BEREIT FÜR DIE DSGVO?

COMPLIANCE DURCH DIE NUTZUNG EINES DATENSCHUTZSTANDARDS

BUREAU VERITAS

BEREIT FÜR DIE DSGVO?

Compliance durch die Nutzung eines Datenschutz-Zertifizierungsprogramms

Inhalt

Im Jahr 2018 haben die Datenschutzbestimmungen ihre größte Veränderung seit zwei Jahrzehnten erfahren.

Die Allgemeine Datenschutzverordnung* (DSGVO) soll den Bedürfnissen des 21. Jahrhunderts gerecht werden. Die Menge digitaler Informationen die wir erstellen, erfassen und speichern, ist durch die Digitalisierung exponentiell gewachsen. Der Missbrauch von Daten durch Unternehmen und Regierungen hat gleichzeitig zu öffentlichem Misstrauen geführt (siehe Seite 3-5).

Vor diesem Hintergrund bietet die DSGVO den Schutz personenbezogener Daten. Sie zielt darauf ab, die Datenschutzgesetze in ganz Europa zu harmonisieren und Einzelpersonen mehr Rechte zu gewähren. Die geänderte Vorschrift zur Verarbeitung und Speicherung von Daten durch Unternehmen und öffentliche Organisationen sieht bei Verstoß Geldbußen von bis zu 4% der Einnahmen vor.

Dieses Dokument wurde im Mai 2018 erstellt und erläutert, wie Sie mit einer freiwilligen Datenschutzzertifizierung die Einhaltung der Vorschriften sicherstellen können.

* Veröffentlicht als Verordnung (EU) 2016/679

BEREIT FÜR DSGVO ?

Über das Datenschutz-Zertifizierungsprogramm

Die neueste Version des technischen Standards zur Einhaltung der (EU) 2016/679-Verordnung zum Schutz personenbezogener Daten (DSGVO) wurde im Juni 2018 veröffentlicht. Entwickelt von Bureau Veritas Certification, einem weltweit führenden Anbieter von Risikomanagement- und Managementsystemzertifizierungen, bietet er ein praktisches und effizientes Verfahren welches die Einhaltung der DSGVO gewährleistet.

DOWNLOAD der technische Standard PDF

WER IST BETROFFEN DURCH DIE DSGVO?

Die DSGVO betrifft alle Organisationen, unterscheidet jedoch zwischen Verantwortlichen und Auftragsverarbeitern. Ein Verantwortlicher ist die Person oder Firma, die den Zweck und die Art und Weise bestimmt, für die personenbezogene Daten verwendet werden. Ein Auftragsverarbeiter ist jeder, der personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, beispielsweise Datenanalyse-Dienste bereitstellt oder Daten auf einem Server speichert. Während die Verordnung für beide gilt, unterliegen Verantwortliche weitaus mehr Verpflichtungen.

ERSTE SCHRITTE MIT DER DSGVO

Die DSGVO ist eine weitreichende Regelung, die einerseits die Datenschutzrechte von Einzelpersonen und andererseits die Pflichten von Unternehmen regelt. Dazu gehört die klare Verantwortung der Unternehmen, die Einwilligung von Personen einzuholen, über die sie Daten erheben. „Daten" umfasst sowohl personenbezogene Daten, die zur Identifizierung einer Person, wie Name oder IP-Adresse, verwendet werden können als auch sensible personenbezogene Daten wie religiöse und politische Ansichten oder sexuelle Orientierung.

Ein Schlüsselbegriff ist die Verantwortlichkeit. Organisationen übernehmen die Rechenschaftspflicht für die von ihnen verarbeiteten Daten und müssen die erforderlichen Ressourcen und Fähigkeiten bereitstellen, um einen optimalen Schutz der persönlichen Daten zu gewährleisten. Die Verpflichtungen sind höher für größere Organisationen sowie für Unternehmen, die eine „regelmäßige und systematische Überwachung" von Einzelpersonen durchführen oder eine Vielzahl sensibler Daten verarbeiten.

