DEKRA Datenschutzprinzipien

I. Grundsätze des Datenschutzes bei DEKRA

DEKRA ist zum Schutze personenbezogener Daten und zur Gewährleistung informationeller Selbstbestimmung verpflichtet. Den fundamentalen Rahmen hierfür geben die nachstehenden Grundsätze des Datenschutzes, die von DEKRA einzuhalten sind. Als allgemeine Grundanforderung beschreiben diese die Zielsetzung von DEKRA bei der Gestaltung und Durchführung von Datenverarbeitungen.

1. Rechtmäßigkeit und Fairness

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte der Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise und fair erhoben und verarbeitet werden. DEKRA verarbeitet dementsprechend personenbezogenen Daten nur dann, wenn eine rechtliche Grundlage vorliegt. Diese rechtliche Grundlage kann sich aus einem Gesetz, einem Vertrag, der vorherigen ausdrücklichen Einwilligung oder einem berechtigten Interesse ergeben.

2. Transparenz

DEKRA beschreibt in Datenschutzhinweisen, wie personenbezogene Daten erhoben, verarbeitet und gespeichert werden, wenn und soweit dies nach geltendem Recht erforderlich ist. Soweit das geltende Recht den Betroffenen bestimmte Rechte einräumt, sind diese Rechte in den Datenschutzhinweisen entsprechend zu erläutern. Datenschutzhinweise sind so zu verfassen, dass sie für die betroffene Person verständlich sind und sind öffentlich zugänglich zu machen (z.B. durch Veröffentlichung auf der regionalen Website). Als Grundregel und falls nach geltendem Recht erforderlich, müssen die betroffenen Personen in der Lage sein, insbesondere Folgendes zu erkennen oder entsprechend über Folgendes informiert zu werden

- Identität der verantwortlichen Stelle;
- Zweck, Rechtsgrundlage sowie Speicherdauer der Datenverarbeitung;
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden.

3. Zweckbindung

Eine Datenverarbeitung darf lediglich eindeutige und erlaubte Zwecke verfolgen, die grundsätzlich vor der Erhebung festzulegen sind. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen genauso wie ihre ursprüngliche Verarbeitung einer Rechtfertigung. Sollte der Verarbeitungszweck geändert werden, ist eine nachträgliche Information der Betroffenen und soweit erforderlich eine Anpassung der Datenschutzdokumentation sicherzustellen. DEKRA verarbeitet personenbezogene Daten nur soweit dies nach Art und Umfang für die Erfüllung der Zwecke erforderlich ist und soweit die Daten relevant und angemessen sind.

4. Datenvermeidung und Datensparsamkeit

Vor Aufnahme einer Datenverarbeitung muss geprüft werden, ob und in welchem Umfang dies notwendig ist, um den mit der Datenverarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte, pseudonymisierte oder statistische Daten zu verwenden, so dass die Identität von Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand ermittelt werden kann. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

5. Speicherbegrenzung und Datenlöschung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr benötigt werden, müssen gelöscht werden. Personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke verarbeitet werden. Statt einer Löschung können die Daten auch anonymisiert werden.

6. Datenqualität

DEKRA verarbeitet im eigenen Interesse ausschließlich korrekte Daten. Personenbezogene Daten müssen unabhängig davon richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand sein. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete personenbezogene Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

7. Systemdatenschutz – Vertraulichkeit, Integrität, Verfügbarkeit

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen vertraulich behandelt und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden. Unter Berücksichtigung der Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit greift insofern die für DEKRA in ihrer jeweils aktuellen Fassung gültige Informationssicherheitsrichtlinie.

8. Datenschutzfreundliche Technikgestaltung und Voreinstellungen

Soweit möglich trifft DEKRA geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass auch durch Voreinstellungen und unter Berücksichtigung des Zwecks der Verarbeitung, im Rahmen von Datenverarbeitungen die oben stehenden Grundsätze eingehalten werden, insbesondere nicht mehr Daten als nötig, nicht länger als nötig und nicht umfassender als nötig verarbeitet werden, und der Zugriff durch Dritte soweit wie möglich eingeschränkt wird.

