Datenschutz-Sicherheitsrichtlinie

I Ziel der Datenschutz-Sicherheitsrichtlinie

Die HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb verpflichtet sich im Rahmen seiner gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten. Diese Datenschutz-Sicherheitsrichtlinie gilt weltweit für die HAAsE-GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb und beruht auf global akzeptierten Grundprinzipien zum Datenschutz. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb als attraktiver Arbeitgeber.

Unsere Datenschutz-Sicherheitsrichtlinie schafft eine der notwendigen Rahmenbedingungen für weltweite Datenübermittlungen zwischen einzelnen Unternehmen. Sie gewährleistet das von der Europäischen Datenschutz-Grundverordnung und den nationalen Gesetzen verlangte angemessene Datenschutzniveau für den grenzüberschreitenden Datenverkehr auch in solche Länder, in denen gesetzlich kein angemessenes Datenschutzniveau besteht.

II Geltungsbereich und Änderung der Datenschutz-Sicherheitsrichtlinie

Diese Datenschutz-Sicherheitsrichtlinie fußt auf den Vorgaben der EU-Datenschutz-Grundverordnung und den dazugehörigen nationalen Gesetzen.

Diese Datenschutz-Sicherheitsrichtlinie gilt für die gesamte HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb an allen Standorten.

Die aktuellste Version der Datenschutz-Sicherheitsrichtlinie kann auf der Internetseite der HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb (http://haase-bahn.de) abgerufen werden.

III Geltung staatlichen Rechts

Diese Datenschutz-Sicherheitsrichtlinie beinhaltet die weltweit akzeptierten Datenschutzprinzipien, ohne dass bestehendes staatliches Recht ersetzt wird. Sie ergänzt das jeweilige nationale Datenschutzrecht. Das jeweilige staatliche Recht geht vor, wenn es Abweichungen von dieser Datenschutz-Sicherheitsrichtlinie erfordert oder weitergehende Anforderungen stellt. Die Inhalte dieser Datenschutz-Sicherheitsrichtlinie sind auch dann zu beachten, wenn es kein entsprechendes staatliches Recht gibt. Die aufgrund staatlichen Rechts bestehenden Meldepflichten für Datenverarbeitungen müssen beachtet werden.

Jedes Unternehmen der HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb ist für die Einhaltung dieser Datenschutz-Sicherheitsrichtlinie und der gesetzlichen Verpflichtungen verantwortlich.

Hat es Grund zu der Annahme, dass gesetzliche Verpflichtungen im Widerspruch zu den Pflichten aus dieser Datenschutz-Sicherheitsrichtlinie stehen, hat das betroffene Konzernunternehmen unverzüglich den Konzernbeauftragten für den Datenschutz zu informieren. Im Falle einer Kollision zwischen nationaler Rechtsvorschrift und der Datenschutz-Sicherheitsrichtlinie wird HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb gemeinsam mit dem betroffenen Konzernunternehmen nach einer praktikablen Lösung im Sinne der Ziele der Datenschutz-Sicherheitsrichtlinie suchen.

IV Prinzipien für die Verarbeitung personenbezogener Daten

1 Fairness und Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten wahren wir das informationelle Selbstbestimmungsrecht des Betroffenen. Personenbezogene Daten werden nur auf rechtmäßige Weise erhoben und verarbeitet.

2 Zweckbindung

Die Verarbeitung personenbezogener Daten verfolgt lediglich die Zwecke, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

3 Transparenz

Der Betroffene wird über den Umgang mit seinen Daten informiert. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten wird der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert:

- → die Identität der verantwortlichen Stelle
- → den Zweck der Datenverarbeitung
- → die hinterlegten Aufbewahrungsfristen
- → Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

4 Datenvermeidung und Datensparsamkeit

Vor einer Verarbeitung personenbezogener Daten wird geprüft, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, werden anonymisierte oder statistische Daten verwendet.

Personenbezogene Daten werden nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder durch ein berechtigtes Interesse begründet.

5 Löschung und Speicherbegrenzung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, werden gelöscht.

Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wird.

