtig bestellt wurde, kann dies bereits zu einer ersten Beanstandung führen, die durch rechtzeitige Umsetzung der erforderlichen Maßnahmen vermieden werden kann.

**Erstellung Datenschutzhinweise für (i) die Website des Unternehmens, (ii) für unternehmenseigene Apps/Software sowie (iii) für Mitarbeiter und Bewerber:**
Die Datenschutzhinweise eines Unternehmens, sei es auf der unternehmenseigenen Website oder intern für die eigenen Mitarbeiter, ist so etwas wie die Datenschutz-Visitenkarte des Unternehmens nach außen. Im Fall aufsichtsbehördlicher Meldungen und Kommunikation geschieht es nicht selten, dass Aufsichtsbehörden zunächst das äußere Erscheinungsbild und die Darstellung des Unternehmens im Hinblick auf datenschutzrechtliche Anforderungen prüfen, um etwaige Schwachstellen auszumachen. Prüfungsgegenstand ist dabei gerne die Datenschutzerklärung auf der Website des Unternehmens, die sich leicht mit wenigen Klicks auffinden lässt. Aufgrund der umfassenden Vorgaben für die Informationspflichten gemäß Art. 13, 14 DSGVO fällt es Aufsichtsbehörden nicht schwer, etwaige erste Verstöße auszumachen und gegebenenfalls im Rahmen eines entsprechenden Verfahrens zu verwerten.

Unternehmen sind gut beraten, sich frühzeitig mit den geltenden gesetzlichen Anforderungen zu den Informationspflichten auseinanderzusetzen und alle in diesem Zusammenhang relevanten Außendarstellungen auf den aktuellen rechtlichen Stand zu bringen. Hierfür empfehlen sich ein Screening und – soweit erforderlich – eine Überarbeitung der jeweiligen Datenschutzhinweise

- für die Website des Unternehmens
- für unternehmenseigene Apps/Software
- für Mitarbeiter und Bewerber im Unternehmen (für Bewerber ggf. auch im Rahmen der Datenschutzhinweise auf der Website des Unternehmens)

**Korrekte Implementierung von Analyse- und Werbetools auf den Webseiten und in den Diensten des Unternehmens sowie Umsetzung erforderlicher Maßnahmen zur Cookie-Compliance und Nutzung von Webseiten-Daten (z. B. durch sog. Cookie-Consent):**
Von wachsender Bedeutung ist die Frage der korrekten Einbindung einzelner Werbe- und Analysetools auf der Website und in anderen digitalen Diensten des Unternehmens, z. B. durch Einsatz sog. Cookies, Social-Media Plug-ins und der entsprechenden Ausgestaltung der Prozesse (z. B. durch Nutzung einer sog. Cookie-Wall, Einholung von Einwilligungen für einschlägige Dienste und entsprechende Hinweise auf der Website). Da die jeweiligen Fragen eine hohe technische wie rechtliche Komplexität aufweisen und die Diskussion hierzu noch im Gange ist, soll an dieser Stelle auf eine vertiefte Darstellung verzichtet werden. Die Entwicklungen sind jedoch genauestens zu beobachten und entsprechende Vorgaben der Behörden mit Priorität umzusetzen.

**Verschlüsselung von Online-Formularen und Kommunikation über die Website:**
Ein weiterer Aspekt, der von Aufsichtsbehörden im Rahmen von Behördenkommunikation häufig geprüft wird, sind technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO. „Dauerbrenner" in diesem Zusammenhang sind ausreichende Verschlüsselungstechnologien bei der Kommunikation mit dem betroffenen Unternehmen z. B. über ein Formular auf der Website oder der ausreichend „starke" Passwortschutz für das Log-in bei Onlinediensten oder Mobile Apps (ggf. auch unter Verwendung einer Mehr-Faktor-Authentifizierung für besonders schutzwürdige Dienste, erweiterte Schutzmaßnahmen gegen sog. Brute-Force-Angriffe etc.).
Die korrekte Umsetzung entsprechender Maßnahmen lässt sich durch Aufsichtsbehörden regelmäßig besonders leicht prüfen und kann insoweit als die sprichwörtlich „low hanging fruit" bezeichnet werden.

