Datenschutzkonzept

Securitas Holding GmbH
Wahlerstraße 2a

47402 Düsseldorf

Inhaltsverzeichnis

	Präambel	Seite 1
1	Zweck des Datenschutzkonzeptes	Seite 2
2	Datenschutz-Grundsätze	Seite 2
2.1	Transparenz der Datenverarbeitung	Seite 2
2.2	Grundsatz der Datenvermeidung und der -sparsamkeit	Seite 2
2.3	Grundsatz der Anonymisierung und Pseudonymisierung	Seite 2
2.4	Datenerhebung beim Betroffenen	Seite 3
2.5	Zweckbindung der Verarbeitung und Nutzung von Daten	Seite 3
2.6	Grundsatz der Verhältnismäßigkeit	Seite 3
3	Datenübermittlung und Offenbarungen	Seite 3
3.1	Datenübermittlung in das Ausland	Seite 3
3.2	Sonstige Auskünfte	Seite 3
3.3	Offenbarungen innerhalb des Unternehmens	Seite 3
4	Rechte der Betroffenen	Seite 3
5	Verpflichtung auf das Datengeheimnis	Seite 4
6	Datenschutzbeauftragter	Seite 4
7	Verfahrensbeschreibung	Seite 4
8	Datenschutzfolgeabschätzung	Seite 4
9	Einweisung in den Datenschutz	Seite 5
10	Schutzeinstufung der Daten	Seite 5
10.1	Personenbezogene Daten	Seite 5
10.2	Betriebswirtschaftliche Daten	Seite 6
11.	Bewertung der Wirksamkeit des Datenschutzmanagements	Seite 6

Präambel

Unser Wirtschaftsleben ist heute von einer zunehmenden Abhängigkeit der Unternehmen von Informationen, einer hohen Komplexität der technischen Systeme und einer zunehmenden Schnelllebigkeit der Arbeitswelt gekennzeichnet. Bestand früher der Wert der Unternehmen aus dem Wissen und Können der Mitarbeiter und den baulichen und technischen Anlagen, spielen heute Informationen sowie deren Richtigkeit und jederzeitige Verfügbarkeit eine immer wichtigere Rolle. Ein hohes Maß an Informationssicherheit ist deshalb von herausragender Bedeutung. Stehen Informationen nicht rechtzeitig oder nicht vollständig zur Verfügung, ist die Richtigkeit der Informationen nicht gewährleistet oder geraten sie in unbefugte Hände, kann einerseits für den Betroffenen eine erhebliche Beeinträchtigung seines Persönlichkeitsrechts, seiner gesellschaftlichen Stellung

oder seiner wirtschaftlichen Verhältnisse entstehen. Andererseits kann ein Missbrauch die betriebliche Funktion, die Umweltbeziehungen oder das Ansehen unseres Unternehmens erheblich beeinträchtigen und dadurch großen Schaden verursachen.
Das Anliegen dieser Datenschutzrichtlinie ist es deshalb, im Interesse der betroffenen Personen und auch des Unternehmens in jeder Phase der Informationsverarbeitung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten zu gewährleisten. Um dieses Ziel zu erreichen, müssen nicht nur gesetzliche Vorschriften zum Schutz der Daten eingehalten, sondern auch geeignete technische und organisatorische Maßnahmen eingerichtet und geregelt werden. Nicht zuletzt kommt es aber auch darauf an, dass sich alle Beschäftigte der mit der Datenverarbeitung und der Benutzung der technischen Systeme und Kommunikationstechnologien verbundenen Risiken bewusst sind und mit Daten und Systemen mit der erforderlichen Vorsicht und Sorgfalt umgehen. Aus diesem Grund werden alle Beschäftigten, die mit personenbezogenen Daten umgehen, in geeigneter Weise im Datenschutz geschult und auf die Einhaltung des Datengeheimnisses verpflichtet.

