

Öffentlich
Group Standard

Informationssicherheit für Externe

Veröffentlicht: 2026.09.24

Version: 1.7DE

Abteilung: Global Information and Cyber Security



Inhalt

1. Zweck.....	4
2. Geltungsbereich.....	4
3. Ziele und Grundsätze.....	4
3.1. Sicherheitsgrundsätze	5
3.2. Allgemeine Bedingungen	5
3.3. Überprüfung	5
4. Allgemeines Informationssicherheitsmanagement	5
4.1. Vertragliche Anforderungen	5
4.2. Informationssicherheits-Managementsystem (ISMS)	6
4.3. Einhaltung des Informations- und Cybersicherheitsstandards.....	6
4.4. ISMS-Sensibilisierungs- und Sicherheitsschulungen.....	7
4.5. Nutzung von DEKRA- und externen Ressourcen	7
4.6. Nichteinhaltung	7
4.7. Umgang mit Ausnahmen	7
5. Einstufung von Informationen.....	7
5.1. Kennzeichnung	9
5.2. Umgang mit Informationen	10
6. Sicherheitskontrollmaßnahmen.....	14
6.1. Physische Zugangskontrolle	14
6.2. Zugangskontrolle	14
6.3. Benutzerzugriffskontrolle.....	16
6.4. Trennungskontrolle	16
6.5. Daten e Medienkontrolle	16
6.6. Transport skontrolle	16
6.7. Sicherheit der System	17
6.8. Verfügbarkeitskontrolle.....	17
6.9. Sicherheitsvorfälle.....	18
7. Zulässige und unzulässige Nutzung durch Lieferanten und deren Mitarbeiter.....	18
7.1. Zulässige Nutzung.....	18
7.2. Unzulässige Nutzung	19
8. Dokumentenlenkung.....	20



9. Versionsverlauf.....	20
-------------------------	----



1. Zweck

Der Zweck dieses Standards für Informations- und Cybersicherheit besteht darin, die Geschäftskontinuität zu gewährleisten und Schäden zu minimieren, während mit externen Parteien (Lieferanten, Dienstleistern, Kunden, Geschäftspartnern, Auszubildenden usw.) zusammengearbeitet wird, indem Sicherheitsvorfälle vermieden oder auf ein Minimum reduziert werden.

Der Informations- und Cybersicherheitsstandard ermöglicht die Nutzung von DEKRA-Informationen in externen Organisationen unter Einhaltung folgender Grundsätze:

- Vertraulichkeit
- Integrität und
- Verfügbarkeit

Mit diesem Informations- und Cybersicherheitsstandard unterstreicht die DEKRA-Geschäftsführung die Bedeutung der Sicherheit von Informationen und Informationssystemen bei DEKRA sowie der Informations- und Cybersicherheit für die Zusammenarbeit mit externen Organisationen.

2. Geltungsbereich

Dieser DEKRA-Standard für Informations- und Cybersicherheit ist als „P public“ eingestuft und richtet sich an folgende Zielgruppe:

- Lieferanten, Geschäftspartner, Dienstleister
- Geschäftskunden und Endkunden
- Auftragnehmer, Berater, Auszubildende, Zeitarbeitskräfte sowie
- Agenturen und Franchise-Nehmer

Je nach Anwendungsfall und nach Rücksprache mit der lokalen DEKRA-Abteilung für Informations- und Cybersicherheit sowie erst nach Unterzeichnung einer Vertraulichkeitsvereinbarung (NDA) und Einholung der Genehmigung durch den Dokumentenverantwortlichen können weitere Richtlinien und Standards zur Anwendung kommen.

3. Ziele und Grundsätze

Das Sicherheitsziel von DEKRA besteht darin, sicherzustellen, dass Informationen in jeglicher Form – schriftlich, mündlich, elektronisch oder gedruckt – während ihres gesamten Lebenszyklus vor versehentlicher oder vorsätzlicher unbefugter Änderung, Löschung oder Offenlegung geschützt sind. Die Sicherheitsmaßnahmen für die Systeme und Programme, die zur Verarbeitung, Übertragung, Speicherung und Löschung von Informationen verwendet werden, müssen ein angemessenes Schutzniveau gewährleisten.



3.1. Sicherheitsgrundsätze

- Unsere Geschäftsprozesse und unser Know-how müssen geschützt werden
- Unsere Sicherheitsmaßnahmen reduzieren die Risiken für das Unternehmen
- Unsere Sicherheitsmaßnahmen entsprechen den Branchenstandards
- Jeder Einzelne ist in seinem Fachgebiet für die Sicherheit unserer Informationen, Einrichtungen und Systeme verantwortlich.
- Wir werden eine klare Trennung der Zuständigkeiten vornehmen, um Interessenkonflikte zu vermeiden
- Wir werden alle gesetzlichen und regulatorischen Anforderungen einhalten
- Wir werden sicherstellen, dass die Sicherheitsanforderungen an sich ändernde geschäftliche Anforderungen angepasst werden

3.2. Allgemeine Bedingungen

Der Standard für Informations- und Cybersicherheit darf nur unter Beachtung der Mitbestimmungsrechte der nationalen Arbeitnehmervertreter sowie der Bestimmungen des geltenden Arbeitsvertrags und der lokalen Gesetze (z. B. Datenschutzrecht) durchgesetzt werden.

Die diesem Standard unterliegenden Parteien sollten regelmäßig prüfen, ob Aktualisierungen des Standards (verfügbar unter [dekra.com/dekra.de](https://www.dekra.com/dekra.de)) vorgenommen wurden, um die Einhaltung aller geltenden Anforderungen sicherzustellen.

3.3. Überprüfung

Dieser Standard wird jährlich oder bei wesentlichen Änderungen der geltenden Vorschriften, Technologien oder geschäftlichen Anforderungen überprüft .

4. Allgemeines Informationssicherheitsmanagement

4.1. Vertragliche Anforderungen

Wenn eine externe Organisation Zugriff auf nicht öffentliche DEKRA-Informationen erhält oder ihr nicht öffentliche DEKRA-Informationen zur Verfügung gestellt werden, muss eine Geheimhaltungsvereinbarung (NDA) in den Vertrag aufgenommen werden, die für alle Mitarbeiter der externen Organisation gilt. Die NDA muss unterzeichnet werden, bevor der Zugriff gewährt wird. Dadurch wird die Vertraulichkeit der DEKRA-Daten gewährleistet.