Sollte die HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb ein berechtigtes Interesse an der Speicherung der Daten haben, wird dies den betroffenen Personen mitgeteilt.

6 Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten werden nach bestem Gewissen richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand gespeichert. Es werden angemessene Maßnahmen getroffen, um sicherzustellen, dass nichtzutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

7 Vertraulichkeit und Datensicherheit

Für personenbezogene Daten gilt das Datengeheimnis.

Die HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb behandeln persönliche Daten vertraulich. Wir schützen nach besten Gewissen alle personenbezogenen Daten durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, versehentlichen Verlust, Veränderung oder Zerstörung.

V Zulässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

1 Kunden und Partnerdaten

1.1 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht.

Im Vorfeld eines Vertrages – also in der Vertragsanbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt.

Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten.

Für darüberhinausgehende Werbemaßnahmen müssen die folgenden Voraussetzungen unter V.1.2 beachtet werden.

1.2 Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an die HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb (z.B. Wunsch nach Zusendung von Informationsmaterial zu einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

Kundenbindungs- oder Werbemaßnahmen bedürfen jedoch 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. Der Betroffene wird in diesem Fall über die Verwendung seiner Daten für Zwecke der Werbung informiert.

Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene wird über die Freiwilligkeit der Angabe von Daten für diese Zwecke informiert. Im Rahmen der Kommunikation mit dem Betroffenen wird eine Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu Werbezwecken eingeholt. Der Betroffene kann im Rahmen der Einwilligung zwischen den verfügbaren Kontaktkanälen wie Post, elektronische Post und Telefon wählen (Einwilligung siehe V.1.3).

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

1.3 Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden.

Vor der Einwilligung wird der Betroffene gemäß dieser Datenschutz-Sicherheitsrichtlinie informiert. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich in Schrift- oder Textform einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Die Erteilung wird dann jedoch dokumentiert.

1.4 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist 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.

1.5 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen werden für jede Verarbeitung geprüft.

1.6 Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. 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.

1.7 Automatisierte Einzelentscheidungen

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

1.8 Nutzerdaten und Internet

Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, werden die Betroffenen hierüber in Datenschutzerklärungen und ggf. Cookie-Hinweisen informiert. Die Datenschutzhinweise und ggf. Cookie-Hinweise werden so integriert, 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), werden die Betroffenen darüber in jedem Fall in der Datenschutz-Sicherheitsrichtlinie informiert. Erfolgt das Tracking unter einem Pseudonym, so wird dem Betroffenen eine Widerspruchsmöglichkeit eröffnet (Opt-out).

Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so wird die Identifizierung und Authentifizierung der Betroffenen so gestaltet, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

2 Mitarbeiterdaten

2.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis werden die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind.

Bei der Anbahnung eines Arbeitsverhältnisses werden personenbezogene Daten von Bewerbern verarbeitet. Nach Ablehnung werden die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen gelöscht, 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 Unternehmensteile oder verbundene Unternehmen erforderlich.

Im bestehenden Arbeitsverhältnis ist die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen, 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, werden die jeweiligen nationalen gesetzlichen Anforderungen berücksichtigt. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.
- → Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

2.2 Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen.

Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen.

2.3 Automatisierte Entscheidungen

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 Mitarbeiter 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 Mitarbeiter muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

2.4 Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. diese sind Arbeitsmittel und Unternehmensressourcen. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden.

Eine generelle Überwachung der Telefone und der E-Mail-Kommunikation bzw. der Intranet- und Internetnutzung findet statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer sind Schutzmaßnahmen an den Übergängen in das HBK-Netzwerk implementiert worden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit und Nachvollziehbarkeit wird die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets sowie der internen sozialen Netzwerke protokolliert.

Personenbezogene Auswertungen dieser Daten erfolgen nur bei einem konkret begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien der HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb. Diese Kontrollen erfolgen nur unter Wahrung des Verhältnismäßigkeitsprinzips. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Konzernregelungen. Die Auswertungen dienen nicht der Leistungserfassung.

VI Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb oder an Empfänger innerhalb der HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten. Der Empfänger der Daten muss vorher darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.