II. Zulässigkeit der Datenverarbeitung

Eine Datenverarbeitung ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Datenverarbeitung gegenüber der ursprünglichen Zweckbestimmung geändert werden soll. Einzelheiten zu den Datenverarbeitungszwecken sind in Datenschutzhinweisen als Teil der maßgeblichen Vertragsunterlagen, Geschäftsbedingungen und/oder den online abrufbaren Datenschutzhinweisen zu erläutern.

1. Interessenten-, Kunden-, Partner- und Nutzerdaten

a. Datenverarbeitung auf Grundlage einer Einwilligung

Soweit Betroffene gegenüber DEKRA eine informierte und freiwillige Einwilligung zur Verarbeitung von personenbezogenen Daten für bestimmte Zwecke (z.B. Weitergabe von Daten im DEKRA Konzern, Auswertung von Daten für Marketingzwecke, Lichtbilder im Rahmen von Veranstaltungen, Newsletter) erteilen, ist die Rechtmäßigkeit dieser Datenverarbeitung auf dieser Basis gegeben. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Der Widerruf einer Einwilligung wirkt erst für die Zukunft und berührt nicht die Rechtmäßigkeit der bis zum Widerruf verarbeiteten Daten.

Sofern keine anderweitigen zwingenden Formerfordernisse bestehen, sind Einwilligungserklärungen aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen und zu verwalten (z.B. automatisiertes Einwilligungsmanagement). Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss dokumentiert werden.

b. Datenverarbeitung für Vertragsbeziehungen

Die Verarbeitung von Interessenten-, Kunden- und Partnerdaten darf zur Erbringung unserer Dienstleistungen bzw. im Rahmen einer sonstigen Zusammenarbeit mit Dritten zur Erfüllung unserer entsprechenden Verträge mit Kunden und Partnern erfolgen. Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners dürfen dabei zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Zur Begründung von Verträgen zählt auch die Durchführung vorvertraglicher Maßnahmen, die auf Anfrage eines Interessenten hin erfolgen (z.B. Erstellung von Angeboten, der Vorbereitung von Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche eines Interessenten). Die Zwecke der Datenverarbeitung richten sich in erster Linie nach unserem konkreten Service (z.B. Hauptuntersuchung, Erstellung von Gutachten, Durchführung von Audits, Schulungen oder Beratungen) sowie dem Gegenstand der Zusammenarbeit mit einem Partner.

c. Datenverarbeitung zu Werbezwecken

Wenden sich Betroffene mit einem Informationsanliegen an DEKRA (z.B. Wunsch nach Zusendung von Informationsmaterial zu einem Service), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

Kundenbindungs- oder Werbemaßnahmen bedürfen weiterer rechtlicher Voraussetzungen. Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und

Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Betroffene sind über die Verwendung ihrer Daten für Zwecke der Werbung bei Datenerhebung sowie bei jeder Verwendung der Daten zu Werbezwecken zu informieren. Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch die Betroffenen freiwillig. Betroffene sind über die Freiwilligkeit der Angabe von Daten für diese Zwecke zu informieren werden. Im Rahmen der Kommunikation mit den Betroffenen ist, sofern gesetzlich erforderlich, eine Einwilligung der Betroffenen in die Verarbeitung ihrer Daten zu Werbezwecken einzuholen. Betroffenen müssen im Rahmen der Einwilligung zwischen den verfügbaren Kontaktkanälen wie Post, elektronische Post und Telefon wählen können.