Auch nach Beendigung der Dienstleistung oder Zusammenarbeit muss die Vertraulichkeit der erhaltenen Informationen vereinbart werden. Dies gilt auch für die Beendigung des Arbeitsverhältnisses einer Person, die bei der externen Organisation beschäftigt war und bei DEKRA eingesetzt wurde. Im Falle des Zugriffs auf unsere Systeme muss ein Verfahren für die Mitteilung der Beendigung des Arbeitsverhältnisses von Mitarbeitern der externen Organisation festgelegt werden. Hierzu ist die Rechtsabteilung von DEKRA zu konsultieren.



Wenn eine externe Organisation Subunternehmer für die Erbringung der mit DEKRA vereinbarten Dienstleistung beauftragt, muss dies DEKRA vor der Beauftragung des Subunternehmers gemeldet werden. Darüber hinaus muss die von DEKRA beauftragte externe Organisation, z. B. Lieferanten, sicherstellen, dass die Subunternehmer über die Bedingungen des Lieferantenvertrags mit DEKRA informiert werden und sich ebenfalls zu diesen Bedingungen verpflichten, um die Sicherheit und den Schutz der IT-Systeme und der darin bei DEKRA gespeicherten Daten zu gewährleisten. Die Subunternehmer müssen daher auch vom Lieferanten oder der externen Organisation an die DEKRA-Vertraulichkeitsvereinbarung (NDA) oder eine NDA eines Dritten mit allen DEKRA-Anforderungen gebunden werden.

Je nach erbrachter Dienstleistung müssen im Vertrag alle Sicherheitsanforderungen, die DEKRA zum Schutz ihrer Informationen definiert hat, schriftlich festgehalten werden. Diese Anforderungen werden vom DEKRA-Vertragsverantwortlichen bereitgestellt, der sicherstellen muss, dass externe Organisationen diesen Standard verstehen und einhalten.

4.2. Informationssicherheits-Managementsystem (ISMS)

DEKRA erwartet, dass die vertraglich gebundene externe Organisation, die DEKRA-Informationen verarbeitet, für Informations- und Cybersicherheit zertifiziert ist (z. B. nach ISO 27001, TISAX oder ISO 27017 usw.). Liegt keine Zertifizierung vor, muss sie über ein Informationssicherheits-Managementsystem verfügen, das auf den Normen ISO 27001 oder TISAX basiert, wenn sie auf DEKRA-Informationen oder -Systeme zugreifen soll. Mit diesen Standards für Informations- und Cybersicherheit wird ein risikobasierter Ansatz umgesetzt, um in regelmäßigen Abständen eine gründliche Analyse aller Informationen und Informationsverarbeitungssysteme durchzuführen. Als Ergebnis werden die Bedrohungen und Schwachstellen für die verarbeiteten Informationen erkannt und zeitnah durch zusätzliche Sicherheitsmaßnahmen behoben, um ein optimales Sicherheitsniveau in der Organisation zu gewährleisten.

4.3. Einhaltung des Informations- und Cybersicherheitsstandards

Dieser DEKRA-Standard für Informations- und Cybersicherheit muss in jeder vertraglich verbundenen externen Organisation eingehalten werden.

Beauftragt eine externe Organisation einen Unterauftragnehmer mit der Erbringung einer Software- oder Hardwaredienstleistung, muss die externe Organisation, die in einem Vertragsverhältnis mit DEKRA steht, sicherstellen, dass sich auch der Unterauftragnehmer zur Einhaltung des DEKRA-Standards für Informations- und Cybersicherheit verpflichtet.

DEKRA behält sich das Recht vor, im Rahmen der vertraglichen Vereinbarungen und der vereinbarten Allgemeinen Geschäftsbedingungen sowohl Mitarbeiter der externen Organisation als auch die externe Organisation selbst auf die Einhaltung der Vertraulichkeitsvereinbarung zu überprüfen. Darüber hinaus werden etwaige vorhandene Zertifikate für Informations- und Cybersicherheit abgefragt. Externe



Organisationen können im Rahmen von Compliance-Prüfungen Sicherheitsaudits unterzogen werden.

4.4. ISMS-Sensibilisierungs- und Sicherheitsschulungen

Die Mitarbeiter der externen Organisation müssen regelmäßig angemessene Schulungen und periodische Auffrischungen zum Thema erhalten.

4.5. Nutzung von DEKRA- und externen Ressourcen

Die Nutzung von DEKRA-Ressourcen darf ausschließlich für genehmigte geschäftliche Zwecke erfolgen; die private Nutzung von IT-Ressourcen ist nicht gestattet. Weitere Einzelheiten hierzu finden Sie im Kapitel „Physische Zugangskontrolle“.

Externe Geräte müssen den Sicherheitsanforderungen von DEKRA entsprechen.

Die externe Organisation darf nur erhaltenen Zugang zu DEKRA-Diensten dem „Need-to-know“-Prinzip und nach Unterzeichnung einer Geheimhaltungsvereinbarung .

Es muss sichergestellt werden, dass alle auf das heruntergeladenen Informationen externe Gerät entsprechend den Schutzanforderungen geschützt werden und dass vertraglich gewährleistet ist, dass externe Geräte auf dem neuesten Stand gehalten und mit Patches versehen werden.

Externe Nutzer müssen sicherstellen, dass alle auf dem gespeicherten Informationen externen Gerät bei Vertragsende wiederhergestellt und vollständig vom Gerät gelöscht werden.

4.6. Nichteinhaltung

Die Nichteinhaltung der DEKRA-Richtlinien und -Standards zur Informations- und Cybersicherheit oder das Versäumnis, angemessene Maßnahmen zum Schutz der Systeme, Daten, Informationen und Vermögenswerte zu ergreifen, kann rechtliche Schritte oder die Meldung an Aufsichtsbehörden, die Kündigung von Verträgen oder Vereinbarungen und/oder den Verlust zukünftiger Geschäftsmöglichkeiten zur Folge haben.

4.7. Umgang mit Ausnahmen

DEKRA muss über alle Ausnahmen oder Abweichungen von diesem Standard für Informations- und Cybersicherheit informiert werden. Diese müssen dokumentiert, begründet und von der zuständigen DEKRA-Abteilung genehmigt werden. Der detaillierte Prozess zur Behandlung von Ausnahmen kann beim lokalen DEKRA-Informationssicherheitsbeauftragten angefordert werden.

