Unternehmensrichtlinie - externe Partner

Inhalt

Unternehmensrichtlinie externe Partner

1. Vorwort (Unternehmen und Geschäftszweck)

Wir, die Allgeier Engineering GmbH, sind ein Dienstleister für Qualitätsmanagement, Systemintegration, Verifikation & Validierung, Softwareentwicklung und Projektmanagement. Im Produktentwicklungsprozess und in der Serienbetreuung betreuen wir verschiedene Bereiche im Automobil- und Bahnumfeld. Durch die Tätigkeiten und die Nähe zu den Entwicklungsbereichen in diesen Branchen benötigen wir ein wirksames Managementsystem, das auch von den relevanten Partnern eingehalten werden muss. Die Unternehmensrichtlinie gibt Auskunft über die wichtigsten Aspekte unseres Managementsystems.

2. Geltungsbereich/Anwendungsbereich

Diese Unternehmensrichtlinie findet Anwendung in allen Bereichen und gilt für alle externen Personen (z.B. Dienstleister, Lieferanten, Kunden und an der Projektarbeit beteiligte Personen, die regelmäßig in unserem Unternehmen tätig sind oder Zugang zu unseren Unternehmenssystemen haben. Sie ist für alle bindend und muss durchgängig eingehalten werden. Eine etwaige Abweichung von der Richtline ist nur nach vorheriger dokumentierter Freigabe durch den Compliance Officer, Datenschutz-, Qualitäts- oder dem Informationssicherheitsbeauftragten zugelassen. Ein Verstoß gegen die Regelungen in der Unternehmensrichtlinie kann zu Konsequenzen führen. Wird die Richtlinie vorsätzlich oder fahrlässig verletzt und entsteht hierdurch dem Auftragnehmer ein Schaden, haftet der Verursacher gegenüber dem Auftraggeber gemäß der im Gesetz und in der Rechtsprechung geltenden Grundsätzen. Bei datenschutzrechtlichen Verletzungen ist zu beachten, dass der Verursacher haftbar wird, wenn er entgegen der oder ohne Weisung des Auftraggebers personenbezogenen Daten in einer Art und Weise verarbeitet, die gegen die datenschutzrechtlichen Vorgaben der EU-Datenschutzgrundverordnung (DS-GVO) und des Bundesdatenschutzgesetzt (BDSG) verstößt. Eine unrechtmäßige Verarbeitung von personenbezogenen Daten kann auch Schadenersatzansprüche eines Betroffenen nach sich ziehen. Die Entscheidung über die einzuleitenden Schritte wird im Management Meeting getroffen und nachgehalten. Die Entscheidung leitet sich aus der Betrachtung jedes Einzelfalls ab, unter Berücksichtigung des aufgetretenen Schadens für das Unternehmen.

3. Einhaltung von Rechtsvorschriften

Bei Umgang mit Informationen und Daten in unserem Unternehmen sind von den externen Personen die geltenden Rechtsvorschriften zu Datenschutz (DS-GVO und BDSG) und Informationssicherheit (z.B. ISO 27001/27002) sowie die Unternehmensregelungen einzuhalten. Sollten externe Personen unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihren unternehmensinternen Ansprechpartner zur Klärung zu wenden. Dieser muss ggf. Unklarheiten mit einem der Managementbeauftragten (CO, DSB, ISB, QMB) abstimmen.

4. Abweichen von Vorgaben

Jegliche Abweichung von den Vorgaben dieser Richtlinie bedarf der vorherigen dokumentierten Freigabe durch einen der Managementsystembeauftragten. Bei Compliance Vorfällen muss der Compliance Officer eingeschalten werden. Bei Qualitätsthemen wird der Qualitätsmanagementbeauftragte, bei Informationssicherheitsthemen der Informationssicherheitsbeauftragte einbezogen. Der Datenschutzbeauftragte ist in die

Entscheidungsfindung mit einzubeziehen, sofern es sich um eine datenschutzrelevante Abweichung handelt.

5. Compliance

Die Allgeier Gruppe steht für integres und ethisches Handeln ebenso wie für die unbedingte Einhaltung von Recht und Gesetz. Das ist nicht nur als börsennotiertes Unternehmen eine grundlegende Selbstverständlichkeit, sondern vor allem auch entscheidend in der Zusammenarbeit mit unseren Partnern und Kunden. Diese Richtlinie stellt unser Engagement für Corporate Social Responsibility (CSR) und dem Nachhaltigkeit Umgang mit Ressourcen da. Wir unterteilen die Anforderungen in vier Bereiche.

