Information Security Standard
Informationssicherheit für Externe

DEKRA

Alles im grünen Bereich.

Inhaltsverzeichnis

1. Einführung

Es ist das Sicherheitsziel der DEKRA, dass Informationen aller Art - geschrieben, gesprochen, elektronisch erfasst oder gedruckt - gegen zufällige oder vorsätzliche unbefugte Änderung, Zerstörung oder Offenlegung über den gesamten Lebenszyklus geschützt werden. Die Schutzmaßnahmen für die Systeme und Programme, mit denen diese Informationen verarbeitet, übertragen und gespeichert werden müssen einem angemessenen Schutzniveau entsprechen.

1.1. Sicherheitsprinzipien

- Unsere Geschäftsprozesse und unser Know-how sollen geschützt werden
- Unsere Sicherheitsmaßnahmen werden die Risiken für das Unternehmen reduzieren.
- Unsere Sicherheitsmaßnahmen entsprechen dem Industriestandard.
- Jeder Einzelne ist in seinem Bereich verantwortlich für die Sicherheit unserer Informationen, Anlagen und Systeme.
- Wir werden eine klare Trennung der Verantwortlichkeiten implementieren, um Interessenskonflikte zu vermeiden.
- Wir werden alle rechtlichen und regulatorischen Anforderungen einhalten.
- Wir werden sicherstellen, dass die Sicherheitsanforderungen den sich ändernden Geschäftsanforderungen angepasst werden.

1.2. Rahmenbedingungen

Die Durchsetzung des Informationssicherheits-Standards darf nur unter Beachtung der Mitbestimmungsrechte der nationalen Arbeitnehmervertretungen, sowie der Vorschriften der geltenden Betriebsvereinbarungen und örtlichen Gesetze (z. Bsp. Datenschutzgesetze) erfolgen.

2. Ziel

2.1. Zweck des Dokuments

Der Zweck des Informationssicherheits-Standards ist die Gewährleistung der Geschäftskontinuität und die Schadensreduktion bei der Zusammenarbeit mit Drittfirmen (Lieferanten, Dienstleister, kunde sowie Geschäftspartner, usw.) durch die Verhinderung oder Minimierung von Sicherheitsvorfällen.

Der Informationssicherheits-Standard ermöglicht die Benutzung von DEKRA Informationen im externen Unternehmen unter Beachtung von:

- Vertraulichkeit
- Integrität

- und Verfügbarkeit.

Mit diesem Informationssicherheits-Standard bringt die Geschäftsleitung die Wichtigkeit der Sicherheit der Informationen und der Informationssysteme für DEKRA und für die Zusammenarbeit mit Drittfirmen zum Ausdruck.

2.2. Geltungsbereich

Dieser DEKRA Informationssicherheits-Standard ist als “öffentliche“ Information klassifiziert und wird folgenden Personenkreisen zur Verfügung gestellt:

- Lieferanten, Geschäftspartner, Dienstleister
- Geschäftskunden und Endkunden
- Vertragsnehmer, Beratern, Aushilfskräften
- sowie Agenturbüros, Franchisenehmer

Weitere Richtlinien oder Standards können je nach dem Anwendungsfall mit Beratung von lokaler DEKRA Information und Cybersicherheit einbezogen werden und nur nach Unterzeichnung einer NDA anwendbar sein und die Genehmigung des Dokumenteneigentümers einholen.

2.3. Überprüfung

Diese Norm wird jährlich oder bei wesentlichen Änderungen der geltenden Vorschriften, Technologien oder geschäftlichen Anforderungen überprüft.

3. Allgemeines Managementsystem für Informationssicherheit (ISMS)

3.1. Vertragliche Anforderungen

Wenn eine Drittfirma auf nicht öffentlich DEKRA Daten zugreifen kann oder ihr nicht öffentlich DEKRA Daten zur Verfügung gestellt werden, muss ein Non-Disclosure Agreement (NDA) in den Vertrag aufgenommen werden, welches für alle Mitarbeiter der Drittfirma gilt. Dadurch wird die Vertraulichkeit der DEKRA Daten sichergestellt.

