Information Security Standard
Informationssicherheit für Drittfirmen

DEKRA

Alles im grünen Bereich.

Content

1. Zusammenfassung

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 Informationen sind schützenswert.
- 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. Grundsatzaussagen

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

2. Einführung

2.1. Zweck des Dokuments

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

Die Informationssicherheitsrichtlinie ermöglicht die Benutzung von DEKRA Informationen im externen Unternehmen unter Beachtung von:

- Vertraulichkeit
- Integrität
- und Verfügbarkeit.

Mit dieser Sicherheitsrichtlinie 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

Diese DEKRA Informationssicherheitsrichtlinie ist als “öffentliche“ Information klassifiziert und wird folgenden Personenkreisen zur Verfügung gestellt:

- Lieferanten, Geschäftspartner, Dienstleister

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

Weitere Richtlinien oder Standards können je nach dem Anwendungsfall mit Beratung von DEKRA SE Information Security (HIT14) einbezogen werden.

3. Allgemeines Managementsystem für Informationssicherheit (ISMS)

3.1. Vertragliche Anforderungen

Wenn eine Drittfirma auf sensible DEKRA Daten zugreifen kann oder ihr sensible 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 SE eingesetzt wurde. Hierzu ist die DEKRA SE Rechtsabteilung hinzuzuziehen.

Stellt eine Drittfirma Subunternehmer für die Erbringung der Leistung ein, welche mit der DEKRA SE vereinbart wurde, so muss dies vor Beauftragung des Subunternehmers der DEKRA SE gemeldet werden. Darüber hinaus muss von dem, durch die DEKRA SE beauftragten Drittfirmen z.B. Lieferanten, sichergestellt sein, dass die Subunternehmer über die Vertragsbedingungen des Lieferanten mit der DEKRA SE 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 SE zu gewährleisten. Die Subunternehmer müssen daher vom Lieferanten bzw. Drittfirmen auch auf das NDA der DEKRA SE verpflichtet werden.

3.2. Aufbau des ISMS

DEKRA SE 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 der Informationssicherheitsrichtlinien (Compliance)

In jeder vertraglich verbundenen Drittfirma ist diese Informationssicherheitsrichtlinie von DEKRA SE einzuhalten.

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

Die DEKRA SE 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.

3.4. Unterstützung und Schulung

Die DEKRA SE Informationssicherheit und die IT-Abteilung können die Drittfirmen durch zielorientierte Schulungen unterstützen. Die grundlegenden Anforderungen an Informationssicherheit werden durch diese Informationssicherheitsrichtlinie mitgeteilt.

3.5. 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.

3.6. Ausnahmen

Ausnahmen oder Abweichungen zu dieser Informationssicherheitsrichtlinie müssen dokumentiert, begründet und seitens des Businessmanagements freigegeben werden. Der detaillierte Ausnahmebehandlungs-Prozess ist bei DEKRA SE Informationssicherheit nachzufragen.

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 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	
intern	Der potenzielle Schaden ist marginal, kurzfristiger Natur und auf eine einzige Entität begrenzt.	Nur Mitarbeiter Die Anderen mit NDA
vertraulich	Das Schadenspotenzial ist beträchtlich oder mittelfristig oder nicht auf ein einzelnes Unternehmen beschränkt.	Nur namentlich genannte Personen (kann vertrauenswürdige Systemadministratoren einschließen)
Streng vertraulich	Das Schadenspotenzial ist existenzbedrohend, langfristig oder nicht auf ein einzelnes Unternehmen beschränkt.	Nur namentlich genannte Personen, eingeschränkte Nutzung

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.

Neben dem Dokumentbesitzer müssen sowohl der Empfänger als auch der Verarbeiter der Information mit den Klassifizierungsstufen vertraut sein und daher die damit verbundenen Anforderungen an den Umgang mit der Information kennen und anwenden.

Eine korrekte Kennzeichnung ist insbesondere bei der Übermittlung vertraulicher oder streng vertraulicher Informationen zwischen Unternehmen (z. B. an Partnerfirmen und Lieferanten) unbedingt erforderlich. Bei der Kennzeichnung von Informationen müssen die Form der Information und ihr Geheimhaltungsgrad berücksichtigt werden.

Wenn Informationen nicht gekennzeichnet sind und die Klassifizierung nicht offensichtlich ist, müssen sie als "intern" betrachtet werden.

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 der ersten Seite des Dokuments	Elektronische Daten: Zugriff auf externe Server eingeschränkt Papierunterlagen: Sollte bei Nichtgebrauch im verschlossenen Schränke/Containers gehalten werden	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 Sicherheitsteam freigegebenem Entmagnetisierungsgerät für die magnetische Speicherung (in Anlehnung an NIST SP 800-88 Rev. 1) 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 Rev. 1) Physische: Vernichtung nach ISO 21964 (DIN 66399), mind. Schutzklasse 2 Sicherheitsstufe 4

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 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	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 Sicherheitsteam freigegebenem Entmagnetisierungsgerät für die magnetische Speicherung (in Anlehnung an NIST SP 800-88 Rev. 1) Physische: Vernichtung nach ISO 21964 (DIN 66399), mind. Schutzklasse 3 Sicherheitsstufe 5
	*Ausnahmen möglich mit unterschriebener Risikoakzeptanz von Business Owner			

5. Sicherheitskontrollmaßnahmen

5.1. Zutrittskontrolle

Die DEKRA Daten, 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.

Die Drittfirmen sollen eine angemessene Gebäudesicherheit und ein geregeltes Besuchermanagement haben.

5.2. Zugangskontrolle

Unbefugte Nutzung der DEKRA datenverarbeitenden 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.
- 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 (VPN-Tunnel) möglich.

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 einer 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.

5.6. Transportkontrolle

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

Datenverkehr, welcher personenbezogene Daten transportiert, z. B. E-Mail, Webzugriff, wird verschlüsselt. Datenübertragungen werden verschlüsselt, z. B. S-FTP, VPN. 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 sollen vor unbeabsichtigter oder beabsichtigter Veränderung oder Zerstörung geschützt.

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 tatsächliche oder vermutete Sicherheitsvorfall muss so schnell wie möglich gemeldet werden:

Information.security@dekra.com

konzerndatenschutz@dekra.com

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

Der zuständige Informationssicherheitsbeauftragte überprüft regelmäßig die gemeldeten Sicherheitsvorfälle, der Rückmeldungen und der getroffenen Maßnahmen.

6. Dokumentenkontrolle

Document Owner	HIT14/Prerna Walhekar
Edited by	Prerna Walhekar
Edited on	2020-10-13
Reviewed by	Thomas Hottewitzsch
Reviewed on	2020-10-16
Approved by	Thomas Hottewitzsch
Approved on	2020-10-17
Version	1.0

7. Version Historie

Date	Version	Name of editor	Revision
2020-10-13	0.1	Prerna Walhekar	Erste Zusammenfassung
2020-10-17	1.0	Prerna Walhekar	Finale Version

DEKRA SE

Abteilung HIT 14
Handwerkstraße 15
70565 Stuttgart
Telefon +49.711.7861-0
Information.security@dekra.com