5.1 Ökonomische Verantwortung

- Verbindliche Anforderungen an Tier-1-Lieferanten zur Weitergabe von Standards entlang der Lieferkette: Zum Beispiel erwarten wir von unseren Hauptlieferanten, dass sie diese Standards an ihre eigenen Lieferanten weitergeben.
- Dekarbonisierung: Zum Beispiel arbeiten wir aktiv daran, unsere CO2-Emissionen zu reduzieren und ermutigen unsere Lieferanten, ähnliche Schritte zu unternehmen.

5.2 Soziale Verantwortung

- Wir erwarten von unseren Lieferanten und ihrer Lieferkette, dass sie die Menschenrechte achten und schützen. Wir lehnen jede Form von Diskriminierung oder Ungleichbehandlung aufgrund von Rasse, ethnischer Zugehörigkeit, Geschlecht, Religion, Weltanschauung, Behinderung, Alter oder sexueller Identität ab. Wir setzen uns für die Gleichstellung der Geschlechter und die Beseitigung von Diskriminierung und Gewalt gegen Frauen in allen Aspekten unserer Geschäftstätigkeit ein. Wir tolerieren keine Belästigung, Mobbing oder moderne Sklaverei (Leibeigenschaft, Zwangsarbeit oder Menschenhandel). Wir respektieren die Rechte von Minderheiten und indigenen Völkern und schätzen die Vielfalt und die kulturellen Unterschiede unserer Mitarbeiter, Kunden und Stakeholder. Außerdem halten wir uns an die gesetzlichen Bestimmungen für Kinderarbeit und junge Arbeitnehmer sowie an die gesetzlich festgelegten Löhne und Sozialleistungen. Wir anerkennen auch das Recht auf Vereinigungsfreiheit und Tarifverhandlungen.
- Einsatz von privaten oder öffentlichen Sicherheitskräften: Wir achten darauf, dass diese Kräfte die Menschenrechte achten und entsprechend geschult sind.
- Tierschutz: Zum Beispiel achten wir darauf, dass alle tierischen Produkte aus artgerechter Haltung stammen.
- Land-, Wald- und Wasserrechte sowie Zwangsräumungen: Wir setzen uns dafür ein, dass lokale Gemeinschaften in den Gebieten, in denen wir tätig sind, ihre Rechte an Land und natürlichen Ressourcen wahren können.

5.3 Umweltverantwortung

Die Erwartungen an den Umweltschutz verlangen von den Lieferanten und ihrer Lieferkette, dass sie verantwortungsbewusst handeln und die Auswirkungen auf die Umwelt berücksichtigen. Hierzu können gehören:

- Wiederverwendung und Recycling: Wir setzen uns für die Wiederverwendung und das Recycling von Materialien ein, wie z. B. die Rückgabe von Verpackungsmaterialien zur erneuten Verwendung.
- Artenvielfalt, Landnutzung und Entwaldung: Wir engagieren uns für den Schutz der Artenvielfalt und vermeiden Geschäftspraktiken, die zur Entwaldung beitragen könnten.
- Bodenqualität: Wir unterstützen Praktiken, die den Boden schützen und seine Qualität für zukünftige Generationen erhalten. Beim Einsatz von Chemikalien muss es klare Vorgaben und Regeln zum Umgang damit geben.
- Lärmemissionen: Wir legen Wert auf leise Betriebsabläufe und ermutigen Lieferanten, Geräuschpegel zu minimieren.

5.4 Governance

- Unternehmensethik: Die Erwartungen an die Unternehmensethik verlangen von den Lieferanten und ihrer Lieferkette, dass sie bei ihren Aktivitäten transparent, verantwortungsvoll und ethisch einwandfrei vorgehen. Hierzu gehört keine Korruption oder Erpressung und Bestechung.Jede Zuwendung ist tranparent zu gewähren, in die Geschäftsunterlagen aufzunehmen und ggf. steuerlich prüfen zu lassen.
- Datenschutz: Der Schutz von Privatsphäre und dem Datenschutz muss gewährleistet sein.
- Kartellrecht: Ein fairer Wettbewerb und das Einhalten des Kartellrechts sowie die Vermeidung oder aber Minimierung von Interessenskonflikten.
- Whistleblowing: Whistleblowing sollte ermöglicht werden und der Schutz vor Vergeltung muss sichergestellt sein.

5.5 Compliance Vorfälle – was passiert, wenn’s passiert?

Das kann immer einmal passieren – wir handeln versehentlich nicht compliant. Wie oben geschrieben wollen wir dabei stets eine positive Fehlerkultur leben.

