1. Datenschutz bei der Nutzung von E-Mails

Beim Versenden von E-Mails ist folgendes zu beachten:

- Möchten Sie eine E-Mail an mehrere Empfänger senden (z.B. Serienbrief an alle Kunden), berücksichtigen Sie bitte, dass E-Mail-Adressen, die im „An“-Feld sowie im „Cc“-Feld stehen, von allen Empfängern gesehen werden können. Dies stellt eine Datenschutzverletzung dar, sofern die Adressaten hinsichtlich des Inhalts der E-Mail nicht zusammenarbeiten. Nutzen Sie daher in solchen Fällen immer das „Bcc“-Feld, sodass der Empfänger lediglich seine eigene E-Mail-Adresse und die des Absenders sieht.
- Möchten Sie eine E-Mail an mehrere Empfänger senden, die hinsichtlich des Inhalts der E-Mail zusammenarbeiten (z.B. Versenden von Informationen innerhalb einer internen Arbeitsgruppe), kann das „Cc“-Feld genutzt werden, sodass die Empfänger sehen, wer aus diesem Verteiler die E-Mail erhalten hat.
- Möchten Sie eine E-Mail weiterleiten, prüfen Sie bitte, ob die E-Mail personenbezogene Daten beinhaltet und ob der Empfänger tatsächlich Kenntnis über diese Daten haben muss. Gegebenenfalls sind einige personenbezogenen Daten unkenntlich zu machen.
- Geben Sie niemals Passwörter oder Transaktionsnummern per E-Mail heraus.
- E-Mails mit personenbezogenen Daten sind verschlüsselt zu versenden. Mindestens sollten jedoch Dateien verschlüsselt und mit einem Passwort geschützt werden. Dieses Passwort ist dem Empfänger der E-Mail auf einem anderen Weg (z.B. telefonisch) mitzuteilen. Mit bestimmten Empfängern kann beispielsweise zuvor auch ein individuelles festes Passwort auf einem anderen Weg (z.B. im persönlichen Gespräch oder per Telefon) abgestimmt werden, welches sodann für den zukünftigen Dokumentenaustausch genutzt wird.
- Prüfen Sie vor dem Versenden von Dateien in einem offenen Dateiformat (z.B. Word- oder Excel-Dateien), ob die Datei wirklich in diesem Format versendet werden muss oder ggf. vor dem Versenden in eine PDF-Datei umgewandelt werden kann.

Beim Empfangen von E-Mails ist folgendes zu beachten:

- Niemals auf Links in einer dubiosen E-Mail klicken.
- Niemals einen Download-Link direkt aus der E-Mail heraus starten.
- Niemals Anhänge einer E-Mail, die Ihnen verdächtig vorkommt, öffnen (Sollten Sie doch einen Anhang öffnen und aufgefordert werden Makros zu aktivieren, fragen Sie telefonisch beim vermeintlichen Absender nach, bevor Sie die Makros aktivieren).
- Sollten Sie eine E-Mail mit einem Dokument von einem bekannten Absender erhalten, der Ihnen üblicherweise keine Dokumente schickt und dies auch nicht angekündigt hat, fragen Sie vorsichtshalber beim Absender telefonisch nach, bevor Sie den Anhang öffnen.

Dieses Dokument ist ausschließlich für eigene Zwecke zu nutzen. Eine kommerzielle Verwendung ist ausgeschlossen.
Bitte beachten Sie, dass dieses Dokument nicht als abschließend zu betrachten ist und auf das jeweilige Bedürfnis/Unternehmen anzupassen ist.
© www.ds-quadrat.de

2. Datenschutz in Telefongesprächen

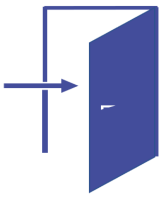
Bei Telefongesprächen ist hinsichtlich des Datenschutzes folgendes zu beachten:

