HAHN+KOLB GROUP

LET'S WORK TOGETHER.

Datenschutzleitlinie

Helmut Pohl, Datenschutzbeauftragter (DSB)

Inhaltsverzeichnis

1 Vorwort

Die Themen Datenschutz und IT-Sicherheit werden für uns und unsere Kunden immer wichtiger und bedeutsamer. Wir haben eine hohe Verantwortung für unser Handeln, für unsere Arbeit, für die Systeme und Daten unserer Kunden, Lieferanten und Mitarbeiter. Unsere Kunden legen Ihre persönlichen und betriebswirtschaftlichen Daten in unsere Hände und damit auch unternehmenswichtige sowie kritischen Informationen.

Für uns in der HAHN+KOLB Werkzeuge GmbH ist es besonders wichtig, mit diesen Daten verantwortungsbewusst umzugehen. Daher nehmen wir den Datenschutz in der Praxis sehr ernst und organisieren uns auch entsprechend.

Diese Datenschutzleitlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten in unserem Unternehmen. Sie soll helfen, die Bedeutung und Wichtigkeit des Datenschutzes zu verdeutlichen und Ihnen dieses Thema transparenter zu machen.

2 Datenschutzziele

Das Thema Datenschutz ist in der HAHN+KOLB Werkzeuge GmbH allgegenwärtig. Der Datenschutz schützt die Personen, die sich hinter den im Unternehmen gespeicherten und zu verarbeiteten Daten verbergen. Mit dieser Datenschutzleitlinie sollen die Grundrechte und Grundfreiheiten von Betroffenen, insbesondere ihr Recht auf Schutz personenbezogener Daten, gewahrt und geschützt werden.

Diese Datenschutzleitlinie gilt für die HAHN+KOLB Werkzeuge GmbH. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der HAHN+KOLB Werkzeuge GmbH als attraktiver Arbeitgeber.

Beim Umgang mit personenbezogenen Daten müssen neben anderen Gesetzen und Vorschriften hauptsächlich die Bestimmungen der europäischen Datenschutzgrundverordnung (EU-DSGVO) und des Bundesdatenschutzgesetzes (BDSG) beachtet werden. Verantwortliches Handeln beim Umgang mit personenbezogenen Daten, aber auch die risikobewusste Nutzung von IT-Systemen und -Anwendungen sind die zentralen Zielsetzungen.

3 Datenschutzprinzipien

Die EU-DSGVO und auch das BDSG legen den Stellen, die für die personenbezogene Datenverarbeitung verantwortlich sind, eine Reihe von Pflichten auf. So gibt es zum Beispiel Auskunfts-, Berichtigungs-, Sperrungs- und Löschungspflichten gegenüber den Betroffenen sowie Verpflichtungen auf den sorgsamen Umgang mit personenbezogenen Daten bei allen Personen, die mit personenbezogenen Daten umgehen.
Die führenden Prinzipien dabei ergeben sich aus Art. 5 Abs. 1 EU-DSGVO:

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
  Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise erhoben und verarbeitet werden.
  Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben.

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

- **Datenminimierung**
  Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, 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, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

- **Richtigkeit**
  Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

- **Speicherbegrenzung**
  Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. 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 wurde oder die Konzernarchive den Datenbestand auf seine Archivwürdigkeit für historische Zwecke bewerten konnten.

- **Integrität und Vertraulichkeit**
  Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

- **Rechenschaftspflichtigkeit**
  HAHN+KOLB ist für die Einhaltung der Grundsätze rechenschaftspflichtig. Die Einhaltung muss nachgewiesen werden können. Beim Datenschutz erfolgt eine „Beweislastumkehr": HAHN+KOLB muss aktiv und unabhängig davon, ob es überhaupt zu Schäden oder Verstößen kam, nachweisen, dass der Datenschutz funktioniert. Dabei genügt es dann nicht mehr, die Prozesse lediglich im Griff zu haben. Stattdessen ist deren Funktionsfähigkeit aktiv nachzuweisen.