Auch nach der Beendigung der Dienstleistung bzw. der Zusammenarbeit ist über die erlangten Informationen Stillschweigen zu vereinbaren. Dies gilt auch für die Beendigung des Arbeitsverhältnisses einer Person, welche bei einer Drittfirma eingestellt war und von diesem bei der DEKRA eingesetzt wurde. Hierzu ist die DEKRA Rechtsabteilung hinzuzuziehen.

Stellt eine Drittfirma Subunternehmer für die Erbringung der Leistung ein, welche mit der DEKRA vereinbart wurde, so muss dies vor Beauftragung des Subunternehmers der DEKRA gemeldet werden. Darüber hinaus muss von dem, durch die DEKRA beauftragten Drittfirmen z.B. Lieferanten, sichergestellt sein, dass die Subunternehmer über die Vertragsbedingungen des Lieferanten mit der DEKRA in Kenntnis gesetzt sind

und diese sich auch auf diese Bedingungen verpflichten, um die Sicherheit und den Schutz der informationstechnischen Systeme und der in ihnen gespeicherten Daten bei der DEKRA zu gewährleisten. Die Subunternehmer müssen daher vom Lieferanten bzw. Drittfirmen auch auf das NDA der DEKRA verpflichtet werden.

Je nach Art der erbrachten Dienstleistung muss der Vertrag alle Sicherheitsanforderungen, die DEKRA zum Schutz seiner Informationen festgelegt hat, schriftlich enthalten. Diese Anforderungen werden vom DEKRA-Vertragsverantwortlichen bereitgestellt, der sicherstellen muss, dass externe Organisationen diesen Standard verstehen und einhalten.

3.2. Aufbau des ISMS

DEKRA erwartet, dass die vertraglich verbundenen Drittfirmen im Umfeld der Informationsverarbeitung von DEKRA-Daten ein Management der Informationssicherheit ausgerichtet an ISO 27001 oder TISAX Standard zu haben. Mit diesen Informationssicherheits-Standards wird ein risikobasierter Ansatz umgesetzt, um eine gründliche Analyse aller Informationen und informationsverarbeitenden Systeme in regelmäßigen Abständen durchzuführen. Dadurch werden die Bedrohungen und Schwachstellen für übertragene und gespeicherte Informationen anerkannt und rechtzeitig mit weiteren Sicherheitsmaßnahmen behandelt, um einen optimalen Sicherheitsniveau in der Organisation sicherzustellen.

3.3. Einhaltung des Informationssicherheits-Standards (Compliance)

In jeder vertraglich verbundenen Drittfirma ist dieser Informationssicherheits-Standard einzuhalten.

Stellt eine Drittfirma einen Subunternehmer für die Erbringung einer Software- oder Hardwaredienstleistung ein, so hat die Drittfirma, welcher mit der DEKRA in einem Vertragsverhältnis steht, dafür Sorge zu tragen, dass sich der Subunternehmer auch auf die Einhaltung des Informationssicherheits-Standard der DEKRA verpflichtet.

Die DEKRA behält es sich vor, im Rahmen der vertraglichen Vereinbarungen und der vereinbarten allgemeinen Geschäftsbedingungen Mitarbeiter der Drittfirmen sowie Drittfirmen auf die Einhaltung des NDA zu prüfen. Zusätzlich werden auch ggfs. vorhandene Zertifikate im Umfeld der Informationssicherheit abgefragt.

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

3.4. ISMS-Sensibilisierung und Sicherheitsschulungen

Die DEKRA Information und Cybersicherheit und die IT-Abteilung können die Drittfirmen durch zielorientierte Schulungen unterstützen. Die grundlegenden Anforderungen an Information und Cybersicherheit werden durch diesen Informationssicherheits-Standard mitgeteilt. Die Mitarbeiter der externen Organisation müssen zum Thema Informationssicherheit regelmäßig geschult werden.

3.5. Nutzung von DEKRA-/externen Ressourcen

Die Nutzung von DEKRA-Ressourcen darf ausschließlich für autorisierte geschäftliche Zwecke erfolgen, eine private Nutzung der IT-Ressourcen ist nicht gestattet. Weitere Informationen zu diesem Thema finden Sie im Kapitel „Physische Zugangskontrolle".

Externe Geräte müssen den Sicherheitsanforderungen von DEKRA entsprechen.