Compliance Vorfälle können sein:

- eine mögliche Verletzung von rechtlichen, insbesondere straf- oder bußgeldrechtlichen Bestimmungen oder Unternehmensvorschriften
- drohende und laufende Auskunftsersuchen oder Ermittlungsverfahren deutscher Behörden
- vorsätzlich begangene Sach- oder Vermögensschäden von mehr als 50 EUR zu unseren Lasten
- vorsätzlich unwahre Meldung von Compliance Vorfällen (falsche Verdächtigung, „Anschwärzen“)

Compliance Vorfälle bzw. Verstöße werden sachlich und rechtlich untersucht sowie, je nach deren Relevanz, in einen schweren oder normalen Vorfall eingeteilt. Je nach Einstufung werden anschließend bestimmte Maßnahmen getroffen. So müssen schwere Verstöße (z.B. solche Vorfälle, die bereits eine Wirkung außerhalb unseres Unternehmens haben) u.a. über den Compliance Officer auch die an ALLGEIER SE gemeldet werden. Falls es Verdachtsmomente in Bezug auf einen möglichen Compliance Verstoß gibt, so kannst Du dich damit vertrauensvoll an den Compliance Officer bzw. Deinen direkten AEN Ansprechpartner wenden.

Dies gilt nicht bei folgenden Ausnahmen:

- Es droht eine unmittelbare Gefahr für die Öffentlichkeit.
- Es drohen interne Vergeltungsmaßnahmen.
- Es erfolgt intern ungerechtfertigt keine Reaktion auf den Hinweis.

Compliance Vorfälle nehmen wir ernst, klären sie auf und treffen dann entsprechende Maßnahmen.

Mögliche Compliance Vorfälle sind zu melden, ggfs. an die hierfür benannten Kontaktpersonen (AEN Ansprechpartner und Compliance Officer). Die Anonymität wird auf Deinen Wunsch hin in jeglicher Form gewahrt. Sind jedoch im Übrigen nicht an Deine sonstigen Weisungen oder Wünsche gehalten. Hinweisgeber, die in gutem Glauben Compliance Vorfälle melden, sind vor Repressalien geschützt: Ein Hinweisgeber darf weder entlassen, degradiert, eingeschüchtert oder in anderer Weise benachteiligt werden. Geschützt wird auch, wer Hinweisgeber unterstützt, wie zum Beispiel Mittelsmänner, Kollegen oder Verwandte. Möglich sind jedoch Disziplinarmaßnahmen, die aufgrund einer eigenen Beteiligung des Hinweisgebers am Vorfall selbst oder aufgrund einer willkürlichen oder vorsätzlich unwahren Anschwärzung durch den Hinweisgeber ergriffen werden.

6. Informationssicherheit und Datenschutz

6.1 Arten von Informationen

Um Unternehmensinformationen schützen zu können müssen die unterschiedlichen Arten von Informationen in unseren Unternehmen klassifiziert werden. Die Informationsklassifizierung bildet damit unsere Basis für den Umgang mit Informationen. Zur Gewährleistung des sicheren und sorgsamen Umgangs mit Informationen sind Rollen zur Informationsverarbeitung und 3 Informationsklassen für die Einstufung von Informationen hinsichtlich Ihres Schutzbedarfes festgelegt.

Bei allen nicht eindeutig klassifizierten Informationen ist zunächst immer davon auszugehen, dass diese Informationen als intern einzustufen sind. Vor der weiteren Verwendung muss mit dem Vorgesetzten und oder mit dem Informationssicherheitsbeauftragten die Klassifizierung bestimmt werden.

6.2 Verantwortlichkeiten der Klassifizierung

Um die Informationssicherheit umzusetzen zu können sind Regelung zu den Verantwortlichkeiten definiert:

Rolle	Wer hat die Rolle?	Aufgaben
Ersteller	jeder Mitarbeiter	- erzeugt Daten - hält sich an die Unternehmensrichtlinien
Informationsverantwortlicher	Vorgesetzter	- klärt Einstufungsfragen mit Erstellern - überwacht Klassifikationsprozess seitens der Ersteller
Benutzer	jeder Mitarbeiter	- benutzt Daten - hält sich an die Unternehmensrichtlinien

		- gibt Feedback zu Einstufungshöhen
Klassifikationsverantwortlicher	Informationssicherheitsbeauftragter	- klärt Einstufungsfragen mit Informationsverantwortlichen und Benutzern - überwacht Klassifikationsprozess seitens der Fachverantwortlichen - stimmt sich mit Risikomanagement, Datenschutz- und Qualitätsmanagementbeauftragter ab

6.3 Informationsklassifizierung und Beispiel Dokumente

Diese Tabelle gibt eine Übersicht über die Mindestschutzanforderung von Informationen. Wir unterscheiden in 3 Informationsklassen (öffentlich, intern und vertraulich) und in 3 Verwendungsarten (Papier, elektronisch und mündlich). Die Verhaltensregeln für den mündliche Umgang werden in Kapitel 7 „Richtiges Verhalten in der Öffentlichkeit und im privaten Umfeld“ aufgezeigt. Zusätzlich gibt es für die Arten Papier und elektronisch Beispiele für Informationen, die der jeweiligen Kategorie zugeordnet werden.