## 3. Basis-Verantwortlichkeiten & Sensibilisierung von Mitarbeitern

Bestimmung eines Verantwortlichen bzw. Ansprechpartners für Datenschutzanfragen und Kommunikation im Unternehmen:
Datenschutz ist Aufgabe der Geschäftsleitung. Der Datenschutzbeauftragte soll beraten und kontrollieren. Die komplette Verantwortlichkeit auf den Datenschutzbeauftragten „abzuschieben", ist spätestens seit der DSGVO keine Option mehr. In einem ersten Schritt gilt es, neben der Bestellung eines Datenschutzbeauftragten und dessen Meldung bei der Aufsichtsbehörde die wesentlichen Verantwortlichkeiten und Basisprozesse zur Umsetzung des Datenschutzes festzulegen.

Die Praxis zeigt: Fehler im Umgang mit datenschutzrechtlichen Anfragen geschehen oftmals dort, wo keine klaren Verantwortlichkeiten und Zuständigkeiten für die Entgegennahme und Bearbeitung datenschutzrechtlicher Fragestellungen bestehen. Unabhängig von der Implementierung eines effektiven Datenschutzmanagementsystems (vgl. hierzu nachfolgend „Arbeitspaket 3") müssen grundlegende Zuständigkeiten und Prozesse für den Umgang mit entsprechenden Themen im Unternehmen definiert werden.

Nur so kann sichergestellt werden, dass Anfragen Betroffener oder der jeweiligen Aufsichtsbehörde sach- und zeitgerecht bearbeitet und datenschutzrechtliche Sanktionen vermieden werden können. Folgende Maßnahmen sollten in diesem Zusammenhang getroffen werden:

- Bestimmung eines Verantwortlichen für datenschutzrechtliche Fragestellungen im Unternehmen neben dem Datenschutzbeauftragten
- Definition der Kommunikationswege zur Einbindung des Datenschutzbeauftragten bzw. der Geschäftsleitung (z. B. durch eine zentrale E-Mail-Adresse für Meldungen eines Vorgangs)
- Kenntnis und Dokumentation der zuständigen Aufsichtsbehörde
- Dokumentation der wesentlichen Prozesse im Rahmen des Umgangs mit Datenschutzanfragen durch die Verantwortlichen einschl. Eskalation an die Geschäftsleitung

**Verpflichtung der Mitarbeiter zur Vertraulichkeit und Schulung der Mitarbeiter**
Mitarbeiter sind gemäß Art. 29 DSGVO auf die Geheimhaltung und den datenschutzkonformen Umgang mit personenbezogenen Daten zu verpflichten. Diese Verpflichtung erfolgt typischerweise durch Unterzeichnung eines entsprechenden Dokuments, idealerweise bereits bei der Einstellung des Mitarbeiters. Sollten entsprechende Dokumentationen im Unternehmen bislang nicht existieren, sollten entsprechende Maßnahmen möglichst schnell umgesetzt werden, da Aufsichtsbehörden danach typischerweise fragen. Je nach Fallgestaltung sind entsprechende Verpflichtungen um weitere spezielle Aspekte zu ergänzen (u a. die Wahrung des Telekommunikationsgeheimnisses, wenn entsprechende Daten betroffen sind). Schulung der Mitarbeiter zu IT-Sicherheit (z. B. unter Einsatz eines externen Dienstleisters/Programms) ist das „A und O", um mögliche Cyberattacken verhindern zu können. Werden Mitarbeiter nicht ausreichend geschult und sensibilisiert, steigt zum einen die Gefahr für erfolgreiche Cyber-Attacken. Zum anderen verletzt das Unternehmen (bzw. die jeweilige Geschäftsleitung) seine Organisationspflichten, was im Ernstfall Anknüpfungspunkt für behördliche Ermittlungen und Sanktionen sowie Schadensersatzforderungen von Betroffenen und Geschäftspartnern werden kann. Also: schulen – schulen – schulen!

