InfiniSafe® Datenschutzmanagement (IDSM)

EU-Datenschutz-Grundverordnung

Überwachung und Bewertung des Datenschutzes im Unternehmen

Stand: Juni 2017

TELEFON FAX E-MAIL

Richard-Strauss-Straße 71, 81679 München +49 89 452 216 72 +49 89 452 216 79 datenschutz@infinisafe.de

InfiniSafe
Inspiring Confidence.

InfiniSafe® Datenschutzmanagement

Datenschutz funktioniert in jeder Branche und in jedem Unternehmen anders weil er sensible Geschäftsbereiche berührt. Um diesem Umstand gerecht zu werden, setzen wir auf moderne Werkzeuge (PDCA-Zyklus) und eine strukturierte prozessorientierte Vorgehensweise. Der PDCA-Zyklus führt zu einer kontinuierlichen Performance-Verbesserung, einer Kernanforderung an alle QM-Aktivitäten und QM-Systeme.

Ziele festlegen, Prozesse analysieren, Maßnahmen festlegen

Alle datenschutzrechtlich relevanten Prozesse, egal ob automatisiert oder manuell, werden elektronisch erfasst und anhand datenschutzrechtlicher Risiken bewertet. Nach Prüfung der datenschutzrechtlichen Zulässigkeit und der jeweiligen betrieblichen Anforderungen, wird der Handlungsbedarf ermittelt, dokumentiert und priorisiert. Hierzu gehören die Überwachung im rechtlichen Bereich, die Überwachung der technischen und organisatorischen Maßnahmen sowie Richtlinien und Betriebsvereinbarungen.

Maßnahmen umsetzen, Mitarbeiterschulungen

Auf Grundlage der Analyse wird in Abwägung der rechtlichen und betriebswirtschaftlichen Notwendigkeit ein effizientes Datenschutzmanagement (IDSM) eingeführt, das auf die individuellen Bedürfnisse des Unternehmens abgestimmt ist. Alle Mitarbeiter werden unter Berücksichtigung ihrer fachlichen Tätigkeitsschwerpunkte für die datenschutzrechtlichen Themen geschult und im Umgang mit vertraulichen Daten sensibilisiert. Die Schulungen erfüllen nicht nur die gesetzlich geforderten Vorschriften, durch laufende Updates bleiben die Mitarbeiter immer auf dem Laufenden. Damit werden Geschäftsrisiken vermieden und Kunden- und Mitarbeitervertrauen gewonnen.

Kontrolle ob Ziele der Maßnahmen erreicht wurden

Durch die wiederkehrende Bewertung können der Stand der jeweiligen Umsetzung und die Entwicklung des Datenschutzes im Unternehmen regelmäßig verfolgt werden. Damit wird der Zustand der Rechtskonformität (Compliance) und der Verbesserungspotenziale zum Datenschutz im Unternehmen als Reifegrad ermittelt und dargestellt. Die Ergebnisse des Bewertungsverfahrens bilden die Grundlage für unternehmerische Entscheidungen, aus denen sich die erforderlichen Managementaufgaben und Maßnahmen ableiten lassen.

Maßnahmen = Routine, Zertifizierung

Ziel des IDSM ist ein nachhaltiger Schutz der vertraulichen personen- und unternehmensbezogenen Daten. Das InfiniSafe® Zertifikat belegt die laufende Kontrolle und kontinuierliche Weiterentwicklung der Datenschutzmaßnahmen, schafft beim Kunden Vertrauen und ermöglicht den werbewirksamen Einsatz in der Unternehmenskommunikation

Ziele festlegen, Prozesse analysieren, Maßnahmen festlegen

Gesetzesauftrag

Nach § 39 Abs. 2 DSGVO hat der Datenschutzbeauftragte die ordnungsgemäße Anwendung der Datenverarbeitung personenbezogener Daten zu überwachen. Die Überwachung vollzieht sich einerseits im rechtlichen Bereich und andererseits im technisch-organisatorischen Bereich. Die Beschränkung der Überwachung auf datenschutzrechtliche Aspekte soll aber nicht daran hindern, die vom Datenschutzbeauftragten erhobenen und bewerteten Ergebnisse in einer weiteren Stufe einer Gesamtbewertung zuzuführen und weitere eventuell erforderliche Maßnahmen vorzunehmen.