Verwendungsart / Informationsklassifizierung	**öffentlich**	**intern**	**vertraulich / streng vertraulich**
Physisch	Keine besonderen Schutzvorkehrungen	Kennzeichnung mit vertraulich, Clean Desktops, Externe Weitergabe in Umschlägen, Vernichtung mit Aktenvernichter Sicherheitsstufe P-04.	Kennzeichnen mit vertraulich, Clean Desktops, Externe Weitergabe in Umschlägen, Vernichtung mit Aktenvernichter Sicherheitsstufe P-05
Digital	Keine besonderen Schutzvorkehrungen	Informationen sind für Benutzer, abhängig der Freigabe, zugänglich. Bei externem Empfänger muss eine gesicherte Übertragung (AEN Mail-Server oder einen freigegebenen Cloud-Dienst) verwendet werden.	Informationen, müssen zusätzlich intern verschlüsselt abgelegt werden. Bei Cloud-Diensten muss eine ISO27001 vorliegen. Bei externer Übertragung muss eine „Ende zu Ende“ Verschlüsselung sichergestellt werden. (z.B. 7-Zip oder Panama) Vertrauliche oder Geheime Kundendaten gelten immer als streng vertraulich und

			sollten, wenn möglich, nur auf dem Kundensystem abgelegt werden.
Mündlich	Keine besonderen Schutzvorkehrungen	siehe Kapitel 7. Richtiges Verhalten in der Öffentlichkeit und im privaten Umfeld	siehe Kapitel 7. Richtiges Verhalten in der Öffentlichkeit und im privaten Umfeld
Beispiele	Marketingunterlagen & Referenzliste, Stellenbeschreibungen	Angebote & Vertriebspräsentationen, Besprechungsprotokolle (keine Kundendaten), Bestellungen, GuV-Info der Projekte, Handbücher, Leitfäden, Richtlinien, Mitarbeitertelefonverzeichnis, Organigramme, Projektabnahmen, Rechnungen, Rollenbeschreibungen, Verträge (nicht Personenbezogen)	Passwörter, Personal- und Bewerberunterlagen, Problemberichte, Managementbewertungen und Entscheidungen, Jahresabschluss, Kunden- und Projektdaten, Vorserien Geräte (Prototypen)

6.4 Richtiger Umgang mit schützenswerten Informationen auf Reisen

Auf den mobilen Endgeräten, die das Unternehmen zur Verfügung stellt (z.B. Laptops, Handys, Smartphones, Tablets, USB-Sticks, ...), sind unternehmenseigene Daten gespeichert. Ihr Verlust oder Diebstahl können schädliche Auswirkungen für das Unternehmen haben. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Nehmen Sie grundsätzlich nur die Unterlagen, die Sie tatsächlich benötigen, mit auf Dienstreisen.
- Bei Reisen in Drittländer (bspw. China, USA, Russland) kann nicht ausgeschlossen werden, dass Behörden bei Einreise Zugriff auf Daten von Endgeräten nehmen. Daher müssen bei Reisen in solche Länder immer von der IT-Administration bereit gestellte Notebooks ohne lokale Datenverfügbarkeit genutzt werden. Zugriff auf die Daten (E-Mails, Dateien) ist über VPN möglich. Das Notebook ist nach Rückkehr unverzüglich ohne Zugriff auf das Firmennetzwerk bei der IT-Administration zur Prüfung abzugeben.
- Bei Smartphones/Tablets ist der E-Mail-Account vor Reiseantritt auf dem Endgerät zu löschen.
- Speichern Sie nur die Daten lokal verschlüsselt ab, die Sie unterwegs benötigen.
- Benachrichtigen Sie bei Verlust oder Diebstahl mobiler Endgeräte Ihren Vorgesetzten und die IT-Abteilung.
- Führen Sie keine mobilen Endgeräte ohne Passwortschutz mit sich.
- Geben Sie mobile Endgeräte bei Reisen nicht mit Ihrem Koffer auf.
- Lassen Sie mitgeführte Unterlagen und mobile Endgeräte nie unbeaufsichtigt (z.B. im Auto) liegen. Auch Temperaturschwankungen können nicht nur die Festplatte, sondern auch andere Speichermedien sowie das LCD-Display beschädigen.