## Arbeitspaket 2: Rechenschaftspflicht

### 1. Dokumentation des Datenschutzes

**Ermittlung und Dokumentation aller relevanten Verarbeitungen und Führen eines Verfahrensverzeichnisses (als Verantwortlicher oder Auftragsverarbeiter):**
Nach dem Grundsatz der Rechenschaftspflicht (vgl. Art. 5 (2) DSGVO) müssen Unternehmen jederzeit die Umsetzung der Vorgaben der geltenden datenschutzrechtlichen Gesetze nachweisen können. Gemäß Art. 30 DSGVO ist ein Verzeichnis über die existierenden Verfahren zu führen. Dies gilt für Unternehmen in der Rolle als Verantwortliche wie Auftragsverarbeiter gleichermaßen. Behörden fragen im Nachgang entsprechender Meldungen vermehrt nach Auszügen aus dem Verfahrensverzeichnis, das im Fall der Fälle zur Verfügung stehen muss, um es zeitnah vorlegen zu können.

**Erstellung eines Löschkonzepts und Löschen nicht mehr benötigter Daten:**
Dies schließt ein Löschkonzept für alle Daten der im Verfahrensverzeichnis beschriebenen Prozesse ein. Dessen Dokumentation und Umsetzung ist insoweit kritisch, als die Speicherung „alter" Daten ggf. schon nicht mehr zulässig ist. Das kann im Fall eines Datenschutzvorfalls zu teils schwer auflösbaren Folgefragen führen (u. a. die Pflicht zur Information Betroffener für Daten, die bereits hätten gelöscht werden müssen).

**Erstellen erforderlicher Datenschutzfolgenabschätzung(en):**
Im Fall der Durchführung besonders sensitiver Datenverarbeitungshandlungen – insbesondere solcher mit Bezug zu besonderen Kategorien personenbezogener Daten gemäß Art. 9 DSGVO – erfordert die DSGVO gemäß Art. 35 DSGVO die Durchführung einer sogenannten Datenschutzfolgenabschätzung. Hierbei handelt es sich um eine Vorabprüfung einzelner Verarbeitungshandlungen, bei der es darum geht, besondere Risiken zu identifizieren und frühzeitig zum Wohle der Betroffenen zu minimieren.

Die in diesem Rahmen erfolgende Risikobetrachtung sowie die getroffenen Maßnahmen sind anhand spezifischer gesetzlicher Vorgaben zu dokumentieren. Die DSGVO bestimmt dabei gewisse Mindestanforderungen, wie eine solche Datenschutzfolgenabschätzung durchzuführen ist. Dazu gehört in der Regel eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, einschließlich des berechtigten Interesses des Verantwortlichen, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck sowie eine Bewertung der Risiken der Rechte und Freiheiten der betroffenen Personen. Schließlich muss eine Auswahl der zur Bewältigung der Risiken geplanten Abhilfemaßnahmen erfolgen, wobei den Rechten und berechtigten Interessen der Betroffenen Rechnung zu tragen ist. Zu den Abhilfemaßnahmen zählen Garantien, Sicherheitsvorkehrungen und Verfahren. Die Maßnahmen sind entsprechend zu erläutern und zu dokumentieren.

Da im Rahmen einer aufsichtsbehördlichen Prüfung Behörden gerne nach dem Vorliegen entsprechender Dokumentationen fragen und das Fehlen der Durchführung einer Datenschutzfolgenabschätzung einen Datenschutzverstoß darstellt, ist es ratsam, für die betroffenen Prozesse zeitnah entsprechende Betrachtungen durchzuführen und zu dokumentieren. Wie immer bei der Umsetzung der Vorgaben der DSGVO, sollte auch hier nach Kritikalität der jeweiligen Prozesse priorisiert werden, um zuerst solche Verfahren einer entsprechenden Betrachtung zu unterziehen, bei denen das Fehlen einer Datenschutzfolgenabschätzung zu einem höheren Beanstandungsrisiko führen würde als bei anderen, ggf. weniger kritischen Datenverarbeitungsprozessen.

