DATENSCHUTZ NEWSLETTER

DATENSCHUTZBEAUFTRAGTER
STEFAN KRUMBHORN
02606-9619270

MAI 2025

IT- Auditor IDW

CISA Certified Information Systems Auditor. An ISACA® Certification

CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification

KOMMUNIKATION PER E-MAIL

Laut dem Datenschutz- Tätigkeitsbericht 2024 (Hessen) werden die meisten Datenschutzverletzungen durch einen Fehlversand von Daten sowie vom Versand offener E-Mail-Verteilern verursacht (Vgl. BCC).

WAS MÜSSEN SIE BEACHTEN:

1. ***Weiterleiten*** (alter Daten). Vor der Weiterleitung empfiehlt es sich, den Gesprächsinhalt zusammenzufassen, damit der Empfänger schnell versteht, was Sie von ihm wollen. **Wichtig**: Manche E-Mails sind nicht zur Weiterleitung bestimmt, da sie sensible Informationen enthalten. Löschen Sie also vor dem Weiterleiten alte Textpassagen aus der ursprünglichen E-Mail, soweit diese Informationen nichts mehr mit dem aktuellen Thema zu tun haben, oder für den Empfänger nicht relevant sind. Auch bei ***Allen Antworten*** und der Nutzung von ***Verteilerlisten*** gelten die genannten Vorsichtsmaßnahmen. Zusätzlich muss sichergestellt sein, dass alle ausgewählten Empfänger die versendete Information auch erhalten dürfen. Im Zweifelsfall sollten Sie "*einzelnes senden*" verwenden, um zu vermeiden, dass Empfänger nicht genehmigte Informationen erhalten.

2. ***E-Mail-Anhänge*** und Verschlüsselung
E-Mails, die sensible Daten enthalten (z.B. Personaldaten, Unternehmenszahlen uvm.) müssen verschlüsselt werden. Da es aus technischer Sicht jedoch vieler Voraussetzungen bedarf eine komplette E-Mail zu verschlüsseln (beim Sender sowie beim Empfänger) ist es einfacher, sensible Informationen in einer kennwortgeschützten Zip-Datei zusammenzufassen bzw. als kennwortgeschützte PDF- Datei anzuhängen. Alternativ können Sie die Dokumente an einen gemeinsamen, geschützten Speicherort hochladen (Next-Cloud) und dem Empfänger einen Zugriffslink zusenden, über den die Dokumente abgerufen werden. **Wichtig**: Das Zugriffskennwort sollte auf einem anderen Weg als die E-Mail an den Empfänger übermittelt werden.

3. ***BCC*** (Blind Carbon Copy)
Die im BCC-Feld angegebenen E-Mail-Empfänger erscheinen nicht in der Kopfzeile oder bei den Empfängern in den Feldern AN oder CC. Die Verwendung von BCC ist eine wichtige Form, wenn Sie die E-Mail-Adresse einer Person vor der Kenntnisnahme durch andere schützen möchten. Z. B. wenn Sie einen Newsletter an Kunden oder Lieferanten verschicken. Mit ***CC*** hingegen können Sie E-Mails schnell an andere Kollegen zur Kenntnis geben und ihnen gleichzeitig signalisieren, dass sie nicht handeln müssen. E-Mail-Adressen, die als CC aufgeführt sind, erhalten auch Antworten auf Ihre ursprüngliche E-Mail.

RECHTSGRUNDLAGEN

Welche Daten unterliegen dem Datenschutz?
„**P**ersonen**b**ezogene“ **D**aten

Kunden bzw. Mandantennamen, Adresse, Kommunikationsdaten
E-MAIL-ADRESSEN
Geburtsdatum (das Alter), Familienangelegenheiten, Fotos.
Kenn-Nummern: Personalausweis-ID, Steuer-ID, Sozialversicherungsnummer.
Besitzmerkmale: Fahrzeuge, Immobilieneigentum, Grundbucheinträge.
Finanzen: Bank und Kreditdaten, Einkommen, Sozialdaten, Steuerdaten, Kontonummern.

WESENTLICHE SCHUTZKATEGORIEN BEI E-MAILS:

E-Mails mit "**hohem" Risiko**“.

a) Z.B. Lohn und Gehaltsdaten, Gesundheitsdaten oder Daten zur sexualen Identität, auch genetische und biometrische Informationen einer Person.
b) Geschäftsgeheimnisse z.B. Finanzen, Rechnungswesen, Forschung und Entwicklung.

IT- SICHERHEIT ARTIKEL 32 DSGVO

Verschlüsselung,
Pseudonymisierung,
Vertraulichkeit,
Integrität und Authentizität.

Kontakt: Stefan Krumbhorn; T: 02606-9619270 oder service@datenschutz-2k.de