- Vorserienteile/Prototypen, die noch nicht in Serie sind, müssen beim Transport blickdicht geschützt werden.

6.5 Richtiges Verhalten in der Öffentlichkeit und im privaten Umfeld

Viele Geschäftsgeheimnisse werden durch Gedankenlosigkeit vor allem in Gesprächen mit Kollegen oder durch Telefongespräche in öffentlichem oder privatem Umfeld (z.B. Flugzeug, Biergarten, Restaurant) preisgegeben. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Seien Sie sich immer bewusst, worüber Sie wo kommunizieren. Achten Sie bei allen Gesprächen auf Vertraulichkeit.
- Geben Sie Informationen in Telefongesprächen nur an persönlich bekannte Geschäftspartner preis.
- Prüfen Sie im Zweifelsfall durch einen Rückruf die Identität des Anrufers.

- Achten Sie unterwegs darauf, dass niemand einsehen kann, woran Sie arbeiten (z.B. Laptop, Dokumente, etc.).
- Geben Sie keine vertraulichen Unternehmensinformationen in privaten Gesprächen preis.
- Führen Sie keine vertraulichen Gespräche in der Öffentlichkeit (z.B. in Flugzeugen, in Hotels, Restaurants).
- Übermitteln Sie keine vertraulichen Informationen über Dritte.
- Lassen Sie mobile Geräte nie unbeaufsichtigt.
- Geben Sie keine vertraulichen Informationen am Telefon preis.
- Geben Sie die Unternehmenshardware nicht an Familienangehörige und Dritte weiter.
- Achten Sie darauf, dass Dritte nicht die Unternehmenshardware nutzen.

Auch bei Tätigkeiten durch Beschäftigte im privaten Umfeld bleibt der Arbeitgeber für die Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DS-GVO). Zur Wahrnehmung der Kontrollrechte des Arbeitgebers im Umgang mit personenbezogenen Daten gewährt der Beschäftigte der Unternehmensleitung, dem Datenschutzbeauftragten und der für den Datenschutz zuständigen Aufsichtsbehörde während der betriebsüblichen Arbeitszeiten nach telefonischer Voranmeldung den uneingeschränkten Zutritt zum Arbeitsplatz. Der Arbeitsnehmer stellt sicher, dass ein etwaiger weiterer Mitinhaber des Wohnraums von dieser Vereinbarung in Kenntnis gesetzt wurde und dem Zutrittsrecht zustimmt.

6.6 Richtiges Verhalten im Internet und bei der E-Mail-Nutzung

Viele Geschäftsgeheimnisse werden auch durch Gedankenlosigkeit und die unsachgemäße Nutzung von elektronischen Kommunikationsmitteln preisgegeben. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Geben Sie keine Informationen über Kundenprojekte in sozialen Netzwerken (XING, Facebook oder ähnliche) preis.
- Beachten Sie, dass bei Kommunikation in sozialen Netzwerken auch eine Verbindung mit dem Unternehmen hergestellt werden kann. Daher sollte auf eine angemessene Ausdrucksweise geachtet werden.
- Persönliche Profile dürfen keine Zusätze wie „arbeitet zurzeit für Kunde XXXX“ oder ähnliches enthalten.

- Besuchen Sie nur vertrauenswürdige Internetseiten.
- Klicken Sie nicht auf Links, die in SPAM-Mails oder „Kettenbriefen“ enthalten sind.
- Verwenden Sie Ihre vom Unternehmen bereitgestellte E-Mail-Adresse nicht in Blogs, Newsgroups oder Gästebüchern im Internet.
- Beantworten Sie keine E-Mails, die persönliche Kennwörter oder PINs anfordern.
- Falls Sie am Absender der E-Mail zweifeln – nicht antworten.
- Versenden Sie wo immer möglich nur Links auf Dokumente
- Versenden Sie vertrauliche Informationen über ein sicheres Austauschlaufwerk oder verschlüsselt
- Geschäftliche E-Mail-Postfächer dürfen nur für die geschäftliche Kommunikation genutzt werden und nicht an externe E-Mail-Postfächer weitergeleitet werden.
- Auch bei Abwesenheit des Mitarbeiters muss es dem Unternehmen möglich sein ggf. auf die geschäftlichen E-Mails im Postfach zuzugreifen. Eine Unterscheidung zwischen geschäftlicher und privater Korrespondenz in dem geschäftlichen E-Mail-Postfach ist technisch nicht möglich. Sie haben die Möglichkeit alle privaten E-Mails aus dem geschäftlichen E-Mail-Postfach zu löschen. Der Arbeitgeber kann auch dann Zugriff auf das E-Mail-Postfach nehmen, wenn Sie nicht alle privaten E-Mails gelöscht haben.