Die Einhaltung der Vorschriften der EU-DSGVO und des BDSG sowie weiterer spezialgesetzlicher Vorschriften, wie beispielsweise des Telekommunikationsgesetzes (TKG), des Telemediengesetzes (TMG) oder des Gesetzes gegen den unlauteren Wettbewerb (UWG) haben bei HAHN+KOLB einen hohen Stellenwert.

4 Begriffsbestimmungen

4.1 **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffener). Kundendaten gehören dabei ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie seine E-Mail-Adresse. Es genügt, wenn die jeweilige Information mit dem Namen des Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z. B. beim Autokennzeichen. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.

4.2 **Besondere Arten personenbezogener Daten** sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.

4.3 **Verarbeitung** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

4.4 **Einschränkung der Verarbeitung** ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

4.5 **Pseudonymisierung** ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

4.6 **Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

4.7 **Empfänger** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

4.8 **Dritter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

4.9 Eine **Einwilligung** des Betroffenen ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der der Betroffene zu

verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist.

5 Grundlegendes

Diese Leitlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit bei HAHN+KOLB bestehenden Verantwortlichkeiten. Alle Mitarbeiter sind zur Einhaltung der Leitlinie verpflichtet.

Die Datenschutzleitlinie richtet sich an:

- alle Abteilungen und jeden einzelnen Mitarbeiter, welcher mit der Verarbeitung personenbezogener Daten betraut ist.

- den betrieblichen Datenschutzbeauftragten (DSB), der ihre Umsetzung beratend und kontrollierend begleitet und die ihm speziell zugewiesenen Aufgaben wahrzunehmen hat.

Dabei gelten die folgenden Grundsätze:

- Die Hard- und Software zur Datenverarbeitung ist für betriebliche Aufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen Verlust und Manipulation zu sichern.

- Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Umsetzung der Leitlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.

- Die für die jeweilige Datenverarbeitung und die hierfür eingesetzten Systeme Verantwortlichen stellen sicher, dass ihre Mitarbeiter über diese Leitlinie informiert werden.

- Der Datenschutzbeauftragte berät bei der Umsetzung der Leitlinie und prüft deren Einhaltung.

Insoweit sind alle Adressaten der Leitlinie dem DSB auskunftspflichtig.

6 Der betriebliche Datenschutzbeauftragte

6.1 Die HAHN+KOLB Werkzeuge GmbH hat nach Maßgabe des Artikels 37 EU-DSGVO einen betrieblichen Datenschutzbeauftragten (DSB) bestellt. Der Datenschutzbeauftragte ist zu erreichen unter datenschutz@hahn-kolb.de. Seine Kontaktdaten sind auch zu finden unter www.hahn-kolb.de. Der DSB nimmt die ihm kraft Gesetzes und aus dieser Leitlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation wahr. Er berichtet unmittelbar der Unternehmensleitung und ist zuständig für die Kommunikation mit Aufsichtsbehörden.

6.2 Der Datenschutzbeauftragte unterrichtet und berät die Unternehmensleitung sowie die Beschäftigten hinsichtlich ihrer Datenschutzpflichten. Dem DSB obliegt die Überwachung der Einhaltung der EU-DSGVO und anderer gesetzlicher Vorgaben zum Datenschutz, einschließlich der Vorgaben dieser Richtlinie, sowie die Überwachung der Strategien von HAHN+KOLB für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an Verarbeitungsvorgängen beteiligten Mitarbeiter. Ausgewählte Prozesse werden stichprobenartig, risikoorientiert und in angemessenen Zeitabständen auf ihre Datenschutzkonformität hin kontrolliert. Darüber

hinaus steht der DSB dem Verantwortlichen bei einer möglichen risikoreichen Datenverarbeitung und der Abschätzung des Risikos beratend zur Seite.

6.3 Der DSB wird frühzeitig in alle Datenschutzfragen eingebunden. Er wird dabei von der Unternehmensleitung und den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.

6.4 Die Unternehmensleitung überträgt die Aufgabe des Führens eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 EU-DSGVO) und des Erteilens von Auskünften (Art. 15 EU-DSGVO) auf den DSB (vgl. Ziff. 9 und 10). Für Meldungen, Auskünfte etc. gegenüber den Datenschutzaufsichtsbehörden bezüglich dem Verzeichnis für Verarbeitungstätigkeiten liegt die Zuständigkeit bei dem DSB.