5. Einstufung von Informationen

Eine Klassifizierung dient dazu, einen angemessenen Schutz vertraulicher Informationen zu gewährleisten. Unabhängig von der Klassifizierung müssen auch die Integrität und die Richtigkeit der Datenklassifizierung geschützt werden. Die externe



Organisation muss ihre Richtlinie zur Informationsklassifizierung vorlegen, um diese mit der DEKRA-Richtlinie L1.P04-Information_Classification abzugleichen. Die zugewiesene Klassifizierung und die damit verbundenen Maßnahmen müssen je nach Sensibilität der Informationen befolgt werden. Informationen, die in verschiedenen Formaten vorliegen (z. B. gedruckte Dokumente, elektronische Sprachaufzeichnungen, elektronische Berichte), müssen unabhängig von ihrem Format dieselbe Klassifizierung aufweisen.

Bei DEKRA werden folgende Informationsklassen umgesetzt:

	Mögliches Schadenpotenzial durch unbefugte Offenlegung, Veränderung oder Vernichtung	Zugriffsbeschränkungen
Öffentlich	Keine	Keine Einschränkungen
Intern	Der potenzielle Schaden ist geringfügig, von kurzfristiger Natur und auf eine einzelne Einheit beschränkt. Geringfügiger Schaden. Informationen, deren unbefugte Änderung behoben werden kann, auch wenn sie für DEKRA geringfügige Verluste verursachen können. In Bezug auf personenbezogene Daten ist nicht zu erwarten, dass deren unsachgemäßer Umgang zu einer nennenswerten Beeinträchtigung der Rechte und Freiheiten natürlicher Personen führt.	Nur Dritte, die davon Kenntnis haben müssen. Andere unterliegen einer Vertraulichkeitsvereinbarung. Authentifizierter Zugriff erforderlich. Rollenbasierte Zugriffskontrolle (RBAC)
Vertraulich	Das Schadenspotenzial ist beträchtlich, mittelfristiger Natur oder nicht auf ein einzelnes Unternehmen beschränkt. Hoher Schaden. Informations , deren unbefugte Änderung schwer zu beheben ist und zu erheblichen Verlusten für DEKRA führen kann. Bei personenbezogenen Daten (PII) könnte eine unsachgemäße Handhabung das soziale Ansehen oder die wirtschaftliche Lage der betroffenen Person erheblich beeinträchtigen.	Nur eine eingeschränkte (oder begrenzte) Gruppe von Dritten (Need-to-know- t durchgesetzt) (kann vertrauenswürdige Systemadministratoren einschließen), bei personenbezogenen Daten nur namentlich genannte Personen mit Kenntnisbedarf. Es sind mindestens zwei Formen der Identitätsprüfung erforderlich (MFA).



Streng vertraulich	Das Schadenspotenzial bedroht die Existenz des Unternehmens, ist langfristiger Natur oder beschränkt sich nicht auf ein einzelnes Unternehmen. Sehr hoher Schaden. Informationen, deren unbefugte Änderung nicht behoben werden kann, die jedoch DEKRA schwerwiegende Verluste verursachen. In Bezug auf personenbezogene Daten könnte ein unsachgemäßer Umgang das soziale Ansehen oder die wirtschaftliche Lage der betroffenen Person erheblich beeinträchtigen oder deren Gesundheit, Leben oder Freiheit gefährden.	Nur namentlich benannte Personen, eingeschränkte Nutzung. Mindestens zwei Formen der Identitätsprüfung sind erforderlich (MFA) Ausdrückliche Genehmigung der Geschäftsleitung für den Zugriff Durchsetzung der Aufgabentrennung
Geheim	Das Schadenspotenzial bedroht die Existenz oder lebenswichtige Interessen der Regierung. Schwerwiegender Schaden. Es handelt sich um die sensibelste Einstufung von Informationen	Nur von der Regierung autorisierte Dritten (ausschließlich namentlich benannte Personen). Es sind mindestens zwei Formen der Identitätsprüfung erforderlich (MFA). Vier-Augen-Prinzip. Just-in-Time-Zugriff mit automatischer Sperrung.

Das unbefugte Kopieren, Weiterleiten oder Verwenden von Informationen ist strengstens untersagt

5.1. Kennzeichnung

Eine ordnungsgemäße Kennzeichnung ist eine Voraussetzung für den sicheren Umgang mit Informationen. Informationen müssen daher entsprechend ihrer Vertraulichkeitsstufe gekennzeichnet werden.

Eine korrekte Kennzeichnung ist besonders wichtig, wenn Informationen der Geheimhaltungsstufen C „onfidential“, S „trictly C“ „onfidential“ oder „Classified“ zwischen Unternehmen (z. B. an Partnerunternehmen und Lieferanten) übermittelt werden, unabhängig davon, ob es sich um digitale oder gedruckte Informationen handelt.

Sind die vom -Kunden bereitgestellten Informationen nicht gekennzeichnet oder beschriftet, kennzeichnet DEKRA diese Informationen mindestens als „C onfidential“.oder „Classified“ . Je nach geschäftlichen Anforderungen, vertraglichen Verpflichtungen oder Risikobewertung können solche Informationen als eingestuft werden „Strictly Confidential“



die Informationen Sind von anderen Dritten als Kunden bereitgestellten nicht gekennzeichnet oder beschriftet, kennzeichnet DEKRA diese Informationen als „Internal“.

5.2. Umgang mit Informationen

DEKRA behandelt Informationen entsprechend der folgenden Klassifizierung:

Einstufung	Kennzeichnung	Ruhende Daten*	Daten während der Übertragung*	Entsorgung
Öffentlich	Neine/optional (z. B. Hinweis im Impressum)	Elektronische Daten: Keine Einschränkungen. Speicherung auf zugelassenen Plattformen Grundlegende Protokollierung von Inhaltsänderungen Papierdaten: Keine Einschränkungen	Elektronische Daten: Keine Einschränkungen Papierdaten: Keine Einschränkungen	Elektronische Löschung: Keine Einschränkungen Physische Entsorgung: Keine Einschränkungen
Intern	Geben Sie die Vertraulichkeitsstufe in der Landessprache oder auf Englisch an bzw. vermerken Sie auf jeder Seite des Dokuments in elektronischer und gedruckter Form „Internal“	Elektronische Daten: Zugriff auf externe Server eingeschränkt Speicherung ausschließlich auf von der Organisation genehmigten Systemen Sicherung gemäß den Richtlinien Papierdaten: Sollten bei Nichtgebrauch in einem verschlossenen Aufbewahrungsort aufbewahrt werden	Elektronische Daten: Verschlüsselt in externen Netzwerken Papierdaten: Externer Transport nur in verschlossenen Umschlägen	Elektronische Löschung: Sichere Löschung durch Überschreiben des Datenträgers mit mindestens einem Schreibdurchgang mit einem festen Datenwert, z. B. ausschließlich Nullen. ODER Vom Sicherheitsteam zugelassenes Entmagnetisierungsgerät für magnetische Speichermedien (gemäß NIST SP 800-88) Physische Entsorgung: Verfahren gemäß ISO 21964-2, mindestens Schutzklasse 1 und Sicherheitsstufe 2
Vertraulich	Geben Sie die Vertraulichkeitsstufe in der	Elektronische Daten: Grundsätzlich zugangsbeschränkt	Elektronische Daten: stets verschlüsselt	Elektronische Löschung: Sichere Löschung durch



