



Datenschutz und Informationssicherheit bei ZEISS


Hinweise für alle Mitarbeiter



Liebe Mitarbeiterinnen und Mitarbeiter,

unser Wissen und unsere Erfahrungen – die Kenntnisse, die Sie und Ihre Kolleginnen und Kollegen gesammelt haben – sind der Schlüssel zum Unternehmenserfolg. Aus ihnen entstehen Innovationen und Strategien, und mit Innovationen und Strategien können wir Wettbewerbsvorsprung erzielen. Dieses wichtigste Kapital des Unternehmens wird in Form von Informationen gespeichert, versandt und ausgetauscht. Offener und schneller Informationsaustausch innerhalb der Unternehmen der ZEISS Gruppe wie auch zu unseren Geschäftspartnern ist einer unserer Erfolgsfaktoren. Diese Offenheit birgt aber auch Risiken, weil Informationen auch unbeabsichtigt an Dritte gelangen können.

Wir alle müssen mitwirken, das Wissenskapital von ZEISS zu sichern. Wir alle wissen, dass es keine absolute Informationssicherheit gibt, aber wir können durch unser Verhalten im Umgang mit Informationen dazu beitragen, bestehende Risiken einzuschränken. Die vorliegende Broschüre gibt einen allgemeinen Überblick zum Thema „Datenschutz und Informationssicherheit bei ZEISS“. Wir bitten Sie bei dieser Aufgabe mitzuwirken, damit wir unsere Position im Wettbewerb durch verantwortungsbewussten Umgang mit Informationen weiter stärken.



Dr. Michael Kaschke
Vorstandsvorsitzender
Carl Zeiss AG

Es scheint sehr einfach, aber:

Richtige Kommunikation ist eine Kunst

Kommunizieren ist Weitergabe und Erhalt von Informationen. Ohne Kommunikation ist kein Leben denkbar.

Auch ein Unternehmen kann sich nur entfalten, wenn die Kommunikation reibungslos funktioniert und alle Partner einbezogen werden. ZEISS arbeitet deshalb ständig daran, die Kommunikationsprozesse zu verbessern. Je intensiver wir kommunizieren, umso größer wird die Gefahr, dass wir Informationen preisgeben, die nicht in fremde Hände gelangen sollten.

Mit E-Mail, Internet, Online-Zugriff etc. besteht die Möglichkeit, von zu Hause oder unterwegs auf Informationen zuzugreifen oder Daten rund um den Globus zu übermitteln. Das ist gut so. Jeder Mitarbeiter, der die modernen Kommunikationsmittel einsetzt, sollte aber auch wissen, dass es damit immer wichtiger wird, schutzwürdige Daten/Informationen zu sichern und abzugrenzen. **Nicht weniger, aber bewusster kommunizieren heißt daher die Aufgabe, der wir uns stellen müssen.**

Wir müssen lernen, schutzwürdige Daten/Informationen zu erkennen und zu schützen.



Umgang mit Informationen:

Daten- und Informationsschutz geht uns alle an

Denn die missbräuchliche Nutzung der Informationen durch andere kann erheblichen Schaden verursachen und sogar das ganze Unternehmen in Gefahr bringen.

Der Verlust wichtiger Informationen kann einen mit hohem Aufwand erarbeiteten Wettbewerbsvorteil im Handumdrehen zunichte machen. Investitionen in Forschung und Entwicklung werden wertlos, wenn die Ergebnisse vor der wirtschaftlichen Nutzung an die Öffentlichkeit gelangen. Bei Ausschreibungen sind wir ohne Chance, wenn unser Angebot vorab einem Konkurrenten bekannt wird.

Ergiebige Quellen für interessierte „Informationssammler“ können neben den technischen Angriffen auf die Kommunikationswege auch Gespräche bei Messen, Tagungen und Kongressen sein. Abends bei der Pflege der geschäftlichen Netzwerke und den sogenannten zwischenmenschlichen Beziehungen ist die Informationsbereitschaft besonders groß.