Die Verordnung zielt auch darauf ab, die Transparenz zu erhöhen, nachdem es zu einer Reihe von Verstößen gegen die Datenschutzbestimmungen bei Millionen von Internetnutzern gekommen ist. Organisationen, die Opfer von Hackern werden oder sensible Kundendaten verlieren, müssen den Vorfall innerhalb von 72 Stunden bei der Datenschutzbehörde ihres Landes melden.

In der DSGVO geht es zum Großteil darum, den Verbrauchern die Datenhoheit zurückzugeben. Beispielsweise können Einzelpersonen kostenlos nach persönlichen Informationen fragen, und Unternehmen müssen die Antwort innerhalb eines Monats geben. Die DSGVO gibt den Verbrauchern auch das Recht auf Löschung ihrer personenbezogenen Daten.

IN SUMMARY Die DSGVO fordert die Unternehmen auf, Compliance nachzuweisen in der Art, wie sie Daten verarbeiten und speichern und auf Informationsanfragen reagieren. Um dies zu erreichen, müssen Unternehmen kohärente Prozesse definieren und sicherstellen, dass sie im gesamten Unternehmen einheitlich angewendet werden. Das Datenschutz-Zertifizierungsprogramm hilft dabei, dies zu erreichen.

SCHUTZ PERSÖNLICHER DATEN: DER KONTEXT

VERBRAUCHER
verhalten sich nicht konsistent

Verbraucher sind besorgt über die Verwendung ihrer persönlichen Daten

Paradoxerweise stimmen die meisten der Teilung ihrer Daten zu

VERBRAUCHER

über **80%**

der Verbraucher befürchten Diebstahl oder Missbrauch ihrer Daten

Quelle: GfK

1/3 der Internet-Nutzer

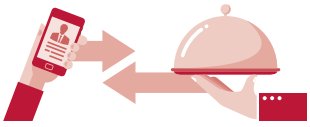
in den USA erlebten im letzten Jahr einen Missbrauch ihrer persönlichen Daten

Quelle: GfK

92% der Internet-Nutzer

in Frankreich glauben, dass Service Provider ihre Daten nutzen können

Quelle: IPSOS for Elia



62% der Verbraucher

stimmen der Weitergabe persönlicher Informationen zu, um auf neue digitale Dienste zugreifen zu können

Quelle: Microsoft Research

Verbraucher haben Angst …

87% mit Werbung verfolgt zu werden

85% ihre digitalen Spuren nicht löschen zu können

77% ein Opfer von Bankdaten- oder Identitätsklau zu werden

Quelle: IPSOS for Elia

Ihrer Meinung nach sind die sensibelsten Daten…

82% Ortsangabe

70% Browser Daten

81% Gesundheit

68% Kommunikation mit Freunden

Quelle: Pew Research Center

BUREAU VERITAS

BEREIT FÜR DSGVO ?

UNTERNEHMEN haben
Probleme die gesammelten Daten zu managen

Alle Organisationen sammeln Daten (Besuche, Profile, Zahlungsdaten)

Aber nur wenige steuern die Daten auf konsistente Art und Weise

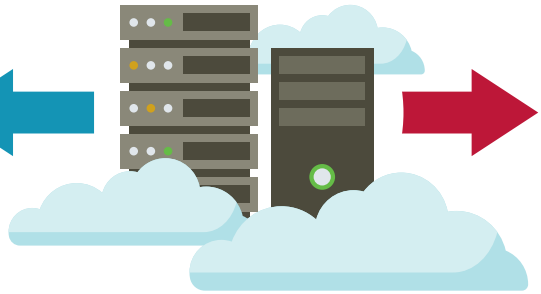
UNTERNEHMEN

Ausgaben

$130Mrd.