**Dokumentation konkreter Prozesse zum Umgang mit Betroffenenrechten (u. a. durch Definition von Standardprozessen und Verantwortlichkeiten), zum Umgang mit Datenschutzverletzungen (u. a. durch Beschreibung von Prozessabläufen), zu „Privacy by Design" (z.B. durch Entwicklung einer Richtlinie zum Datenschutz durch Technikgestaltung) und Erstellung eines Konzepts im Umgang mit Datenschutzanfragen:**
Kern des Aufbaus eines Datenschutzmanagementsystems ist die Dokumentation konkreter Prozesse im Umgang mit datenschutzrelevanten Fragen. Diese dienen dem Nachweis, dass sich Unternehmen vorab Gedanken darüber gemacht haben, wie mit entsprechenden Fällen umzugehen ist. Das Fehlen entsprechender Festlegungen führt nicht nur zur Unsicherheit im Fall der Fälle. Das Fehlen kann an sich schon einen Organisationsmangel darstellen, der es dem Unternehmen erheblich erschwert, sich im Fall eines Vorfalls zu exkulpieren.

### 2. Verträge mit Dienstleistern, Kooperationspartnern und Gruppenunternehmen regeln

**Abschluss notwendiger Vereinbarungen zur Auftragsverarbeitung mit Dienstleistern, wenn Dienste Dritter genutzt werden:**
Im Verhältnis zu Dienstleistern und Kooperationspartnern, die im Rahmen ihrer Tätigkeit Zugriff auf personenbezogene Daten des Unternehmens erhalten, sind regelmäßig spezielle Regelungen zum Datenschutz zu treffen. Im Falle einer Auftragsverarbeitung gemäß Art. 28 DSGVO ist es gesetzlich vorgeschrieben, spezielle Standardverträge unter Beachtung gesetzlicher Mindestanforderungen abzuschließen. Im Falle eines sog. Joint Controllership (gemeinsame Verantwortlichkeit) schreibt Art. 26 DSGVO den Abschluss spezieller Verträge vor. Je nach Anzahl der eingesetzten Dienstleister und bestehenden Kooperationen kann dies für Unternehmen zu einem erheblichen

Aufwand führen und längere Zeit in Anspruch nehmen. Je nach Kritikalität der betroffenen Prozesse sollten Unternehmen deshalb umgehend die Zusammenarbeit mit externen Dienstleistern und anderen Partnern im Hinblick auf entsprechende Anforderungen analysieren und Maßnahmen einleiten, um möglichst schnell entsprechende Verträge „in place“ zu haben. Diese Anforderungen gelten für die gesamte Lieferkette, sodass darauf geachtet werden sollte, dass auch die jeweiligen Dienstleister notwendige Auftragsverarbeitungsverträge mit ihren Kunden abschließen.

### Arbeitspaket 3: Verfeinerung und Maintenance

**1. Umsetzung von Prozessen und Erstellung interner Richtlinien**

**Aufbau eines integrierten Datenschutzmanagementsystems, das mit anderen Prozessen (Compliance-Management, Incident-Management) eng verknüpft ist:**
Die DSGVO verpflichtet Unternehmen, ein System für das Management datenschutzrechtlicher Fragestellungen sowie die Implementierung der gesetzlichen Vorgaben im Unternehmen zu etablieren (sog. Datenschutzmanagementsystem, „DSMS“). Der Aufbau eines DSMS erfordert effiziente Planung, die möglichst lückenlose Definition entsprechender Prozesse und die Schaffung ausreichender Dokumentation zur Umsetzung aller datenschutzrechtlichen Anforderungen. Kernbestandteil eines solchen Systems sind regelmäßig eine Vielzahl verschiedener Guidelines und Policies, mit denen insbesondere die Mitarbeiter des Unternehmens bei der Umsetzung und Anwendung datenschutzrechtlicher Vorgaben unterstützt werden. Wesentlicher weiterer Bestandteil ist die Definition von Kernprozessen, insbesondere zur Meldung datenschutzrelevanter Vorgänge und Definition entsprechender Verantwortlichkeiten (u. a. bei Datenschutzvorfällen).