Vor allem auf Reisen sind die Gefahren hoch. Mehr und mehr werden mitgenommene, mobile IT-Systeme wie Laptops oder USB Sticks als gestohlen gemeldet. Daten / Informationen können unbemerkt kopiert werden oder Dritte können bei Benutzung in öffentlichen Räumen mitlesen. Beim Benutzen von Laptops / Notebooks außerhalb der Firma sind bestimmte Vorsichts- und Sicherheitsmaßnahmen zu beachten. Unterlagen können angefordert oder im Intranet unter zeissnet.zeiss.org/sicherheit, Rubrik IT-Sicherheit abgerufen werden.

Besonders zu berücksichtigen sind Datentransfers ins Ausland, insbesondere außerhalb der EU. Hierzu sollte man sich bei einem Ausfuhrreferenten informieren, um nicht gegen bestehende Ausfuhrbeschränkungen oder Regeln zu Dual-Use-Gütern zu verstoßen. Gleiches gilt bei der Übermittlung personenbezogener Daten. Hier sollten Sie sich mit dem jeweiligen Data Protection Coordinator in Verbindung setzen (siehe Rückseite Booklet).

Das System:

Informationssicherheit bei ZEISS

Die Sicherheitsorganisation bei ZEISS lässt sich wie folgt beschreiben:

- Die Führungskräfte sind für die Festlegung der Schutzklassen der zu schützenden Informationswerte und die Auswahl der gegebenen Sicherheitsmaßnahmen verantwortlich.
- Die Konzernsicherheit ist für die Weiterentwicklung und die Überwachung des Sicherheitskonzepts zuständig.
- Die Betreiber von IT-Systemen sorgen für die Sicherstellung der Vertraulichkeit, der Verfügbarkeit und der Integrität der IT-Systeme (= IT-Sicherheit).
- Jeder einzelne Mitarbeiter ist für den ordnungsgemäßen Umgang mit den Informationen und den zur Verfügung gestellten IT-Systemen verantwortlich.

Was haben Sie zu beachten?

Kennzeichnen Sie Ihre Dokumente!

Es gibt bei ZEISS klare Vorgaben durch vier Sicherheitsklassen, die weltweit gültig sind:

- Offen (public)
- ZEISS intern bzw. nur für den internen Gebrauch (ZEISS internal or for internal use only)
- Vertraulich (confidential)
- Streng vertraulich (strictly confidential)

Der Informationseigentümer (Ersteller = Fachbereich) legt die Schutzwürdigkeit fest und entscheidet, wer Zugang zu den Informationen haben darf. Alles, was nicht als offen einzustufen ist, muss geschützt und darum gekennzeichnet werden.

Vorsichtig mit Unterlagen/Kopien umgehen

- Kopieren Sie nur in den tatsächlich benötigten Stückzahlen.
- **Streng vertrauliche Dokumente** müssen einen Verteiler haben und die Vertraulichkeitsstufe muss auf jeder Seite erkennbar sein.
- Die Weitergabe von Kopien von **streng vertraulichen Unterlagen** ist nur mit ausdrücklicher Genehmigung der Ersteller möglich.

- Bei Weiterleitung **vertraulicher** Unterlagen an Stellen außerhalb der ZEISS Unternehmen bedarf es einer Abstimmung mit dem Ersteller.
- Fehldrucke oder nicht mehr benötigte Unterlagen bitte datenschutzgerecht entsorgen (Benutzen Sie die aufgestellten Datenentsorgungsboxen oder Aktenvernichter).

Unterlagen sicher aufbewahren

Betriebliche Unterlagen sind nach Arbeitsende verschlossen aufzubewahren (clean desk). Vertrauliche und streng vertrauliche Unterlagen sind so aufzubewahren, dass niemand unbefugt Einblick nehmen kann. Bei Speicherung auf Servern sind die Zugriffsberechtigungen auf die Verzeichnisse entsprechend einzurichten.