in 2016 für Daten- und Businessanalyse

Quelle: IDC

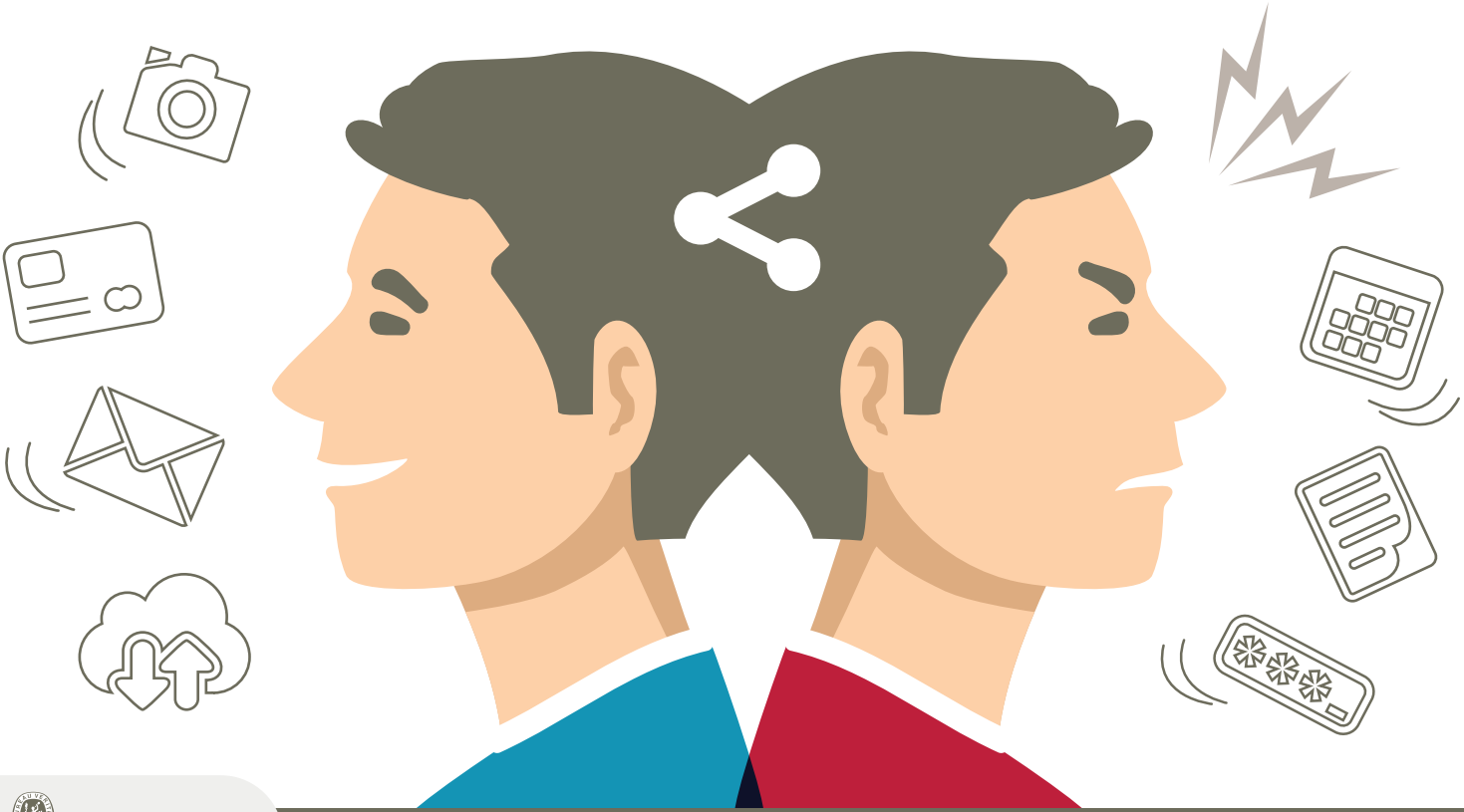


Nur

16.000

E-commerce-, staatliche und andere Organisationen in Frankreich haben einen offiziellen Datenschutzbeauftragten

