Datenschutz

- Jeder Mitarbeiter ist bei der Verarbeitung personenbezogener Daten Teil der datenverarbeitenden Stelle und insofern für den Datenschutz mitverantwortlich. Behandeln Sie Daten anderer so, wie Sie Ihre eigenen Daten behandelt wissen wollen.

- Beachten Sie, dass persönliche Informationen wie bspw. Gehalts-, Beurteilungs- sowie Bankdaten nur datenschutzgerecht (über verschlossene Hauspost sowie verschlüsselte E-Mails) weitergeleitet werden dürfen.

- Bei Telefonauskünften bzw. Herausgabe vertraulicher Informationen prüfen Sie bitte, ob diese Informationen herausgegeben werden dürfen, wie bspw. Telefondurchwahl, Handynummer, Kundenliste oder Auskünfte über Urlaub, Krankheitsinformationen, etc. Beachten Sie, dass jede unbefugte Weitergabe der Daten unzulässig und strafbar ist.

- Entsorgen Sie entsprechende Unterlagen datenschutzgerecht (in Entsorgungsboxen oder durch mechanisches Vernichten der Unterlagen, z.B. mittels Schredder).

- Verhalten Sie sich im Internet / Social Media so, wie Sie es auch im realen Leben tun würden. Denken Sie daran, das Internet vergisst nichts.

- Beachten Sie die Rechte anderer bei Veröffentlichungen von Bildern.

Compliance

- Treffen Sie keine Absprachen mit Wettbewerbern hinsichtlich wettbewerbsrelevanter Parameter, wie z. B. Preisen, Preisänderungen, Kunden- oder Lieferantenbeziehungen.

- Tauschen Sie auch keine Informationen dieser Art mit Wettbewerbern aus.

- Beachten Sie, dass unseren Kunden nicht vorgeschrieben werden darf, zu welchen Konditionen sie unsere Produkte weiterverkaufen dürfen.

- Achten Sie darauf, dass Insiderinformationen, d. h. kursrelevante Informationen, die Sie über börsennotierte Gesellschaften haben, bevor sie allgemein bekannt sind, weder direkt noch indirekt zum Kauf / Verkauf von Aktien genutzt werden dürfen.

- Die Gewährung von Zuwendungen (z. B. Sachgeschenken oder Einladungen) gegenüber Amtsträgern ist unzulässig. Darüber hinaus ist die Gewährung oder Entgegennahme von Zuwendungen auch unzulässig, wenn sie im Zusammenhang mit der Vergabe von Aufträgen stehen.

- Jeder Anschein von korruptem Verhalten ist zu vermeiden, d. h. Einladungen oder Geschenke dürfen den Rahmen der Üblichkeit nicht überschreiten. Eine Wertgrenze von 50 Euro kann als Anhalt dienen.

http://zeissnet.zeiss.org/sicherheit

Ihre Ansprechpartner:

Heiko Winkler
Leiter Konzernfunktion
Konzernsicherheit
Telefon: +49 7364 20-5538
heiko.winkler@zeiss.com

Ulrich Hoffmann
Chief Compliance Officer
Telefon: +49 7364 20-3931
ulrich.hoffmann@zeiss.com

Wolfgang Schüler
Leiter Konzerndatenschutz
Telefon: +49 7364 20-3841
wolfgang.schueler@zeiss.com

DE_90_010_00041 Printed in Germany ZD-CZ-III/2015 PNoo

Das Wichtigste zum Thema Sicherheit bei ZEISS

We make it visible

Konzern- und Informationssicherheit

Unser Wissen und unsere Erfahrungen sind der Schlüssel zu unserem Unternehmenserfolg. Um unsere Position im Wettbewerb nicht zu gefährden, sind alle Mitarbeiter aufgefordert, verantwortungsbewusst mit Informationen umzugehen. Dies bezieht sich auch auf Daten, die ZEISS von Geschäftspartnern bezieht. Deshalb möchten wir Sie mit den wesentlichen Grundsätzen zur IT-Sicherheit, allgemeiner Konzern- und Informationssicherheit und Datenschutz sowie Compliance bei ZEISS vertraut machen.

