expertenReport

DSGVO: Verschlüsselung von personenbezogenen Daten notwendig

Matthias Stauch, Vorstand der INTERVISTA AG und Experte für digitalen Vertrieb, zur Unzulässigkeit der unverschlüsselten Übersendung von Vertragsdaten nach Einführung der Datenschutz-Grundverordnung:

Matthias Stauch, Vorstandsvorsitzender und Mitbegründer, Intervista AG

Auf Unternehmensseite wirken sich ausbleibende Portokosten für einen Postversand positiv im Ergebnis aus, Auftraggeber dagegen erwarten heute einen schnellen Digitalversand: eine Win-win-Situation. Doch die DSGVO untersagt die Übermittlung solcher Daten ohne Verschlüsselung. Artikel 5 (1), f) legt fest, dass bei der Verarbeitung personenbezogener Informationen Sicherheit gewährleistet sein muss. Dies gilt auch für den Schutz vor unbefugtem und unrechtmäßigem Zugriff sowie Verlust oder der unbeabsichtigten Zerstörung beziehungsweise Schädigung durch geeignete technische Maßnahmen.

Gesetzte Hürden überspringen

Auch Artikel 32 (1) thematisiert nochmals die Verantwortung von Unternehmen – genauer des Verantwortlichen für die Sicherheit der Verarbeitung – ein angemessenes Schutzniveau für die Daten zu garantieren. In den Unterpunkten fordert der Artikel notwendige Maßnahmen wie die Pseudonymisierung und Verschlüsselung personenbezogener Informationen oder die dauerhafte Funktionalität genutzter Systeme und Dienste zur Sicherstellung. Sollten Daten doch einmal verloren gehen, durch einen physischen oder technischen Zwischenfall, müssen diese schnell wiederhergestellt werden können.

Zudem ist es notwendig, alle Maßnahmen und Mittel regelmäßig auf Wirksamkeit zu überprüfen, damit die Sicherheit der Verarbeitung bestehen bleibt. Eine verschlüsselte Übersendung per E-Mail zwischen Mailserver und Client via TLS beziehungsweise SSL kann hierbei als sicherer Übertragungsweg dienen.

Doch: Der Absender kann nie gewährleisten, dass auch der Empfänger mit seinem Mailserver codiert kommuniziert. Nach der DSGVO reicht es also nicht aus, sich auf eine verschlüsselte Aussendung zu verlassen.

Gesicherter Bereich macht’s möglich

Um eine Codierung zu garantieren, bedarf es einer separaten Software, eines Verständnisses zum genauen Ablauf einer Verschlüsselung sowie eines vertrauenswürdigen zentralen Systems – zur Bestätigung der Identitäten von Absender und Empfänger.

Möglichkeiten wie die Sendung via S/MIME bieten zwar eine Ver- und Entschlüsselung ohne, zusätzliche Software in einer Vielzahl von Mailclients. Dies gilt jedoch nicht für alle E-Mail-Programme, beispielsweise ältere Versionen oder Webmail werden nicht unterstützt. Somit werden Compliance-Richtlinien und rechtliche Anforderungen auf diese Weise nicht eingehalten. Kundenbezogene Daten sollten daher nicht per E-Mail oder über einen alternativen Kanal versandt werden.

Ein gesicherter Bereich, der ohne vorhandenes oder erst zu schaffendes Kundenportal funktioniert, sich außerdem in ein bestehendes Anwendungssystem integrieren lässt und Unterlagen wie Verträge, Rechnungen oder Auftragsbestätigungen zugriffssicher zur Verfügung stellt, schafft hier Abhilfe. Eine solche Lösung umfasst den gesamten Cycle vom Versand der Benachrichtigung bis zur Bereitstellung der Kundendokumente. Ebenso lassen sich auf diese Art schlecht zu dokumentierende Lesebestätigungen prozessgesteuert und DSGVO-konform einholen.

Zusätzlich minimiert eine solche Vorgehensweise potenzielle Fraud-Fälle. Es müssen sich also vor allem die Unternehmen mit der passenden Umsetzung der neuen Vorgaben um die Gewährleistung der sicheren Datenverarbeitung kümmern.“

Bilder: (1) © zimmytws / fotolia.com (2) © Intervista AG

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4945186/dsgvo-verschluesselung-von-personenbezogenen-daten-notwendig/