Quelle : AFDCP, Fevad

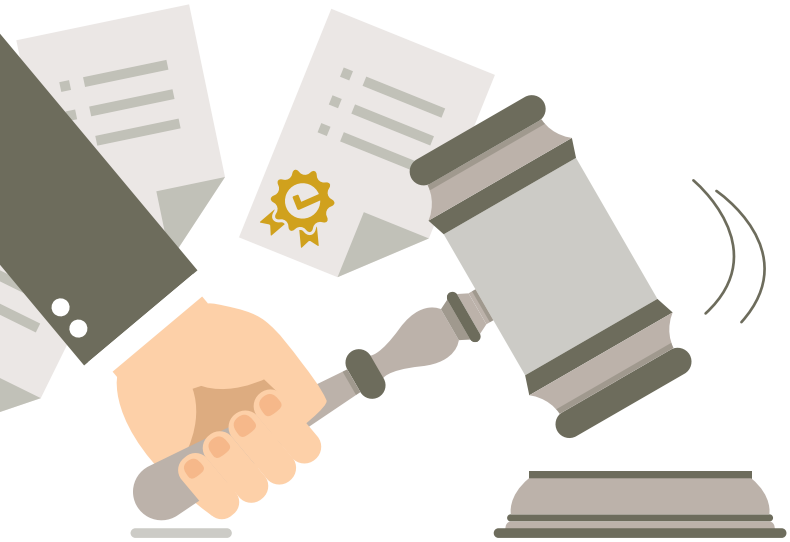


Strenge Vorschriften sind EIN TREIBER FÜR WANDEL

UNTERNEHMEN versuchen, die Dinge positiv zu beeinflussen

+

VORSCHRIFTEN zwingen sie, sich zu organisieren



Die meisten Organisationen veröffentlichen eine «sanfte» Datenschutzrichtlinie, die nur 10% der Internetnutzer, die sich bei ihnen anmelden, vollständig lesen

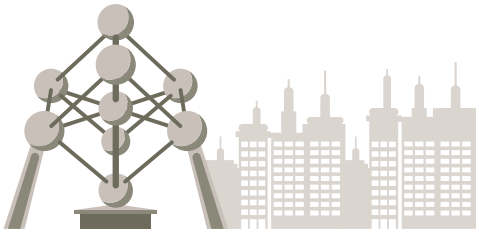
(Quelle CNIL)

Wenige große Unternehmen veröffentlichen Ethik-Chartas und Guidelines

In den USA

Der Entwurf der Bill of Rights zum Datenschutz wurde bereits zweimal vorgestellt

1 1 0 1 1 0 1 1 0 1
1 0 1 0 0 0 1 0 1 0
1 1 0 1 1 0 1 1 0 1



In der Europäischen Union

Die DSGVO wurde 2016 angenommen und verankert stärkere Verpflichtungen bis 2018: Recht auf Vergessenheit, Datenportabilität, obligatorische Benachrichtigung bei der Verletzung des Schutzes personenbezogener Daten, einschließlich der Daten die außerhalb Europas übertragen werden. Es sind Geldbußen von bis bis 4% des weltweiten Jahresumsatzes möglich.

UNABHÄNGIGE ZERTIFIZIERUNG

ist der einzige Weg Vertrauen in Ihr Unternehmen aufrecht zu erhalten und zu steigern.

Die Zertifizierung Ihres Systems zur Behandlung von Daten zeigt, dass Sie den Datenschutz ernst nehmen

- Verständlich für die Öffentlichkeit
- Glaubwürdig im Markt
- Anpassungsfähig und offen

- Verantwortliche
  versichern Endnutzer, dass ihre persönlichen Daten sicher sind
- Auftragsverarbeiter
  zeigen Glaubwürdigkeit gegenüber Verantwortlichen

Die Zertifizierung ist am besten von einer unabhängigen Stelle mit:

- Glaubwürdigkeit
- Unparteilichkeit
- transparenten Analysewerkzeugen
- einem weltweit bekannten Zertifizierungssiegel

Move Forward with Confidence

BUREAU VERITAS

Datenschutz-Zertifizierungsprogramm
ÜBERBLICK

Das System basiert auf einem technischen Standard, der sechs Hauptthemen abdeckt, um der Regulierung zu entsprechen. Er enthält auch hilfreiche Tabellen, die es Compliance-Verantwortlichen, Risikomanagern und Datenschutzbeauftragten ermöglichen, die Compliance zu überprüfen. Am Ende dieses Whitepapers wird die Beziehung der Klauseln zu ISO 27001 und ISO 9001 aufgezeigt, um die Integration von Prozessen in vorhandene Managementsysteme zu erleichtern.