6.7 Sicherheitszonen

Für alle Standorte ist ein Sicherheitszonenkonzept vorhanden. Innerhalb der jeweiligen Standorte gibt es verschiedene Sicherheitszonen:

Bereich	**Verhalten**	**Beispiele**
Zone 3 - Hochsicherheitsbereich	Zutritt nur in Begleitung von für die Sicherheitszone 3 autorisierten Personen	- Serverräume, Büros der IT-Administration, Verteilerräume
Zone 2 - Interner Bereich	Zutritt nur in Begleitung von für die Sicherheitszone 2 autorisierten Personen	- Personalbüros, Projektbüros, Büros der Finanz- und der Rechtsabteilung
Zone 1 - Kontrollierter Innenbereich	Zutritt erhalten nur Berechtigte (Mitarbeiter, geladene Besucher)	- alle sonstigen Räume des Unternehmens
Zone 0 - Außenbereich	keine Einschränkungen	- öffentliche Bereiche in einem Gebäude

6.8 Richtiges Verhalten in unseren Geschäftsräumen

Beim Betreten unserer Geschäftsräume müssen folgende Sicherheitshinweise eingehalten werden:

- Externe Personen müssen sich am Empfang registrieren.
- Die standortbezogenen Sicherheitshinweise müssen eingehalten werden (z.B. Fotografieverbot, Schutzausrüstung usw.).
- Fremdgeräte dürfen nur nach Freigabe an das Unternehmensnetzwerk angeschlossen werden.

6.9 Sichere Aufbewahrung von Informationen und Geräten

Die sichere Aufbewahrung von Informationen ist die Basis für die Wirksamkeit der Informationssicherheit. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Schließen Sie vertrauliche Unterlagen, wenn möglich in Rollcontainern, Schränken bzw. Tresoren ein.
- Sperren Sie Ihren Computer vor dem Verlassen des Arbeitsplatzes (Tasten "Windows Taste + L" klicken), oder beenden Sie die Sitzung an Ihrem Computer immer durch "Herunterfahren" und nicht durch "Ruhezustand" oder "Standby".
- Lassen Sie keine Unterlagen (insbesondere Aufzeichnungen auf Flip-Charts oder Whiteboards etc.) in Besprechungszimmern liegen.
- Lassen Sie nie vertrauliche Arbeitsunterlagen unbeaufsichtigt auf Ihrem Schreibtisch liegen.
- Lassen Sie nie mobile Geräte unbeaufsichtigt liegen. Wenn möglich sollten Notebooks mit einem Kensington-Schloss abgesichert oder wegeschlossen werden.
- Vorserienteile/Prototypen, die noch nicht in Serie sind, dürfen nur in Bereichen der Zone 2 oder 3 gelagert werden.

6.10 Richtiger Umgang mit Betriebsmitteln (Assets) und privaten Geräten (BYOD)

Auf elektronischen Speicher- und Kommunikationsmedien (z.B. Notebooks, USB-Sticks, CDs, DVDs, etc.) sind oft vertrauliche Unternehmensinformationen gespeichert. Um diese Informationen zu schützen, ist ein sicherer Umgang mit diesen Medien zwingend notwendig. Daher sind die folgenden Sicherheitshinweise einzuhalten:

- Vertrauliche Daten nur verschlüsselt auf mobilen Speichermedien speichern.
- Verstauen Sie bei Flugreisen Ihre mobilen Endgeräte im Handgepäck.
- Verwahren Sie Laptops, Handys, Schlüssel etc. sicher auf, auch außerhalb der Arbeitszeiten.
- Lassen Sie mitgeführte Unterlagen und Geräte nie sichtbar und unbeaufsichtigt (z.B. im Auto, Bahnhöfen, Flughäfen, Restaurants) liegen.
- Lassen Sie nie mobile Endgeräte unbeaufsichtigt auf Ihrem Schreibtisch liegen.
- Bilder von vertraulichen Informationen dürfen nur mit einem zugewiesenen Firmengerät erstellt werden.
- Daten auf mobilen Geräten unterliegen keiner Datensicherung (z.B. lokale Laptop Festplatte, USB Sticks, USB-Festplatten)
- Die Nutzung von privater Hardware oder eigener/nicht im Eigentum unseres Unternehmens befindlicher Hardware ist nur nach Freigabe durch die IT-Abteilung zugelassen.
- Die Nutzung von privaten Geräten mit Foto/Video/Ton Aufnahmefunktionen ist in Zone 2 und Zone 3 Bereichen untersagt.
- Für Prüf- und Messmittel die eine Eichung/Kalibrierung benötigen bestehen erweiterte Anforderungen. Klären Sie diese bitte mit ihrem Ansprechpartner.