1 Zweck des Datenschutzkonzeptes

Das Datenschutzmanagementsystem (DSM) folgt in der Dokumentenstruktur der Datenschutzgrundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz (BDSG) und regelt mit den mitgeltenden Unterlagen die rechtlichen, technischen und organisatorischen Maßnahmen zum Datenschutz. Die Einzelheiten zu den eingerichteten technischen Maßnahmen und die organisatorischen Regelungen befinden sich in den Informationssicherheitsrichtlinien. Weil ein wirksamer Datenschutz nicht alleine durch Regelungen und Bestimmungen erreicht werden kann, sondern von einem ausgeprägten Datenschutz- und Sicherheitsbewusstsein der Mitarbeitenden getragen wird, ist es ein besonderes Anliegen dieser Richtlinie, diese für das Anliegen des Datenschutzes zu sensibilisieren und ihnen Informationen und Regelungen an die Hand zu geben, die es ermöglichen, die mit dem Betrieb komplexer und offener Datenverarbeitungs- und Kommunikationssysteme verbundenen Risiken zu erkennen und damit umzugehen.
Auf der Grundlage der Bewertung der datenschutzrechtlichen und betriebswirtschaftlichen Sensibilität der Daten und der anschließenden Einstufung in Schutz- und Vertraulichkeitsstufen wurden die erforderlichen technischen und organisatorischen Maßnahmen definiert und beschrieben. Damit besteht für Revisoren, Auditoren und auch für die Datenschutz-Aufsichtsbehörde eine fundierte und schlüssige Möglichkeit, die Vollständigkeit, Notwendigkeit und Angemessenheit der technischen und organisatorischen Maßnahmen zu beurteilen.

2 Datenschutz-Grundsätze (Artikel 5 DS-GVO)

2.1 Transparenz der Datenverarbeitung

Die Betroffenen (Beschäftigte, Kunden, Lieferanten, Geschäftspartner) werden bei der Erhebung der Daten über die Zwecke der Erhebung, Verarbeitung oder Nutzung und im Falle einer Datenübermittlung auch über die Übermittlungszwecke und Kategorien von Empfängern und über ihre Datenschutzrechte unterrichtet. Im Internetauftritt des Unternehmens werden diese Informationen ebenfalls an leicht erreichbarer Stelle angeboten.

2.2 Grundsatz der Datenvermeidung und der Datensparsamkeit

Ein Anliegen des Datenschutzes besteht darin, den Umfang der Verarbeitung personenbezogener Daten auf das Maß des Notwendigen zu begrenzen und nur diejenigen Datenarten zu erheben und zu verarbeiten, die für das Erreichen des jeweiligen Verarbeitungszwecks auch erforderlich sind. Datenverarbeitungsverfahren werden deshalb, soweit es im Hinblick auf den zu erreichenden Zweck der Anwendungen möglich ist, so gestaltet, dass möglichst wenig personenbezogene Daten verarbeitet werden. Eine Datenerhebung auf Vorrat verbietet sich.

2.3 Grundsatz der Anonymisierung und Pseudonymisierung

Soweit wirtschaftlich vertretbar, sollen personenbezogene Daten bei der Verarbeitung und Nutzung frühzeitig anonymisiert oder pseudonymisiert werden. Bei Auswertungen, z.B. im Zusammenhang mit Controlling Maßnahmen, wird deshalb anonymisierten Auswertungen, soweit möglich, der Vorzug vor personenbezogenen Auswertungen gegeben. Ebenso werden Daten möglichst in anonymisierter oder pseudonymisierter Form übermittelt, wenn der Personenbezug zur Erreichung des Übermittlungszwecks nicht erforderlich ist.

2.4 Datenerhebung beim Betroffenen
Personenbezogene Daten werden grundsätzlich vom Betroffenen selbst erhoben, es sei denn, der Betroffene hat diese Daten selbst über allgemein zugängliche Quellen, z.B. durch öffentliche Verzeichnisse oder das Internet, verfügbar gemacht. Bei der Erhebung von personenbezogenen Daten beim Betroffenen ist der Betroffene gemäß Artikel 13 DS-GVO über die Identität der verantwortlichen Stelle, über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und bei Übermittlungen auch über die Kategorien von Empfängern zu unterrichten. Besteht für eine Erhebung, Verarbeitung oder Nutzung keine ausreichende Rechtsgrundlage, ist eine Einwilligung des Betroffenen einzuholen, wobei der Betroffene unmissverständlich über die Freiwilligkeit der Einwilligung unterrichten wird.