	Landessprache oder auf Englisch an bzw. vermerken Sie „Confidential“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form	Verschlüsselung im Ruhezustand erforderlich Datenmaskierung oder Schwärzung, soweit möglich Zugriffsprotokollierung aktiviert und überprüft Papierdaten: Unter Verschluss zu halten, wenn sie nicht direkt genutzt oder beaufsichtigt werden; dürfen nicht an öffentlichen Orten ausliegen	Nur zugelassene sichere Kanäle. Mündliche Gespräche an öffentlichen Orten oder über unsichere Kanäle sind nicht gestattet, einschließlich der Hinterlassung von Nachrichten auf Anrufbeantwortern oder ähnlichen Geräten Zugriffsprotokollierung aktiviert und überprüft Daten in Papierform: Nur in ordnungsgemäß verschlossenen Umschlägen	Überschreiben der Datenträger mit mindestens einem Durchgang mit einem festen Datenwert, z. B. ausschließlich Nullen. ODER Vom Sicherheitsteam zugelassenes Entmagnetisierungsgerät für magnetische Speichermedien (gemäß NIST SP 800-88) Physische Entsorgung: Verfahren gemäß ISO 21964-2, mindestens Schutzklasse 2 und Sicherheitsstufe 5
Streng vertraulich	Geben Sie den Vertraulichkeitsgrad in der Landessprache oder auf Englisch an bzw. vermerken Sie „Strictly Confidential“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form	Elektronische Daten: Grundsätzlich zugangsbeschränkte, individuell verschlüsselte Dateien, Nachrichten oder Datenbanken; Speicherung auf physisch ungesicherten Geräten (Cloud, mobile Datenspeicher, Laptop, Smartphone) nur, wenn dies namentlich ausdrücklich gestattet ist Speicherung beschränkt auf gehärtete, überwachte Umgebungen. Keine lokale Speicherung, sofern nicht ausdrücklich genehmigt Papierdaten: Unter Verschluss, wenn sie nicht direkt genutzt oder beaufsichtigt werden; Standortbeschränkung; dürfen nicht an	Elektronische Daten: Ende-zu-Ende-verschlüsselt Übertragungsvereinbarungen müssen getroffen und eingehalten werden. Verbot unsicherer Kommunikationskanäle Mündliche Gespräche an öffentlichen Orten oder über unsichere Kanäle sind nicht gestattet, einschließlich der Hinterlassung von Nachrichten auf Anrufbeantwortern oder ähnlichen Geräten Verstärkte Überwachung und Warnmeldungen	Elektronische Löschung: Sichere Löschung durch Überschreiben der Datenträger mit mindestens einem Schreibdurchgang mit einem festen Datenwert, z. B. ausschließlich Nullen. ODER Vom Sicherheitsteam zugelassenes Entmagnetisierungsgerät für magnetische Speichermedien (gemäß NIST SP 800-88) Physische Entsorgung: Verfahren gemäß ISO/IEC 21964-1:2018-08, mindestens Schutzklasse 3 und Sicherheitsstufe 6



		öffentlichen Orten verwendet werden	Regelmäßige Neuzertifizierung der Zugriffsrechte Daten in Papierform: Ausschließlich spezieller Kurierdienst Führen Sie interne Protokolle mit Angaben zu Inhalt, autorisiertem Empfänger, Zeitpunkt der Übergabe und Zeitpunkt des Empfangs Übertragungsvereinbarungen müssen erstellt und gepflegt werden	
Vertraulich	Geben Sie die Vertraulichkeitsstufe in der Landessprache oder auf Englisch an bzw. kennzeichnen Sie „Classified“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form	Elektronische Daten: Zugriffsbeschränkte, <u>individuell</u> verschlüsselte Dateien, Nachrichten oder Datenbanken; die Speicherung auf physisch ungesicherten Geräten (Cloud, mobile Datenspeicher, Laptop, Smartphone) ist verboten. Isolierte oder getrennte Umgebungen Hardware-Sicherheitsmodule (HSMs), sofern zutreffend Keine Replikation, sofern nicht ausdrücklich genehmigt Kontinuierliche Überwachung und Echtzeit-Warnmeldungen	Elektronische Daten: Durchgehend verschlüsselt, enthalten nur die unbedingt erforderlichen Informationen, und die „-Übertragung muss protokolliert werden – wann und von wem Zusätzliche Out-of-Band-Überprüfung der Empfänger Übertragungsvereinbarungen müssen getroffen und eingehalten werden Mündliche Gespräche an öffentlichen Orten oder über unsichere Kanäle sind nicht gestattet,	Elektronische Löschung: Sichere Löschung durch Überschreiben der Datenträger mit mindestens einem Durchgang mit einem festen Datenwert, z. B. lauter Nullen. ODER Vom Sicherheitsteam zugelassenes Entmagnetisierungsgerät für magnetische Speichermedien (gemäß NIST SP 800-88 Rev. 1). Überprüfung der Löschung, entweder am Ende des Vorgangs oder nach jedem Überschreibdurchgang, um



		Unabhängige, vor Manipulation geschützte Audit-Protokollierung Papierdaten: Unter Verschluss, wenn sie nicht direkt genutzt oder beaufsichtigt werden; an bestimmten Orten aufbewahrt; dürfen nicht an öffentlichen Orten verwendet werden	einschließlich der Hinterlassung von Nachrichten auf Anrufbeantwortern oder ähnlichen Geräten. Bei mündlichen Gesprächen müssen angemessene Raumkontrollen eingehalten werden. Kontinuierliche Überwachung und Echtzeit-Warmmeldungen Daten in Papierform: Ausschließlich Spezialkurierdienst, keine Kennzeichnung auf dem äußeren Umschlag und keine Empfangsbestätigung Führen Sie interne Protokolle mit Angaben zu Inhalt, autorisiertem Empfänger, Zeitpunkt der Übergabe und Zeitpunkt des Empfangs Übergabevereinbarungen müssen getroffen und eingehalten werden	sicherzustellen, dass Physische Entsorgung: Verfahren gemäß ISO/IEC 21964-1:2018-08, mindestens Schutzklasse 3 und Sicherheitsstufe 7; Schütteln der Säcke mit geschreddertem Material, um den Inhalt zu vermischen
	*Ausnahmen sind möglich, sofern eine Risikoakzeptanzerklärung vom Geschäftsinhaber und Geschäftsführer unterzeichnet und von der Abteilung für Informations- und Cybersicherheit genehmigt wurde			

Die Aufbewahrungsfrist muss festgelegt, mit dem Geschäftsinhaber abgestimmt und auf der Grundlage der geschäftlichen Anforderungen dokumentiert werden.