3.6. Durchsetzung

Die Nichteinhaltung der DEKRA Informationssicherheitsrichtlinien und -standards oder die Missachtung angemessener Maßnahmen zum Schutz der Systeme, Daten, Informationen und Vermögenswerte kann zu rechtlichen Schritten führen oder Meldungen an Aufsichtsbehörden, Kündigung von Verträgen oder Vereinbarungen und/oder Verlust künftiger Geschäftsmöglichkeiten.

3.7. Ausnahmen

Ausnahmen oder Abweichungen zu diesem Informations- und Cybersicherheitsstandard müssen dokumentiert, begründet und seitens des Businessmanagements freigegeben werden.

Der detaillierte Prozess der Ausnahmebehandlung kann beim DEKRA Beauftragten für Informationssicherheit erfragt werden.

4. Informationsklassifizierung

Eine Klassifikation wird zur Gewährleistung angemessener Schutzmaßnahmen für vertrauliche Informationen eingesetzt. Unabhängig von der Klassifizierung müssen auch die Integrität und die Richtigkeit der Informationenklassifikation geschützt werden. Die externe Organisation muss ihre Richtlinie zur Informationsklassifizierung zur Verfügung stellen, um dieses mit der DEKRA Richtlinie zur Informationsklassifizierung abzugleichen. Die zugewiesene Klassifikation und die damit verbundenen Maßnahmen müssen in Abhängigkeit von der Sensibilität der Informationen umgesetzt werden. Die sensibelsten Elemente der Information definieren den Klassifikationsgrad. Informationen, die in verschiedenen Formaten aufgezeichnet wurden (z. Bsp. gedruckte Dokumente, elektronische Sprachaufzeichnungen, elektronische Berichte), müssen unabhängig von ihrem Format die gleiche Klassifizierung haben.

Die anzuwendenden Klassifizierungsstufen sind:

	Potenzielle Schaden durch unautorisierte Bekanntgabe, Änderungen oder Vernichtung	Zugangsbeschränkung
öffentlich	keine	Keine Einschränkung
intern	Der potenzielle Schaden ist marginal, kurzfristiger Natur und auf eine einzige Entität begrenzt. Geringfügiger Schaden. Informationen, deren unbefugte Veränderung repariert werden kann, obwohl sie DEKRA einen geringfügigen Schaden zufügen kann. In Bezug auf PII, deren unsachgemäßer Umgang voraussichtlich keine besondere Beeinträchtigung der Rechte und Freiheiten natürlicher Personen zur Folge hat	Nur Mitarbeiter Die Anderen nur mit NDA
vertraulich	Das Schadenspotenzial ist beträchtlich oder mittelfristig oder nicht auf ein einzelnes Unternehmen beschränkt. Hoher Schaden. Informationen, deren unbefugte Veränderung schwer zu beheben ist und zu erheblichen Verlusten für DEKRA führen kann. Ein unsachgemäßer Umgang mit personenbezogenen Daten könnte die soziale Stellung oder die wirtschaftlichen Verhältnisse der betreffenden Person erheblich beeinträchtigen.	Nur eine eingeschränkte (oder begrenzte) Gruppe von Mitarbeitern (kann vertrauenswürdige Systemadministratoren einschließen), für PII nur namentlich genannte Personen, die es wissen müssen
Streng vertraulich	Das Schadenspotenzial ist existenzbedrohend, langfristig oder nicht auf ein einzelnes Unternehmen beschränkt. Sehr hoher Schaden. Informationen, deren unbefugte Veränderung nicht behoben werden kann, die aber bei DEKRA schwere Schäden verursachen. Ein unsachgemäßer Umgang mit personenbezogenen Daten könnte die soziale Stellung oder die wirtschaftlichen	Nur namentlich genannte Personen, eingeschränkte Nutzung

	Verhältnisse oder die Gesundheit, das Leben oder die Freiheit der betroffenen Person erheblich beeinträchtigen.	
Geheim	Das Schadenspotenzial bedroht die Existenz oder lebenswichtige Interessen des Staates. Schwerer Schaden. Sie ist die sensibelste der Informationsklassifizierungen	Nur von der Regierung autorisierten Mitarbeitern

Das unbefugte Kopieren, Übertragen oder Verwenden von Informationen ist strengstens untersagt.

4.1. Kennzeichnung von Informationen

Die ordnungsgemäße Kennzeichnung ist eine Voraussetzung für den sicheren Umgang mit Informationen. Informationen sollten daher entsprechend ihrer Vertraulichkeitseinstufung gekennzeichnet werden.