2.5 Zweckbindung der Verarbeitung und Nutzung von Daten
Personenbezogene Daten werden nur für die Zwecke verarbeitet und genutzt, für die sie erhoben wurden und die dem Betroffenen auch als Erhebungszweck dargelegt worden sind. Für andere Zwecke werden die Daten nur genutzt, soweit dies nach den Vorschriften der DS-GVO, des BDSG oder einer anderen Rechtsvorschrift ausdrücklich zulässig ist. Die Einhaltung dieses Zweckbindungsgebots folgt auch dem Grundsatz von Treu und Glauben.

2.6 Grundsatz der Verhältnismäßigkeit
Nach dem Grundsatz der Verhältnismäßigkeit muss die Erhebung und Verarbeitung von personenbezogenen Daten für die Zweckerreichung geeignet, erforderlich und angemessen sein. Dies bedeutet, dass für die jeweiligen Geschäftszwecke immer nur das mildeste, gleich gut geeignete Mittel, also die Verfahrensweise gewählt wird, die am wenigsten in das Persönlichkeitsrecht der Betroffenen eingreift und dafür nur die zur Zweckerreichung erforderlichen Daten erhoben werden. Eventuelle Nachteile oder Risiken für die Betroffenen dürfen nicht außer Verhältnis zum Nutzen der Datenverarbeitung stehen.

3 Datenübermittlung und Offenbarungen

3.1 Datenübermittlung in das Ausland
Bei einer Datenübermittlung innerhalb der EU/EWR gelten die gleichen datenschutzrechtlichen Voraussetzungen wie innerhalb der Bundesrepublik Deutschland.
Eine Datenübermittlung in Drittstaaten erfolgt nur, wenn dies zur Erfüllung eines Vertrags mit dem Betroffenen erforderlich ist oder sonstige Erlaubnistatbestände nach den Vorschriften des Datenschutzgesetzes erfüllt sind oder der Betroffene eingewilligt hat. Vor einer Übermittlung in ein Drittland wird der Datenschutzbeauftragte zur Prüfung der Zulässigkeit der Übermittlung eingeschaltet.

3.2 Sonstige Auskünfte
Auskünfte an Dritte sind nur zulässig, wenn eine Rechtsvorschrift dies vorschreibt, der Betroffene eingewilligt hat oder aufseiten der Auskunft verlangenden Stelle oder des Unternehmens ein berechtigtes Interesse besteht und schutzwürdige Interessen der Betroffenen nicht verletzt sind. Die Auskunft erteilende Stelle im Unternehmen hat sich die Rechtsgrundlagen für die Auskunft belegen zu lassen. Auskünfte werden grundsätzlich nur schriftlich erteilt. Bei Zweifelsfällen ist der Vorgesetzte, ggf. der Datenschutzbeauftragte, einzuschalten.

3.3 Offenbarungen innerhalb des Unternehmens
Eine Offenbarung von Daten an Stellen innerhalb des Unternehmens ist grundsätzlich nur zulässig, soweit dies zur Erfüllung der Aufgaben der empfangenden Stelle erforderlich ist (ErwG 48). Dies gilt für Personaldaten auch gegenüber den Vorgesetzten und dem Betriebsrat.