Überwachung im rechtlichen Bereich

Für die Überwachung im rechtlichen Bereich empfiehlt sich folgende Vorgehensweise:

- Identifizierung der datenschutzrelevanten operativen Geschäftsprozesse
- Verknüpfung der Datenschutzprozesse mit Aktionen und Tätigkeiten in den operativen Prozessen
- Identifizierung aller datenschutzrelevanten Prüfungen und Entscheidungen auf Grundlage der Datenschutzprozesse

Praktische Umsetzung

Die praktische Umsetzung der Rechtsvorschriften erfolgt in folgenden Schritten:

- Erstellung und Pflege der nach DSGVO vorgeschriebenen Verfahrensübersichten und regelmäßige Überprüfung der darin enthaltenen Angaben.
- Durchführung der internen Verfahrensübersicht und Schutzeinstufung der Daten.
- Notwendigkeit einer Folgeabschätzung (Art.35 DSGVO) und Melde- Informationspflicht (Art. 33-34) prüfen.
- Entwicklung von Richtlinien zur Realisierung der Anforderungen des Datenschutzes.
- Überprüfung der datenschutzgerechten Gestaltung des Internetauftritts des Auftraggebers (Datenschutzerklärung, Impressum, Cookies etc.).
- Datennutzung für Werbezwecke nach DSGVO und UWG prüfen.
- Mitwirkung hinsichtlich des Datenschutzes bei der Vertragsgestaltung zur Auftragsverarbeitung (Art. 26-28 DSGVO).
- Sicherstellung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung, Weitergabe).
- Darstellung der Datenschutzorganisation nach innen und nach außen.

Überwachung der technischen und organisatorischen Maßnahmen

Um den gesetzlichen Anforderungen zu genügen werden alle anzuwendenden technischen und organisatorischen Maßnahmen erfasst und regelmäßig hinsichtlich der Angemessenheit und ihrer Wirksamkeit überprüft. Für die Durchführung der Audits (Ist-Analyse) werden automatisierte Checklisten in Anlehnung an die Erfordernisse der DSGVO verwendet, die von den jeweiligen Fachabteilungen oder der IT-Abteilung auszufüllen sind. Es gilt, die technischen und organisatorischen Maßnahmen für die relevanten Prozesse und Verfahren im Unternehmen zu prüfen und einen dem Schutzbedarf der Daten angemessenen Datenschutz zu garantieren.

IDSM-Checklisten

Die nachfolgende Übersicht zeigt einen Auszug der vorhandenen Arbeitshilfen der IDSM-Online Datenbank:

- Ist-Analyse Datenschutz im Unternehmen
- Einsatz von Multifunktionsgeräten
- Homepage-Analysesystem
- Instant Messaging
- Onlinekalender
- Internetauftritt
- Telefonanlage und Mobiltelefone
- Voice over IP
- Mobile Datenträger
- Datenübermittlung an Kreditauskunfteien
- Bestehende Verträge über Datenverarbeitung im Auftrag
- Löschung und Entsorgung von Daten
- Erfassung der IT-Infrastruktur
- Gemeinsame Angaben zum Verfahrensverzeichnis
- ....

Eine vollständige Übersicht können Sie auf Anfrage erhalten.

Rechtliche und technisch-organisatorische Maßnahmen umsetzen

Die angebotenen Dokumentationen und Bewertungen unterstützen durch ihre transparente Darstellung die Einführung und Umsetzung der erforderlichen Maßnahmen.

Rechtliche Maßnahmen - Datenschutzprozesse

Die im IDMS vorgesehenen Datenschutzprozesse helfen den im Unternehmen für den Datenschutz Verantwortlichen, die Relevanz der Forderungen aus der DSGVO systematisch zu prüfen sowie deren Umsetzung durchzuführen und zu verfolgen. Wenn die Maßnahmen vollständig durchgeführt sind, wird man immer zu den Ergebnissen zulässig oder unzulässig geführt. Damit wird sichtbar, welche Anforderungen noch zu erfüllen sind oder welche Anforderungen nicht relevant sind. Die Inhalte und Aufgaben der Datenschutzprozesse bilden somit den Rahmen für die Beurteilung und Umsetzung der unternehmensspezifischen Anforderungen aus der DSGVO mittels gezielter Prüfschritte und konkreten Handlungen.

Technische und organisatorische Maßnahmen (TOM'S) - Verfahrensverzeichnisse

Bei der Umsetzung der TOM's empfiehlt es sich zunächst, die IT-Infrastruktur und IT-Technik grob zu erfassen. Im Anschluss daran werden die technischen und organisatorischen Maßnahmen gemäß Art. 32 erhoben und dokumentiert.

Verfahrensspezifische Regelungen (wie z.B. besondere Eingabekontrollen) werden im Verfahrensverzeichnis bei den dortigen Verfahrenserhebungen abgebildet. Parallel dazu kann dann das Schutzniveau der Daten auf Grundlage der Erhebungen für das Verfahrensverzeichnis festgelegt werden. Das Ergebnis der Einstufung der Daten in Schutzstufen liefert Hinweise für eventuelle Schwerpunkte bei der Umsetzung der Maßnahmen.

