IHR 10-PUNKTE-PLAN

DATENSCHUTZ UND INFORMATIONSSICHERHEIT. DSGVO-KONFORM UND ZUKUNFTSSTARK.

Bechtle IT-Security

BECHTLE

ABSTRACT

DATENSCHUTZ UND INFORMATIONSSICHERHEIT KÖNNEN SPÄTESTENS SEIT DER EINFÜHRUNG DER DSGVO NICHT MEHR GETRENNT VONEINANDER BETRACHTET WERDEN.

Welche Punkte gibt es dabei für Unternehmen zu beachten?

Welche konkreten Schritte sollten Unternehmen jetzt gehen, um ihr IT-Sicherheits- und Datenschutz-niveau zu erhöhen?

Erfahren Sie mehr dazu im Whitepaper.

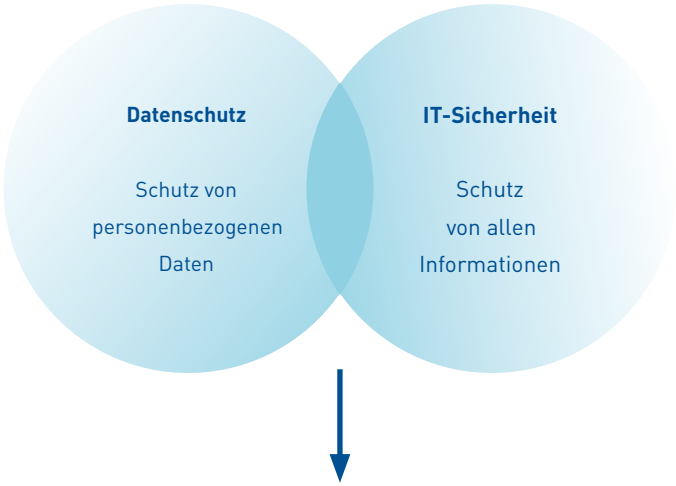
EINLEITUNG

An den Themen Datenschutz und Informationssicherheit kommt heute kein Unternehmen mehr vorbei. Der richtige Einsatz von Datenschutz und IT-Sicherheit sowie der Aufbau und die Pflege klarer „Spielregeln" im Unternehmen sind entscheidende Erfolgs- und Wettbewerbsfaktoren – sowohl im nationalen als auch im internationalen Umfeld. Warum? Die Sicherheit und Stabilität sämtlicher IT-Aktivitäten sind grundlegend für Unternehmen, Daten das höchste Gut, welches es zu schützen gilt. Darum sind heutige Geschäftsprozesse ohne effiziente Datenschutz- und Informationssicherheit nicht mehr vorstellbar. Diesen Sachverhalt spiegelt auch die Gesetzgebung wider: Mit der Einführung der europäischen Datenschutz-Grundverordnung im Mai 2018 sind Organisationen mehr denn je zu einer rechtmäßigen Datenverarbeitung und dem Nachweis darüber verpflichtet. Aber damit noch nicht genug: Das Zusammenspiel von Datenschutz und Informationssicherheit wurde im Zuge der DSGVO grundlegend verändert. Wurden bis dato der traditionelle Datenschutz und die rein auf Abschottung basierende IT-Sicherheit getrennt voneinander betrachtet, stehen seit der Einführung der Datenschutz-Grundverordnung die beiden Disziplinen in direkter Abhängigkeit.

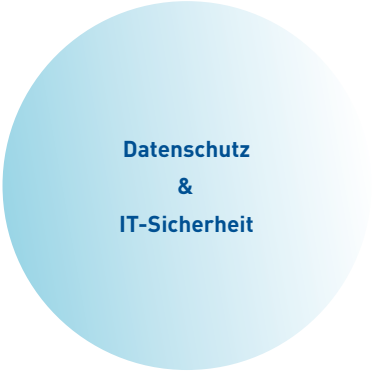
DSGVO

Verschmelzung von Datenschutz und Informationssicherheit

Betrachtung vor der Einführung der DSGVO:



Betrachtung nach der Einführung der DSGVO:



SYMBIOSE DATENSCHUTZ UND INFORMATIONSSICHERHEIT.