Sichere Weitergabe von vertraulichen Unterlagen

Bei der Weiterleitung von Unterlagen ist es nicht ökonomisch, jeweils den Eigentümer eines Dokuments einzubinden. Beachten Sie deshalb nachstehende Aspekte:

- Den Verteiler so klein wie möglich halten.
- Handelt es sich bei dem Empfänger um einen Adressaten außerhalb des Konzerns, so ist die Weitergabe mit dem Eigentümer abzustimmen.

- Machen Sie einen Vermerk, an wen Sie was wann weitergeleitet haben.
- Bei mündlicher Weitergabe von Informationen gilt dies entsprechend.
- Auf jeden Fall verschlüsselt bei Weitergabe als E-Mail (Outlook). Bei Verteilung über das Internet die vorgegebenen Tools (Brainloop, Hightail, etc.) nutzen.
- Externer Postversand: Die Sicherheitsklasse nicht auf dem sichtbaren Umschlag vermerken. Einsatz von entsprechenden Absicherungen, zum Beispiel blickdichte Umschläge oder Innenumschläge.
- Hauspost: Hauspostumschläge verschlossen verschicken.

Sichere Weitergabe von streng vertraulichen Unterlagen

In Anlehnung an oben stehende Hinweise sind bei streng vertraulichen Unterlagen weiter gehende Maßnahmen sicherzustellen: Streng vertrauliche Datenträger (Papier, USB Sticks etc.) müssen einen Verteiler haben. Die im Verteiler genannten Personen dürfen die Dokumente weder kopieren noch weiterleiten. Werden die Dokumente nicht mehr benötigt, so sind sie kontrolliert zu vernichten oder an den Verteiler zurückzugeben, der gegebenenfalls für die kontrollierte Vernichtung sorgt. Streng

vertrauliche Informationen sollten nicht telefonisch (es sei denn verschlüsselt) weitergegeben werden. Bei Versand mit der Hauspost einen geschlossenen und entsprechend gekennzeichneten Innenumschlag verwenden.

Passwörter niemals weitergeben!

Die Benutzer-ID (User-ID) und die daraus resultierende Zugriffsberechtigung (geschützt durch Passwort) sind persönlich und nur für Sie gültig. Dasselbe gilt für eToken oder Smartcard, falls Sie diese einsetzen.

Schützen Sie Ihre Passwörter!

Passwörter sind der Zugang zu IT-Systemen und damit der Schlüssel zu Ihren Informationen.

- Ein Passwort muss mindestens aus acht Zeichen bestehen und Buchstaben, Zahlen und Sonderzeichen enthalten.
- Die Passwortänderung sollte regelmäßig, spätestens nach zwei Monaten (sofern technisch machbar) erfolgen.
- Geben Sie Ihr Passwort niemals weiter. Sofern dies in einem konkreten Fall unabwendbar ist, ändern Sie es anschließend sofort.
- Keine Trivialpasswörter (wie z. B. Vor- oder Familienname) verwenden!

Verwenden Sie Zeichen und Ziffern aber keine Leerzeichen, Tabs oder User-ID.

- Verwenden Sie bei der Arbeit keine Passwörter, die Sie privat verwenden.
- Verwalten Sie Ihre Passwörter mit KeePass.

Verantwortungsbewusster Umgang mit dem Internetzugang

Der Zugriff aus dem Firmennetz darf nur über Proxy-Server und Firewall erfolgen.

Die Internet-Nutzungsbedingung ist zu beachten. Verändern Sie nicht selbstständig die Einstellung Ihres Internet-Browsers.

Sorgsame Handhabung der Kommunikationseinrichtungen

Die Benutzer von IT-Systemen müssen mit den ihnen anvertrauten Systemen sorgsam umgehen. Hardware-Installationen wie Anschlüsse an das lokale Netzwerk dürfen nur durch die IT oder den LSS (Local Support Service) erfolgen. Software-Installationen sind zu dokumentieren (Lizenznachweis) und erfolgen bei Software, die von der IT zur Verfügung gestellt wird, durch den Anwender selbst (Self-Service). Andere Software muss vorab geprüft und durch Ihre IT installiert werden.

Die Anwender haben betriebliche Daten / Informationen auf zentralen Systemen (z. B.