WICHTIG: Diese Festlegung sollte immer in Abstimmung mit den jeweiligen Fachbereichen geschehen.

Auf Grundlage der durchgeführten Erhebungen können Bedrohungen und Gefährdungen, denen die Daten ausgesetzt sind, erfasst und Risiken bewertet werden. Je nach Art des Unternehmens, der Position des Unternehmens in der Öffentlichkeit, der Sensibilität der Daten und des möglichen Schadens bei einer Datenschutzverletzung können unterschiedliche Vorgehensweisen angezeigt sein. Während bei einer eher unkritischen Situation des Unternehmens eine methodisch einfache Vorgehensweise ausreichend ist, kann bei kritischen Situationen eine methodisch durchaus aufwendige Risikoanalyse notwendig sein.

Gemessen am Schutzbedarf der Daten, dem Grad der Vertraulichkeit und der Schutzziele sowie der identifizierten Gefährdungen und Risiken werden danach die technischen und organisatorischen Maßnahmen bewertet und der Handlungsbedarf aus Datenschutzsicht ermittelt.

Mitarbeiterschulungen, Gesetzesauftrag

Der Datenschutzbeauftragte hat insbesondere die bei der Verarbeitung von personenbezogenen Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften der DSGVO sowie anderen Vorschriften über den Datenschutz und den jeweiligen besonderen Erfordernissen des Datenschutzes im Unternehmen vertraut zu machen. (Art. 39 Abs.1 DSGVO)

Grundschulungen und Schwerpunktschulungen

Für die Datenschutzunterweisung aller im Unternehmen Beschäftigten stehen folgende 5chulungen zur Verfügung:

- Datenschutz am Arbeitsplatz - Grundlagenschulung
- Beschäftigtendatenschutz – Schwerpunktschulung
- Datenschutz für Betriebsräte – Schwerpunktschulung
- Datenschutz für lT-Mitarbeiter und Administratoren - 5chwerpunktschulung
- Informationssicherheit und Datenschutz E-Learning-Portal

Flexibilität

ln welcher Weise die Schulung durchgeführt werden soll wird mit der Unternehmensleitung abgestimmt. Es besteht die Möglichkeit einer Präsenzschulung vor Ort oder einer internbasierenden Online-Schulung (E-Learning).

ln Abhängigkeit vom speziellen Aufgabengebiet des Mitarbeiters kann die Einweisung mit Schwerpunktschulungen z.B. für Betriebsräte oder für lT-Mitarbeiter und Administratoren (Telekommunikationsgesetz) vertieft werden.

E-Learning-Portal „“

Die E-Learning-Portal für Informationssicherheit und Datenschutz ist als selbstständiges Schulungsmodul konzipiert.

Die Schulung wendet sich an alle Beschäftigten, die auf der Ausführungs- und Bearbeitungsebene mit personenbezogenen Daten umgehen. Das Portal enthält deshalb einen Überblick über die allgemeinen Regelungen zum Datenschutz mit den am Arbeitsplatz besonders relevanten Schwerpunkten wie Datengeheimnis, Rechte der Betroffenen, Informations- und Einwilligungspflichten sowie Übermittlungs- und Offenbarungsbefugnisse. Ergänzt wird die Schulung durch Hinweise zur Passwortsicherheit, zum sicheren und datenschutzgerechten Verhalten am Arbeitsplatz, insbesondere im Hinblick auf die Nutzung von E-Mail und Internet, von sozialen Netzwerken sowie bei Nutzung von mobilen Datenträgern.

Kontrolle ob Ziele der Maßnahmen erreicht wurden

Die Bewertung der Erhebungsergebnisse in Bewertungstabellen ist aufgrund der inhaltlichen Abstimmung der vorgegebenen Arbeitshilfen einfach durchzuführen, da die Bewertung mit integrierten Funktionen zum großen Teil automatisiert durchgeführt wird.

Bewertung der technisch organisatorischen Maßnahmen

Die Konformität der technischen und organisatorischen Maßnahmen mit den gesetzlichen Forderungen wird anhand einzelner Bewertungskriterien geprüft und bewertet. Dabei werden die betriebsspezifische Relevanz, die Gewichtung und die aktuelle Erfüllung der Kriterien beurteilt. Daraus wird der jeweilige Erfüllungsgrad berechnet.

