Ihr 10-Punkte-Plan:

Datenschutz und Informationssicherheit. DSGVO-konform und zukunftsstark.

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE

Datenschutz und Informations-sicherheit 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 Datenschutzniveau zu erhöhen?

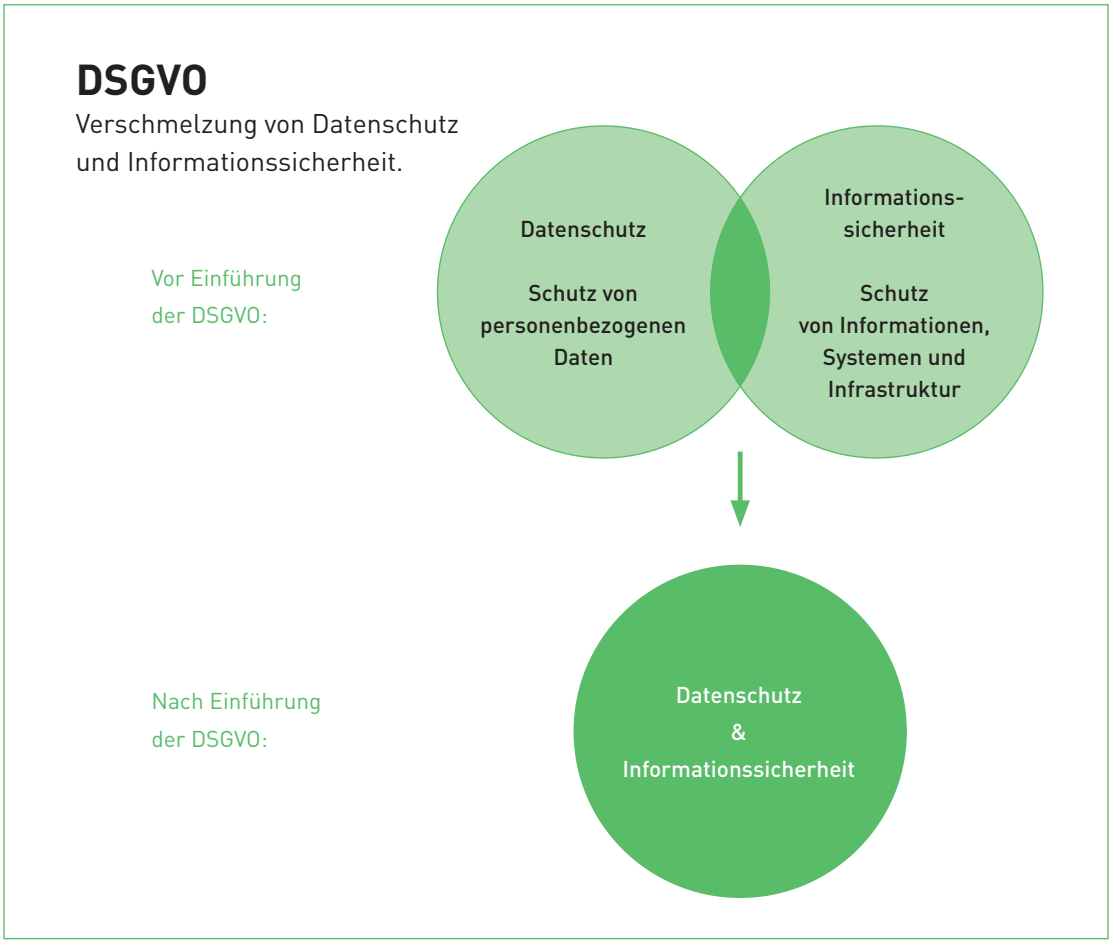
Erfahren Sie mehr dazu auf den folgenden Seiten.

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. Sensible Daten sind heute das höchste Gut und müssen geschützt werden. 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.