4 Rechte der Betroffenen

Jeder Betroffene hat ein Recht auf Auskunft und ggf. auf Berichtigung, Löschung oder Sperrung seiner personenbezogenen Daten (Artikel 15 ff. DS-GVO), wenn die Daten unrichtig sind oder für den Zweck, für den sie erhoben und gespeichert worden sind, nicht mehr erforderlich sind und keiner Aufbewahrungspflicht mehr unterliegen. Zur Wahrnehmung seiner Rechte kann sich jeder Betroffene an jede beliebige Stelle des Unternehmens wenden und Auskunft über die zu seiner Person gespeicherten Daten verlangen. Soweit die Daten unrichtig sind, kann er deren Berichtigung und, soweit sie zur Aufgabenerfüllung nicht mehr erforderlich sind, im Rahmen der rechtlichen Möglichkeiten ihre Löschung verlangen. Unterliegen die Daten noch Aufbewah-

rungsvorschriften oder ist die Löschung wegen der Art ihrer Speicherung nur mit einem unverhältnismäßig hohen Aufwand möglich, tritt anstelle einer Löschung eine Sperrung. Zu diesem Zweck werden die Daten im Rahmen der gegebenen Möglichkeiten als gesperrt gekennzeichnet. Die gesperrten Daten dürfen ohne Einwilligung des Betroffenen oder einer Rechtsvorschrift (z.B. Abgabenordnung) nicht mehr genutzt oder übermittelt werden.
Im Falle eines Auskunftsverlangens oder eines Verlangens einer Löschung oder Sperrung hat die angesprochene Stelle umgehend den Beauftragten für den Datenschutz über den Vorgang zu informieren. Der Beauftragte für den Datenschutz und die für die Daten fachverantwortliche Stelle stimmen die notwendigen Maßnahmen ab.
Auskunftsverlangen sind unverzüglich zu bearbeiten und dem Betroffenen eine Bestätigung über die Änderung oder Löschung der betroffenen Daten zu erteilen. Falls in der Bearbeitung Verzögerungen auftreten, ist dem Betroffenen eine Zwischennachricht zu erteilen.

5 Verpflichtung auf das Datengeheimnis

Jeder Beschäftigte, der mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt ist, ist auf das Datengeheimnis zu verpflichten. Diese Verpflichtung ergibt sich aus dem Artikel 28, Abs.3, lit.b DS-GVO.
Danach ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Die Verpflichtung gilt auch für andere Beschäftigte, die unbeaufsichtigt in Räumen tätig sind, in denen personenbezogene Daten zugänglich sind, z.B. für Sicherheitskräfte. Soweit Personal von fremden Unternehmen eingesetzt wird, z.B. externes Reinigungspersonal etc., wird dieses Personal ebenfalls verpflichtet oder die Verpflichtung dieser Personen wird mit den beauftragten Unternehmen vertraglich vereinbart. Verpflichtet werden auch Praktikanten, Leiharbeiter und sonstige externe Mitarbeiter (Berater etc.), wenn sie im Rahmen ihrer Tätigkeiten personenbezogene Daten zur Kenntnis nehmen können.
Die Verpflichtung ist für die Beschäftigten in der Personalakte und für alle betriebsfremden Personen bei den jeweiligen Vertragsunterlagen zu dokumentieren.

6 Datenschutzbeauftragter

Die DS-GVO, und insbesondere das BDSG, schreibt für die Securitas Holding GmbH die Bestellung eines Datenschutzbeauftragten vor. Dieser ist bei der jeweiligen Aufsichtsbehörde gemeldet. Die Aufgaben des Datenschutzbeauftragten richten sich nach den Vorgaben der DS-GVO. Zu seiner Unterstützung sind im erforderlichen Umfang Datenschutzkoordinatoren bestellt.
Jeder von der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch die Securitas Holding GmbH Betroffene kann sich an den Beauftragten für den Datenschutz wenden. Ebenso kann sich jeder Mitarbeiter in allen Fragen des Datenschutzes an ihn wenden. Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen verpflichtet, soweit er nicht durch den Betroffenen davon entbunden ist.