6. Sicherheitskontrollmaßnahmen

6.1. Physische Zugangskontrolle

DEKRA-Informationen, die von externen Organisationen gespeichert oder verarbeitet werden, müssen so verwendet werden, dass keine unbefugte Person diese Daten einsehen oder darauf zugreifen kann. Vertrauliche, Strictly C-Confidential- und Classified-Dokumente dürfen niemals unbeaufsichtigt gelassen werden, um den Zugriff durch unbefugte Personen zu verhindern.

Gleiches gilt für DEKRA-IT-Geräte oder -Systeme, die von externen Organisationen genutzt werden. Die bereitgestellten Geräte müssen ordnungsgemäß behandelt und vor Verlust oder unbefugten Veränderungen geschützt werden. Bei der Nutzung mobiler Systeme sind besondere Sicherheitsmaßnahmen erforderlich.

Alle externen Organisationen, die das DEKRA-Gebäude betreten, müssen sich ordnungsgemäß mit einem Ausweis ausweisen.

Das Betreten oder der Aufenthalt im DEKRA-Gebäude ohne Begleitung von befugtem Personal, insbesondere in für Außenstehende zugangsbeschränkten Bereichen, ist nicht gestattet, es sei denn, die betreffenden Personen werden von befugtem DEKRA-Personal begleitet und haben die Vertraulichkeitsvereinbarung unterzeichnet.

Die Außentür zum allgemeinen Lager dient ausschließlich dem Ein- und Ausgang von Waren; die Nutzung durch Kunden oder andere externe Personen ist nicht gestattet. Das externe Personal der Transportunternehmen hat ausschließlich für administrative Vorgänge Zugang zum Lagerbüro.

Drittunternehmen müssen an ihren Standorten über eine angemessene Gebäudesicherheit und ein geregeltes Besuchermanagementsystem verfügen.

6.2. Zugangskontrolle

Um eine unbefugte Nutzung der internen Verarbeitungssysteme von DEKRA oder der mit diesen internen Systemen verbundenen externen Systeme zu verhindern, müssen die folgenden Anforderungen erfüllt sein:

- Die Registrierung im Netzwerk bzw. auf dem PC ist nur mit einem gültigen Konto möglich; die Benutzeridentifikation ist personengebunden. Alle externen Benutzer müssen eindeutig identifiziert werden; die gemeinsame Nutzung von Konten ist untersagt.
- Die Nutzung einer Benutzer-ID oder eines Kontos einer anderen Person ist nicht gestattet.
- Die Weitergabe von Identifikationsmitteln (z. B. SmartCards oder SecurID-Karten) ist nicht gestattet.
- Die Verwendung eines individuellen und sicheren Passworts ist gewährleistet.
 - Passwörter oder PINs einer für den persönlichen Gebrauch bestimmten Benutzer-ID werden als „persönliche Benutzer-ID“ bezeichnet und



müssen streng vertraulich behandelt und dürfen nicht weitergegeben werden.

- Das Speichern oder Aufschreiben von Passwörtern (z. B. auf Papier, über mobile Geräte oder in Dateien) ist nicht gestattet, es sei denn, dies wird als sichere Methode angegeben.
- Bei Verdacht, dass ein Passwort oder eine PIN kompromittiert wurde oder bekannt geworden ist, muss es/sie umgehend gemeldet werden unverzüglich geändert und als Vorfall der Informationssicherheit an .
- Temporäre Passwörter (z. B. für neue Konten) müssen bei der ersten Anmeldung geändert werden.
- Alle Passwörter oder PINs müssen bei der ersten Verwendung und spätestens nach drei Monaten unter ; bei giltgeändert werden Passwörtern .
- Das Ausspähen von Passwörtern ist nicht gestattet.
- Passwörter sind mindestens als Confidential einzustufen.
- Verwenden Sie kein identisches Passwort für private und berufliche Zwecke.
- Die vom System vorgeschriebene Mindestlänge für Passwörter muss eingehalten werden. Sie richtet sich nach den Vorgaben der entsprechenden Richtlinie.
- Triviale Passwörter (z. B. „Test123456“) oder Passwörter mit persönlichem Bezug (z. B. Name, Geburtsdatum) sind nicht zulässig.
- Wenn bestimmte Systeme oder Anwendungen komplexere Passwörter erfordern , wie in der Richtlinie L2.S15-Secure_Password_Handling definiert, müssen diese Anforderungen erfüllt werden.
- Auf allen Clients/PCs ist ein Bildschirmschoner installiert, der ein Passwort erfordert, um das System wieder zu aktivieren.
- Es ist sicherzustellen, dass die zur Nutzung eines automatisierten Verarbeitungssystems Berechtigten nur Zugriff auf die Daten haben, die unter ihre Zugriffsberechtigung fallen.
- Zugriffsrechte und Rollen werden nach dem „Need-to-know“-Prinzip vergeben, wobei die jeweiligen Berechtigungen gemäß dem („Least-Privilege“-Prinzip) auf die jeweilige Rolle zugeschnitten sind.
- Die Zugriffs- und Verwaltungsrechte für PCs und/oder Server sind genau dokumentiert.
- Nicht mehr benötigte Berechtigungen werden im Rahmen eines Benutzeridentitätsmanagementsystems umgehend entzogen.
- Der Zugriff auf die PC-/Serverumgebung von außen ist nur über eine verschlüsselte Kommunikations über den DEKRA Corporate VPN-Tunnel möglich.
- Beim Zugriff auf interne, vertrauliche, streng vertrauliche oder geheime Informationen muss bei externen Konten eine Multi-Faktor-Authentifizierung verwendet werden.