Eine korrekte Kennzeichnung ist insbesondere bei der Übermittlung vertraulicher oder streng vertraulicher Informationen zwischen Unternehmen (z. B. an Partnerfirmen und Lieferanten) unbedingt erforderlich.

Wenn die von der externen Organisation zur Verfügung gestellten Informationen nicht gekennzeichnet sind, wird DEKRA diese Informationen als "intern" kennzeichnen.

4.2. Umgang mit Informationen

Klassifikation	Kennzeichnung	Data at rest*	Data in transit*	Vernichtung
öffentlich	keine/optional (z.B. Vermerk im Impressum)	Elektronische Daten: keine Einschränkungen Papierunterlagen: keine Einschränkungen	Elektronische Daten: keine Einschränkungen Papierunterlagen: keine Einschränkungen	Elektronisch: keine Einschränkungen Physische: keine Einschränkungen
intern	Angabe der Vertraulichkeitsstufe in Landessprache oder englisch/keine oder „Intern“ auf jeder Seite des Dokuments in	Elektronische Daten: Zugriff auf externe Server eingeschränkt Papierunterlagen: Sollte bei Nichtgebrauch im verschlossenen Schränke/Contain	Elektronische Daten: Verschlüsselung auf externe Server Papierunterlagen: Äußerer Transport nur in verschlossenen Umschlägen	Elektronisch: Sicheres Löschen durch Überschreiben von Medien mit mindestens einem Schreibdurchgang mit einem festen Datenwert, z. B. allen Nullen. ODER Nutzung von

	elektronischer und gedruckter Form	ers gehalten werden		Sicherheitsteam freigegebenem Entmagnetisierungsgerät für die magnetische Speicherung (in Anlehnung an NIST SP 800-88) Physische: Vernichtung nach ISO 21964 (DIN 66399), mind. Schutzklasse 1 Sicherheitsstufe 2
vertraulich	Angabe der Vertraulichkeitsstufe in Landessprache oder englisch /„Vertraulich“ auf jeder Seite des Dokuments in elektronischer und gedruckter Form.	Elektronische Daten: grundsätzlich Zugriffsbeschränkt Papierunterlagen: Eingesperrt, wenn sie nicht direkt benutzt werden und nicht beaufsichtigt werden, nicht an öffentlichen Orten ausgesetzt werden	Elektronische Daten: immer verschlüsselt Papierunterlagen: Nur in entsprechend verschlossenen Umschlägen	Elektronisch: Sicheres Löschen durch Überschreiben von Medien mit mindestens einem Schreibdurchgang mit einem festen Datenwert, z. B. allen Nullen. ODER Nutzung von Sicherheitsteam freigegebenem Entmagnetisierungsgerät für die magnetische Speicherung (in Anlehnung an NIST SP 800-88) Physische: Vernichtung nach ISO 21964 (DIN 66399), mind. Schutzklasse 2 Sicherheitsstufe 5
Streng vertraulich	Angabe der Vertraulichkeitsstufe in Landessprache oder englisch/„streng vertraulich“ auf jeder Seite des Dokuments	Elektronische Daten: grundsätzlich Zugriffsbeschränkt, individuell verschlüsselte Dateien, Nachrichten oder Datenbanken, Speicherung auf	Elektronische Daten: Ende-zu-Ende-Verschlüsselung Papierunterlagen: Nur Sonderkurierdienst	Elektronisch: Sicheres Löschen durch Überschreiben von Medien mit mindestens einem Schreibdurchgang mit einem festen Datenwert, z. B. allen Nullen. ODER Nutzung von