6.5 Der DSB berichtet jährlich innerhalb des Managementreviews der Geschäftsführung über seine Tätigkeiten wie stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel.

7 Beschaffung / Hard- und Software

7.1 Die Beschaffung von Hard- und Software erfolgt grundsätzlich auf Anforderung der über die Verarbeitungen entscheidenden Einkaufs-Abteilung durch die zentrale IT-Beschaffung. Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet. Die Arbeitsanweisung AA24-003 „Beachtung der Anforderungen an Privacy-by Design und Privacy-by-Default“ ist maßgebend.

7.2 Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist der Datenschutzbeauftragte rechtzeitig vorab von der anfordernden Stelle zu informieren. Die Beschaffung erfolgt erst nach Stellungnahme des DSB. Der DSB berät dahingehend, ob die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist.

7.3 Private Hard- und Software dürfen nicht zur Verarbeitung personenbezogener Daten verwendet werden. Die dienstliche Nutzung privater Hard- und Software im heimischen und außerbetrieblichen Bereich (z. B. private Notebooks) bedarf der Genehmigung durch die IT-Abteilung im Einzelfall.

7.4 Die IT-Abteilung führt ein Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme. Der DSB kann auf das Verzeichnis jederzeit zugreifen.

7.5 Bei Verdacht des unbefugten Zugriffs auf personenbezogene Daten, der Sabotage, des Diebstahls von Hard- und Software etc. sind die IT-Abteilung, der DSB und der Compliance Officer unverzüglich zu informieren.
Näheres regelt die Arbeitsanweisung AA24-001 „Umgang mit Datenpannen“.

8 Verpflichtung / Schulung der Mitarbeiter

8.1 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 zu sein und für die keine Rechtsgrundlage besteht. Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

8.2 Jeder Mitarbeiter, der Zugang zu personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten zu verpflichten. Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars „Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen" und unter Aushändigung der Datenschutzleitlinie durch die Personalabteilung.

8.3 Der DSB ist über die Verpflichtung von Mitarbeitern und deren Arbeitsplatz zwecks von ihm vorzunehmenden weiteren Schulungen und die Feststellung evtl. Kontrollbedarfs zu informieren.

8.4 Für in Abstimmung mit den jeweiligen Abteilungsleitungen angesetzte Schulungstermine sind die betroffenen Mitarbeiter freizustellen.

9 Verzeichnis von Verarbeitungstätigkeiten

9.1 Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt der Datenschutzbeauftragte ein Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 EU-DSGVO.

9.2 Der für ein Verfahren Verantwortliche bzw. die zuständige Fachabteilung meldet dieses zeitnah gemäß den vom DSB definierten Vorgaben mit dem Formular „Meldebogen Verarbeitungstätigkeit". Gleiches gilt für Veränderungen.

9.3 Unabhängig von dieser Meldung ist der DSB bei der Planung der Einführung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und die Erfüllung der Benachrichtigungspflicht zu informieren. Bei standardisierten Erhebungen (Fragebögen, Preisausschreiben, Eingabefelder auf der Internet-Homepage etc.) ist der Erhebungsbogen etc. dem DSB zur Abstimmung vorzulegen.

9.4 Soweit der DSB feststellt, dass die beabsichtigte Verarbeitung einer Datenschutz-Folgenabschätzung unterliegt, teilt er dies umgehend mit. Die Verarbeitung darf erst nach Zustimmung des DSB durchgeführt werden. Im Zweifel entscheidet die Geschäftsleitung.

10 Betroffenenrechte

10.1 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.

10.2 Betroffene haben nach Art. 15 EU-DSGVO das Recht auf Auskunft über die im Unternehmen über ihre Person gespeicherten personenbezogenen Daten.

10.3 Bei der Bearbeitung von Anträgen ist die Identität des Betroffenen zweifelsfrei festzustellen. Bei begründeten Zweifeln an der Identität können zusätzliche Angaben vom Antragsteller angefordert werden.