- Für Benutzer- und technische Benutzerkonten muss ein Passwortschutz durchgesetzt werden.

6.3. Benutzerzugriffskontrolle

Die geschäftlichen Anforderungen für den Zugriff auf DEKRA-Informationssysteme müssen vor ihrer Genehmigung definiert und dokumentiert werden. Die Zugriffsanforderungen basieren auf den geschäftlichen Anforderungen.

Der Informationsverantwortliche und der Systemverantwortliche genehmigen den Zugriff auf Daten und IT-Dienste gemäß den geschäftlichen Anforderungen und Sicherheitsvorgaben. Die Informationssysteme von DEKRA werden ausschließlich für genehmigte geschäftliche Zwecke genutzt, sofern nichts anderes vereinbart ist. Alle relevanten Sicherheitsvorfälle werden dokumentiert, einschließlich einer Aufzeichnung erfolgreicher und erfolgloser Anmeldeversuche.

Der physische und logische Zugriff auf C onfidential und I nternal Informationen sowie auf Datenverarbeitungssysteme ist geregelt. Um ein angemessenes Zugriffsniveau zu gewährleisten, werden vom zuständigen Informationssicherheitsbeauftragten verschiedene Sicherheitsmaßnahmen festgelegt.

6.4. Trennungskontrolle

Falls externe Organisationen auch mit anderen Kunden zusammenarbeiten, ist die Trennung in einer Multi-Tenant-Architektur gemäß den DEKRA-Anforderungen logisch und physisch gewährleistet.

Auf der Grundlage einer Risikobewertung muss eine Systemtrennung für Test- und Produktionsumgebung implementiert werden.

6.5. Daten e Medienkontrolle

Datenträger (wie CDs, DVDs, USB-Sticks und Festplatten) müssen vor Verlust, Zerstörung und Verwechslung sowie vor unbefugtem Zugriff geschützt werden.

Nicht mehr benötigte Datenträger müssen gemäß den Beschreibungen im Kapitel „Umgang mit Informations “ sicher entsorgt werden. Der Transport von Datenträgern mit personenbezogenen Daten zu einem zertifizierten Aktenvernichtungsunternehmen darf nur in geschlossenen Behältern und in geschlossenen Fahrzeugen erfolgen, damit kein Material verloren gehen kann, und nur nach schriftlicher Genehmigung durch DEKRA.

6.6. Transport skontrolle

Bei der Übertragung von Informationen müssen die Vertraulichkeit und Integrität der Daten gewährleistet sein.

Der Datenverkehr, bei dem personenbezogene Daten übertragen werden (z. B. E-Mail, Webzugriff), wird verschlüsselt. Datenübertragungen werden verschlüsselt (z. B. S-FTP,



DEKRA Corporate VPN). Die unbefugte Weitergabe oder Übertragung von Daten ist nicht gestattet.

Faxnummern und E-Mail-Adressen sind aus aktuellen Verzeichnissen zu entnehmen oder beim Empfänger anzufordern, um fehlerhafte Übermittlungen zu vermeiden. Der Absender ist für den Inhalt und die Verteilung einer E-Mail verantwortlich. Der Empfänger ist für die weitere Verarbeitung und Verteilung verantwortlich. Das Erstellen und Versenden von Ketten-E-Mails ist nicht gestattet.

Bei allen Gesprächen (einschließlich Telefonaten, Video- und Webkonferenzen), die Confidential-, Strictly Confidential- oder Classified-Informationen betreffen oder enthalten, muss sichergestellt werden, dass diese Informationen nicht unbefugt mitgehört oder aufgezeichnet werden können.

Eine Weitergabe von Informationen darf ausschließlich gemäß den jeweiligen vertraglichen Vereinbarungen erfolgen. Diese Weitergabe muss zudem protokolliert werden. Das Netzwerk bzw. die PCs sind durch ein Firewall-System vor unbefugtem Zugriff von außen sowie durch ein Zonenkonzept zur Perimetersicherheit geschützt. Es muss sichergestellt werden, dass die Informationen auf dem neuesten Stand sind.

6.7. Sicherheit der System

Informationen sollten vor versehentlicher oder vorsätzlicher Offenlegung, Änderung oder Vernichtung geschützt werden.

Es müssen Maßnahmen wie die Protokollierung umgesetzt werden, die im Nachhinein überprüft und feststellt, ob und von wem Informationen in Datenverarbeitungssysteme eingegeben, geändert oder daraus entfernt wurden.

Es muss sichergestellt werden, dass gespeicherte Informationen nicht durch Systemstörungen beschädigt werden können. Der Status der Systeme wird kontinuierlich und automatisch überwacht, um Störungen frühzeitig zu erkennen. Zudem müssen regelmäßige Wartungsmaßnahmen festgelegt werden, um die Integrität von z. B. Datenbanken zu überprüfen. Es müssen Schwachstellen-Scans durchgeführt werden. Nur autorisiertes und qualifiziertes Personal darf während des Änderungsprozesses Änderungen an den Systemen vornehmen und Störungen beheben.

Die Sicherheitsanforderungen an ein Informationssystem gelten über den gesamten Lebenszyklus hinweg, und die Verantwortung für deren Einhaltung liegt bei der zuständigen Unternehmensleitung. Die Einführung neuer Technologien darf das Sicherheitsniveau von DEKRA nicht gefährden.

6.8. Verfügbarkeitskontrolle

Informationen und Dienste müssen bei Bedarf stets verfügbar sein – durch ordnungsgemäße Archivierung, den Einsatz eines Virenschutzkonzepts, eine unterbrechungsfreie Stromversorgung sowie ein geeignetes Backup- und Wiederherstellungskonzept.



Die Verantwortlichen für Informationssysteme entwickeln, pflegen und testen regelmäßig Pläne, um den Betrieb kritischer Informationssysteme gemäß regulatorischen, vertraglichen oder sonstigen geschäftlichen Anforderungen aufrechtzuerhalten.

6.9. Sicherheitsvorfälle

Jeder bestätigte Sicherheitsvorfall, jede Datenpanne oder jeder Verstoß gegen Richtlinien bei „ “ muss unverzüglich dem folgenden Empfänger sowie der zuständigen DEKRA-Rechtsperson gemeldet werden:

Information.security@dekra.com

Bei allen anderen juristischen Personen ist unverzüglich der DEKRA-Geschäftsführer für den „ zuständige Bereich “ zu benachrichtigen.