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke gesperrt werden. Darüber hinaus bestehende Beschränkungen einiger Länder bezüglich der Verwendung von Daten für Werbezwecke sind zu beachten.

d. Datenverarbeitung aufgrund gesetzlicher Vorgaben oder im öffentlichen Interesse

Die Verarbeitung personenbezogener Daten ist rechtmäßig, wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der DEKRA unterliegt. DEKRA unterliegt diversen rechtlichen Verpflichtungen, das heißt gesetzlichen Anforderungen (z.B. zur Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen strafbaren Handlungen oder zur Einhaltung von Steuergesetzen). Zu den Zwecken der Verarbeitung gehören unter anderem Arbeitssicherheitsmaßnahmen, die Kreditwürdigkeitsprüfung, die Identitätsprüfung, Betrugs- und Geldwäscheprävention, die Erfüllung steuerrechtlicher Kontroll- und Meldepflichten sowie die Bewertung und Steuerung von Risiken im DEKRA Konzern.

e. Datenverarbeitung zum Schutze lebenswichtiger Interessen

Die Wahrung lebenswichtiger Interessen kann in Notsituationen Vorrang gegenüber dem Schutz personenbezogener Daten genießen. Insbesondere bei durch Natur oder Mensch verursachten Katastrophen, kann also eine Verarbeitung von personenbezogenen Daten durch DEKRA erforderlich sein (z.B. für humanitäre Zwecke einschließlich der Überwachung von Epidemien bzw. Pandemien und deren Ausbreitung). Der Zweck und der Umfang bestimmen sich in diesen Fällen nach dem konkreten Ereignis.

f. Datenverarbeitung aufgrund berechtigten Interesses

Sofern nach lokalem Datenschutzrecht zulässig, kann die Verarbeitung personenbezogener Daten auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses von DEKRA oder einem Dritten erforderlich ist. Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen von Betroffenen das Interesse von DEKRA an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen und das Ergebnis dieser Interessensabwägung ist stets nach den Vorgaben der zuständigen Datenschutzaufsichtsbehörden zu dokumentieren.

g. Verarbeitung besonders schutzwürdiger personenbezogener Daten

Besonders schutzwürdige personenbezogene Daten sind insbesondere Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder weltanschauliche Überzeugungen, über Gewerkschaftszugehörigkeiten oder über Genetik, Biometrie, Gesundheit oder das Sexualleben von Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein.

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf grundsätzlich nur erfolgen, wenn dies gesetzlich erforderlich ist oder die Betroffenen ausdrücklich eingewilligt haben.

Eine Einwilligung ist nicht erforderlich, wenn Verarbeitung von besonders schutzwürdigen personenbezogenen Daten zum Schutz lebenswichtiger Interessen der Betroffenen oder einer anderen natürlichen Person erforderlich ist und die Betroffenen aus körperlichen oder rechtlichen Gründen nicht dazu in der Lage sind, eine Einwilligung abzugeben. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen oder wenn Betroffene ihre entsprechenden Daten offensichtlich öffentlich gemacht haben. Zulässig ist die Verarbeitung solcher Daten auch dann, wenn dies zum Zwecke der Gesundheitsvorsorge oder sonstiger medizinischer Notwendigkeiten erforderlich ist.

Ebenfalls ist eine derartige Verarbeitung – sofern erforderlich – zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung zulässig.

Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der aus der internationalen Datenschutzorganisation zuständige Ansprechpartner im Vorfeld zu informieren.

h. Automatisierte Einzelentscheidungen

Zur Begründung und Durchführung der Geschäftsbeziehung nutzt DEKRA derzeit grundsätzlich keine vollautomatisierte Entscheidungsfindung. Sofern ein solches Verfahren in Einzelfällen für den Abschluss oder die Erfüllung eines Vertrags erforderlich ist oder gestützt auf eine Einwilligung der Betroffenen oder auf eine anderweitige gesetzlichen Erlaubnis eingesetzt wird, sind die Betroffenen über Ihre diesbezüglichen Rechte gesondert zu informieren, sofern dies gesetzlich vorgegeben ist. Vor Einführung einer automatisierten Entscheidungsfindung konsultiert DEKRA den zuständigen Ansprechpartner der internationalen Datenschutzorganisation.