Was bedeutet das für Unternehmen?

Auch wenn es vielen Unternehmensverantwortlichen oftmals nicht klar ist: Die DSGVO bedeutet, dass sie sich zwangsläufig auch mit dem Thema IT-Sicherheit auseinandersetzen müssen . Denn dies ist ein stärkerer Bestandteil des Datenschutzes als zuvor: Die DSGVO macht mit ihren Vorgaben zum Datenschutz gleichzeitig auch klare Vorschriften zum Thema IT-Sicherheit. Die Logik dahinter ist einleuchtend, denn Datenschutz kann ohne eine vernünftige IT-Sicherheit kaum erfolgreich in den Unternehmen umgesetzt werden.

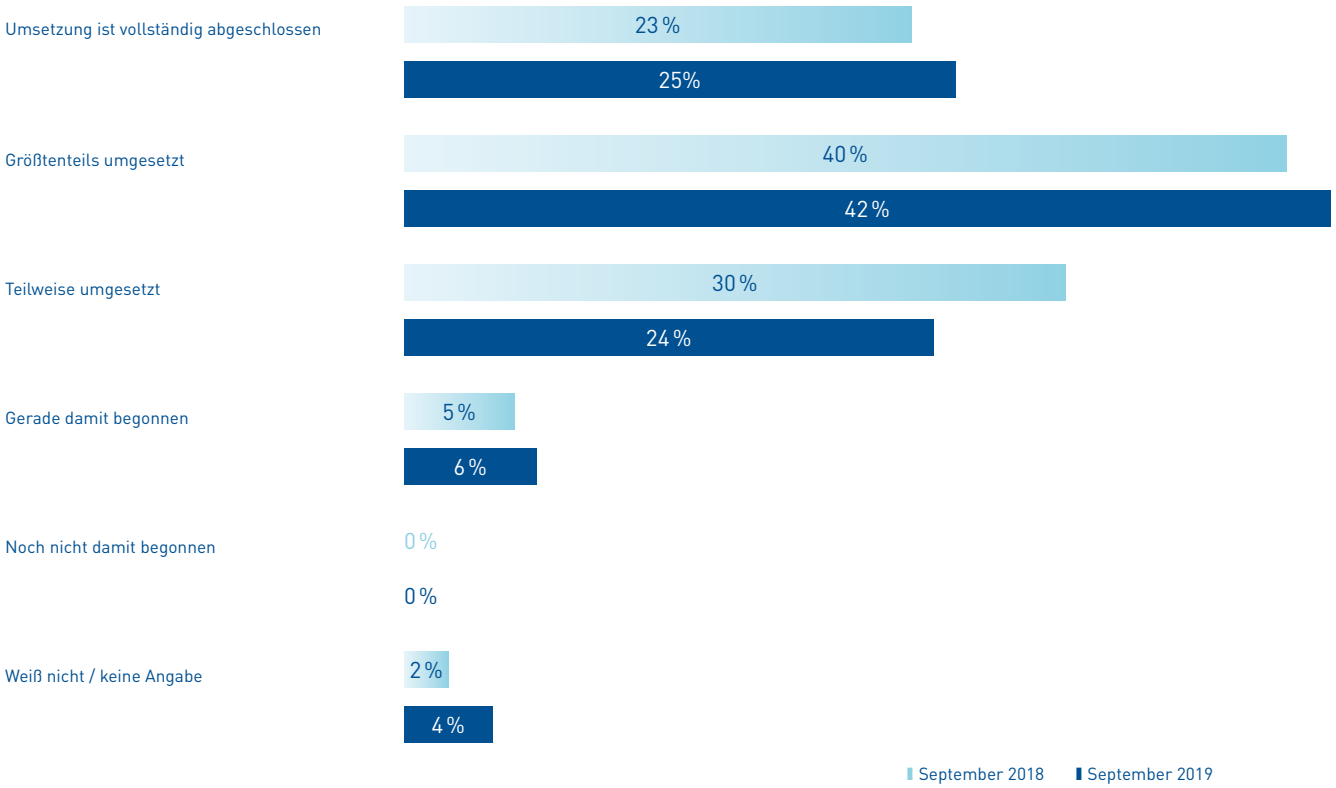
Für Organisationen bedeutet dies: Wer seine DSGVO-Konformität erreichen möchte, muss auch die IT-Sicherheit im Unternehmen in den Griff bekommen. Somit bildet eine stabile und verlässliche IT-Sicherheitsstrategie die Basis für die Umsetzung von Datenschutzmaßnahmen. Das vorliegende Whitepaper verdeutlicht den Zusammenhang zwischen Datenschutz und Informationssicherheit und gibt Ihnen konkrete Empfehlungen an die Hand, um Ihr Unternehmen in puncto Datenschutz und Informationssicherheit nach vorne zu bringen.