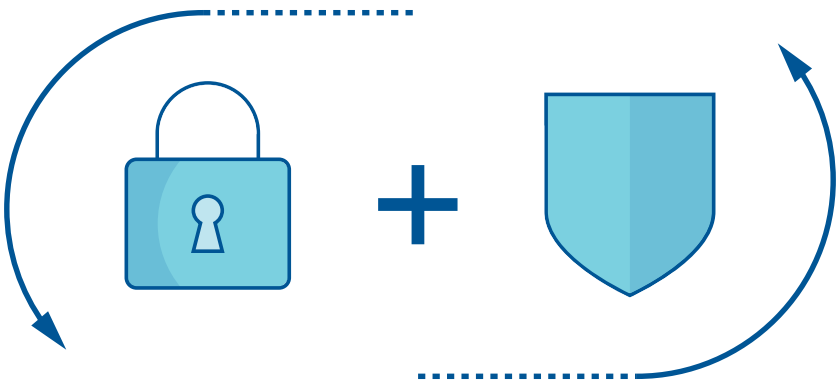


Symbiose Datenschutz und Informationssicherheit.

Was bedeutet das für Unternehmen?

Auch wenn es vielen Unternehmensverantwortlichen oft nicht klar ist: Die DSGVO bedeutet, dass sie sich zwangsläufig auch mit dem Thema Informationssicherheit auseinandersetzen müssen. Denn dies ist ein stärkerer Bestandteil des Datenschutzes als zuvor: Die DSGVO macht mit ihren Vorgaben zum Schutz von Daten gleichzeitig auch klare Vorschriften für diesen Bereich. Die Logik dahinter ist einleuchtend, denn das eine kann ohne eine vernünftige Strategie zur sicheren Verarbeitung von Informationen kaum erfolgreich umgesetzt werden. Für Organisationen bedeutet dies: Wer DSGVO-Konformität erreichen möchte, muss auch die IT-Sicherheit in den Griff bekommen. Somit bildet eine stabile und verlässliche Strategie die Basis für die Umsetzung der entsprechenden Maßnahmen.

Das vorliegende Whitepaper verdeutlicht den Zusammenhang zwischen Datenschutz und Informationssicherheit und gibt Ihnen konkrete Empfehlungen an die Hand, um Ihr Unternehmen in diesen Bereichen nach vorne zu bringen.