Risikobewertung und -behandlung

Abbildung der Risiken und Compliance-Verpflichtungen, denen die Organisation ausgesetzt ist. Dazu gehört das Datenschutzfolgeabschätzung, um alle Aktivitäten, Produkte und Dienstleistungen zu bestimmen, die die Vertraulichkeit und Integrität oder die persönlichen Daten beeinflussen können. Es werden auch Prozesse zur Verwaltung von Datenschutzverletzungen behandelt.

Steuerung von Produkten und Dienstleistungen

Nennt detailliert die Notwendigkeit, Compliance-Verpflichtungen und Anforderungen an Produkte und Dienstleistungen ab der Entwurfs- und Entwicklungsphase zu überprüfen, zu definieren und zu dokumentieren. Dies beinhaltet die Integration einer kontinuierlichen Compliance während des gesamten Lebenszyklus.

Steuerung betrieblicher Abläufe

Erläutert die Notwendigkeit, dokumentierte Verfahren und Arbeitsanweisungen zu entwickeln und zu implementieren. Dadurch können Mitarbeiter und externe Dienstleister Compliance-Anforderungen erfüllen.

Organisation und Struktur

Betont die Notwendigkeit von Führung und Engagement des Top-Managements sowie einer dokumentierten Organisationsstruktur. Dabei werden Rollen und Verantwortlichkeiten für das Management personenbezogener Daten im gesamten Unternehmen festgelegt und zugewiesen. Dazu gehört die Ernennung eines Datenschutzbeauftragten und die Ausarbeitung einer Richtlinie zum Schutz personenbezogener Daten.

Managementsystem

Befürwortet einen systematischen Ansatz für das Management von Datenschutzrisiken, der in organisatorische Prozesse integriert ist. Dies beinhaltet die Dokumentation in Bezug auf die Datenverarbeitung und den Schutz personenbezogener Daten sowie die Kommunikation mit Mitarbeitern und externen Parteien. Der Fokus des Standards liegt auf der kontinuierlichen Verbesserung, die durch regelmäßige Überwachung, interne Audits und Managementbewertungen wird.

Ressourcen

Beschreibt die für die Umsetzung des Standards erforderlichen Ressourcen, einschließlich Infrastruktur, Personalkenntnisse, Bewusstsein und Wissen.

Welches Ziel will die Datenschutz-Zertifizierung ERREICHEN?

Für Unternehmen ist es eine der größten Herausforderungen der kommenden Jahre, das richtige Gleichgewicht zwischen Ermittlung der Information über Kunden durch die Analyse von Big Data und der Verwendung dieser Informationen zur Schaffung von Mehrwert zu finden, ohne dabei die individuellen Rechte zu beeinträchtigen.

Das Datenschutz-Zertifizierungsprogramm ermöglicht es Organisationen, die Datenschutzanforderungen der DSGVO von Anfang an als Standard zu integrieren und wichtige Details zu berücksichtigen - Einholung der Zustimmung, Verhältnismäßigkeit und das Recht auf Portabilität - ohne die Prozesse der Organisation grundlegend zu ändern.

Der Standard unterstützt Unternehmen bei der Ausarbeitung und Umsetzung der Richtlinien und Verfahren zur Einhaltung der DSGVO

Er verwendet einen Prozessansatz, der den Plan-Do-Check-Act-Zyklus und das risikobasierte Denken beinhaltet. Um dem Schlüsselprinzip der Verantwortlichkeit des Datenschutzbeauftragten Rechnung zu tragen - für die Verarbeitung personenbezogener Daten, die von ihm selbst oder in seinem Namen von einer anderen Organisation durchgeführt werden - müssen interne Regeln und ein proaktiver Ansatz zum Nachweis der Einhaltung der Vorschriften festgelegt werden.