7 Verzeichnis von Verarbeitungstätigkeiten (VVT)

Der Datenschutzbeauftragte überwacht das interne VVT, die Übersicht über die technischen und organisatorischen Maßnahmen zum Datenschutz und die Informationspflichten. Das VVT enthält auch alle datenschutzrechtlichen Prüfungen über die Zulässigkeit der Erhebung, Verarbeitung, Nutzung und Übermittlung der Daten und ist damit ein wichtiger Nachweis für die Prüfung der Ordnungsmäßigkeit der Datenverarbeitungsverfahren. Zur Aufnahme der Verarbeitungstätigkeiten in das VVT ist der Datenschutzbeauftragte rechtzeitig vor Einführung von neuen Verarbeitungstätigkeiten zu unterrichten. Dies gilt auch bei datenschutzrelevanten Änderungen an bestehenden Verarbeitungstätigkeiten, z.B. bei einer Änderung des Datenkatalogs, zusätzlichen Übermittlungen oder Nutzungen oder Änderung des Verarbeitungsverfahrens.

8 Datenschutzfolgeabschätzung (DSFA)

Datenverarbeitungsverfahren sollen bereits im Planungsstadium vom Datenschutzbeauftragten auf ihre datenschutzrechtliche Verträglichkeit überprüft werden. Soweit automatisierte Verarbeitungen besondere Risiken

für die Rechte und Freiheiten der Betroffenen aufweisen (z.B. Verfahren zur Verarbeitung von Personaldaten und insbesondere solche zur Verarbeitung von besonderen Daten-arten oder Verfahren zur Bewertung der Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens), besteht eine gesetzliche Verpflichtung gemäß Artikel 35 DS-GVO zur Durchführung der DSFA. Der Datenschutzbeauftragte ist frühzeitig von den projektverantwortlichen Stellen über datenschutzrelevante Vorhaben zu unterrichten und in den Planungsprozess einzubeziehen. Dadurch soll gewährleistet werden, dass die Datenverarbeitungsverfahren den Regelungen des Datenschutzes entsprechen und nachträgliche und kostenintensive Verfahrensänderungen vermieden werden. Die Ergebnisse der Vorabkontrolle werden vom Datenschutzbeauftragten an die Geschäftsleitung berichtet und in der internen Verfahrensübersicht bei den jeweiligen Verfahren dokumentiert.

9 Einweisung in den Datenschutz

Der Datenschutzbeauftragte hat die mit der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten Beschäftigten in den Vorschriften zum Datenschutz zu unterweisen. Die Unterweisung kann in Form einer Präsenzschulung, durch Onlineschulung oder schriftliche Information geschehen. Die Art und Weise der Unterweisung und ihrer Durchführung wird in Abhängigkeit vom Kreis der Teilnehmer im Einzelfall festgelegt. Die Durchführung der Unterweisung einschließlich der Teilnehmer ist zu dokumentieren. Die Dokumentation über die durchgeführten Unterweisungen führt die jeweilige Gesellschaft, soweit die betrieblichen Fortbildungsmaßnahmen nicht an einer anderen festgelegten zentralen Stelle dokumentiert werden.

10 Schutzeinstufung der Daten

Datenverarbeitende Stellen haben diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der DS-GVO als auch des BDSG zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Um beurteilen zu können, welches Schutzniveau erforderlich ist und welche technischen und organisatorischen Maßnahmen als geeignet und angemessen bezeichnet werden können, werden die Daten der einzelnen Datenverarbeitungsverfahren nach dem Grad ihrer datenschutzrechtlichen und betriebswirtschaftlichen Sensibilität beurteilt und einer Schutzstufe zugeordnet. Anschließend werden die Daten nach ihren Schutzzielen skaliert. Die Schutzeinstufungen und Schutzziele werden bei den Freigabeunterlagen dokumentiert.

10.1 Personenbezogene Daten

Die datenschutzrechtliche Sensibilität der personenbezogenen Daten beurteilt sich an der Frage, inwieweit der Betroffene bei einer Datenschutzverletzung in seinen Persönlichkeitsrechten oder seinem persönlichen oder wirtschaftlichen Ansehen verletzt oder eingeschränkt ist bzw. verletzt oder eingeschränkt werden kann. In die Beurteilung fließen zudem alle Kriterien des Artikel 9 und 10 DS-GVO ein.