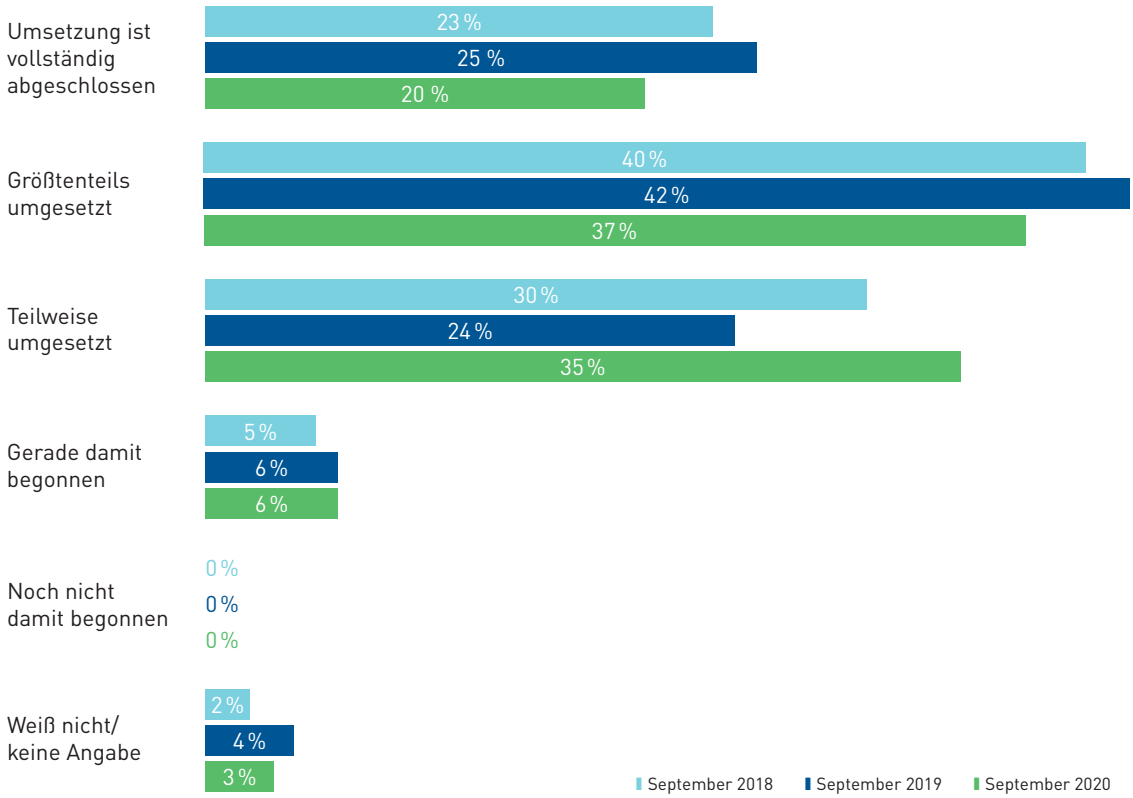


Status quo in vielen Unternehmen.

Auch im dritten Jahr seit ihrem Inkrafttreten sind längst noch nicht alle Unternehmen auf einem adäquaten Stand hinsichtlich der DSGVO-Konformität angekommen. Einer Bitkom-Umfrage zufolge geben rund 35 % der befragten Unternehmen an, die DSGVO-Vorschriften erst teilweise in ihrem Unternehmen umgesetzt zu haben – 6 % haben (Stand 09/2020) erst mit der Umsetzung begonnen. Lediglich bei einem Fünftel der Unternehmen ist die Umsetzung abgeschlossen.

DSGVO

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-Checkliste:
Die wichtigsten Punkte im Überblick

1. Datenschutz und Informationssicherheit:
Keine Produkte, sondern eine Unternehmenskultur.

Die Vorgaben zur Informationssicherheit und somit auch die der „technischen und organisatorischen Maßnahmen" haben sich im Zuge der Einführung der DSGVO geändert. Diese Maßnahmen mussten bislang nur in „angemessener Weise" erfolgen – doch im Zuge der DSGVO ist eine stärkere 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 Informationssicherheit 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.