STATUS QUO IN VIELEN UNTERNEHMEN.

Noch immer sind längst nicht alle Unternehmen auf einem adäquaten Stand hinsichtlich der DSGVO-Konformität angekommen. Einer Bitkom-Umfrage zufolge gaben rund 24 Prozent der befragten Unternehmen an, dass sie die DSGVO-Vorschriften erst teilweise in ihrem Unternehmen umgesetzt haben – fünf Prozent haben (Stand September 2019) noch immer nicht mit der Umsetzung begonnen.

DS-GV(N)O

Fortschritt von Unternehmen bei der Umsetzung der Datenschutz-Grundverordnung (gerundet)



Die Folge: Datenschutzverstöße, drohende Bußgelder – aber auch negative Wahrnehmung bei Kunden oder Reputationsverlust. Doch welche Inhalte und Bestandteile gilt es im Zuge der DSGVO überhaupt zu beachten? Welche davon sind für Unternehmen noch nicht geläufig und bedingen dringend eine Handlung auf Firmenseite? Wir haben die wichtigsten Punkte für Sie zusammengestellt:

DSGVO-CHECKLIST

Die wichtigsten Punkte im Überblick

1. DATENSCHUTZ UND IT-SICHERHEIT: KEINE PRODUKTE, SONDERN EINE UNTERNEHMENSKULTUR.

Im Zuge der Einführung der DSGVO haben sich die Vorgaben zur IT-Sicherheit und somit auch die der „technischen und organisatorischen Maßnahmen" geändert. Diese Maßnahmen mussten bislang nur in „angemessener Weise" erfolgen – doch im Zuge der DSGVO sind eine höhere Compliance- und IT-Risikobetrachtung gefordert. Der Gesetzgeber verlangt von Unternehmen den adäquaten „Stand der Technik" zur Einhaltung des Datenschutzes sowie ein stärkeres Risikomanagement. Darüber hinaus müssen Unternehmen laut DSGVO nicht nur die Art, den Umfang und den Zweck der Verarbeitung, den Stand der Technik und die Kosten berücksichtigen, sondern auch die Eintrittswahrscheinlichkeit von Risiken für die Betroffenen.

Unternehmen müssen sich mit all diesen Punkten auseinandersetzen. Die einfache Einführung „neuer Produkte" reicht hier nicht aus; vielmehr müssen eine genaue Betrachtung der abzuleitenden Maßnahmen und die daraus resultierenden Schritte erfolgen.

2. INFORMATIONSSICHERHEIT UND DATENSCHUTZ SIND „CHEFSACHE".

Das Management trägt nicht nur die strategische Verantwortung, sondern auch die Haftung für die IT-Sicherheit und das Risikomanagement. Darüber hinaus ist die Unternehmensleitung auch dafür verantwortlich, dass ein Informationssicherheitsmanagementsystem (ISMS) umgesetzt und kontinuierlich verbessert wird. Denn ein ISMS ist allgemein betrachtet ein Rahmenwerk von Richtlinien, Verfahren und Regelungen einer Organisation.

Hierfür müssen Unternehmen geeignete Ressourcen bereitstellen, welche die Informationssicherheit dauerhaft definieren, steuern, kontrollieren, aufrechterhalten und kontinuierlich verbessern: Diese Verpflichtungen sind auch in einigen Gesetzestexten verankert. Die Verantwortlichen müssen laut unterschiedlichster Gesetze und Vorschriften den Fortbestand der Gesellschaft sichern.