**Erstellung eines „Incident Response Plan“ und Simulation des Ernstfalls**
Ein Incident Response Plan hilft, den Überblick im Fall einer Cyber Attacke zu behalten. Er verknüpft verschiedene Themen- und Fachbereiche miteinander und stellt sicher, dass im Ernstfall an alles gedacht und alles in der richtigen Reihenfolge nacheinander abgearbeitet wird. Die implementierten Maßnahmen sollten regelmäßig durch die Simulation eines Cyberangriffs überprüft werden. Dabei sollten insbesondere die Reaktion, Verantwortlichkeiten und Abläufe getestet werden. Die simulierten Angriffe und die daraus resultierenden Ergebnisse sollten dokumentiert werden, damit bei Bedarf eine Anpassung bestehender Konzepte vorgenommen werden kann.

**2. Keeping up to date**

Die Etablierung von Prozessen für die regelmäßige Prüfung und Qualitätssicherung des Datenschutzmanagementsystems sowie die regelmäßige Fortentwicklung und Anpassung auf Basis rechtlicher Neuerungen der datenschutzrechtlichen Vorgaben (Rechtsfeldbeobachtung) sind erforderlich, um stets mit einem aktuellen System unterwegs zu sein, das alle Anforderungen erfüllt.

## 3. CYBER-ATTACKEN – WAS TUN, WENN’S BRENNT?

Wenn tatsächlich etwas passiert, kann die folgende Anleitung für den Ernstfall eine wertvolle Hilfe sein, um die wesentlichen „rechtlichen“ Themen ausreichend zu beachten und so die richtigen Maßnahmen einleiten zu können:

### SCHRITT 1: GEFAHR BESEITIGEN – KRISENPLAN ABARBEITEN

IT-Sicherheitsvorfälle sind Extremsituationen, die mitunter zu großer psychischer Belastung für die handelnden Personen führen können. Ein Krisenplan hilft! Diesen im Ernstfall abzuarbeiten, ist entscheidend, um keine wesentlichen Schritte zu übersehen, und bringt rechtliche Sicherheit.

Einen solchen Krisenplan erhalten alle Hiscox Kunden im Rahmen der Krisenprävention, die eine Cyberdeckung als eigenständigen Vertrag oder als Teil ihrer Haftpflichtpolice abgeschlossen haben. Aus Erfahrung sind die richtige Klassifizierung und dann unmittelbare Einbindung von IT- und Krisenexperten entscheidend. Bei der Hiscox Cyberversicherung geschieht dies exklusiv durch die Firma HiSolutions. So ist gewährleistet, dass bereits von Beginn an qualifizierte Expertise im Bereich IT-Sicherheit zur Verfügung steht und der drohende Schaden möglichst effektiv bekämpft wird. Erst in einem zweiten Schritt erfolgt typischerweise die Schadenmeldung an den Versicherer, der dann je nach Sachlage weitere Experten hinzuzieht.

## SCHRITT 2: VORFALL UND REAKTION AUSREICHEND DOKUMENTIEREN

Alle Erkenntnisse über die entdeckte oder vermutete Cyber-Attacke sind gründlich zu ermitteln und zu dokumentieren. Maßgebliche Fristen sind frühzeitig zu ermitteln und zu dokumentieren (z. B. die Meldefrist für Behördenmeldung von 72 Std. ab „Kenntnisnahme“). Beweismittel müssen rechtzeitig gesichert werden. Diese Maßnahmen sind unerlässlich, um im Fall der Fälle Behörden und Betroffene ausreichend informieren und im Nachgang die Vorgänge analysieren und Prozesse verbessern zu können.

Auch hierbei können spezialisierte Dienstleister wie die Firma HiSolutions oder Taylor Wessing im Schadenfall wertvolle Hilfestellung leisten.