Netzlaufwerke, Sharepoint) abzulegen, damit eine Datensicherung gewährleistet ist. Antivirus-Software muss auf jedem Arbeitsplatzcomputer, einschließlich Laptops installiert sein. Die Aktualisierung der Antivirus-Software wird durch die IT durchgeführt.

Zusammenarbeit mit externen Mitarbeitern

Unternehmen der ZEISS Gruppe arbeiten intensiv mit anderen Firmen zusammen. Die Übermittlung von Daten/Informationen an diese und von diesen Personen darf nur im Rahmen der Aufgabenstellung erfolgen. Der ZEISS Auftraggeber muss sicherstellen, dass mit den externen Unternehmen vor Arbeitsaufnahme eine vertragliche Regelung (Geheimhaltungsvereinbarung, bei Zugang zu personenbezogenen Daten ist eine datenschutzrechtliche Vereinbarung erforderlich) abgeschlossen wird. Falls externe Mitarbeiter bei ZEISS beschäftigt werden, müssen diese die notwendigen Regeln und IT-Sicherheitsmaßnahmen von ZEISS kennen und beachten.

Sicherheit ist Ihre Aufgabe:

Reden ist Silber, Schweigen ist Gold

Was schutzwürdig ist, können Sie in den meisten Fällen sehr gut selbst bewerten, indem Sie abschätzen, welche Wirkung die Information bei gezielter Nutzung durch Unbefugte haben könnte. Setzen Sie Ihre Erfahrung und Sachkenntnis ein. Die nachstehenden Beispiele beschreiben betriebliche und geschäftliche Unterlagen, die auf keinen Fall in falsche Hände gelangen dürfen.

Betriebliche Informationen (Betriebsgeheimnisse):

- Entwicklungsergebnisse mit Berichten
- Werk- und Konstruktionsunterlagen
- Rezepturen und optische Designunterlagen
- Software
- Informationen über besondere Produktionsverfahren
- Arbeitsbeschreibungen
- Muster und Modelle etc.

Ferner geschäftliche Informationen (Geschäftsgeheimnisse):

- Kalkulationsbedingungen
- Besondere Konditionen
- Einkaufsquellen und -bedingungen
- Marketingstrategien und -maßnahmen
- Organigramme und Hierarchien
- Bilanz- und Steuerunterlagen
- Personal- und Pensionsunterlagen
- Ein- und Mehrjahresplanungen, Geschäftspläne
- Kommunikationsverzeichnisse wie Telefonbücher und Adressverzeichnisse

Unsere Bitte an Sie: Richten Sie Ihr Kommunikationsverhalten immer auf die Schutzbedürfnisse von ZEISS aus. Werden Sie sich bewusst, wo die Grenze liegt, wo Sie lieber schweigen als reden sollten oder besondere Schutzmaßnahmen notwendig werden. Auch in Ihrem privaten Umfeld sollten Sie sich dieser Grenze bewusst sein.

Datenschutz heißt:

Persönlichkeitsrechte wahren

Datenschutz bedeutet, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Personenbezogene Daten sind Informationen über eine natürliche Person, die diese direkt oder indirekt identifizierbar machen. Eine direkte Identifikation ist beispielsweise über Name, Anschrift oder Bild möglich. Indirekt identifizieren lassen sich Personen unter anderem durch Merkmale wie Größe, Gewicht oder Gesundheitsdaten.

Um den vielfältigen Gefahren durch missbräuchlichen Umgang mit personenbezogenen Daten begegnen zu können, wurde für den Umgang mit personenbezogenen Daten eine konzernweite Vorgabe geschaffen. Darin werden die gesetzlich begründeten Regeln für das Erheben, Verarbeiten, Übermitteln und Nutzen von personenbezogenen Daten bei ZEISS festgelegt. Nationale gesetzliche und ggf. kollektivrechtliche Regelungen zum Datenschutz gelten vorrangig. Das Ziel, ein wirksamer Datenschutz, kann aber nur erreicht werden, wenn die Vorschriften in die betriebliche Praxis umgesetzt werden. Sie müssen im Rahmen Ihrer beruflichen Tätigkeit dafür sorgen, dass die personenbezogenen Daten Anderer vertraulich behandelt werden.