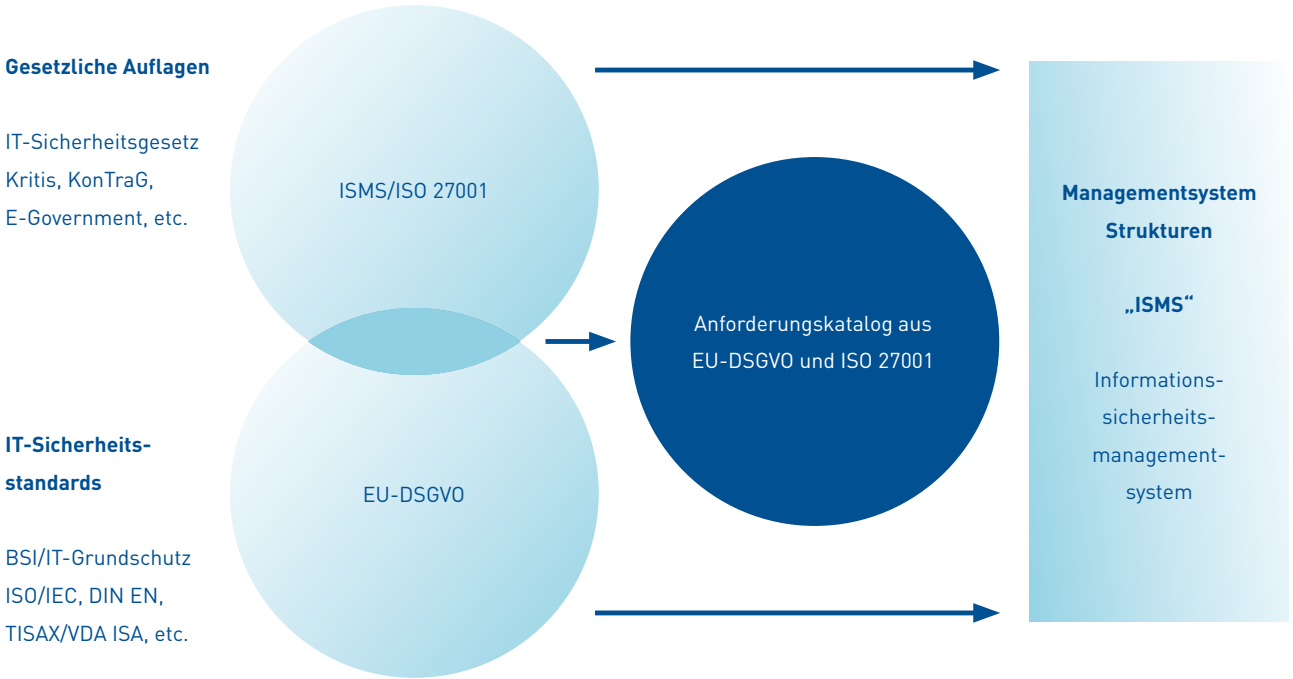
3. GESETZLICHE AUFLAGEN: IT-COMPLIANCE UND DIE ROLLE DER GESCHÄFTSFÜHRUNG.

Was bedeutet Compliance? Im Grunde genommen die Einhaltung des Rechts auf allen Gebieten des Unternehmens – also das Erreichen der Rechtskonformität. IT-Compliance betrifft hauptsächlich die IT-Systeme in Unternehmen. Dazu gehören auch Informationssicherheit, Verfügbarkeit, Datenschutz und Datenaufbewahrung. Nachfolgend einige Beispiele gesetzlicher Verankerungen von IT-Compliance neben der DSGVO:

- IT-Sicherheitsgesetz (KRITIS): Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- KonTraG: Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
- GoBD: Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Unterlagen in elektronischer Form
- SOX: Sarbanes-Oxley Act
- Basel II/III und MaRisk: Bonitäts- und Risikobetrachtung auf Basis von Ranking-Systemen
- KWG: Kreditwesengesetz mit bankenaufsichtlichen Anforderungen an die IT
- Produkthaftungsgesetz bzw. § 823 BGB (z. B. bei Softwarekauf)
- Teledienstgesetz (TDG): Gesetz über die Nutzung von Telediensten
- Telekommunikationsgesetz (TKG) (das den Wettbewerb im Bereich der Telekommunikation reguliert)
- Grundgesetz Art. 10 und G10-Gesetz (Brief-, Post- und Fernmeldegeheimnis zählt zu den Grundrechten)
- Urheberrechtsgesetz (UrhG)
- StGB: u. a. IT-bezogene Straftaten §§ 202a (Ausspähen von Daten), 202b (Abfangen von Daten)