10.4 Die Auskunftserteilung erfolgt schriftlich, es sei denn der Betroffene hat den Antrag auf Auskunft elektronisch gestellt. Der Auskunft ist eine Kopie der Daten des Betroffenen beizufügen, die neben den zur Person vorhandenen Daten, auch die Empfänger von Daten, den Zweck der Speicherung sowie alle weiteren gesetzlich geforderten Informationen nach Art. 15 EU-DSGVO beinhaltet, um den Betroffenen die Verarbeitung bewusst zu machen und die Rechtmäßigkeit selbst beurteilen zu lassen. Auf besonderen Wunsch des Betroffenen werden die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt. Die zuständige IT-Abteilung legt den hierfür vorzusehenden Standard fest.

10.5 Betroffene haben nach Art. 16 EU-DSGVO einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger personenbezogener Daten verlangen.

10.6 Der Betroffene hat nach Art. 17 EU-DSGVO das Recht auf Löschung seiner personenbezogenen Daten unter den folgenden Voraussetzungen:

- die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich,
- der Betroffene hat eine Einwilligung widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung,
- ihre Verarbeitung ist unzulässig,
- der Betroffene legt Widerspruch gegen die Verarbeitung zu Zwecken der Werbung und Marktforschung ein oder beruft sich auf ein Widerspruchsrecht aufgrund einer besonderen – zu begründenden – persönlichen Situation,
- es handelt sich um besondere personenbezogene Daten, deren Richtigkeit nicht bewiesen werden kann, oder
- es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung.

10.7 Besteht eine Verpflichtung zur Löschung und wurden die personenbezogenen Daten zuvor öffentlich gemacht, sind weitere Verantwortliche für die Datenverarbeitung über ein Löschbegehren des Betroffenen hinsichtlich aller Kopien seiner Daten sowie aller Links zu diesen Daten zu informieren.

10.8 Der Betroffene kann nach Art. 18 EU-DSGVO die Einschränkung der Verarbeitung seiner Daten verlangen, wenn

- die Richtigkeit der personenbezogenen Daten strittig ist, jedoch nur so lange, wie die Richtigkeit durch die zuständige Fachabteilung überprüft wird oder
- die Verarbeitung unzulässig ist, der Betroffene die Datenlöschung aber ablehnt, oder
- das Unternehmen die personenbezogenen Daten für Zwecke der Verarbeitung nicht mehr benötigt, der Betroffene die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
- der Betroffene Widerspruch gegen die Verarbeitung aufgrund einer besonderen Situation eingelegt hat und die zuständige Fachabteilung noch mit der Prüfung des Widerspruchs befasst ist.

10.9 Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 EU-DSGVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 EU-DSGVO Gebrauch, so erfolgt die zentrale Bearbeitung durch den DSB. Die Fachabteilungen stellen die dafür erforderlichen Informationen zur Verfügung. Näheres regelt die Arbeitsanweisung AA24-004 „Meldung einer Betroffenenanfrage“.

10.10 Der Betroffene ist spätestens innerhalb eines Monats über alle ergriffenen Maßnahmen, die auf seinen Antrag hin erfolgt sind, zu informieren.

10.11 Der Datenschutzbeauftragte steht bei der Wahrung der Betroffenenrechte beratend zur Verfügung.

10.12 Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch die Personalabteilung erfüllt.

11 Erhebung / Verarbeitung von personenbezogenen Daten

11.1 Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 EU-DSGVO zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen. Weitere Erlaubnistatbestände, die den Umgang mit personenbezogenen Daten im Unternehmen legitimieren können, werden in der Arbeitsanweisung AA24-002 „Umgang mit personenbezogene Daten – Erlaubnistatbestände“ dargestellt.

11.2 Es wird sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (bspw. Profiling).

11.3 Vor Einführung neuer Arten von Erhebungen ist die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Hierbei sind insbesondere die vernünftigen Erwartungen des oder der Betroffenen hinsichtlich einer solchen Weiterverarbeitung gegen HAHN+KOLB, die Art der verwendeten Daten, die Folgen für den Betroffenen sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu prüfen. Die Prüfung ist darüber hinaus zu einem ordnungsgemäßen Nachweis zu dokumentieren. Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

11.4 Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der DSB zu kontaktieren.