- Achten Sie darauf, dass sich Tagesbesucher – gekennzeichnet mit einem roten Besucherausweis – nicht unbeaufsichtigt auf dem ZEISS Gelände aufhalten dürfen.
- Beachten Sie das Fotografierverbot auf dem ZEISS Gelände.
- Kennzeichnen Sie Informationen entsprechend der betrieblichen Vorgaben als offen (public), Nur für den internen Gebrauch (for internal use only), Vertraulich (confidential) und Streng vertraulich (strictly confidential).
- Schließen Sie alle geschäftsrelevanten und vertraulichen Unterlagen abends und bei längerer Abwesenheit weg („Clean Desk").

IT-Sicherheit

- Nutzen Sie die vom Unternehmen zur Verfügung gestellten IT-Systeme sowie E-Mail- und Internet-Accounts ausschließlich im ausdrücklich genehmigten Rahmen.
- Installieren Sie keine Software ohne Lizenz auf betrieblichen IT-Systemen und verwenden Sie keine privaten IT-Geräte oder Software für betriebliche Tätigkeiten.
- Installieren Sie unverzüglich sicherheitsrelevante Updates, sobald Sie darüber informiert werden.

- Sperren Sie bei Abwesenheit vom Arbeitsplatz Ihren Rechner ab (Tastenkombination „Windows-Zeichen" plus „Taste L").
- Verwenden Sie ein sicheres Passwort (Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen). Geben Sie das Passwort in keinem Fall weiter.
- Erwähnen Sie auf Ihren privaten Webseiten oder in Diskussionsforen keine Belange des Unternehmens. Im Social Web treten Sie als Privatperson auf.
- Beachten Sie, dass die Mitnahme von vertraulichen Informationen außerhalb des Firmengeländes „sicher" erfolgen muss. Das bedeutet, dass Daten verschlüsselt und Papierunterlagen verschlossen mitzuführen sind.

Sicherer Umgang mit Smartphones und Tablets

- Achten Sie bei Ihren Aktivitäten auf die sichere Herkunft der Daten, die Sie auf Ihr mobiles Gerät laden. Daten aus zweifelhaften Quellen, zum Beispiel Musik- oder Videodateien, können Gefahren wie Schadsoftware enthalten. Ähnliche Gefahren lauern, wenn unsichere Geräte, zum Beispiel ungeschützte private Computer, mit Ihrem Smartphone verbunden sind.
- Achten Sie genau darauf, welche Daten eine App von Ihnen verlangt, bevor Sie sie installieren. Viele Apps, vor allem kostenlose Anwendungen, greifen – quasi als Gegenleistung – auf eine Reihe von Daten zu, die nicht für die Funktion der App relevant sind, zum Beispiel Positions-oder Kontaktdaten. Die Messenger-App „WhatsApp" liest zum Beispiel Ihre Kommunikation vollständig mit und analysiert sie. Beachten Sie auch, welche Daten möglicherweise in unsicheren Cloud-Speichern abgelegt werden. Schutzbedürftige geschäftliche Daten dürfen nicht in der Cloud abgelegt werden.
- Tauschen Sie schutzbedürftige geschäftliche Informationen nur über die sicheren Kanäle E-Mail und SMS aus. Messenger-Dienste wie WhatsApp oder Threema sind dafür nicht geeignet.
- Beschränken Sie die Ortungsfunktion Ihrer Geräte auf das absolute Minimum, zum Beispiel auf Navigation.
- Entfernen Sie keine Nutzungsbeschränkungen (sogenanntes Jailbreak). Der Gebrauch von Hackertool-Software ist ausdrücklich untersagt. Sie begehen damit möglicherweise eine Straftat.
- Informieren Sie bei Verlust oder Diebstahl Ihres Smartphones / Tablets unverzüglich das IT Service-Desk.