

Maßnahmen- und Kontrollbericht zu Risiko

mangelndes Bewusstsein bzgl.
Datenschutz

Das gegenständliche Dokument gilt als vertraulich und ist ausschließlich für den internen Gebrauch bestimmt. Es ist nicht gestattet, dieses Dokument oder Teile daraus in irgendeiner Form zum Gebrauch durch Dritte zu vervielfältigen und/oder ganz bzw. auszugsweise zu veröffentlichen.

Inhaltsverzeichnis

mangelndes Bewusstsein bzgl. Datenschutz(DSO_001)	1
Offene Maßnahmen	1
Vertraulichkeitsvereinbarungen mit Geschäftspartnern abschließen (M_DSMS_028)	1
Datenübermittlungen in Drittländer DSGVO-konform durchführen (M_DSMS_035)	1
Ausgesetzte Maßnahmen	1
Abgeschlossene Maßnahmen	2
Management Awareness und Commitment sicherstellen (M_DSMS_001)	2
Verantwortlichkeiten iZm Datenschutz festlegen (M_DSMS_002)	2
Datenschutzrichtlinie erstellen (M_DSMS_004)	2
Dokumentation und Kommunikation der Datenschutzrichtlinie (M_DSMS_005)	2
Datenschutzschulung für Mitarbeiter (M_DSMS_025)	3
Vertraulichkeitsvereinbarungen mit Mitarbeitern abschließen (M_DSMS_026)	3
Aktive Kontrollen	3
Aktualität der Datenschutzrichtlinie überprüfen (K_DSR_002)	3
Kommunikation der aktuellen Datenschutzrichtlinie (K_DSR_001)	4
Aktualität von Vertraulichkeitsvereinbarungen überprüfen (K_DSA_002)	4
Ausgesetzte Kontrollen	4
Deaktivierte Kontrollen	4

mangelndes Bewusstsein bzgl. Datenschutz(DSO_001)

Identifiziert am:	08.01.2018	Letzte Änderung:	
Eintrittswahrscheinlichkeit:	Wahrscheinlich	Schadensausmaß:	Hoch
Verantwortliche(r):	Tom Leisch		
Beschreibung:	Awareness in Bezug auf Datenschutz ist seitens des Managements und der Mitarbeiter nicht ausreichend ausgeprägt. Dies kann zu Datenschutzverletzungen mit teils gravierenden Folgen führen.		
Schutzziele:	Rechtskonformität	● ● ● ●	

Offene Maßnahmen:

Vertraulichkeitsvereinbarungen mit Geschäftspartnern abschließen (M_DSMS_028)

OrgEH:	TeSA
Beschreibung:	Geschäftspartner (Lieferanten, Kunden, sonstige Partner), die im Zuge der Zusammenarbeit Zugang zu personenbezogenen Daten haben, sollten auf das Datengeheimnis verpflichtet werden. Darüber hinaus sollten Regelungen zum gemeinsamen Umgang mit personenbezogenen Daten getroffen werden, sofern dies nicht ohnedies zB im Zuge einer allenfalls erforderlichen Auftragsverarbeitervereinbarung erfolgen muss. Die Vertraulichkeitsvereinbarung in Bezug auf personenbezogene Daten kann zB auch in die allgemeine Vertraulichkeitsvereinbarung mit Bezug auf Betriebs- und Geschäftsgeheimnisse integriert werden, sofern sie klar ersichtlich und verständlich ist.
Fortschritt:	0%

Datenübermittlungen in Drittländer DSGVO-konform durchführen (M_DSMS_035)

OrgEH:	TeSA_RE
Beschreibung:	Überprüfen Sie, ob in Ihrem Unternehmen personenbezogene Daten an Unternehmen/Einrichtungen/ Institutionen in Drittländer übertragen werden. Wenn dies der Fall ist, stellen Sie sicher, dass im Drittland ein der DSGVO entsprechendes Datenschutzniveau herrscht. Dieses kann nachgewiesen werden durch: - einen Angemessenheitsbeschluss der EU Kommission - das Vorhandensein geeigneter Garantien, zB in Form von verbindlichen internen Datenschutzvorschriften oder von der Kommission erlassenen oder genehmigten Standardvertragsklauseln (gem. Art 46 und 47) - das Bestehen eines Ausnahmetatbestands gemäß Art 49 (zB ausdrückliche Einwilligung der betroffenen Person, Erfüllung eines Vertrages auf Antrag der betroffenen Person, etc.)
Fortschritt:	0%