		physisch unsicheren Geräten (Cloud, mobile Datenspeicherung, Laptop, Telefon) nur mit expliziter Freigabe Papierunterlagen: Eingesperrt, wenn sie nicht direkt benutzt werden und nicht beaufsichtigt werden, Standort eingeschränkt, nicht an öffentlichen Orten zu benutzen		Sicherheitsteam freigegebenem Entmagnetisierungsgerät für die magnetische Speicherung (in Anlehnung an NIST SP 800-88) Physische: Vernichtung nach ISO 21964 (DIN 66399), mind. Schutzklasse 3 Sicherheitsstufe 6
Geheim	Angabe des Vertraulichkeitsgrades in der Landessprache oder in Englisch / oder Kennzeichnung "geheim" auf jeder Seite des Dokuments in elektronischer und gedruckter Form Sie ist die sensibelste der Informationsklassifizierungen	Zugriffsbeschränkte, individuell verschlüsselte Dateien, Nachrichten oder Datenbanken, Speicherung auf physisch unsicheren Geräten (Cloud, mobiler Datenspeicher, Laptop, Telefon) sind verboten.	Ende-zu-Ende verschlüsselt, nur das notwendige Minimum an Informationen enthalten und die Übertragung muss aufgezeichnet werden, wann und von wem	Verfahren in Anlehnung an ISO/IEC 21964-1:2018-08 (DIN 66399), Mindestschutzklasse 3 und Sicherheitsstufe 7 und Umrühren von Säcken mit geschreddertem Material zur Durchmischung des Inhalts
	*Ausnahmen möglich mit unterschriebener Risikoakzeptanz von Business Owner und Geschäftsführer inkl. Zustimmung von Informations- und Cybersicherheit			

Die Dauer der Datenaufbewahrung muss festgelegt, mit dem Geschäftsinhaber vereinbart und auf der Grundlage der Geschäftsanforderungen dokumentiert werden.

5. Sicherheitskontrollmaßnahmen

5.1. Zutrittskontrolle

Die DEKRA Informationen, die bei Drittfirmen gespeichert oder verarbeitet werden, sind so zu verwenden, dass keine Unbefugten diese Daten einsehen oder darauf zugreifen können. Vertrauliche und streng vertrauliche Dokumente dürfen niemals unbeaufsichtigt liegen gelassen werden, um Einsichtnahme durch Unberechtigte zu verhindern.

Dasselbe gilt auch für DEKRA IT-Geräte oder Systeme, die bei Drittfirmen im Einsatz sind. Die zur Verfügung gestellten Geräte sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen. Besondere Vorsicht ist bei der Verwendung mobiler Systeme geboten.

Alle externen Organisationen, die das DEKRA Gebäude betreten, werden mit einem Ausweis ordnungsgemäß identifiziert.

Das Betreten oder Umhergehen im DEKRA Gebäude, insbesondere (ohne Begleitung von autorisiertem Personal) in Bereichen mit beschränktem Zugang für Externe ist nicht gestattet, es sei denn, sie werden von autorisiertem DEKRA Personal begleitet und haben die NDA unterzeichnet.

Eine externe Zugangstür zum allgemeinen Lager ist für den Ein- und Ausgang von Waren bestimmt und darf nicht von Kunden oder anderen externen Personen benutzt werden. Externes Personal der Transportunternehmen hat nur zu administrativen Zwecken Zugang zum Büro des Lagers.

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

5.2. Zugangskontrolle

Unbefugte Nutzung der DEKRA Informationen Systeme oder verbundener externen Systeme soll wie folgt verhindert werden:

- Die Anmeldung im Netzwerk/am PC erfolgt nur mit einem gültigen Account, die Nutzererkennung ist personifiziert. Alle externen Benutzer müssen eindeutig identifiziert werden; gemeinsame Konten sind verboten.
- Die Verwendung der Benutzerkennung oder des 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 Passwortes ist gewährleistet.
    - Passwörter oder PINs einer Benutzerkennung, die zur persönlichen Verwendung bestimmt ist (bezeichnet als „persönliche

