1. Kundenanforderungen

Immer stärker gerät bei vielen Kunden in den Fokus, wie ihre Lieferanten mit Informationen umgehen. Die Anforderungen an Lieferanten wie uns steigen immer mehr. Allgemein gibt es hier noch keinen einheitlichen Standard, der zertifizierbar ist.

Die Kunden – vor allem größere – versuchen sich daher abzusichern und fassen unter Informationsmanagement verschiedenste Dinge wie

- ob der **Datenschutz** eingehalten wird (DSGVO),
- ob vertraulich mit den **Daten des Kunden** umgegangen wird („Geheimhaltungsvereinbarung"),
- ob ein **Code of Conduct** oder **ESG**-Richtlinien umgesetzt werden (ethisches Verhalten),
- ob die **Daten** beim Lieferanten **gesichert** werden (IT-Security, Zugriffsrechte).

Grob gesagt, kann das alles bei uns mit „Ja, natürlich" beantwortet werden.

Zum **Datenschutz**:

Informationen werden bei uns nach 4 verschiedenen Kategorien separiert:

a) öffentlich zugängliche, b) interne, c) vertrauliche und d) streng vertrauliche.

Zu d): Zu letzteren zählen u.a. Personenbezogene Daten aus dem Personalbereich, Krankeninformationen, aber auch „Geschäftsgeheimnisse" wie Buchführungsdaten / Datev, Betriebswirtschaftliche Analysen (BWA), „Controlling-Cockpit", Planungen (Umsatz, Ertrag, Kosten, Liquidität etc.). Diese Daten sind nur für ausgewählte Personen verfügbar. Sie sind sonst unter Verschluss.

Zu c): Ebenfalls nicht für alle verfügbar, aber aus Datenschutzsicht nicht ganz so problematisch sind die vertraulichen Daten. Dazu gehören z.B. „Chef-Info"-Daten aus TimeLine, die „Balanced Scorecard" (Ziele, Strategien + Maßnahmen und Zielerreichung), Zahlungsanalyse (von Kunden), der ELO-Bereich Geschäftsführung, Geschäftsleitungssitzungen und Besprechungen, die jährliche Management-Bewertung aus dem Qualitätsmanagement-Bereich und Interna aus Mitarbeitergesprächen. Protokolle für Besprechungen sind einsehbar, enthalten aber keine vertraulichen Informationen, die besprochen wurden. Das heißt aber auch, dass keine vertraulichen Dinge aus Besprechungen weitererzählt oder weitergegeben werden dürfen. Auch diese vertraulichen Dinge sind entweder gar nicht aufgeschrieben worden oder sind unter Verschluss. Der Rest ist nur autorisierten Personen zugänglich.

Zu b): Auch interne Dinge müssen intern bleiben und dürfen nicht an Dritte weitergegeben werden. Viele, die in Abb. 1 aufgeführt sind, beinhalten „Geschäftsgeheimnisse", die nicht nach außen dringen dürfen. Aus den IT-Systemen dürfen beispielsweise keine Daten an Kunden weitergegeben werden, die sie nicht betreffen (-> Daten des Kunden).

Zu a): Nur öffentlich zugänglich(gemacht)e Informationen dürfen an Dritte weitergegeben werden. Das sind insgesamt recht wenige. Doch Daten aus den IT-Systemen (Angebote, Auftragsbestätigungen, Kontrakte etc.) und physische Dinge wie Muster dürfen und müssen natürlich an die Kunden weitergegeben werden, die es betrifft, – aber eben nur an die!

Zu **Daten des Kunden**:

Hier beachten wir den Datenschutz (DSGVO) und geben keine Kunden-Informationen an Dritte weiter – und zwar egal ob wir zusätzlich auch noch eine spezielle „Geheimhaltungsvereinbarung" gezeichnet haben. Kunden haben vor allem vor ihrer direkten Konkurrenz Angst. Es geht ihnen also vor allem darum, dass keine sensiblen Daten an andere Kunden, Ex-Kunden und Interessenten ihrer Branche weitergegeben werden. Aber wir dehnen dies im Sinne von „Geschäftsgeheimnissen von Kunden" auch auf alle anderen Dritten aus, die keine Mitarbeiter des Kunden sind.