## SCHRITT 3: MELDE-/INFORMATIONSPFLICHT PRÜFEN UND HANDELN, WENN ES ERFORDERLICH IST

Meldungen an Datenschutzaufsichtsbehörden haben innerhalb von 72 Stunden zu erfolgen, an Betroffene „unverzüglich“. Ob solche Meldungen erforderlich sind, bedarf oftmals einer intensiven rechtlichen Prüfung.

**1. Hinweise zur Meldung bei der zuständigen Datenschutzaufsichtsbehörde (Art. 33 DSGVO)**
Das Bestehen einer Meldepflicht hängt vom „Risiko“ für Betroffene ab; erforderlich ist daher die Durchführung einer Risikobewertung anhand der vorliegenden Erkenntnisse. Es gilt der Grundsatz: Je höher der anzunehmende Schaden, desto geringere Anforderungen sind an die Wahrscheinlichkeit des Schadenseintritts zu stellen. Im Rahmen der Risikobeurteilung ist die Schwere des drohenden Schadens mit der Eintrittswahrscheinlichkeit des Schadensereignisses abzuwägen. Nach Auffassung der Behörden kann auch ein sehr geringes Risiko eine Meldepflicht auslösen, ein Einzelfall auch dann, wenn z. B. nur B2B-Daten betroffen sind oder Daten „bloß“ verschlüsselt wurden. Auch der auf den ersten Blick „unverdächtige Postfehlversand“ kann zu einer Meldepflicht führen. Vor einer Meldung sollte die weitere Kommunikations- und Verteidigungsstrategie genau festgelegt werden. „Vorausschauend“ melden ist das Stichwort. Schon aus diesem Grund sollte einer Meldung immer eine zumindest kurze Prüfung der Datenschutz-Compliance des Unternehmens vorangehen, um auf Nachfragen vorbereitet zu sein.

Und: Es hat sich bewährt, stets kooperativ und konstruktiv mit Behörden zusammenzuarbeiten. Ungeachtet dessen ist bei der Beschreibung solcher Umstände Zurückhaltung geboten, die ein mögliches Fehlverhalten des Unternehmens indizieren können (z. B. nicht ausreichende TOMs). Schon aus diesem Grund ist anwaltliche Beratung beim Verfassen einer solchen Meldung ratsam.

**2. Hinweise zur Benachrichtigung Betroffener (Art. 34 DSGVO)**
Die Pflicht zur Benachrichtigung Betroffener besteht im Falle eines „hohen Risikos“, was wiederum die Durchführung einer Risikobewertung der vorliegenden Erkenntnisse anhand der zuvor dargestellten Grundsätze erfordert.

Auch Betroffene sollten „vorausschauend“ informiert werden, da jede Information zu kritischen Nachfragen, Auskunftsansprüchen, Löschbegehren oder sogar Schadensersatzansprüchen führen kann. Sollte eine Behördenmeldung erfolgt oder eine Strafanzeige gestellt worden sein (oder ist dies geplant), sollte hierauf hingewiesen werden, da dies Vertrauen schafft und Nachfragen vermeidet.
Insbesondere für die Benachrichtigung Betroffener sollte die Expertise von IT-Rechtsspezialisten eingeholt werden.

**Melde- und Informationspflichten in besonderen Konstellationen**
Besondere Herausforderungen bestehen bei Datenschutzvorfällen, von denen mehrere Unternehmen einer Unternehmensgruppe betroffen sind. Hier ist genau zu klären, wer wie an welche Behörde was genau zu melden hat. Rechtzeitige Kommunikation zwischen den Unternehmen und abgestimmtes Vorgehen sind wesentliche Bausteine für die erfolgreiche Bewältigung der Aufgaben.
Grenzüberschreitende Cyberattacken erfordern neben der Abstimmung mit den Betroffenen eine auf mehrere Jurisdiktionen ausgerichtete Rechtsberatung, die frühzeitig organisiert werden muss, um in allen Ländern bestehenden rechtlichen Pflichten nachkommen zu können.