6.11 Löschung und Vernichtung von Speichermedien und Informationen

Sie sind als Nutzer von elektronischen und nicht elektronischen Speicher- und Kommunikationsmedien für ein ordnungsgemäßes Vernichten verantwortlich. Unternehmenseigene und unternehmensfremde Informationen gehören nicht in den Papierkorb, sondern müssen speziell entsorgt werden. Nutzen Sie dazu z.B. die bereitgestellten Aktenvernichter/Shredder in der Nähe der Multifunktionsdrucker zum Entsorgen und Beachten Sie zusätzlich die nachfolgenden Sicherheitshinweise:

- Löschen oder zerstören Sie nicht mehr benötigte vertrauliche Informationen.
- Entsorgen Sie vertrauliche Informationen in Papierform ausschließlich in den dafür bereit gestellten „Aktenvernichter/Shredder“.

- Zerschneiden Sie CDs und Disketten in kleinstmögliche Teile, wenn keine Container oder Shredder zur Verfügung stehen.
- Löschen Sie alle Daten (auch Papierkörbe) auf Ihren Endgeräten, bevor Sie diese wieder zurückgeben.

Generell sind alle Speichermedien und Informationen, deren Inhalt nicht öffentlich ist, nach den folgenden Vorgaben zu löschen.

Datenträgerart	**Vorgehen**
Festplatten aus Notebooks, Desktops und Servern sowie externe Festplatten, NAS-Platten und Sicherungsbänder.	Abgabe bei der IT-Abteilung zur sicheren Löschung/Entsorgung.
Kleingeräte mit eingebauten Speichermedien (Smartphones, Tablets, Kameras, etc..) oder Speicherkarten, USB-Sticks, etc.	Rücksetzen auf Werkseinstellungen danach Abgeben bei der IT-Abteilung zur Wiederverwendung oder zur sicheren Entsorgung.
CDs, DVDs und andere optische Speichermedien	Zerkratzen, Löschen und Abgeben bei der IT-Abteilung
Papier und Mikrofilm	Shreddern mit Schreddern der Sicherheitsstufe 4 der DIN 66399
Sonstige Datenträger, unabhängig davon, ob elektronischer oder physischer Natur	Elektronische Datenträger zurücksetzen, zerstören oder sicheres löschen durchführen; nicht elektronische Datenträger zerstören.

6.12 Passwörter und Multifaktor Authentifizierung

Zur Sicherstellung eines ausreichenden Zugangs- und Zugriffsschutzes ist es zwingend erforderlich, dass die Zugangsberechtigten mit Zugang zu den IT-Systemen sichere Passwörter verwenden. Jeder Zugangsberechtigte zu unseren Systemen erhält einen ihm zugeordneten, eindeutigen Benutzernamen, mit dem der Benutzer eindeutig am jeweiligen System identifiziert wird. Die nachfolgenden Passwort-Regelungen sind daher unbedingt von jedem Zugangsberechtigten einzuhalten:

- Startpasswörter, die die Zugangsberechtigten im Rahmen der ersten Anmeldung erhalten, sind umgehend durch eigene (individuelle) Passwörter zu ersetzen.
- Passwörter dürfen nicht aufgeschrieben oder am Arbeitsplatz hinterlegt werden.
- Passwörter dürfen nicht an Dritte (auch Kollegen der Abteilung) weitergegeben werden.
- Eine Anmeldung mit den Anmeldedaten eines anderen Benutzers ist verboten.
- Bei der Eingabe von Passwörtern ist darauf zu achten, dass Dritte Passwörter nicht zur Kenntnis nehmen.
- Passwörter müssen mindestens 10 Zeichen haben.
- Passwörter müssen mindestens 3 der 4 Möglichkeiten enthalten: einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und oder ein Sonderzeichen.
- Trivialpasswörter dürfen nicht verwendet werden (z.B. qwertz, 12345678, abcdefg).
- Das Geburtsdatum des Benutzers oder dessen Angehörigen darf nicht als Passwort verwendet werden.
- Passwörter müssen regelmäßig selbstständig vom Benutzer gewechselt werden, jedoch wenigstens alle 90 Tage, bzw. sind die Passwörter auf Verlangen des Informationssicherheitsbeauftragten sofort zu wechseln, wenn die Anweisung durch ihn explizit erfolgt.