Zum Datenschutz finden jährliche Schulungen über die Plattform Perseus statt, wo alle Mitarbeiter Zertifikate nachweisen müssen.

Zum „**Code of Conduct**“ (Verhaltenskodex) / **ESG-Richtlinien**:

Manche Kunden lassen uns einen „**Code of Conduct**“ unterschreiben. Meistens geht es dabei um ethisches Verhalten im Geschäftsleben und um Beachtung der einschlägigen Gesetze. Wir haben mit der ISO 26000 der Europäischen Union einen ähnlichen Kodex, lassen aber keine Kunden diesen unterschreiben. Bisher haben wir jeden CoC unterschreiben können, den Kunden uns vorlegten. Dies geschieht nur durch Mitarbeiter, die der Geschäftsleitung angehören und Prokura haben.

Zu **ESG**-Richtlinien (Quelle: Wikipedia-Artikel):

Environmental, Social and Corporate Governance (kurz ESG; englisch für: Umwelt, Soziales und Unternehmensführung) sind Kriterien und Rahmenbedingungen der Vereinten Nationen (UN) und Finanzinstituten für die Berücksichtigung von Umwelt-, Nachhaltigkeits- und Sozialfragen innerhalb von Unternehmensführungen, öffentlichen Körperschaften, Regierungen und Behörden. .. Neben den Interessen und Bedürfnissen der Unternehmen weltweit sollen laut ESG-Kriterien auch die Bedürfnisse aller Stakeholder (engl. für Interessengruppen) wie Mitarbeiter, Kunden, Lieferanten, Finanzinstitute, NGOs, Sozial- und Umweltvertreter zukünftig berücksichtigt werden. Die ESG-Kriterien sind so konzipiert, dass sie zukünftig in die Strategie aller Unternehmen weltweit eingebettet werden sollen. …

ESG umfasst drei Schlüsselbereiche, die bei der Analyse der Nachhaltigkeitsleistung eines Unternehmens bewertet werden:

Umwelt (Environment): Dieser Aspekt bezieht sich auf die Auswirkungen eines Unternehmens auf die Umwelt, einschließlich Themen wie Klimawandel, Energieeffizienz, Ressourcenverbrauch, Abfallmanagement und Umweltverschmutzung. Unternehmen, die sich auf umweltfreundliche Praktiken konzentrieren und ihre ökologischen Auswirkungen minimieren, werden positiv im ESG-Rating bewertet. ..

Soziales (Social): Der soziale Aspekt von ESG betrifft die Beziehungen eines Unternehmens zu seinen Mitarbeitern, Kunden, Lieferanten, Gemeinschaften und anderen relevanten Stakeholdern. Dazu gehören Themen wie Arbeitsbedingungen, Menschenrechte, Vielfalt und Inklusion, Gesundheit und Sicherheit am Arbeitsplatz sowie das Engagement in der Gemeinschaft. Unternehmen, die sozial verantwortlich handeln und sich um das Wohlergehen ihrer Stakeholder kümmern, erhalten positive Bewertungen. ..