- Bitte vergewissern Sie sich vor der Herausgabe von personenbezogenen Daten, ob die Person diese Daten erhalten darf. Gegebenenfalls ist die Identität der anrufenden Person zu prüfen (z.B. durch Abfrage der Kundennummer o.ä.).
- Es sind nur so viel personenbezogene Daten wie erforderlich mitzuteilen (z.B. Anruf für einen Kollegen, der aufgrund Krankheit nicht da ist: Bitte nicht: „Frau Müller ist bis Ende April krankgeschrieben.“ Sondern besser: „Frau Müller ist bis Ende April nicht im Haus.“).
- Bitte achten Sie darauf, dass Unbefugte das Telefongespräch nicht mithören können. Kann dies nicht gewährleistet werden, ist der Gesprächspartner darüber zu informieren. Das Telefonat sollte sodann zeitlich so verschoben werden, dass ein diskretes Gespräch wieder möglich ist.

3. Datenschutz in persönlichen Gesprächen

Bei persönlichen Gesprächen ist hinsichtlich des Datenschutzes folgendes zu beachten:

- Bitte vergewissern Sie sich, ob Ihr Gegenüber dazu befugt ist, die personenbezogenen Informationen zu erfahren. Bei nicht persönlich bekannten Personen ist die Identität zu prüfen (z.B. durch Vorzeigen des Personalausweises).
- Es sind nur so viel personenbezogene Daten wie erforderlich preiszugeben.
- Bitte achten Sie darauf, dass Unbefugte das Gespräch nicht mithören können. Wahren Sie Diskretion, sofern Unbefugte mithören könnten.



4. Datenschutz beim Verlassen des Büros

Sobald Sie Ihren Arbeitsplatz/Ihr Büro verlassen, beachten Sie bitte folgendes:

- Bitte sperren Sie Ihren Bildschirm - auch, wenn Sie das Büro nur für kurze Zeit verlassen (Windows-Taste und L gleichzeitig drücken).
- Bitte sorgen Sie dafür, dass keine Unterlagen mit personenbezogenen Daten auf Ihrem Arbeitsplatz liegen.
- Sofern Sie als letzter den Raum verlassen, schließen Sie bitte die Tür zu Ihrem Arbeitsplatz ab.

Dieses Dokument ist ausschließlich für eigene Zwecke zu nutzen. Eine kommerzielle Verwendung ist ausgeschlossen.
Bitte beachten Sie, dass dieses Dokument nicht als abschließend zu betrachten ist und auf das jeweilige Bedürfnis/Unternehmen anzupassen ist.
© www.ds-quadrat.de

5. Datenschutz bei Besuchern

Empfangen Sie Besucher (z.B. Kunden oder Vertreter eines Dienstleisters), ist folgendes zu beachten:

- Bitte achten Sie darauf, dass Dokumente mit personenbezogenen Daten anderer Personen nicht offen herumliegen.
- Sollten Sie im Beisein des Besuchers am PC arbeiten, achten Sie bitte darauf, dass er personenbezogene Daten von anderen Personen auf dem Bildschirm nicht einsehen kann (z.B. durch Wegdrehen des Bildschirms oder Nutzung einer Sichtschutzfolie).
- [*Jedem Besucher ist ein Besucherausweis auszuhändigen, den dieser sichtbar zu tragen hat. Bitte sammeln Sie den Besucherausweis am Ende des Besuches wieder ein.*]
- Besucher dürfen sich nur in Begleitung eines Mitarbeiters auf dem Betriebsgelände aufhalten.
- Sollte sich eine Ihnen unbekannte Person ohne Begleitung eines Mitarbeiters [*und ohne Besucherausweis*] auf dem Betriebsgelände aufhalten, sprechen Sie Ihn bitte an und geleiten Ihn ggf. zum entsprechenden Ansprechpartner.

6. Datenschutz im Außendienst und auf Dienstreisen

Im Auto:

- Bitte stellen Sie sicher, dass personenbezogenen Daten von außen nicht einsehbar sind.
- Das Auto ist bei Verlassen unverzüglich abzuschließen.
- Lassen Sie keine Unterlagen oder Laptop/Smartphone sichtbar im Auto liegen, wenn Sie das Auto verlassen.

