Interview mit einem Datenschutzexperten

Entgeltabrechnung – Dos and Don'ts beim Datenschutz

Wie viel ein Mitarbeitender verdient, welcher Konfession er angehört und wie viele Kinder er hat – Entgeltabrechner arbeiten mit personenbezogenen und damit mit besonders sensiblen Datenkategorien.

Salvatore Piciocchi ist Geschäftsführer des Münchner Lohn- und Buchhaltungsbüros dilohver und gleichzeitig zertifizierter Datenschutzexperte. Als externer Datenschutzbeauftragter weiß er, worauf es beim Schutz etwaiger Informationen in seinem Beruf ankommt, und er ist sich sicher: Digitalisierung wird den Datenschutz enorm verändern – gleichzeitig aber auch extrem vereinfachen.

Foto: Salvatore Piciocchi

Herr Piciocchi, viele Lohnbuchhalter entscheiden sich nach wie vor, die Lohn- und Gehaltsabrechnungen an die jeweiligen Mitarbeiter per Post zu versenden. Ist das aus datenschutzrechtlicher Sicht der sicherste Weg?
Nein, in meinen Augen ist das nicht der sicherste Weg. Zwar hat der Gesetzgeber im Grundgesetz das Postgeheimnis verankert, aber Post kann im Zweifelsfall verloren gehen oder der Empfänger ist umgezogen und die Adresse stimmt schlichtweg nicht mehr. Das sind Risiken, die die Gefahr bergen, dass die Abrechnung am Ende des Tages nicht bei der richtigen Person ankommt.

Übrigens ist auch die Hauspost keine geeignete Alternative. Lohnabrechnungen, die auf dem Schreibtisch des jeweiligen Mitarbeitenden landen, können leicht in falsche Hände geraten, deswegen ist der digitale Versand die bessere Option.

Sprechen wir hier von einer klassischen E-Mail?
Nein, auch eine klassische E-Mail ist datenschutzrechtlich bedenklich. Stellen Sie sich einmal vor, der Versender vertippt sich bei der E-Mail-Adresse und die sensiblen Daten kommen am falschen Ende an. Mag vielleicht nach „blöd gelaufen" klingen, ist aber ein klarer Datenschutzverstoß.

Wenn Unternehmen sich dazu entscheiden, HR-Dokumente per E-Mail zu verschicken, empfehle ich eine Zwei-Faktor-Authentifizierung. Dabei sollten Betriebe über ihren Anbieter zunächst sicherstellen, dass der E-Mail-Verkehr SSL-verschlüsselt ist. Im nächsten Schritt sollten Entgeltabrechner die Lohnabrechnung, die sie versenden, mit einem vom Mitarbeiter gewählten Passwort schützen. Was die Wenigsten wissen: Diese Dokumente müssen digital signiert werden und dürfen nicht nachträglich veränderbar sein, deswegen bietet sich das PDF an.

Übrigens müssen Mitarbeiter in den digitalen Versand einwilligen. Diese Einwilligung ist aber mit Vorsicht zu

genießen. Hier handelt es sich keinesfalls um einen Freifahrtschein in Sachen Datenschutz, aber – und dafür ist das Dokument hilfreich – sollte es zu einem Datenverstoß kommen, können Unternehmen zumindest darlegen, dass sie sensibel mit der Thematik umgegangen sind.

Welche sinnvollen Alternativen beim Versand der Lohndokumente gibt es dann zur Post und zur E-Mail?
Eine entsprechende Cloud-Lösung eines seriösen Anbieters. Ich nutze hierfür beispielsweise das Personal-Portal meines Software-Anbieters: Agenda. Das ist SSL-verschlüsselt und ich kann mir sicher sein, dass die Lohnabrechnungen dem Mitarbeiter konform mit der Datenschutz-Grundverordnung (DS-GVO) bereitgestellt werden.