DATENSCHUTZ BY DESIGN, DATENSCHUTZ BY DEFAULT

Zwei wesentliche Konzepte für den Standard:

DATENSCHUTZ BY DESIGN fordert Organisationen auf, Datenschutz personenbezogener Daten bei der Gestaltung von Produkten und Dienstleistungen zu berücksichtigen.

DATENSCHUTZ BY DEFAULT fordert Unternehmen auf, über ein Informationssystem zu verfügen, das jederzeit ein hohes Datenschutzniveau gewährleistet. Das Ergebnis ist ein hohes Maß an Datensicherheit sowie die Einhaltung der DSGVO.

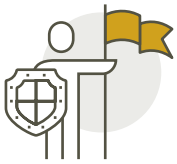
HAUPTVORTEILE
des Datenschutz-Zertifizierungsprogramms

Ein systematischer Ansatz zum Schutz personenbezogener Daten kann dem Top-Management Informationen liefern, um langfristig Erfolg zu haben. Er ermöglicht Ihnen:

1

Nachweis der Einhaltung von gesetzlichen Anforderungen

Das Datenschutz-Zertifizierungsprogramm verfolgt die Anforderungen der DSGVO und bietet einen Rahmen für die Implementierung von Richtlinien und Prozessen zur Einhaltung gesetzlicher Anforderungen.



2

Schutz der Reputation

Das Zertifizierungsprogramm hilft, Verstöße gegen personenbezogene Daten zu verhindern oder abzumildern. Es wird ein Verständnis dafür geschaffen, wie Verstöße gegen personenbezogene Daten auftreten und was dagegen getan werden kann. Darüber hinaus können Sie sich auf Datenverstöße vorbereiten, indem das Personal geschult wird und Verfahren zur Schadensbegrenzung sowie zur Information von betroffenen Personen, Behörden, Kunden und Mitarbeitern vorhanden sind.

3

Erfüllung der Kundenanforderungen

Damit Unternehmen das Vertrauen ihrer Kunden, Mitarbeiter und anderer Interessengruppen gewinnen und halten können, müssen sie digitale Verantwortung beweisen. Das Zertifizierungsprogramm verfolgt eine Lebenszyklusperspektive und betont die Kontrolle der Art und Weise, wie Produkte und Dienstleistungen in Bezug auf personenbezogene Daten entworfen, entwickelt und verarbeitet werden.

4

Risiken mindern und Chancen nutzen

Die DSGVO entwickelte sich aus einem mangelnden Vertrauen von Verbrauchern und Aufsichtsbehörden in Unternehmen, die immer größere Datenmengen nutzen, auf die sie Zugriff haben. Die Datenschutzzertifizierung fördert das Vertrauen in die Verwendung von Big Data in Ihrem Unternehmen und ermöglicht Ihnen, die Möglichkeiten der digitalen Transformation zu nutzen.

NÄCHSTE SCHRITTE

Bureau Veritas bietet eine Vielzahl von Dienstleistungen an, auf dem Weg zur Einhaltung der DSGVO

ZERTIFIZIERT WERDEN

Mittels Zertifizierung dieses technischen Standards durch Bureau Veritas wird unabhängig sichergestellt, dass ein Unternehmen den Standard in seiner gesamten Organisation implementiert hat, dieser von den Mitarbeitern verstanden und konsequent angewendet wird und dass etwaige Abweichungen behoben werden. Auf diese Weise kann die Organisation die Einhaltung gesetzlicher Vorschriften* erreichen.

SCHULUNG DER MITARBEITER ZUR KONSISTENTEN IMPLEMENTIERUNG

Das Bewusstsein und das Verständnis der Mitarbeiter für Datenschutzfragen und die Prozesse, die Sie zu ihrer Bewältigung ansetzen, sind von entscheidender Bedeutung. Bureau Veritas unterstützt Sie bei der Schulung von Mitarbeitern und Auftragnehmern.

IMPLEMENTIERUNG DES STANDARDS

Laden Sie zu Beginn eine Kopie des technischen Standards herunter. Sie können diesem Standard folgen, um die Prozesse, Richtlinien und Dokumentation zu entwickeln, die Sie zur Einhaltung der DSGVO implementieren müssen.