Behandeln Sie Daten Anderer so, wie Sie Ihre eigenen Daten behandelt wissen wollen.

Sie sind dafür verantwortlich, dass die Ihnen anvertrauten personenbezogenen Daten nur im Rahmen Ihrer Aufgabenstellung und des erhobenen Zwecks verarbeitet oder genutzt werden. Grundsätzlich ist die Erhebung und Verarbeitung auf das notwendige Minimum einzuschränken. Eine Verarbeitung darf nur stattfinden, wenn eine angemessene Sicherheit der Daten gewährleistet werden kann. Gelöscht werden personenbezogenen Daten, sobald diese nicht mehr für den erhobenen Zweck benötigt werden, die nötigen Aufbewahrungspflichten erloschen sind oder keine Rechtsgrundlage mehr für eine Verarbeitung vorliegt. Auskünfte oder Beschwerden im Umgang mit personenbezogenen Daten werden immer von der zentralen Datenschutzstelle beantwortet (siehe Rückseite Booklet). Geben Sie selbst keinerlei Auskünfte und leiten solche Vorgänge immer an Ihren Vorgesetzten oder direkt an den Datenschutz bei ZEISS weiter! Jeder Missbrauch, jede unbefugte Weitergabe dieser Daten ist unzulässig und strafbar. Alle, die mit personenbezogenen Daten zu tun haben, sind zur Wahrung des Datengeheimnisses verpflichtet – auch über die Zeit ihrer Beschäftigung bei ZEISS hinaus.

Nur wenn wir gemeinsam handeln, können wir unsere Ziele erreichen



Wir müssen sicherstellen, dass wir uns und unsere Geschäftspartner vor dem Missbrauch unternehmens- und personenbezogener Informationen schützen. Setzen Sie die Empfehlungen dieser Broschüre um und helfen Sie mit, unsere Position im Wettbewerb durch verantwortungsbewussten Umgang mit Daten und Informationen zu stärken.

Sicherheit ist Ihre Aufgabe:

- Sicherer und sorgsamer Umgang mit dem Passwort
- Notwendige Zugriffe auf gespeicherte Informationen/Daten nur über zugeteilte Zugriffsberechtigungen vornehmen
- Betriebliche Unterlagen vor Unbefugten sicher aufbewahren (clean desk)
- Speichern Sie Ihre Daten auf zentralen Systemen (Netzlaufwerke, Sharepoint, etc.)
- Softwareinstallationen im Rahmen des Self-Services sind erlaubt, andere Soft- und Hardwareinstallationen nur durch Ihre IT vornehmen lassen
- Eine Informationsweitergabe darf nur im Rahmen der Aufgabenstellung erfolgen
- Nicht mehr benötigte Datenträger (Schriftgut, USB Sticks, Festplatten) sind sicher zu entsorgen
- Bei Verwendung von mobilen IT-Systemen wie Laptops, Smartphones oder Tablets außerhalb der Firma sind die Sicherheitshinweise zu beachten

Informieren Sie uns, wenn Sie auf Informationen zugreifen können, ohne dazu die Erlaubnis zu haben. Sprechen Sie uns auch an, wenn es etwas zu verbessern gibt.

Ansprechpartner für**IT- & Informationssicherheits-Themen:**

Oliver Ortlieb

Information Security Governance

E-Mail: corporate-security@zeiss.com

Telefon: 07364 20 4408

oder anonym per Post (Carl Zeiss AG, CSE)

Ansprechpartner für**Datenschutz-Themen:**

Andreas Karl

Corporate Data Protection Officer

E-Mail: dataprivacy.internal@zeiss.com

Telefon: 07364 20 3841

oder anonym per Post (Carl Zeiss AG, CLP-D)

Weitere Informationen finden Sie im Intranet unter: <http://zeissnet.zeiss.org/sicherheit>