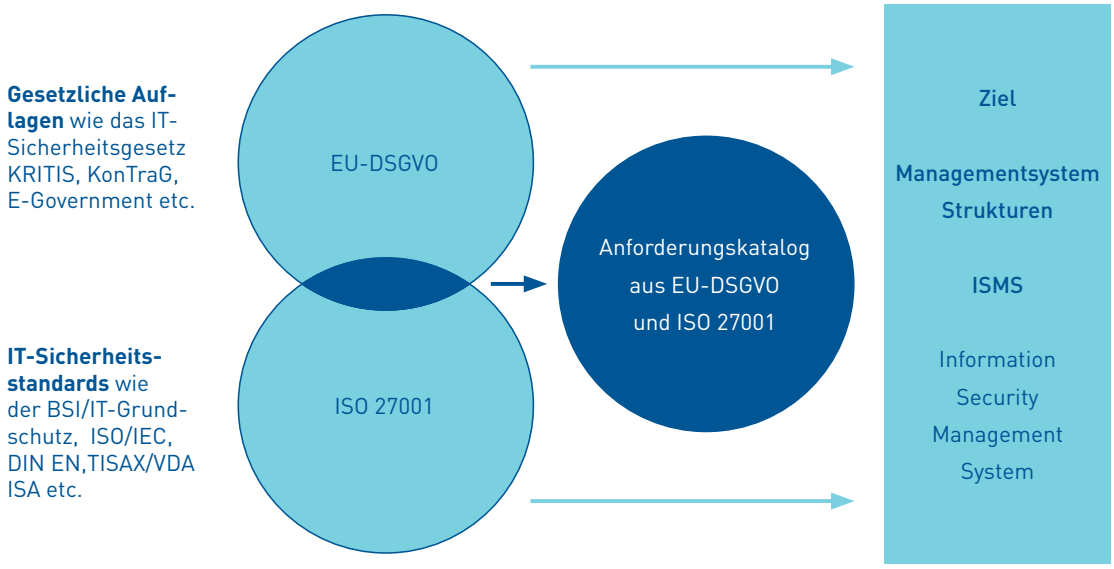
Die Haftungsfrage

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 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)
- Teledienstegesetz (TDG): Gesetz über die Nutzung von Telediensten
- Telekommunikationsgesetz (TKG, es regelt den Wettbewerb im Bereich der Telekommunikation)
- 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)

Verknüpfen Sie gesetzliche Auflagen zur Compliance mit IT-Sicherheits-standards für Ihre Organisation.



Mit einem ISMS lassen sich gesetzliche Auflagen und Compliance konform umsetzen.

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

Gelebte Sicherheit

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 der Aspekt Informationssicherheit thematisiert wird. Unternehmen müssen das IT-Sicherheits- und Datenschutzkonzept korrekt umsetzen und befolgen. Das gilt vor allem für die Mitarbeiter. Dabei gibt es klare gesetzliche Nachweispflichten. Ohne das Bewusstsein für Informationssicherheit und Datenschutz können Unternehmen das betriebswirtschaftlich und rechtlich notwendige Sicherheitsniveau nicht erreichen. Aus diesem Grund sind regelmäßige Mitarbeiterschulungen und die Sensibilisierung für diese Themen (Awareness) unerlässlich.

Meldungen von Mitarbeitern sind der häufigste Weg, über den Cyberangriffe innerhalb von Unternehmen bemerkt werden. So ist das beste Sicherheitskonzept wirkungslos, wenn Mitarbeiter beispielsweise den Anhang einer Phishing-Mail öffnen, da sie sich der Bedrohung nicht bewusst sind.

Natürlich gelten die strengen Vorgaben der DSGVO für den Umgang mit personenbezogenen Daten ebenso bei Remote Work im Homeoffice. Auch der Umgang mit privaten sowie geschäftlichen mobilen Geräten wie Laptops und Smartphones etc. unterliegt diesen Regeln.

Welche Anforderungen gilt es bei der Übermittlung von Daten ins Ausland (Drittländer) zum Schutz der Persönlichkeitsrechte zu beachten? Was hat der Brexit mit Datenschutz und DSGVO zu tun und wie habe ich mich zu verhalten?

Diese wichtigen Fragen sollten Unternehmen und Organisationen ihren Mitarbeitern im Rahmen von Awareness und Sensibilisierungsmaßnahmen beantworten können.

!

Alle diese Punkte unterstreichen die immense Bedeutung von Datenschutz und Informationssicherheit. 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:

Sicherheit lernen

5. Mitarbeiterqualifizierung leicht gemacht: E-Sensecurity.

Viele Unternehmen scheuen sich vor Schulungen, da diese Mitarbeiter, Ressourcen und auch Räumlichkeiten binden. Doch das muss nicht sein.

Bechtle E-Sensecurity ist das E-Learning-Tool für Informationssicherheit und Datenschutz. Dank E-Learning kann jeder Abteilung das Wissen passgenau und kostengünstig vermittelt werden – und das direkt am eigenen Arbeitsplatz.