DOWNLOAD technischer Standard PDF

iCHECK APPLICATION

Beurteilen Sie Ihre Bereitschaft zur Zertifizierung nach DSGVO mit der App "icheck for Cyber and Data", die kostenlos im App Store und bei Google Play erhältlich ist.

icheck for Cyber & Data
A BUREAU VERITAS SOLUTION

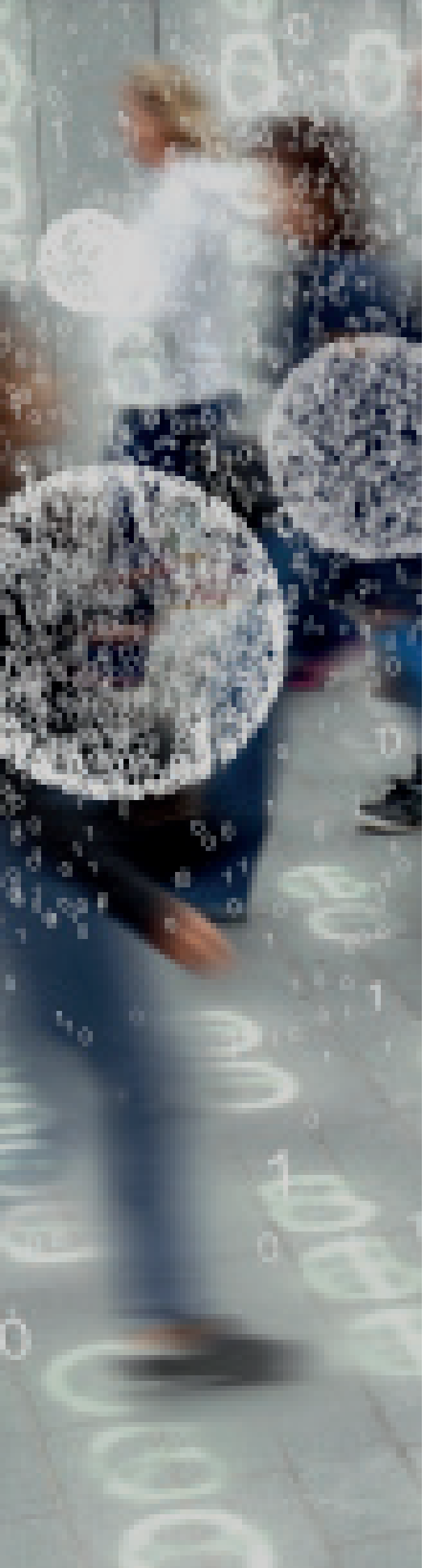
GET IT ON Google Play

Download on the App Store

Mehr zu ZERTIFIZIERUNGEN

Mehr zu SCHULUNGEN

* Die Anwendung dieses technischen Standards hat keinen Einfluss auf die Verantwortlichkeit des Datenverantwortlichen oder des Datenverarbeiters.



ÜBER BUREAU VERITAS

Bureau Veritas steht für qualitativ hochwertige Services, die Unternehmen aller Branchen helfen, dem steigenden Anspruch an Qualität, Gesundheit & Sicherheit, Umweltschutz (QHSE) und Soziale Verantwortung gerecht zu werden. Als zuverlässiger Partner bietet Bureau Veritas innovative Lösungen an, die über die bloße Bestätigung der Konformität mit Vorschriften und Standards hinausgehen. Weltweit verfolgen unsere Teams ein gemeinsames Ziel: Menschen, Anlagen und Umwelt zu schützen, indem sie Risiken minimieren, Leistung verbessern und nachhaltige Entwicklung fördern.

Für weitere Information, kontaktieren Sie Bureau Veritas:

Bureau Veritas Certification Germany GmbH

Veritaskai 1

21079 HAMBURG

cert-germany@de.bureauveritas.com

Besuchen Sie unsere Website

Laden Sie sich unseren technischen Standard herunter

BUREAU VERITAS

Editorial & Design: hollisbean.com / +33 1 83 62 20 41