Ausgesetzte Maßnahmen:

Keine ausgesetzten Maßnahmen

Abgeschlossene Maßnahmen:

Management Awareness und Commitment sicherstellen (M_DSMS_001)

OrgEH:	TeSA
Beschreibung:	Stellen Sie sicher, dass sich das Management der Anforderungen aus der DSGVO und der möglichen Folgen bei Nichterfüllung bewusst ist. Definieren Sie den Bedarf an Ressourcen, der sich aus der Umsetzung der DSGVO in Ihrem Unternehmen ergibt und holen Sie das Commitment des Managements ein, diese bereit zu stellen und die Aktivitäten im Zusammenhang mit der Umsetzung zu unterstützen.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittmeldung:	initialer Workshop zu Themenstellungen der DSGVO durchgeführt. Ressourcen soweit definiert und frei gegeben

Verantwortlichkeiten iZm Datenschutz festlegen (M_DSMS_002)

OrgEH:	TeSA
Beschreibung:	Definieren Sie die Rollen im Rahmen des Datenschutzkonzepts und legen Sie die Verantwortlichkeiten zur Erstellung und Umsetzung der einzelnen Prozesse fest. Ermitteln Sie, ob die benötigten Ressourcen innerhalb Ihres Unternehmens vorhanden sind, oder ob Sie auf externe Ressourcen zurückgreifen müssen. Denken Sie dabei ua an Verantwortliche für folgende Prozesse: - Erstellen und Aufrechterhalten des Datenschutzkonzeptes - Erfüllung der Informationspflichten - Umsetzung der Betroffenenrechte - Erstellung und Pflege des Verzeichnisses von Verarbeitungstätigkeiten - Data Breach - Umsetzung technischer und organisatorischer Maßnahmen Überlegen Sie in diesem Zusammenhang auch die Benennung eines Datenschutzbeauftragten, sofern ein solcher für Ihr Unternehmen nicht ohnehin verpflichtend ist.
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittmeldung:	erledigt

Datenschutzrichtlinie erstellen (M_DSMS_004)

OrgEH:	TeSA_RE
Beschreibung:	Erstellen Sie eine unternehmensspezifische Datenschutzrichtlinie, die zumindest folgende Punkte regelt: - rechtliche Rahmenbedingungen im Unternehmen - die wesentlichen Vorgaben zu den Datenschutzgrundsätzen (Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung und Speicherbegrenzung, Richtigkeit, Integrität und Vertraulichkeit) - grundsätzliche technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes - generelle unternehmensinterne Regeln zum Datenschutz
Fortschritt:	100% am 16.04.2018 12: 0
Fortschrittmeldung:	Richtlinie erstellt

Dokumentation und Kommunikation der Datenschutzrichtlinie (M_DSMS_005)

OrgEH:	TeSA
Beschreibung:	Die Datenschutzrichtlinie sollte regelmäßig in aktueller Fassung an alle Mitarbeiter und sonstige relevante Interessensgruppen kommuniziert werden. Es sollte jederzeit ein Zugriff auf die aktuelle Fassung ermöglicht werden.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittmeldung:	Richtlinie kommuniziert.

Datenschutzschulung für Mitarbeiter (M_DSMS_025)

OrgEH:	TeSA_PER
Beschreibung:	Mitarbeiter sollten regelmäßig hinsichtlich Datenschutz geschult werden. Neben allgemeinen Inhalten, die alle Mitarbeiter betreffen wie zB: - Datenschutzrichtlinie - Vertraulichkeitsvereinbarungen - Datenschutzerklärung für Mitarbeiter sollten auch bereichsspezifische Informationen im Umgang mit personenbezogenen Daten thematisiert werden. Die Schulungen müssen hinsichtlich Inhalt und Durchführung nachweislich dokumentiert werden
Fortschritt:	100% am 23.01.2019 10:45
Fortschrittmeldung:	Alle Mitarbeiter initial mit den neuen Unterlagen geschult. Jährliche Auffrischung bereits geplant