Benutzerkennung“, sind streng vertraulich zu halten und dürfen nicht weitergegeben werden.
    - Das Speichern oder das Aufschreiben von Passwörtern (z. B. auf Papier, über Mobilgeräte oder in Dateien) ist nicht zulässig, sofern dies nicht als sichere Methode festgelegt ist.
    - Sobald der Verdacht der Kompromittierung oder des Bekanntwerdens eines Passworts oder einer PIN besteht, ist dieses bzw. diese unverzüglich zu ändern.
    - Alle Passwörter oder PINs sind bei der ersten Verwendung zu ändern sowie spätestens nach einem Jahr (Letzteres gilt nur für Passwörter).
    - Temporäre Passwörter (z. B. für neue Konten) sind bei der ersten Anmeldung zu ändern.
    - Alle Passwörter oder PINs sind bei der ersten Verwendung zu ändern sowie spätestens nach drei Monaten (Letzteres gilt nur für Passwörter).
    - Das Ausspähen von Passwörtern ist nicht gestattet.
    - Passwörter sind mindestens als vertraulich zu klassifizieren.
    - Kein identisches Passwort für private und berufliche Zwecke verwenden
    - Die von Systemen erzwungene Mindestlänge für Passwörter ist einzuhalten. Sie richtet sich nach den Vorgaben der entsprechenden Regelung.
    - Triviale Passwörter (z.B. „Test123456“) oder Passwörter mit persönlichem Bezug (z. B. Namen, Geburtsdatum) sind nicht zulässig.
    - Erfordern bestimmte Systeme oder Anwendungen komplexere Passwörter (gemäß Definition in der Passwort-Regelung), dann sind diese Vorgaben zu erfüllen.
    - Auf allen Clients/PCs ist ein Bildschirmschoner installiert, welcher zur Reaktivierung des Systems ein Kennwort benötigt.
- Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten, ausschließlich zu den von ihren Zugangsberechtigungen umfassten Daten Zugang haben.
- Rechte und Rollen werden dem „Need to know“-Prinzip folgend vergeben, wobei die jeweiligen Berechtigungen auf die Rolle zugeschnitten sind (least privilege).
- Die Zugriffs-/Administrationsrechte für PCs und/oder Server werden exakt dokumentiert.
- Nicht mehr benötigte Berechtigungen werden im Rahmen eines Nutzer-Identifikationsmanagements zeitnah entfernt.
- Der Zugriff auf die PCs/Serverumgebung von außen ist nur über eine verschlüsselte
  Kommunikation (DEKRA Unternehmens-VPN-Tunnel) möglich.
- Beim Zugang zu internen, vertraulichen, streng vertraulichen oder als Verschlusssache eingestuften Informationen muss für die externen Konten eine Mehrfaktor-Authentifizierung verwendet werden.

- Passwortschutz muss für Benutzer- und technische Benutzerkonten durchgesetzt werden

5.3. Zugriffskontrolle

Die Geschäftsanforderungen an Zugriffe auf DEKRA Informationssysteme sind vor deren Freigabe zu definieren und zu dokumentieren. Die Zugriffsvoraussetzungen orientieren sich an den geschäftlichen Erfordernissen.

Der Informationseigentümer und der Systemverantwortliche autorisieren den Zugang zu Daten und IT-Dienstleistungen in Übereinstimmung mit den Geschäftsanforderungen und Sicherheitsvorgaben. Die Informationssysteme der DEKRA werden nur für autorisierte dienstliche Zwecke eingesetzt, sofern keine abweichenden Vereinbarungen gelten. Alle relevanten Sicherheitsvorfälle werden dokumentiert, einschließlich einer Aufzeichnung der erfolgreichen und nicht erfolgreichen Anmeldeversuche.

Der physische und logische Zugriff auf vertrauliche und interne Informations- und Datenverarbeitungssysteme wird kontrolliert. Um einen angemessenen Zugriffslevel sicherzustellen, werden vom zuständigen Informationssicherheitsbeauftragten verschiedene Sicherheitsmaßnahmen vorgegeben.

5.4. Trennungskontrolle

Wenn die Drittfirmen auch mit anderen Kunden arbeiten, eine Mandantenfähigkeit entsprechend den Kundenanforderungen, logisch und physikalisch sichergestellt ist.

Eine Systemtrennung für Test und Produktion muss implementiert sein, basierend auf eine Risiko-Abschätzung.

5.5. Datenträgerkontrolle

Datenträger (wie z. B. CDs, DVDs, USB-Sticks und Festplatten) sind vor Verlust, Zerstörung und Verwechslung sowie vor unbefugtem Zugriff zu schützen.

Nicht mehr benötigte Datenträger sind auf sichere Weise nach Kap. 4.2 zu entsorgen. Ein Transport von Datenträgern mit personenbezogenen Daten zu einem zertifizierten Aktenvernichtungsunternehmen darf nur in geschlossenen Behältnissen und in „geschlossenen“ Fahrzeugen durchgeführt werden, sodass kein Material verloren gehen kann und nach schriftlicher Genehmigung durch DEKRA.