Und wie funktioniert so eine Cloud-Lösung?
Zunächst stimmt der Mitarbeiter zu, dass er die Cloud-Lösung aktivieren möchte. Als Lohnbüro schalte ich diesen dann im System frei – wir haben also bereits eine Einwilligung. Der Betroffene erhält eine E-Mail, mit der er seine Adresse bestätigt – hier gehen wir sicher, dass die E-Mail-Adresse stimmt. Anschließend bekommt der Mitarbeiter einen Aktivierungscode und kann sich mit einem eigenen Passwort seinen persönlichen Zugang zum Portal einrichten. Damit erreichen wir den bestmöglichen Schutz durch Einwilligung, Bestätigung der korrekten E-Mail und ein eigenes vergebenes Passwort.

Angenommen, ich entscheide mich als Unternehmen für eine Cloud-Lösung. Worauf sollte ich bei der Wahl des Anbieters achten?
Wer sichergehen möchte, dass datenschutzrechtlich hierzulande übliche Standards eingehalten werden, sollte einen deutschen Anbieter wählen. Gleichzeitig sollten Unternehmen zusätzlich darauf achten, wo sich der Server des Dienstleisters befindet, bestenfalls auch in Deutschland.

Unternehmen sollten sich fragen, inwieweit die Datenschutzkompatibilität bei dem jeweiligen Anbieter

Foto: VideoFlow

gegeben ist. Ist dieser beispielsweise ISO-zertifiziert, dann ist das ein Indiz dafür, dass der Partner vertrauensvoll sein kann.

Auch sollten Unternehmen Wert darauf legen, dass, wie bereits erwähnt, die Datenübertragung verschlüsselt und der Datentransfer nachvollziehbar ist. Sprich: Sie sollten einsehen können, wann welche Daten übermittelt worden sind.

Durch die Beauftragung eines Partners erfolgt auch in diesem Fall eine Auftragsdatenverarbeitung gemäß Art. 28 DS-GVO. Mein Softwarepartner Agenda hat den Auftragsdatenverarbeitungsvertrag direkt nach meinem Vertragsabschluss für mich bereitgestellt.

Gibt es als externer Dienstleister Besonderheiten, auf die Sie beim Datenschutz achten müssen?
Ja, auf jeden Fall – wie bereits erwähnt, muss ich natürlich auch einen Auftragsdatenverarbeitungsvertrag, einen AAV, mit meinen Mandanten abschließen. Sonst würde ich mich strafbar machen. Außerdem muss ich mein VVT, das sog. Verzeichnis für Verarbeitungstätigkeiten, aktuell halten und stetig führen. Gleiches gilt für meine TOM – Liste – die technischen und organisatorischen Maßnahmen.

Gemäß DS-GVO muss jedes Unternehmen, das mit besonderen Datenkategorien arbeitet – und das tun wir im Lohn –, einen Datenschutzbeauftragten benennen. Mein Tipp an alle, die sich hier einen externen Datenschutzbeauftragten leisten: Hinterfragen Sie das Angebot. Es besteht hierzulande keine Pflicht, als Datenschutzbeauftragter ausgebildet zu sein. Genau aus diesem Grund lohnt es sich, explizit danach zu fragen, um sicherzugehen, dass der vermeintliche Experte auch wirklich ein Experte auf diesem Gebiet ist. Schließlich ist der Datenschutzbeauftragte der erste Ansprechpartner, falls es Probleme gibt – auch für Behörden.

Wie lange müssen Unternehmen Daten aus der Entgeltabrechnung überhaupt speichern?
Sechs Jahre, um Arbeitsverhältnisse und Betriebsrentenzahlungen nachzuweisen.

Um diese Daten sicher aufzubewahren: Worauf sollte ein Unternehmen bei der Wahl seiner Software das Augenmerk legen?
Programme, die ITSG-zertifiziert sind, sind in der Regel auch DS-GVO-konform und entsprechen den IT-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI).
Nur wer das als Software-Anbieter gewährleistet, kann sich überhaupt ISO-zertifizieren lassen. Folglich sind solche Merkmale aus Datenschutzsicht immer eine gute Orientierung bei der Wahl des entsprechenden Produkts.

Herr Piciocchi, vielen Dank für das Gespräch. ■

Das Interview führte Susanne Hoffmann.