Bewertung der Datenschutzprozesse

Die Prüfkriterien der Bewertungstabelle für die Datenschutzprozesse sind in Ihrer Struktur mit den Forderungen der DSGVO und den Aktivitäten der einzelnen Datenschutzprozesse identisch. Unter Verwendung der Bewertungstabelle kann der Erfüllungsgrad jedes Datenschutzprozesses anhand sorgfältig ausgewählter Prüfschritte bewertet werden. Die verdichtete Übersicht der Erfüllungsgrade erlaubt einen schnellen und transparenten Überblick über die Umsetzung der betriebsspezifischen Forderungen aus der DSGVO.

Die Grafik der Erfüllungsgrade für die relevanten Maßnahmen stellt den Realisierungsgrad und die Rangfolge notwendiger Verbesserungsmaßnahmen im Unternehmen transparent dar und dient als Entscheidungsvorlage für Verantwortliche und Entscheidungsträger. Siehe Grafik „Erfüllungsgrad der Datenschutzprozesse“.

InfiniSafe® Datenschutzmanagement

Maßnahmen = Routine

Die Einführung eines prozessorientierten Datenschutzmanagements mittels PDCA-Zyklus führt zu einer Verbesserung des allgemeinen Organisationsstandards.

- Die kontinuierliche Kontrolle erhöht die IT-Sicherheit
- Die Sensibilisierung der Mitarbeiter im Umgang mit sensiblen Daten vermeidet Geschäftsrisiken
- Das gesteigerte Kundenvertrauen führt zu Wettbewerbsvorteilen
- Das gewonnene Mitarbeitervertrauen sorgt für ein verbessertes Betriebsklima und steigert die Produktivität.
- Die Umsetzung der Datenschutzprozesse und der Technischen und organisatorischen Maßnahmen werden zur Routine.

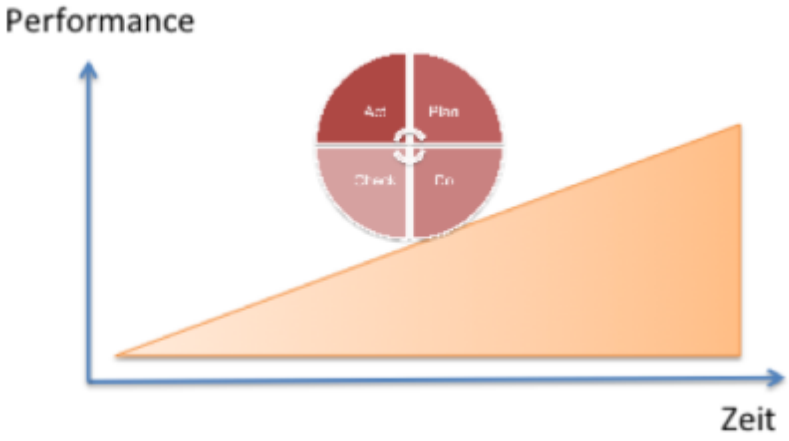
Zertifizierung

Nach erfolgreicher Einführung des Datenschutzmanagements wird ein Zertifikat ausgestellt.

Das InfiniSafe® Zertifikat belegt die laufende Kontrolle und kontinuierliche Weiterentwicklung der Datenschutzmaßnahmen, schafft beim Kunden Vertrauen und ermöglicht den werbewirksamen Einsatz in der Unternehmenskommunikation.

Kontinuierliche Performance-Verbesserung

Ist der PDCA-Zyklus einmal durchlaufen erfolgen neue Planungen und neue Zielvorgaben. Dieser sich ständig wiederholende Kreislauf führt zu einer kontinuierlichen Performance-Verbesserung, einer Kernanforderung an alle QM-Aktivitäten und QM-Systeme.



InfiniSafe® Datenschutzmanagement – Datenschutz und Betriebsrat

Mitbestimmungspflicht bei Bestellung des Datenschutzbeauftragten?

Der Datenschutzbeauftragte wird vom Arbeitgeber ausgewählt und schriftlich bestellt. Meist taucht bereits hier die Frage auf, ob die Bestellung der Zustimmung durch den Betriebsrat bedarf. Hierzu gilt, dass ein Mitbestimmungsrecht gesetzlich nicht vorgesehen ist. Grundsätzlich besteht also keine Mitbestimmungspflicht bei der Bestellung eines Datenschutzbeauftragten. Es gibt jedoch eine Ausnahme, die dann gilt, wenn mit der Bestellung z.B. eines internen Datenschutzbeauftragten gleichzeitig andere Personalmaßnahmen verbunden sind, die ein Mitbestimmungsrecht begründen können. Die Mitbestimmungsrechte des Betriebsrats sind in **§ 87 BetrVG** abschließend aufgezählt.