Governance: Governance bezieht sich auf die Art und Weise, wie ein Unternehmen geführt und kontrolliert wird. Dies umfasst die Unternehmensführung, ethische Grundsätze, Integrität, Transparenz, Vorstandszusammensetzung, unabhängige Prüfung und die Einhaltung von Vorschriften. Unternehmen mit guter Governance-Struktur und -Praxis werden als vertrauenswürdig angesehen und erzielen eine höhere ESG-Bewertung. …

Dies können wir zu 100 % unterschreiben, weil wir uns vollständig daran halten:

Unsere **Umweltpolitik** ist genauso vorbildlich wie unser Qualitätsmanagement (Ressourcenverbrauch, Abfallmanagement), auch in Bezug auf Energieeffizienz. Auch wenn wir weder nach ISO 14001 noch nach 50001 zertifiziert sind, setzen wir intern viel strengere Vorgaben als in den Normen gefordert um. Beispielsweise sind wir seit Jahren 100 % klimaneutrales Unternehmen durch Kompensation unserer selbst verursachten Treibhausgas-Emissionen (Scope 1+2 des GHG Protocol) durch Unterstützung des Projektes Togo unseres Partners natureOffice, das 12 der 17 UN-Nachhaltigkeitsziele erfüllt.

Unsere Energiemanagement-Maßnahmen am neu errichteten Standort seit 2016 (u.a. Photovoltaik-Anlage, Heizung, Gebäude) sind so gut, dass nach Expertise eines Gutachtens kaum noch Verbesserungen möglich sind. Auch dies war ein Grund für uns, uns in diesen Bereichen nicht zertifizieren zu lassen.

Bei Thema **Soziales** haben wir in unserer grundlegenden Strategie und unseren Unternehmensgrundsätzen festgelegt, dass wir sehr langfristige, vertrauensvolle Beziehungen zu Kunden, Lieferanten und Mitarbeitern pflegen, was wir auch als starke Wettbewerbsvorteile ansehen. Dazu schaffen wir gute Arbeitsbedingungen und halten Mitarbeiter- und Menschenrechte ein. Vielfalt und Inklusion fördern wir beispielsweise durch eine enge Kooperation mit den Iserlohner Werkstätten. Gesundheit und Sicherheit am Arbeitsplatz sind uns wichtig, wofür Qualitätsmanagement und Betriebsarzt eng zusammenarbeiten. Unsere soziale Verantwortung nehmen wir u.a. durch Spenden, Engagement in Organisationen (u.a. die Allianz für Entwicklung und Klima), Sponsoring und Kooperation mit den Iserlohner Werkstätten wahr.

Bei der **Führung und Kontrolle** des Unternehmens orientieren wir uns an der ISO 26000 der Europäischen Union. Als familiengeführter Mittelständler sind wir Werte-orientiert, ehrlich und transparent. Davon zeugt auch unsere Vision. Der Mensch soll hier im Mittelpunkt stehen. In unseren Unternehmensgrundsätzen steht:

Als Familienunternehmen sind wir Werte-orientiert und sozial engagiert, kooperieren bei den Mitarbeitern mit den „Iserlohner Werkstätten“ und setzen auf sehr langfristige, vertrauensvolle Beziehungen zu Kunden, Lieferanten und Mitarbeitern. Unser Leitbild dafür ist der internationale EU-„Leitfaden zur gesellschaftlichen Verantwortung von Organisationen (DIN ISO 26000)“.

Zur **Datensicherung** bei uns:

Zu den Bereichen IT-Security und Zugriffsrechte könnten wir viel schreiben, weil wir hier so viel tun bzw. schon umgesetzt haben. Wir tun hier in der Tat alles Menschenmögliche, um Bedrohungen von außen und von innen zu minimieren. Dazu haben wir in eine sehr gute IT-Infrastruktur (u.a. neuer Server) und eine sehr gute Firewall investiert.

Zugriffsrechte beschränken den Zugang zu Daten auf autorisierte Personen. Dies stellt der jeweilige Administrator ein.

Zur IT-Security gehören neben den ganzen systembezogenen Dingen bei IT-Systemen (Server, Rechner, Firewall etc., Software), bei denen wir uns von IT-Fachleuten beraten lassen (u.a. SchueCom), auch die jährlichen Kurse für Mitarbeiter bei Perseus in den Bereichen

- Phishing,

- Cybersicherheit und

- neu Ransomware.