In der Öffentlichkeit sowie in öffentlichen Verkehrsmitteln:

- Bitte stellen Sie sicher, dass unbefugte Dritte keine Einsicht in Dokumente mit personenbezogenen Daten haben. Beim Arbeiten am Laptop oder Smartphone ist darauf zu achten, dass der Bildschirm von Unbefugten nicht einsehbar ist. Achtung: Sitzt eine Person unmittelbar hinter Ihnen (z.B. im Zug), kann es sein, dass dieser trotz Sichtschutzfolie den Bildschirm erkennen kann.
- Sofern Sie telefonieren müssen, wahren Sie Diskretion und beachten Sie die Anweisungen unter „Datenschutz in Telefongesprächen“.

WLAN-Nutzung:

- Von der Nutzung öffentlichen WLANs wird abgeraten, da dieses häufig keine sichere Verbindung herstellt.

Dieses Dokument ist ausschließlich für eigene Zwecke zu nutzen. Eine kommerzielle Verwendung ist ausgeschlossen.
Bitte beachten Sie, dass dieses Dokument nicht als abschließend zu betrachten ist und auf das jeweilige Bedürfnis/Unternehmen anzupassen ist.
© www.ds-quadrat.de

7. Datenschutz im Homeoffice

Bei der Homeoffice-Arbeit ist hinsichtlich des Datenschutzes folgendes zu beachten:

- Das Homeoffice wird in einem eigenen, abschließbaren Raum eingerichtet, sodass keine weiteren Personen (weder Familienmitglieder, Mitbewohner, noch andere unbefugte Dritte) den Bildschirm sehen oder auf die Daten zugreifen können. Achten Sie bitte auch darauf, dass von außen (z.B. durch ein Fenster) keine personenbezogenen Daten eingesehen werden können.
- Der private Internet-Anschluss darf nur über Kabel oder das verschlüsselte WLAN (und Einwahl nur mit sicherem Passwort) genutzt werden.
- Beim Verlassen des Arbeitsplatzes ist der Bildschirm zu sperren (Windows-Taste + L gleichzeitig drücken).
- In das Unternehmens-Netzwerk ist sich über eine sichere Verbindung (VPN) einzuwählen.
- Dienstliche Papierdokumente sind nicht im privaten Papiermüll zu entsorgen, sondern zu sammeln. Die gesammelten Dokumente sind beim nächsten Mal mit ins Büro zu bringen und wie gewohnt datenschutzkonform dort zu entsorgen.

Konkrete Anweisungen bezüglich der Homeoffice-Arbeit entnehmen Sie bitte der aktuell geltenden Homeoffice-Richtlinie.

8. Verhalten bei Datenpannen

Das Wichtigste, was zu tun ist: Etwaigen Schaden von den betroffenen Personen und vom Unternehmen abwenden.

- Wenn Sie einen Datenschutzvorfall erkennen, wenden Sie sich sofort an Ihren Vorgesetzten und an [*die vorgesehene Instanz*].
- Sofern dies in Ihrem Aufgabenbereich liegt:
  - Datenschutzvorfall muss der zuständigen Datenschutzaufsichtsbehörde (sofern ein Risiko für die Rechte und Freiheiten natürlicher Personen führt) und gegebenenfalls den betroffenen Personen (bei hohem Risiko) gemeldet werden.
  - Achtung: Die Meldung an die Aufsichtsbehörde muss innerhalb von 72 Stunden erfolgen.
  - Auch nicht meldepflichtige Vorfälle sind sorgfältig zu dokumentieren und zu analysieren, um die Wiederholungsgefahr zu mindern.

Dieses Dokument ist ausschließlich für eigene Zwecke zu nutzen. Eine kommerzielle Verwendung ist ausgeschlossen.
Bitte beachten Sie, dass dieses Dokument nicht als abschließend zu betrachten ist und auf das jeweilige Bedürfnis/Unternehmen anzupassen ist.
© www.ds-quadrat.de