Alle Mitarbeiter der externen Organisation und aller Subunternehmer müssen über das Verfahren zur Meldung von Sicherheitsvorfällen informiert werden.

Externe Organisationen müssen bei der Untersuchung und Behebung von Vorfällen uneingeschränkt kooperieren.

Der zuständige lokale DEKRA-Informationssicherheitsbeauftragte überprüft regelmäßig die gemeldeten Sicherheitsvorfälle unter , gibt Rückmeldung und bezieht die Verantwortlichen so früh wie möglich ein.

7. Zulässige und unzulässige Nutzung durch Lieferanten und deren Mitarbeiter

7.1. Zulässige Nutzung

DEKRA-Ressourcen dürfen ausschließlich für ethische und rechtmäßige Aktivitäten genutzt werden, nicht jedoch für unethische oder illegale Aktivitäten, darunter unter anderem:

- Das vorsätzliche Erstellen, Herunterladen, Ansehen, Speichern, Kopieren oder Übertragen von sexuell explizitem, sexuell orientiertem, Glücksspiel- oder Hassmaterial ist nicht gestattet.
- Die vorsätzliche Erstellung, das Herunterladen, das Ansehen, die Speicherung, das Kopieren oder die Übertragung von Materialien im Zusammenhang mit Glücksspiel, illegalen Waffen, terroristischen Aktivitäten und sonstigen illegalen oder anderweitig verbotenen Aktivitäten ist nicht gestattet.
- Der unbefugte Erwerb, die unbefugte Nutzung, Vervielfältigung, Übertragung oder Verbreitung von durch DEKRA als vertraulich definierten Informationen.
-



7.2. Unzulässige Nutzung

Die nachstehende Auflistung erhebt keinen Anspruch auf Vollständigkeit, soll jedoch einen Rahmen für Aktivitäten bieten, die unter die Kategorie der unzulässigen Nutzung fallen.

- Verstöße gegen die Rechte von Personen oder Unternehmen, die durch Urheberrecht, Geschäftsgeheimnisse, Patente oder anderes geistiges Eigentum sowie ähnliche Gesetze oder Vorschriften geschützt sind, einschließlich, aber nicht beschränkt auf die Installation oder den Vertrieb von „Raubkopien“ oder anderen Softwareprodukten, für deren Nutzung durch DEKRA keine ordnungsgemäße Lizenz vorliegt.
- Unbefugte NutzungInhalte, einschließlich, aber nicht beschränkt auf die Digitalisierung und Verbreitung von Fotos aus Zeitschriften, Büchern oder anderen urheberrechtlich geschützten Quellen, urheberrechtlich geschützter Musik sowie die Installation jeglicher urheberrechtlich geschützter Software, für die DEKRA oder der Endnutzer keine gültige Lizenz besitzt.urheberrechtlich geschützter
- Der Zugriff auf Daten, einen Server oder ein Konto zu anderen Zwecken als der Ausübung der Geschäftstätigkeit von DEKRA ist untersagt, selbst wenn Mitarbeiter des Lieferanten über eine Zugriffsberechtigung verfügen.
- Der Export von Software, technischen Informationen, Verschlüsselungssoftware oder -technologie, der gegen internationale oder regionale Exportkontrollgesetze verstößt, ist unzulässig, sofern er nicht ausdrücklich von DEKRA genehmigt wurde.
- Das Einschleusen von Schadprogrammen in das Netzwerk oder auf den Server.
- Die Weitergabe des Passworts für das Konto von Lieferantenmitarbeitern an Dritte oder die Erlaubnis zur Nutzung des Kontos von Lieferantenmitarbeitern durch Dritte. Dies schließt Kollegen, Freunde, Familienangehörige und andere Haushaltsmitglieder ein, wenn von zu Hause aus gearbeitet wird.
- Die Weitergabe von Informationen über oder Listen von DEKRA-Mitarbeitern an Dritte außerhalb von DEKRAUnbefugte .
- Durchführung jeglicher Form der Netzwerküberwachung, durch die Daten abgefangen werden, die nicht für den Host des Lieferantenpersonals bestimmt sind, es sei denn, diese Tätigkeit ist Teil der normalen Arbeit/Aufgaben des Lieferantenpersonals.
- Die Umgehung der Benutzerauthentifizierung oder der Sicherheit eines Hosts, Netzwerks oder Kontos.
- Das Einrichten von Honey pots, Honeynets oder ähnlichen Technologien im DEKRA-Netzwerk.
- Verursachen von Sicherheitsverletzungen oder Störungen der Netzwerkkommunikation. Zu den Sicherheitsverletzungen zählen unter anderem der Zugriff auf Daten, für die das Personal des Lieferanten nicht der vorgesehene Empfänger ist, oder die Anmeldung bei einem Server oder Konto,



das das Personal des Lieferanten , fürnicht ausdrücklich autorisiert es sei denn, diese Tätigkeiten fallen in den Rahmen der regulären Aufgaben. ist

- Das Versenden unaufgeforderter E-Mail-Nachrichten oder anderer Werbematerialien an Personen, die solche Materialien nicht ausdrücklich angefordert haben (E-Mail-Spam).
- Jede Form der Belästigung per E-Mail, Telefon oder Pager, sei es durch die Wortwahl, die Häufigkeit oder den Umfang der Nachrichten.
- Die unbefugte Nutzung oder Fälschung von E-Mail-Kopfzeileninformationen.
- Das wissentliche Erstellen, Herunterladen, Hochladen, Anzeigen oder Aufrufen von Websites, die Pornografie oder anderes „unangemessenes“ Material enthalten, das als illegal, obszön oder anstößig angesehen werden kann.
- Die Anmeldung bei, der Zugriff auf oder die Nutzung von Peer-to-Peer-Netzwerken sowie die Installation von Software, die den Austausch von Musik-, Video- oder Bilddateien ermöglicht.
- Die Anmeldung bei, der Zugriff auf oder die Nutzung von Echtzeit-Chat-Diensten, wie z. B. Chatrooms, SMS- oder Pager-Diensten.
- Sich bei Online-Glücksspiel- oder Wettseiten anzumelden, diese zu besuchen oder zu nutzen.
- Sich bei „Geldverdien“-Websites anzumelden oder diese zu besuchen oder „Geldverdien“-Programme zu nutzen.
- Ein privates Unternehmen zu betreiben.
- Das Herunterladen von Software, die nicht dem DEKRA-Software-Standard entspricht.