5.6. Transportkontrolle

Es wird gewährleistet, dass bei der Übermittlung von Informationen die Vertraulichkeit und die Integrität der Daten geschützt werden.

Datenverkehr, welcher personenbezogene Daten transportiert, z. B. E-Mail, Webzugriff, wird verschlüsselt. Datenübertragungen werden verschlüsselt, z. B. S-FTP, DEKRA

Unternehmens-VPN-Tunnel. Eine unautorisierte Weitergabe von Daten findet nicht statt.

Faxnummern und E-Mail-Adressen sind aktuellen Verzeichnissen zu entnehmen oder beim Empfänger zu erfragen, um fehlerhafte Übertragungen zu vermeiden. Für den Inhalt und die Verteilung einer E-Mail ist der Absender verantwortlich. Für die weitere Verarbeitung und Verteilung ist der Empfänger verantwortlich. Die Erstellung und der Versand von Ketten-E-Mails sind unzulässig.

Bei allen Gesprächen (einschließlich Telefonaten, Video- und Webkonferenzen), die vertraulichen oder streng vertraulichen Informationen betreffen oder enthalten, ist sicherzustellen, dass diese nicht unberechtigt mitgehört oder aufgezeichnet werden können.

5.7. Systems-Sicherheit

Informationen sollten vor versehentlicher oder absichtlicher Offenlegung, Änderung oder Zerstörung geschützt werden.

Es müssen Maßnahmen wie Protokollierung umgesetzt werden, die nachträglich überprüft und feststellt, ob und von wem Informationen in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Eine Übertragung der Informationen muss ausschließlich gemäß der jeweiligen vertraglichen Vereinbarungen stattfinden. Diese Übertragung muss auch protokolliert werden. Das Netzwerk/die PCs sind durch ein Firewall-System gegenüber unberechtigten Zugriffen von außen, sowie durch ein Zonenkonzept von innen geschützt. Es erfolgt eine Überprüfung auf Aktualität.

Es muss sichergestellt sein, dass gespeicherte Informationen nicht durch Fehlfunktionen des Systems beschädigt werden können. Systemzustände werden kontinuierlich und automatisiert überwacht, um Fehlfunktionen frühzeitig zu erkennen. Eine regelmäßige Wartung muss auch festgelegt werden, um die Integrität von z. B. Datenbanken zu überprüfen. Nur autorisierte und fachkundige Mitarbeiter dürfen an Systeme während des Änderungsprozesses Veränderungen durchführen und Fehlfunktionen beheben.

Die Sicherheitsanforderungen an ein Informationssystem gelten über den gesamten Lebenszyklus, die Verantwortung für die Einhaltung liegt beim zuständigen Business-Management. Die Einführung neuer Technologien darf das Sicherheitsniveau der DEKRA nicht gefährden.

5.8. Gewährleistung der Verfügbarkeit

Informationen und Dienstleistungen sollen durch ordnungsgemäßen Archivierung, einen Einsatz von einem Virenschutzkonzept, eine unterbrechungsfreie Stromversorgung und ein angemessenes Backupkonzept sowie Recovery-Konzept stets verfügbar sein, wenn sie benötigt werden.

Die Verantwortlichen der Informationssysteme entwickeln, pflegen und testen regelmäßig Pläne zur Aufrechterhaltung des Betriebs kritischer Informationssysteme entsprechend regulatorischen, vertraglichen oder anderen Business-Vorgaben.

5.9. Sicherheitsvorfälle

Jeder tatsächlich bestätigte oder vermutete Sicherheitsvorfall, jede Datenverletzung oder jeder Verstoß gegen Richtlinien muss unverzüglich und so schnell wie möglich an den folgenden Empfänger sowie an die zuständige DEKRA-Rechtsperson gemeldet werden:

Information.security@dekra.com

Darüber hinaus müssen Vorfälle, die personenbezogene Daten betreffen, unverzüglich dem zuständigen Datenschutzbeauftragten der DEKRA-Rechtseinheit gemeldet werden. Sie können auf die folgende Webseite zugreifen, um die Empfänger in den deutschen DEKRA Rechtsträgern zu erfahren:Datenschutz und Verarbeitung personenbezogener Daten | DEKRA

Für jede andere juristische Person ist unverzüglich der entsprechende Ansprechpartner von DEKRA zu benachrichtigen..