Aus diesen und weiteren gesetzlichen Auflagen lässt sich auch die direkte Verantwortung der Geschäftsführung für die IT-Sicherheit und Datensicherheit im Unternehmen ableiten. Im Klartext bedeutet dies: Eine Nichteinhaltung kann zu persönlicher Haftung der Geschäftsleitung führen.

Verschmelzung von gesetzlichen Auflagen und IT-Sicherheitsstandards



4. DIE MITARBEITER INS BOOT HOLEN: AWARENESS UND SENSIBILISIERUNG.

Nach Art. 39 Abs. 1 lit. a DSGVO müssen Mitarbeiter Schulungen zur Sensibilisierung erhalten. Unternehmen sollten außerdem dafür Sorge tragen, dass im Rahmen einer Datenschutzschulung auch die IT-Sicherheitsaspekte des Datenschutzes thematisiert werden. Unternehmen müssen das IT-Sicherheits- und Datenschutzkonzept korrekt umsetzen und befolgen. Das gilt vor allem für die Mitarbeiter. Es gibt hier klare gesetzliche Nachweispflichten. Ohne das Bewusstsein für Informationssicherheit und Datenschutz können Unternehmen ein betriebswirtschaftlich und rechtlich notwendiges Sicherheitsniveau nicht erreichen. Aus diesem Grund sind regelmäßige Mitarbeiterschulungen und die Sensibilisierung für diese Themen (Awareness) unerlässlich.

Darüber hinaus sind Meldungen von Mitarbeitern der häufigste Weg, wie Cyberangriffe innerhalb von Unternehmen bemerkt werden – noch dazu ist das beste Sicherheitskonzept wirkungslos, wenn Mitarbeiter beispielsweise den Anhang einer Phising-Mail öffnen, da sie sich der Bedrohung nicht bewusst sind.

!

All diese Punkte unterstreichen die immense Bedeutung von Datenschutz und IT-Sicherheit. Doch oftmals wissen Unternehmen nicht, welche konkreten Schritte sie nun gehen sollten, um einen angemessenen Schutz in ihrem Unternehmen sowie eine Gesetzeskonformität zu gewährleisten. Wir haben darum einen kurzen 10-Punkte-Plan mit den wichtigsten Schritten für Sie zusammengestellt:

IHR 10-PUNKTE-PLAN

für eine Erhöhung des Sicherheits- und Datenschutzniveaus in Ihrem Unternehmen:

1. Zuerst sollten Sie sich für die Anwendung eines qualifizierten Sicherheitsstandards in Ihrem Unternehmen entscheiden. Dies können sein: ISO 27001/ISMS native oder IT-Grundschutz (BSI) unter Berücksichtigung der DSGVO.
2. Implementieren Sie ein Datenschutz- und Sicherheitsmanagement in Ihrem Unternehmen (DSGVO/ISMS).
3. Setzen Sie in angemessener Weise auf fachliche und personelle Ressourcen.
4. Legen Sie gemeinsam die benötigten Schutzmaßnahmen fest, beachten Sie dabei Leitlinien und das Thema IT-Compliance.
5. Führen Sie eine Bestandsaufnahme der Datenverarbeitung durch.
6. Ermitteln Sie das Schutzniveau der Daten und Prozesse mittels einer Risikoanalyse.
7. Überprüfen und kontrollieren Sie in definierten Zeiträumen die Einhaltung der Maßnahmen (Rechenschaftspflicht).
8. Dokumentieren Sie die IT-Systeme und Prozesse in einem Datenschutz- und Informationssicherheitskonzept.
9. Bei Bedarf: Zertifizieren Sie Ihr Unternehmen gemäß aktuellen Sicherheitsstandards zur Einhaltung der DSGVO bzw. ISMS.
10. Sensibilisieren und schulen Sie alle Mitarbeiter. Achtung: Hier besteht eine Nachweispflicht.