E-Sensecurity besteht aus Audio- und Videosequenzen, Präsentationen und Texten – zugeschnitten auf die Bedürfnisse Ihres Unternehmens. Mit E-Sensecurity werden Sie allen Sensibilisierungsanforderungen und Nachweispflichten gerecht. Zum Beispiel sind in der ISO 27001 IT-Grundschutzzertifizierungen sowie Datenschutzzertifizierungen oder Wirtschaftsprüfungen gefordert. Selbstverständlich erfüllt E-Sensecurity auch alle Sensibilisierungserfordernisse nach dem IT-Sicherheitsgesetz oder der EU-DSGVO (europäischen Datenschutz-Grundverordnung).

E-Learning ist computergestütztes Lernen, wann und wo Sie möchten.

Ziel der Awareness-Schulung ist es, mit personenbezogenen Daten und sensiblen Unternehmensinformationen sicher und bewusst umzugehen. Jeder Anwender lernt nach eigenem Tempo und dann, wenn es sein Tagesablauf erlaubt. Die professionellen Inhalte bereiten wir für Führungskräfte und Mitarbeiter abteilungs- und zielgruppengerecht auf. Wir bieten Ihnen ein großes Spektrum an multimedialen Gestaltungsmöglichkeiten: anschauliche Animationen, verständliche Sprache, abwechslungsreiche Texte und ansprechendes Design. Eine laufende Aktualisierung des jeweiligen Themas in regelmäßigen Abständen sorgt zusätzlich für eine hohe Effektivität der Maßnahme.

E-Sensecurity wird einfach in Ihr Intranet integriert und kann über den Webbrowser ausgeführt werden. Es sind aber auch weitere Optionen möglich. Sprechen Sie einfach mit uns.

Von Anfang an ein Erfolg.

Im Verlauf der Mitarbeitersensibilisierung werden die Nutzer aktiv in Lerninhalte eingebunden. Das Besondere: Die Mitarbeiter schauen nicht nur zu, sondern machen mit. Durch ein eigenes Testmodul mit Multiple-Choice- und Wissensfragen wird am Ende jeder Schulung der Erfolg gemessen.

Weitere Themen und Schulungsarten können nach Ihren Bedürfnissen integriert werden. Wählen Sie eine Schulungsmethode oder kombinieren Sie mehrere miteinander. Ob Vortrag, Workshop oder Konferenz – wir passen E-Sensecurity Ihren Anforderungen an. Dadurch ist E-Sensecurity für Unternehmen und Behörden gleichermaßen geeignet.

Ihr 10-Punkte-Plan
für eine Erhöhung des Informations-sicherheits- und Datenschutz-niveaus 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: Es besteht eine gesetzliche 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.

Mit Sicherheit an erster Stelle:

Bechtle IT-Security

37 Jahre Erfahrung

>300 Zertifizierungen

>200 Experten

15 Competence Center

>40 Hersteller-partner

Das Bechtle Competence Center Datenschutz und Informationssicherheit.

Profitieren Sie von unseren qualifizierten Spezialisten in den Bereichen Datenschutz und Informationssicherheit 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.

Kompetenz und Erfahrung

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:
it-security@bechtle.com

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. Bechtle unterstützt Sie 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.

MIT SICHERHEIT AN ERSTER STELLE
Bechtle IT-Security.

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 der zu Ihrem Geschäftsmodell passenden Vorgehensweise.

Quellen

Joerg Heidrich: FAQ: Der neue Datenschutz im IT-Alltag. Technisch betrachtet. In: iX 5/2018 (https://www.heise.de/select/ix/2018/5/1524785715597695).

Intersoft: Datenschutz-Grundverordnung – DSGVO (https://dsgvo-gesetz.de/).

Statista: Wie weit sind Sie mit der Umsetzung der Datenschutz-Grundverordnung? Stand der Umsetzung der DSGVO durch Unternehmen in Deutschland im September 2020 (https://de.statista.com/statistik/daten/studie/917518/umfrage/stand-der-umsetzung-der-dsgvo-durch-unternehmen-in-deutschland/).