<u>Skalierung für die Schutzeinstufung</u>

Stufe A:
Frei zugängliche Daten, in die Einsicht gewährt wird, ohne dass der Einsichtnehmende ein berechtigtes Interesse geltend machen muss, z.B. Daten, die im Internet oder in Broschüren veröffentlicht bzw. in öffentlich zugänglichen Verzeichnissen zur Verfügung stellt werden.

Stufe B:
Personenbezogene Daten, deren Zerstörung, Verfälschung oder Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch an ein berechtigtes Interesse des Einsichtnehmenden gebunden ist, z.B. interne Telefondurchwahlnummern, interne Zuständigkeiten.

Stufe C:
Personenbezogene Daten, deren Zerstörung, Verfälschung oder Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann (Stichwort: Beeinträchtigung des Ansehens), z.B. Daten über Vertragsbeziehungen, Höhe des Einkommens, etwaige Sozialleistungen, Ordnungswidrigkeiten.

Stufe D:
Personenbezogene Daten, deren Zerstörung, Verfälschung oder Missbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann (Stichwort: soziale Existenz), z.B. Unterbringung in Anstalten, Straffälligkeit, dienstliche Beurteilungen, psychologisch-medizinische Untersuchungsergebnisse, Schulden, Pfändungen, Insolvenzen.

Stufe E:
Daten, deren Zerstörung, Verfälschung oder Missbrauch Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen kann (Stichwort: physische Existenz), z.B. Adressen von verdeckten Ermittlern, Adressen von Personen, die mögliche Opfer einer Straftat sein können.

10.2 Betriebswirtschaftliche Daten
Die betriebswirtschaftliche Sensibilität der Daten beurteilt sich am Ausmaß der möglichen Störungen der Betriebsabläufe oder der betrieblichen Erwerbstätigkeit oder der Beeinträchtigung des Ansehens des Unternehmens in der Öffentlichkeit, bei den Beschäftigten den Kunden oder Geschäftspartnern, wenn die erforderlichen Daten nicht oder nicht rechtzeitig zur Verfügung stehen, nicht richtig sind oder in unbefugte Hände geraten.

Betriebswirtschaftliche Sensibilität der Daten

A (Gering):
Die betriebswirtschaftlichen Daten sind frei zugänglich, müssen aber richtig sein.

B (Mittel):
Interne betriebswirtschaftliche Daten. Ein Missbrauch verursacht keine besondere Beeinträchtigung der betrieblichen Funktion oder des Ansehens der Umweltbeziehungen des Unternehmens.

C (Hoch):
Ein Missbrauch von betriebswirtschaftlichen Daten kann die betriebliche Funktion, die Umweltbeziehungen oder das Ansehen des Unternehmens erheblich beeinträchtigen.

D (Sehr hoch):
Ein Missbrauch kann die finanzielle oder marktwirtschaftliche Situation oder die Existenz eines Unternehmens erheblich beeinträchtigen.

11 Bewertung der Wirksamkeit des Datenschutzmanagements

Die Erfüllung der datenschutzrechtlichen Anforderungen und die Angemessenheit der technischen und organisatorischen Maßnahmen werden vom Datenschutzbeauftragten kontrolliert und auf deren Erfüllungsgrad hin bewertet. Für die Kontrolle und Bewertung wird ein standardisiertes und prozessbasiertes Erhebungs- und Bewertungsverfahren eingesetzt. Zu diesem Zweck führt der Datenschutzbeauftragte regelmäßige Kontrollen und Auswertungen durch, in denen der Grad der Erfüllung der rechtlichen und der technischen und organisatorischen Anforderungen erhoben, bewertet und dokumentiert wird. Der Datenschutzbeauftragte berichtet der Geschäftsleitung jährlich (im 1. Quartal eines Jahres) über die Ergebnisse der Kontrollen und Bewertungen.