8. Dokumentenlenkung

Besitzer des Dokuments	Beauftragter für Informationssicherheit
Erstellt von	Prerna Walhekar
Rezensiert von	Inmaculada Nuñez
Rezensiert am	2026.09.07
Genehmigt durch	Dražen Morog
Genehmigt am	2026.09.22
Version	1.7DE

9. Versionsverlauf

Datum	Version	Name des Herausgebers	Revision
2020.10.26	0.1	Prerna Walhekar	Erste übersetzte Fassung
2020.10.27	1.0	Prerna Walhekar	Endgültige Fassung



2021.01.22	1.1	Prerna Walhekar	DEKRA-Umfangskorrektur
2021.11.24	1.2	Mabel Gonzalez und Prerna Walhekar	Neue Anforderungen an die Kündigung in Kapitel 3.1, Anforderungen an die physische Sicherheit in Kapitel 5.1 sowie geringfügige Änderungen Geringfügige Änderungen in Kapitel 3.2 bezüglich der Zertifizierung und in Kapitel 5.9 bezüglich der E-Mail-Adressen
2023.01.26	1.3	Mabel Gonzalez	Eine neue Informationsklasse wurde in Kapitel 4 aufgenommen In Kapitel 3.4 wurde eine obligatorische Sicherheitsschulung für Mitarbeiter externer Organisationen aufgenommen. Anpassung der Richtlinie an die neue Klassifizierungskategorie und geringfügige Änderungen Änderung der Kennzeichnung dieses Dokuments von „Intern“ in „Öffentlich“ Das Kapitel „Dokumentenverweise“ wurde gestrichen, da es interne Verweise gab
2023.10.05	1.4	Mabel Gonzalez	Anpassung an L1.P04 für die Zugriffsbeschränkungen in der Klasse „Vertrauliche Informationen“ Anpassung an das neue Design und die neue Typografie
2024.04.29	1.5	Mabel Gonzalez	Geringfügige Änderungen am Namen des DEKRA-Teams. Die Anforderung zur Unterzeichnung einer Vertraulichkeitsvereinbarung (NDA) wurde in <i>das Kapitel „Geltungsbereich“</i> aufgenommen, um alle weiteren erforderlichen Richtlinien oder Standards zu berücksichtigen. Anpassung an L1.P04 hinsichtlich der Zugriffsbeschränkungen für die Klasse „Vertrauliche Informationen“ und der Festlegung der Aufbewahrungsfristen im <i>Kapitel „Umgang mit Informationen“</i> Erhöhung der Geheimhaltungsstufe für Informationen, die von externen



			Organisationen bereitgestellt werden, im <i>Kapitel „Kennzeichnung“</i> Neue Anforderung (Passwortschutz) für technische Konten im <i>Kapitel „Zugriffskontrolle“</i> Anforderung einer schriftlichen Genehmigung für die Entsorgung von Informationen über Dienste Dritter im <i>Kapitel „Kontrolle von Datenträgern“</i> Die Offenlegung ist ebenfalls beim Schutz von Informationen im <i>Kapitel „Systemsicherheit“</i> berücksichtigt Die Liste der Empfänger für deutsche DEKRA-Rechtsträger wurde aktualisiert, und im <i>Kapitel „Sicherheitsvorfälle“</i> wurde ein Link zur DEKRA-Webseite eingefügt, auf der diese Informationen gespeichert sind.
2025.07.09	1.6	Mabel Gonzalez	Ein neues Kapitel <i>„Überprüfung“</i> wurde aufgenommen Je nach erbrachter Dienstleistung müssen alle Sicherheitsanforderungen schriftlich in den Verträgen im Kapitel <i>„Vertragliche Anforderungen“</i> festgehalten werden Externe Organisationen können im Rahmen von Compliance-Prüfungen im Kapitel <i>„Einhaltung der Standards für Informations- und Cybersicherheit“</i> Sicherheitsaudits unterzogen werden Das neue Kapitel <i>„Nutzung von DEKRA-/externen Ressourcen“</i> wurde aufgenommen Im Kapitel <i>„Nichteinhaltung“</i> wurden neue Maßnahmen aufgenommen: Meldung an Aufsichtsbehörden, Kündigung von Verträgen oder Vereinbarungen und/oder Verlust zukünftiger Geschäftsmöglichkeiten Verbotene Nutzung von Informationen im Kapitel <i>„Informationsklassifizierung“</i> Gemeinsam genutzte Konten sind im Kapitel <i>„Zugriffskontrolle“</i> nicht zulässig.



			Klarstellung zur Nutzung des VPN: Es muss sich um das Unternehmens-VPN von DEKRA handeln. Die Liste der Empfänger für deutsche DEKRA-Rechtsträger wurde gestrichen; im Kapitel „<i>Sicherheitsvorfälle</i>“ wird die uneingeschränkte Zusammenarbeit bei der Untersuchung und Behebung von Vorfällen sowie die unverzügliche Meldung im Falle eines Sicherheitsvorfalls gefordert
2026.09.07	1.7	Mabel Gonzalez Inmaculada Nuñez Carsten Eisenmann	Die Dokumentstruktur wird geändert, um sie an die neuen Kapitel anzupassen Ein neues Kapitel „<i>Zweck und Geltungsbereich</i>“ wurde hinzugefügt Das Kapitel „<i>Einleitung</i>“ wurde in „<i>Ziele und Grundsätze</i>“ umbenannt Die Anforderungen im Kapitel „<i>ISMS-Sensibilisierung und Sicherheitsschulungen</i>“ wurden geändert Bestehende Anforderungen wurden in die Kapitel „<i>Allgemeine Bedingungen</i>“, „<i>Einstufung von Informationen</i>“, „<i>Kennzeichnung</i>“ und „<i>Umgang mit Informationen</i>“ aufgenommen Das Kapitel „<i>Nutzung von DEKRA- und externen Ressourcen</i>“ () enthält nun die Anforderungen aus L2.S29 – „<i>Benutzerendgeräte und Remote-Arbeit</i>“ Kapitel „<i>Zulässige und unzulässige Nutzung durch Lieferanten und deren Mitarbeiter</i>“ wurde aus L2.S11 „Lieferantenmanagement“ verschoben Geringfügige Änderungen
2026.09.07	1.7DE	Inmaculada Nuñez	Überarbeitung der Übersetzung der genehmigten Norm

DEKRA SE

Global Information and Cyber Security – CISO

Handwerkstraße 15

70565 Stuttgart

Telefon +49.711.7861-0

Information.security@dekra.com