Automatisierte Datenverarbeitungen durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, dürfen nicht die ausschließliche Grundlage für Entscheidungen mit negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für die Betroffenen sein. Dem Betroffenen muss die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben werden. Zur Vermeidung von Fehlentscheidungen muss eine Kontrolle und eine Plausibilitätsprüfung durch einen Mitarbeitenden gewährleistet werden.

i. Nutzerdaten und Internet

Wenn auf Webseiten oder in Anwendungen personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen und ggf. Cookie-Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind. Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt („Tracking“), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert werden. Ein personenbezogenes Tracking darf nur erfolgen, wenn das nationale Recht dies zulässt oder der Betroffene eingewilligt hat. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden („Opt-out“). Werden bei Webseiten oder Anwendungen in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

2. Beschäftigtendaten

a. Datenverarbeitung auf Grundlage einer Einwilligung

Eine Verarbeitung von Beschäftigtendaten kann aufgrund einer informierten Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Eine erteilte Einwilligung kann jederzeit widerrufen werden. Der Widerruf einer Einwilligung wirkt erst für die Zukunft und berührt nicht die Rechtmäßigkeit der bis zum Widerruf verarbeiteten Daten.

Sofern keine anderweitigen zwingenden Formerfordernisse bestehen, sind Einwilligungserklärungen aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen und zu verwalten (z.B. automatisiertes Einwilligungsmanagement).

b. Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten von Bewerbern unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren oder vor der Weitergabe der Bewerbung an andere Konzerngesellschaften erforderlich.

Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.

Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.

c. Datenverarbeitung aufgrund gesetzlicher Vorgaben oder im öffentlichen Interesse

Die Verarbeitung personenbezogener Beschäftigtendaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeitenden berücksichtigt werden.

d. Kollektivregelungen für Datenverarbeitungen im Arbeitsverhältnis

Geht eine Verarbeitung über den Zweck der Vertragsabwicklung hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivregelung gestattet wird. Kollektivregelungen sind Tarifverträge oder Vereinbarungen zwischen Arbeitgeber und Arbeitnehmervertretungen im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des staatlichen Datenschutzrechts gestaltbar.

Soweit eine Kollektivregelung als Rechtsgrundlage im Sinne des Datenschutzrechts dient, ist dies in dieser Kollektivregelung selbst festzuhalten. Zudem sind angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde und der berechtigten Interessen und der Grundrechte der Mitarbeitenden zu vereinbaren. Dies betrifft etwa Vereinbarungen zur Transparenz der Verarbeitung, ggf. zur Übermittlung an verbundene Unternehmen oder zur Zulässigkeit und zu den Grenzen der Überwachung von Mitarbeitenden. Enthält eine Kollektivregelung spezifische Regeln zu Datenverarbeitungen, vermerkt der Verarbeitungsverantwortliche dies im Verarbeitungsverzeichnis. Alle Mitarbeitenden beachten bei der Verarbeitung personenbezogener Daten die Bestimmungen der anwendbaren Kollektivregelungen. Der Verarbeitungsverantwortliche bringt die konkreten Anforderungen den Mitarbeitenden entsprechend zur Kenntnis und implementiert und dokumentiert die notwendigen Prozesse.

e. Datenverarbeitung zum Schutze lebenswichtiger Interessen

Die Wahrung lebenswichtiger Interessen kann in Notsituationen auch im Arbeitsverhältnis Vorrang gegenüber dem Schutz personenbezogener Daten genießen. Etwa, wenn bei einem Arbeitsunfall für die Behandlung notwendigen Daten eines nicht mehr handlungsfähigen Arbeitnehmers an den Notarzt oder das Krankenhaus übermittelt werden müssen, kann also eine Verarbeitung von personenbezogenen Daten durch DEKRA erforderlich sein. Der Zweck und der Umfang bestimmen sich in diesen Fällen nach dem konkreten Ereignis.

f. Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Beschäftigtendaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses von DEKRA erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich (z.B. Bewertung von Unternehmen) begründet.

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeitenden das Interesse an der Verarbeitung überwiegen. Das Vorliegen

schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.