Im Falle einer Datenübermittlung an einen Empfänger außerhalb der HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb in einem Drittstaat muss dieser ein zu dieser Datenschutz-Sicherheitsrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt.

Im Falle einer Datenübermittlung von Dritten an die HAAsE GmbH Bahnservice und HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb wird sichergestellt, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

VII Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen wird mit externen Auftragnehmern eine Vereinbarung über eine Auftragsdatenverarbeitung abgeschlossen.

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

1. Der Auftragnehmer wird nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.
2. Der Auftrag ist in Schrift- oder Textform zu erteilen. Dabei werden die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers dokumentiert.
3. Der Auftraggeber wird sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.
4. Bei einer grenzüberschreitenden Auftragsdatenverarbeitung werden die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland beachtet und erfüllt. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftragnehmer ein zu dieser Datenschutz-Sicherheitsrichtlinie gleichwertiges Datenschutzniveau nachweist

VIII Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

1. Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt.
2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
4. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.
5. Der Betroffene ist berechtigt, die Löschung seiner Daten („Recht auf Vergessenwerden“) zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.
6. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.
7. Der Betroffene hat das Recht auf Datenübertragbarkeit. Nach Anfrage werden dem Betroffenen die personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format von dem Verantwortlichen zur Verfügung gestellt. Eine Weiterleitung an einen andern Verantwortlichen darf von uns nicht behindert werden.
8. Wenn der Betroffene der Ansicht ist, dass die Verarbeitung Ihrer Daten gegen die DS-GVO verstößt, hat der Betroffene das Recht Beschwerde bei der Aufsichtsbehörde einzulegen. Hierzu muss sich an die zuständige Aufsichtsbehörde gewendet werden.

IX Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt.

Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

X Sicherheit der Verarbeitung

Personenbezogene Daten werden nach bestem Gewissen jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung geschützt. 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, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren.

Die technisch organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des unternehmensweiten Informationssicherheits- und Datenschutz-Managements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

XI Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem Konzernbeauftragten für den Datenschutz, den Datenschutzkoordinatoren und weiteren, mit Audit-Rechten ausgestatteten Unternehmensbereichen oder -beauftragten externen Prüfern. Die Ergebnisse der Datenschutzkontrollen sind dem Konzernbeauftragten für den Datenschutz mitzuteilen. Dem Datenschutzbeauftragten der HAAsE GmbH Bahnservice & HAAsE GmbH Ausbildungs-Akademie für sicheren Eisenbahnbetrieb ist im Rahmen der jeweiligen Berichtspflichten über wesentliche Ergebnisse zu informieren. Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

XII Datenschutzvorfälle

Jeder Mitarbeiter soll der Geschäftsleitung unverzüglich Fälle von Verstößen gegen diese Datenschutz-Sicherheitsrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) melden.

In Fällen von

- → unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
- → unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder
- → bei Verlust personenbezogener Daten

sind die im Unternehmen vorgesehenen Meldungen (Information Security Incident Management) unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

XIII Verantwortlichkeiten und Sanktionen

Die Geschäftsleitung ist für die verordnungskonforme Datenverarbeitung der Daten verantwortlich.

Kontaktdaten:

Sarah Haase
info@haase-bahn.de
0151-10869990
Friedenstr. 14a
93053 Regensburg

Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutz-Sicherheitsrichtlinie enthaltenen Anforderungen des Datenschutzes eingehalten werden (z.B. nationale Meldepflichten).

Es ist eine Managementaufgabe der Geschäftsleitung, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter.

Aufgrund der rechtlichen Vorgaben (weniger als neun regelmäßig automatisiert personenbezogene Daten verarbeitende Mitarbeiter) bestellt die Geschäftsführung keinen Datenschutzbeauftragten. Es ist allerdings eine Ansprechperson für Datenschutz benannt und kommuniziert.

Dieser ist vor Ort Ansprechpartner für den Datenschutz. Er kann Kontrollen durchführen und hat die Mitarbeiter mit den Inhalten der Datenschutz-Sicherheitsrichtlinien vertraut zu machen. Die Geschäftsleitung ist verpflichtet, diesen Ansprechpartner in seiner Tätigkeit zu unterstützen. Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen den Ansprechpartner rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Ansprechpartner schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten.