Besondere Pflichten können zudem für Unternehmen bestimmter Branchen oder für kapitalmarktorientierte Unternehmen bestehen. So existieren entsprechende Meldepflichten u. a. für sog. KRITIS-Unternehmen an das Bundesamt für Sicherheit in der Informationstechnik (BSI). Dies gilt auch für bestimmte Anbieter digitaler Dienste sowie Unternehmen im besonderen öffentlichen Interesse. Für kapitalmarktorientierte Unternehmen kann sich die Pflicht zur Abgabe einer Ad-hoc-Meldung gemäß Art. 17 MAR ergeben. Schließlich können Meldepflichten aus Geheimschutz bestehen.

Für die Prüfung der jeweiligen Vorgaben ist frühzeitig spezialisierte rechtliche Expertise einzuholen.

TaylorWessing

HISCOX BUSINESS ACADEMY

## SCHRITT 4: STRAFVERFOLGUNGSBEHÖRDEN EINSCHALTEN

Die Strafverfolgungsbehörden sind rechtzeitig einzuschalten, um Ermittlungsmaßnahmen unterstützen zu können. Für Cyberattacken auf Unternehmen gibt es oftmals Spezialstellen, die kontaktiert werden sollten.

## SCHRITT 5: IN DER RUHE LIEGT DIE KRAFT – DATENSCHUTZ AUCH WÄHREND DES VORFALLS BEACHTEN

Auch wenn es heiß hergeht, sollte immer die Ruhe bewahrt werden. Unbedachte Maßnahmen können den Schaden im Fall einer Cyberattacke oftmals noch vergrößern. Profis können helfen, solche Fehler zu vermeiden.

## SCHRITT 6: AUFRÄUMEN UND DATENSCHUTZFEHLER BESEITIGEN

Nach dem Angriff ist vor dem Angriff! Ohne „Aufräumen“ geht es nicht, wenn man für den nächsten Angriff auch rechtlich gut vorbereitet sein will. Die im Rahmen des Datenschutzfalls festgestellten Mängel sind gründlich zu analysieren, Abhilfemaßnahmen sind umgehend zu ergreifen. Ergänzen Sie auch Ihren Incident Response Plan um die „learnings“ und „findings“ des Angriffs.

## IHR EXPERTENTEAM


**Thomas Kahl**
Fachanwalt für Informationstechnologierecht, Frankfurt

+49 69 97130-111
T.Kahl@taylorwessing.com

**Dajin Lie**
Rechtsanwältin, Frankfurt

+49 69 97130-136
D.Lie@taylorwessing.com


Taylor Wessing ist eine internationale Wirtschaftskanzlei und berät nationale wie internationale Unternehmen aller Branchen zu allen Fragen des Datenschutzrechts, bei Datenschutzvorfällen und im Rahmen aufsichtsbehördlicher Verfahren.
Die Datenschutzpraxis von Taylor Wessing wird regelmäßig als Tier 1 Law Firm für Datenschutz gerankt (u. a. in Legal 500 Germany, JUVE) und gehört zu den führenden Kanzleien in diesem Bereich in Deutschland.

**www.taylorwessing.com**

HISCOX BUSINESS ACADEMY

**Das vorliegende Whitepaper ist ein Service der Hiscox Business Academy.**

Als Hiscox Kunde haben Sie mit der Hiscox Business Academy Zugriff auf viele weitere starke Inhalte zum Support Ihres Business wie Checklisten, rechtssichere Vorlagen, E-Learning & mehr.

**Neugierig?** Jetzt mehr erfahren unter **hiscox.de/business-academy-entdecken**

Weitere Infos, News und Hintergründe zu digitalen Risiken, Cyber-Sicherheit u. v. m. für Unternehmen und Selbstständige finden Sie in den Hiscox Business Tipps & Insights unter **hiscox.de/blog**.


Hiscox
Arnulfstraße 31, D - 80636 München
www.hiscox.de