Bei Bestellung eines externen Datenschutzbeauftragten hat der Betriebsrat jedoch ein Prüfrecht zu der Frage, ob ein Datenschutzbeauftragter bestellt werden muss

Mitbestimmungspflicht des Betriebsrats und Datenschutz

Die Erhebung, Verarbeitung und Nutzung von Mitarbeiterdaten ist nur zulässig, soweit die DSGVO oder eine *andere Rechtsnorm* dies erlaubt oder anordnet oder der Betroffene zustimmt. Andere Rechtsnormen in diesem Sinne können auch Betriebsvereinbarungen sein. Wird die Mitbestimmungspflicht des Betriebsrats nicht beachtet, ist die Erhebung, Verarbeitung und Nutzung der Daten rechtsfehlerhaft, weil die gemäß Art. 5 und Art. 6 erforderliche Rechtsgrundlage fehlt. Es ist Aufgabe des Datenschutzbeauftragten, darauf zu achten, dass eventuell fehlende Betriebsvereinbarungen nachgeholt werden, um die Rechtssicherheit der Datenverarbeitungsverfahren herzustellen.

Kontrollrechte des Datenschutzbeauftragten

Der Datenschutzbeauftragte wirkt auf die Einhaltung des Datenschutzgesetzes und anderer Vorschriften für den Datenschutz im Unternehmen hin. Damit obliegen ihm bestimmte Kontrollrechte. Der Betriebsrat ist rechtlich gesehen ein Teil des Unternehmens, woraus sich ergibt, dass die Unternehmensleitung für die Einhaltung des Datenschutzes beim Betriebsrat verantwortlich ist. Es wäre deshalb naheliegend den Datenschutzbeauftragten die Einhaltung des Datenschutzes beim Betriebsrat kontrollieren zu lassen. Dazu hat aber das Bundesarbeitsgericht schon 1997 die Meinung vertreten, dass der Betriebsrat für die Einhaltung des eigenen Datenschutzes selbst zuständig ist und nicht durch den Datenschutzbeauftragten kontrolliert werden darf. Diese unbefriedigende Regelung hat das BAG in seinem Urteil nicht aufgelöst.

Ungeachtet dieser Entscheidung hat sich natürlich der Betriebsrat genauso wie alle anderen Stellen im Unternehmen an die jeweils geltenden Datenschutzvorschriften zu halten. Er unterliegt ebenfalls in vollem Umfang der Aufsichtsfunktion der Aufsichtsbehörden. Andererseits steht dem Betriebsrat auch keine Kontrollfunktion über den Datenschutzbeauftragten zu.

Fazit

Der Datenschutzbeauftragte und der Betriebsrat haben im Datenschutz, wenn auch nur in Teilbereichen, gemeinsame Schnittstellen und Aufgaben. So hat der Betriebsrat die freie Entfaltung der Persönlichkeitsrechte der Beschäftigten zu schützen und zu fördern (§ 75 Abs. 2 BetrVG). Der Datenschutzbeauftragte seinerseits schützt das Recht auf informationelle Selbstbestimmung der Mitarbeiter(Art. 37 und Art. 38).

Auch wenn keine gesetzliche Verpflichtung zur Zusammenarbeit besteht, kann diese in vielen Fällen von Nutzen sein. Am besten funktioniert die Zusammenarbeit, wenn der Datenschutzbeauftragte den Betriebsrat berät ohne ihn kontrollieren zu wollen und andererseits der Datenschutzbeauftragte auf die Beratungskompetenz des Betriebsrats zurückgreift.

Praxistip: Die Befolgung der nachfolgenden Punkte dient einer guten Zusammenarbeit zwischen Betriebsrat und dem Datenschutzbeauftragten:

- Transparenz der Prüfergebnisse des Datenschutzbeauftragten gegenüber dem Betriebsrat
- Beachtung des Mitbestimmungsrechts bei Abschluss von Betriebsvereinbarungen mit entsprechenden Datenschutzregelungen
- Regelmäßiger Knowhow-Transfer zwischen Betriebsrat und Datenschutzbeauftragtem

Impressum

InfiniSafe GmbH
Datenschutzmanagement (IDSM)
Richard-Strauss-Straße 71, 81679 München

Tel. +49 89 45 221 672
Fax. +49 89 45 221 679
E-Mail: datenschutz@infinisafe.de
Web: www.infinisafe.de

Vertretungsberechtigte Geschäftsführer:
Dipl. Kfm. Peter Paul Rother und
Dipl. Ing. Stanislaw Panow
Handelsregister München HRB 188848
Umsatzsteuer-Ident-Nr.: DE274783128