Kontrollmaßnahmen, die eine Verarbeitung von Beschäftigtendaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen von DEKRA an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeitenden am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse von DEKRA und die möglichen schutzwürdigen Interessen der Mitarbeitenden müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen) berücksichtigt werden.

g. Verarbeitung besonders schutzwürdiger personenbezogener Daten

Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder weltanschauliche Überzeugungen, über Gewerkschaftszugehörigkeiten oder über Genetik, Biometrie, Gesundheit oder das Sexualleben von Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein.

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf grundsätzlich nur erfolgen, wenn dies gesetzlich erforderlich ist oder die Betroffenen ausdrücklich eingewilligt haben.

Eine Einwilligung ist nicht erforderlich, wenn Verarbeitung von besonders schutzwürdigen personenbezogenen Daten zum Schutz lebenswichtiger Interessen der Betroffenen oder einer anderen natürlichen Person erforderlich ist und die Betroffenen aus körperlichen oder rechtlichen Gründen nicht dazu in der Lage sind, eine Einwilligung abzugeben. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen oder wenn Betroffene ihre entsprechenden Daten offensichtlich öffentlich gemacht haben. Zulässig ist die Verarbeitung solcher Daten auch dann, wenn dies zum Zwecke der Gesundheitsvorsorge oder sonstiger medizinischer Notwendigkeiten (z.B. Beurteilung der Arbeitsfähigkeit) erforderlich ist.

Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit DEKRA den bestehenden Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Daten, die Straftaten betreffen, können häufig nur unter besonderen, von staatlichem Recht vorgegebenen Voraussetzungen verarbeitet werden.

Schließlich ist eine derartige Verarbeitung – sofern erforderlich – zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung zulässig.

Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der aus der internationalen Datenschutzorganisation zuständige Ansprechpartner im Vorfeld zu informieren.

h. Automatisierte Einzelentscheidungen

Zur Begründung und Durchführung von Arbeitsverhältnissen nutzt DEKRA derzeit grundsätzlich keine vollautomatisierte Entscheidungsfindung. Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne Persönlichkeitsmerkmale bewertet werden (z.B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeitenden sein. Um Fehlentscheidungen zu vermeiden, muss in automatisierten Verfahren gewährleistet sein, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist. Dem betroffenen Mitarbeitenden müssen außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

i. Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung von DEKRA als Arbeitsmittel zur Verfügung gestellt. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften, Kollektivregelungen und der unternehmensinternen Richtlinien genutzt werden.

Im Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das jeweils nationale geltende Telekommunikationsrecht zu beachten, soweit diese Anwendung finden.

Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer können Schutzmaßnahmen an den Übergängen in das DEKRA-Netz implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren.

Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets sowie der internen sozialen Netzwerke zeitlich befristet protokolliert werden. Eine derartige Protokollierung erfolgt auch, sofern diese nach dem jeweils geltenden nationalen Datenschutzrecht erforderlich ist (z.B. zur Eingabe- und Zugriffskontrolle).

Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien von DEKRA erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Konzernregelungen (z.B. Kollektivregelungen).

III. Datenverarbeitung im Auftrag

Eine Datenverarbeitung im Auftrag liegt vor, wenn ein Auftragnehmer von DEKRA oder DEKRA von einem Auftraggeber mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass dabei die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist – sofern gesetzlich vorgesehen – sowohl mit externen Auftragnehmern als auch zwischen Unternehmen innerhalb von DEKRA eine Vereinbarung über eine Auftragsverarbeitung abzuschließen.

Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung und die Zulässigkeit der Datenverarbeitung. Der Auftragnehmer („Auftragsverarbeiter“) darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Verarbeitungsverantwortliche muss ihre Umsetzung sicherstellen.

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen unter Einbindung des Zuständigen Ansprechpartners der Informationssicherheitsorganisation von DEKRA auszuwählen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen.
2. Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
3. Die von der internationalen Datenschutzorganisation von DEKRA für den Datenschutz bereitgestellten Vertragsstandards müssen grundsätzlich beachtet werden. Dies gilt nicht, wenn sich dies gegenüber einem Auftragnehmer nicht erreichen lässt und diese über eigene die rechtlichen Anforderungen angemessen berücksichtigende Vertragsstandards verfügen. In diesem Fall und bei von einem Auftragnehmer gewünschten Änderungen der von DEKRA bereitgestellten Vertragsstandards ist der zuständige Ansprechpartner der internationalen Datenschutzorganisation von DEKRA zu konsultieren.

Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.

IV. Datenverarbeitung in Gemeinsamer Verantwortlichkeit

Entscheiden zwei oder mehrere DEKRA Konzerngesellschaften oder eine DEKRA Konzerngesellschaft und ein Dritter gemeinsam über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten, erfolgt die Datenverarbeitung in Gemeinsamer Verantwortlichkeit.

Für jeden Fall einer solchen Datenverarbeitung in Gemeinsamer Verantwortlichkeit legen die beteiligten DEKRA Konzerngesellschaften ihre Rolle und jeweiligen Pflichten in Bezug auf die Datenverarbeitung transparent fest. Die Festlegung muss die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber den Betroffenen gebührend widerspiegeln. Ziel dieser Vorgabe ist der Schutz der Rechte und Freiheiten der Betroffenen und eine Zuordnung von Verantwortung und Haftung, auch mit Blick auf die Überwachungs- und sonstigen Maßnahmen der Aufsichtsbehörden. Sofern gesetzlich vorgesehen, bedarf es des Abschlusses einer Vereinbarung über die Datenverarbeitung in gemeinsamer Verantwortlichkeit.

V. Datensicherheit

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung, Weitergabe, Offenlegung sowie gegen Verlust, Verfälschung oder Vernichtung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik (gemeint sind nicht die neuesten technischen Entwicklungen und Fortschritte, sondern

die am Markt verfügbaren Technologien), den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten zu orientieren. Bei den Risiken sind die Schwere des potentiellen Schadens für die Betroffenen und die Eintrittswahrscheinlichkeit zu berücksichtigen. Darüber hinaus dürfen die Implementierungskosten nicht außer Verhältnis zu den ermittelten Risiken stehen. Der Verarbeitungsverantwortliche zieht dazu insbesondere den zuständigen Ansprechpartner aus der Informationssicherheitsorganisation von DEKRA zu Rate. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des konzernweiten Informationssicherheitsmanagements müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden. Ihre Wirksamkeit ist durch den Verarbeitungsverantwortlichen unter Hinzuziehung der Informationssicherheitsorganisation regelmäßig zu überprüfen.

VI. Meldung von Datensicherheitsvorfällen

DEKRA ist dazu verpflichtet, Verletzungen der Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit im Umgang mit personenbezogenen Daten („Datensicherheitsvorfall“) zu dokumentieren und diese in bestimmten Fällen innerhalb der gesetzlich vorgesehenen Meldefristen den Datenschutz-Aufsichtsbehörden zu melden und gegebenenfalls die Betroffenen zu benachrichtigen. Ob eine derartige Melde- bzw. Benachrichtigungspflicht besteht, gilt es für die folgenden drei Arten von Datensicherheitsvorfällen zu prüfen:

- **Vertraulichkeitsbruch** – unberechtigte(r)/unbeabsichtigter(r) Veröffentlichung, Zugriff oder Zugang
- **Integritätsbruch** – unberechtigte/unbeabsichtigter Veränderung
- **Verfügbarkeitsbruch** – unberechtigte(r)/unbeabsichtigter(r) Zugangsverhinderung oder Verlust

DEKRA hat daher über ein entsprechend ausgestaltetes Incident Report Management sicherzustellen, dass unverzüglich ab Kenntnis eines Datensicherheitsvorfalles der jeweils zuständige Ansprechpartner der Informationssicherheitsorganisation sowie der Datenschutzorganisation hierüber informiert wird, um rechtzeitig das Vorliegen einer etwaigen Meldepflicht zu prüfen und diese erfüllen zu können.

Jeder tatsächliche oder vermutete Datensicherheitsvorfall ist danach so schnell wie möglich zu melden.