Vertraulichkeitsvereinbarungen mit Mitarbeitern abschließen (M_DSMS_026)

OrgEH:	TeSA_PER
Beschreibung:	Mitarbeiter müssen auf das Datengeheimnis verpflichtet werden, sofern sie nicht ohnedies einer gesetzlichen Verschwiegenheitspflicht unterliegen . Dies kann auf mehrere Arten erfolgen, zB: - Teil des Dienstvertrages - separate Vertraulichkeitserklärung (eventuell gemeinsam mit einer generellen Geheimhaltungsvereinbarung) Die Mitarbeiter sollten jedenfalls ausdrücklich auf das Datengeheimnis hingewiesen werden und im Zuge regelmäßiger Datenschutzschulungen darauf hingewiesen werden.
Fortschritt:	100% am 15.11.2018 12: 0
Fortschrittmeldung:	mit allen MAs Vereinbarung getroffen

Aktive Kontrollen:

Aktualität der Datenschutzrichtlinie überprüfen (K_DSR_002)

OrgEH:	Team Secure AG
Umsetzter:	Tom Leisch
Prüfer:	Clarissa Hammer Peter Innereiter
Prüfverhalten:	Alle müssen akzeptieren
Erstmalig:	02.07.2018 12:00
Wiederkehrend:	<input checked="" type="checkbox"/> Alle 1 Jahr(e)
Deadline:	<input type="checkbox"/>
Beschreibung:	Überprüfen Sie regelmäßig, ob die Datenschutzrichtlinie noch den gesetzlichen und unternehmensinternen Anforderungen genügt und bringen Sie sie gegebenenfalls auf den neuesten Stand.
Bemerkung:	

Durchgeführte Kontrollen:

1. Kontrolle ausgelöst am 02.07.2018 12:00 Status: Abgeschlossen am 10.07.2018 12:00
 Geprüft von: Clarissa Hammer (Akzeptiert) am 10.07.2018 12:00
 Begründung: geht in Ordnung
 Peter Innereiter (Akzeptiert) am 09.07.2018 12:00
2. Kontrolle ausgelöst am 02.07.2019 12:00 Status: Ausstehend

Kommunikation der aktuellen Datenschutzrichtlinie (K_DSR_001)

OrgEH:	Team Secure AG
Umsetzter:	Tom Leisch
Prüfer:	
Prüfverhalten:	Alle müssen akzeptieren
Erstmalig:	06.08.2018 12:00
Wiederkehrend:	<input checked="" type="checkbox"/> Alle 1 Jahr(e)
Deadline:	<input type="checkbox"/>
Beschreibung:	Die Datenschutzrichtlinie sollte in ihrer aktuellen Fassung regelmäßig an alle relevanten Interessensgruppen kommuniziert werden. Diese kann zB entweder im Zuge einer wiederkehrenden Datenschutzbildung erfolgen oder in Form einer Aussendung im Zuge einer außerplanmäßigen Aktualisierung.
Bemerkung:	

Durchgeführte Kontrollen:

1. Kontrolle ausgelöst am 06.08.2018 12:00 Status: Abgeschlossen am 06.08.2018 12:00

Geprüft von:

Aktualität von Vertraulichkeitsvereinbarungen überprüfen (K_DSA_002)

OrgEH:	Team Secure AG
Umsetzter:	Max Mustermann
Prüfer:	
Prüfverhalten:	Alle müssen akzeptieren
Erstmalig:	28.05.2019 12:00
Wiederkehrend:	<input checked="" type="checkbox"/> Alle 1 Jahr(e)
Deadline:	<input type="checkbox"/>
Beschreibung:	Überprüfen Sie regelmäßig, ob mit allen relevanten Interessensgruppen gültige Vertraulichkeitsvereinbarungen abgeschlossen sind, die alle datenschutzrelevanten Anforderungen umfassend regeln.
Bemerkung:	

Durchgeführte Kontrollen:

1. Kontrolle ausgelöst am 28.05.2019 12:00 Status: Ausstehend

Ausgesetzte Kontrollen:

Keine ausgesetzten Kontrollen

Deaktivierte Kontrollen:

Keine deaktivierten Kontrollen