!

Diese Vorgehensweise unterstützt Sie bei der Einhaltung gesetzlicher Vorschriften und hilft dabei, Cyberangriffe einzudämmen und somit Betriebsausfälle und Reputationsverlust möglichst zu vermeiden. Handeln Sie jetzt, um wirtschaftliche Schäden und persönliche Haftungsansprüche zu vermeiden. Wenn Sie einen zuverlässigen und erfahrenen Partner an Ihrer Seite benötigen, steht Ihnen Bechtle gerne rund um die Themen Datenschutz und Informationssicherheit zur Seite:

Damit Sie sicher sind:

IT SICHERHEIT. MACHT BECHTLE.

36
Jahre Erfahrung

>300
Zertifizierungen

>200
Experten

8
Kompetenz-zentren

>40
Hersteller-partner

Das Bechtle Competence Center Datenschutz und Informationssicherheit.

Profitieren Sie von unseren hoch qualifizierten Spezialisten in den Bereichen Datenschutz und IT-Sicherheit für Ihr Unternehmen. Wir bieten ganz gezielt Lösungen für die sensiblen Bereiche der Unternehmensorganisation. Das setzt fundiertes Fachwissen und stetige Weiterbildung voraus, um ein starkes und nachhaltiges Datenschutz- und IT Sicherheitsmanagement implementieren zu können. Branchenneutrale und herstellerunabhängige Beratungsleistung sowie die Übernahme operativer Verantwortung als externer Partner ergänzen das maßgeschneiderte Angebot für unterschiedlichste Branchen.

Wie wir Sie unterstützen.

Datenschutz- und IT-Sicherheitsexperten stehen Ihnen zur Seite, wann immer es um die Verfügbarkeit, Integrität und Vertraulichkeit von personenbezogenen Daten, Unternehmensinformationen und IT-Systemen geht. Dies beinhaltet auch die Umsetzung von Auflagen der DSGVO und anderen gesetzlichen Bestimmungen. Sie unterstützen das Risikomanagement der Unternehmen im IT-Bereich, von der Risikoanalyse bis zur Notfallvorsorge, erstellen Konzepte und bereiten auf Zertifizierungen vor. Wir helfen dabei, Lücken im Datenschutz und in der IT-Sicherheitsstruktur zu schließen. Als externe Datenschutzbeauftragte und IT-Sicherheitsbeauftragte werden Sie von erfahrenen Spezialisten begleitet.

WIR UNTERSTÜTZEN UND BETREUEN MITTELSTÄNDISCHE UND INTERNATIONALE UNTERNEHMEN SOWIE ÖFFENTLICHE EINRICHTUNGEN. DATENSCHUTZ- UND IT-SICHERHEITSBEAUFTRAGTE BILDEN GEMEINSAM MIT ZERTIFIZIERTEN AUDITOREN EIN KOMPETENTES TEAM. DIESES STELLT SICH INDIVIDUELL AUF KUNDEN BRANCHENORIENTIERT EIN UND BIETET SPEZIELL AUF UNTERNEHMENSBEDÜRFNISSE ZUGESCHNITTENE LEISTUNGEN.

Ob im Bereich Datenschutz oder Informationssicherheit: Mit uns sind Sie sicher. Setzen Sie sich jetzt mit uns in Verbindung und erfahren Sie mehr über unser Leistungsspektrum. Darüber hinaus beraten wir Sie gerne individuell zu Ihrer passenden Vorgehensweise und Rechtslage.

Ich bin mir sicher. IT-Sicherheit. Macht Bechtle.

Autor und fachlicher Ansprechpartner: Heiner Golombek
Bechtle Neckarsulm, Leitung Competence Center Datenschutz und Informationssicherheit
Kontakt: Heiner.Golombek@bechtle.com

Weiterführende Anfragen über das Thema hinaus zu Bechtle Security richten Sie bitte an:
Security.ls@bechtle.com

[1] https://www.heise.de/select/ix/2018/5/1524785715597695

[2] https://dsgvo-gesetz.de