12 Datenhaltung / Versand / Löschung

12.1 Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu zur Verfügung gestellten Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern ist separat geregelt. Eine Regelung bezüglich Cloudanwendungen ist im sog. „Cloud Ban“ ebenfalls festgelegt. Bei Netzwerken ist die IT-Abteilung für die Sicherung der Daten verantwortlich, die auf dem

Server gespeichert sind.

12.2 Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z. B. auf dem lokalen Laufwerk des Firmen PC`s) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich.

12.3 Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Die IT-Abteilung ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten in Sicherungskopien zu informieren.

12.4 Bei der Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten ist die Abteilung IT verpflichtet, dafür zu sorgen, dass sämtliche Daten wirksam gelöscht werden.

13 Externe Dienstleister / Auftragsverarbeitung / Wartung

13.1 Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z. B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z. B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist der DSB vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 EU-DSGVO genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

13.2 Entsprechendes gilt, falls HAHN+KOLB entsprechende Tätigkeiten im Auftrag Dritter wahrnehmen will.

14 Interne Ermittlungen

14.1 Maßnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen im Arbeitsverhältnis sind unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchzuführen. Insbesondere muss die damit einhergehende Datenerhebung und -verwendung zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen des Betroffenen verhältnismäßig sein.

14.2 Der Betroffene ist so bald wie möglich über die zu seiner Person durchgeführten Maßnahmen zu informieren.

14.3 Bei allen Formen der internen Ermittlungen ist der DSB hinsichtlich der Auswahl und Ausgestaltung der Maßnahmen vorab einzubeziehen.

15 Sicherheit der Verarbeitung

15.1 Für jedes Verfahren, welches sich nicht von Beginn an als frei von Risiken für den Betroffenen darstellt, ist in Abhängigkeit der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen.

15.2 Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie der Belastbarkeit der Daten verarbeitenden Systeme ist von der der Abteilung IT ein allgemeines Sicherheitskonzept zu erstellen. Das Konzept orientiert sich an der zuvor erstellten Schutzbedarfsfeststellung und der Risikoanalyse. Dieses Konzept ist maßgeblich für alle weiteren Verfahren. Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen, zu bewerten und zu evaluieren.

16 Arbeitsanweisungen und Regelungen

16.1 Neben dieser Datenschutzleitlinie bestehen ergänzende Regelungen, die insbesondere die zur Realisierung des Datenschutzes und der Datensicherungsgebote des Art. 32 EU-DSGVO zu treffende Maßnahmen dienen. Hierzu gehören u. a.:

- Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen
- Verschwiegenheitserklärung für Führungskräfte (WÜRTH)
- Richtlinie Arbeitsordnung
- Arbeitsanweisungen und Formulare bezüglich Datenschutz im integrierten Managementsystem (IMS) im Geschäftsprozess 5.3.1 „Datenschutz“

17 Rechenschafts- und Dokumentationspflicht

17.1 Die Einhaltung der Vorgaben, die sich aus dieser Leitlinie ergeben, muss jederzeit nachweisbar sein („Accountability“). Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.

17.2 Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer und organisatorischer Veränderungen werden diese Richtlinie und die dazugehörigen Arbeitsanweisungen und Regelungen regelmäßig auf Anpassungs- und Ergänzungsbedarf hin überprüft.

17.3 Änderungen dieser Richtlinie sind formlos wirksam. Die Beschäftigten und leitenden Angestellten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

18 Datenschutz-Governance-Struktur

Die Datenschutz-Governance-Struktur ist in den konzernweiten „Policy and Procedure“ (PAP) IT Compliance unter der Überschrift IT Compliance-Organisation, zum einen mit den Funktionen der Konzernebene und zum anderen mit den Funktionen der Gesellschaftsebene ausgewiesen.

Ludwigsburg, 7. August 2018

Katrin Hummel	Andreas Kräutle	Steffen Vogl
Geschäftsführerin	*Geschäftsführer*	*Geschäftsführer*