Alle Mitarbeiter und externen Vertragspartner müssen über das Verfahren zur Meldung von Sicherheitsvorfällen informiert sein.

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

Der zuständige lokale Informationssicherheitsbeauftragte und Datenschutzbeauftragte überprüfen regelmäßig die gemeldeten Sicherheitsvorfälle, der Rückmeldungen und der getroffenen Maßnahmen.

6. Dokumentenlenkung

Dokumentbesitzer	Global Information Security
Übersetzung durch	Prerna Walhekar
Geprüft durch	Mabel Gonzalez
Geprüft am	2025.07.09
Freigegeben durch	Drazen Morog
Freigegeben am	2025.07.21
Version	1.6DE

7. Versionsverlauf

Datum	Version	Name	Revision
2020.10.13	0.1	Prerna Walhekar	Erste Übersetzung
2020.10.27	1.0	Prerna Walhekar	Finale Version
2021.01.22	1.1	Prerna Walhekar	Finale Version, Einheitliche Anpassungen zum DEKRA Scope
2022.02.24	1.2	Prerna Walhekar	Anpassungen nach aktueller englischer Version
2023.02.01	1.3	Prerna Walhekar	Anpassungen nach aktueller englischer Version
2023.10.05	1.4	Mabel Gonzalez	Angleichung an L1.P04 für die Klasse der Zugangsbeschränkungen bei vertraulichen Informationen Anpassung an das neue Design und die Typografie
2024.04.29	1.5DE	Mabel Gonzalez	Geringfügige Änderungen im Namen des DEKRA Teams Das Erfordernis der NDA-Signatur ist im Kapitel "Anwendungsbereich" enthalten, um alle anderen erforderlichen Richtlinien oder Standards zu erhalten. Angleichung an L1.P04 für die Zugangsbeschränkungen in der Klasse der vertraulichen Informationen und die Festlegung der Datenaufbewahrungsfrist im Kapitel *Umgang mit Informationen*. Erhöhung des Geheimhaltungsgrades für die von der externen Organisation bereitgestellten Informationen im Kapitel *Etikettierung* Neue Anforderung (Passwortschutz) für technische Konten im Kapitel *Zulassungskontrolle* Schriftliches Genehmigungserfordernis für die Entsorgung von Informationen über Drittdienste im Kapitel *Datenträgerkontrolle*

			Offenlegung ist auch beim Schutz von Informationen im Kapitel *Systemsicherheit enthalten* Die Liste der Empfänger für deutsche DEKRA-Rechtspersonen wurde aktualisiert und ein Link zur DEKRA-Webseite, auf der diese Informationen gespeichert sind, wurde in das Kapitel *Sicherheitsvorfälle aufgenommen*.
2025.07.09	1.6DE	Mabel Gonzalez	Neues Kapitel „*Überprüfung*" wurde hinzugefügt. Je nach Art der erbrachten Dienstleistung müssen alle Sicherheitsanforderungen schriftlich in Verträgen im Kapitel „*Vertragliche Anforderungen*" festgehalten werden. Externe Organisationen können im Rahmen von *Compliance-Prüfungen* im Kapitel „Einhaltung von Informations- und Cybersicherheitsstandards" Sicherheitsaudits unterzogen werden. Neues Kapitel „*Nutzung von DEKRA/externen Ressourcen*" wurde hinzugefügt. Im Kapitel „*Nichteinhaltung*" wurden neue Maßnahmen hinzugefügt: Meldung an Aufsichtsbehörden, Kündigung von Verträgen oder Vereinbarungen und/oder Verlust zukünftiger Geschäftsmöglichkeiten. Verbotene Nutzung von Informationen im Kapitel „*Informationsklassifizierung*" Gemeinsam genutzte Konten sind im Kapitel „*Zugangskontrolle*" 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, uneingeschränkte Zusammenarbeit bei der Untersuchung und Behebung von

			Vorfällen sowie sofortige Benachrichtigung im Falle eines Sicherheitsvorfalls im Kapitel *„Sicherheitsvorfälle“* Name of the standard change from *Informationssicherheit für Drittfirmen* to *Informationssicherheit für Externe*

DEKRA SE

Global Information and Cyber Security – CISO
Handwerkstraβe 15
70565 Stuttgart
Telefon +49.711.7861-0
Information.security@dekra.com