Die Geschäftsleitung hat sicherzustellen, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

XIV Der Ansprechpartner für Datenschutz bei der HAAsE GmbH

Der Ansprechpartner für Datenschutz wirkt auf die Einhaltung der Datenschutzvorschriften hin.

Er ist verantwortlich für die Überwachung der Einhaltung der Richtlinien zum Datenschutz. Er wird die Geschäftsleitung zeitnah über Datenschutzrisiken informieren.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an ihn wenden. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.

Kontaktdaten:

Fey Mathias
0151-50982033
datenschutz@haase-bahn.de

XV Definitionen

» Ein angemessenes Datenschutzniveau von Drittstaaten wird von der EU Kommission dann anerkannt, wenn der Kernbestand der Privatsphäre, so wie er in den Mitgliedstaaten der EU übereinstimmend verstanden wird, im Wesentlichen geschützt wird. Die EU Kommission berücksichtigt bei ihrer Entscheidung alle Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Dies schließt die Beurteilung staatlichen Rechts sowie der jeweiligen geltenden Standesregeln und Sicherheitsmaßnahmen ein.

» Anonymisiert sind Daten dann, wenn ein Personenbezug dauerhaft und von niemandem mehr hergestellt werden kann bzw. wenn der Personenbezug nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden könnte.

» Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

» Betroffener im Sinne dieser Datenschutzrichtlinie ist jede natürliche Person, über die Daten verarbeitet werden. In einigen Ländern können auch juristische Personen Betroffener sein.

» Datenschutzvorfälle sind alle Ereignisse, bei denen der begründete Verdacht besteht, dass personenbezogene Daten rechtswidrig ausgespäht, erhoben, verändert, kopiert, übermittelt oder genutzt wurden. Das kann sich sowohl auf Handlungen durch Dritte als auch Mitarbeiter beziehen.

» Dritter ist jeder außerhalb des Betroffenen und der für die Datenverarbeitung verantwortlichen Stelle. Auftragsdatenverarbeiter sind innerhalb der EU nicht Dritte im Sinne des Datenschutzrechtes, da sie gesetzlich der verantwortlichen Stelle zugeordnet sind.

- Drittstaaten im Sinne der Datenschutzrichtlinie sind alle Staaten außerhalb der Europäischen Union/EWR. Ausgenommen sind Staaten, deren Datenschutzniveau von der EU Kommission als angemessen anerkannt worden ist.
- Einwilligung ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.
- Erforderlich ist die Verarbeitung personenbezogener Daten, wenn der zulässige Zweck oder das berechtigte Interesse ohne die jeweiligen personenbezogenen Daten nicht oder nur mit unverhältnismäßig hohem Aufwand zu erreichen ist.
- Der Europäische Wirtschaftsraum (EWR) ist ein mit der EU assoziierter Wirtschaftsraum, dem Norwegen, Island und Liechtenstein angehören.
- Personenbezogene Daten sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Bestimmbar ist eine Person z.B. dann, wenn der Personenbezug durch eine Kombination von Informationen mit auch nur zufällig vorhandenem Zusatzwissen hergestellt werden kann.
- Übermittlung ist jede Bekanntgabe von geschützten Daten durch die verantwortliche Stelle an Dritte.
- Verarbeitung personenbezogener Daten ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang zur Erhebung, Speicherung, Organisation, Aufbewahrung, Veränderung, Abfrage, Nutzung, Weitergabe, Übermittlung, Verbreitung oder der Kombination und der Abgleich von Daten. Dazu gehört auch das Entsorgen, Löschen und Sperren von Daten und Datenträgern.

XVI Inkraftsetzung

Dieses Dokument wird einmal jährlich sowie bei Bedarf auf Vollständigkeit und Aktualität überprüft.

Änderungen dieses Dokuments liegen in der Verantwortung des Zuständigen für Datenschutz-Management.

Dieses Dokument ist allen Mitarbeitern, Geschäftspartnern und Interessenten zugänglich zu halten.

Sarah Haase, Geschäftsführer

18.05.2018