- Passwörter müssen umgehend gewechselt werden, wenn der Verdacht besteht, dass diese kompromittiert wurden oder wenn der Informationssicherheitsbeauftragter diesen Wechsel anweist.
- Der Benutzername darf nicht Bestandteil des Passwortes sein.
- Passwörter dürfen ohne entsprechende Schutzmechanismen nicht in dem Datenverarbeitungssystem (bspw. im einem Internet-Browser) gespeichert werden.
- Die innerhalb des Unternehmens (Netzwerk) verwendeten Passwörter dürfen nicht für Anwendungen im Internet oder im privaten Umfeld verwendet werden.
- Die Speicherung der Passwörter ist nur unter Verwendung eines von der IT-Administration freigegebenen Passwortsafes zulässig.
- Zusätzlich zu dem Passwort sollte immer wo möglich eine Multifaktor Authentifizierung genutzt werden.

6.13 Grundsätze beim Umgang mit personenbezogenen Daten

Beim Umgang mit personenbezogenen Daten müssen die nachfolgenden Grundsätze zwingend eingehalten werden:

- Können oder wurden die Grundsätze nicht eingehalten, muss unverzüglich der Datenschutzkoordinator oder der Datenschutzbeauftragter kontaktiert werden.
- Alle Tätigkeiten in denen personenbezogene Daten verarbeitet werden, müssen an ims@allgeier-engineering.com gemeldet werden.
- Alle Datenverarbeitungsverfahren müssen transparent gestaltet und dokumentiert werden. Jede Änderung muss erfasst werden.
- Die Verarbeitung personenbezogener Daten bedarf immer einer Rechtsgrundlage oder der nachweisbaren Einwilligung eines Betroffenen.
- Die Betroffenen müssen über die Datenverarbeitung informiert werden.
- Alle Datenverarbeitungsverfahren müssen transparent gestaltet werden.
- Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie tatsächlich erhoben wurden.
- Es dürfen nur die personenbezogenen Daten verarbeitet werden, die tatsächlich für die Durchführung der jeweiligen Aufgabe benötigt werden.
- Personenbezogene Daten sind immer direkt beim Betroffenen zu erheben.
- Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Bearbeitungstätigkeit notwendig ist.
- Die Möglichkeit der Anonymisierung oder Pseudonymisierung von personenbezogenen Daten ist zu berücksichtigen.
- Personenbezogene Daten müssen immer zugriffsgeschützt gespeichert bzw. verwahrt werden.
- Personenbezogene Daten müssen vor zufälligem bzw. ungewolltem Verlust geschützt werden.
- Anfragen auf Auskunft, Aufforderung zur Berichtigung, Löschung oder Übertragung von personenbezogenen Daten werden an ims@allgeier-engineering.com geschickt und von dort beantwortet.

6.14 Verhalten bei Vorfällen

Sollten Sie als externer Partner merken, dass der Schutz oder die Sicherheit von Informationen in irgendeiner Weise gefährdet sein könnte, haben sie sich unverzüglich an die Ihren internen Ansprechpartner zu wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf

personenbezogene Daten bezieht. Sollten Sie merken, dass die Qualität der Arbeit in irgendeiner Weise gefährdet sein könnte, wenden Sie sich unverzüglich an Ihren Vorgesetzten. Das Verhalten bei Vorfällen ist im Problemmanagement Prozess beschrieben.

7. Kontaktdaten

Sie erreichen uns wie folgt:

Compliance Officer (CO)

Marcus Reimann

Wilhelm-Wagenfeld-Straße 28 - 80807 München

Mail: marcus.reimann@allgeier-engineering.com

IMS Beauftragte (DS,ISB,QMB)

Allgeier Engineering GmbH

Wilhelm-Wagenfeld-Straße 28 - 80807 München

Tel: +49 89 1241487 43

Mail: IMS@allgeier-engineering.com

Datenschutzbeauftragter

Ralf Zlamal IITR Regional-Partner Baden-Württemberg

Schubertstraße 2

73660 Urbach

Tel. 08918917360

Email: zlamal@iitr.de

Allgeier Ombudsleute (Extern)

Compliance - Allgeier Deutsch

Einsteinstraße 172 - 81677 München

Formular: Herzlich Willkommen auf dem Hinweisgebersystem der Allgeier SE Unternehmensgruppe - Ombudsstelle & Hinweisgebersystem (ihre-ombudsstelle.de)