

## Datenschutz bei Begrüßungsmails für neue Kunden

**Zusammenfassung:** Senden Unternehmen ihren neuen Kunden, die sich online registriert haben, eine Bestätigungsmail zu und diese enthält Name, Anschrift, Kundenkennwort und Bankverbindung in unverschlüsselter Form, so liegt ein Verstoß gegen die Weitergabekontrolle gemäß der Anlage zu § 9 Satz 2 Ziffer 4 vor.

**Der Praxisfall:** Ein Unternehmen betreibt einen Online-Shop. Dort können sich neue Kunden über eine per https geschützte Seite registrieren. Dabei geben sie Namen, Adresse, E-Mailadresse, Kundenkennwort und die Kontoverbindung oder eine Kreditkarte ein. Nach Abschluss des Bestellvorgangs erhält der neue Kunde eine Begrüßungsmail, in der die genannten Daten aufgeführt sind. Der neue Kunde hat so die Möglichkeit noch einmal zu überprüfen ob seine personenbezogenen Daten korrekt registriert wurden. Die Begrüßungsmail ist nicht verschlüsselt.

**Berechtigtes Anliegen:** Das Unternehmen hat ein berechtigtes betriebliches Interesse an korrekten Kundendaten, daher kann das Anliegen, die genannten Daten dem neuen Kunden zur Prüfung zuzusenden, als gerechtfertigtes betriebliches Interesse im Sinne des § 28 Abs. 1 BDSG angesehen werden.

**Rechtslage:** Bei der Übermittlung von personenbezogenen Daten in elektronischer Form sind die technischen und organisatorischen Maßnahmen aus der Anlage zu § 9 BDSG zu beachten. Hier gilt insbesondere die Weitergabekontrolle. Demzufolge hat die zuständige Stelle „zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“.

**Risiko:** Da eine unverschlüsselte Mail diesen Anforderungen nicht entspricht, droht eine Intervention der zuständigen Aufsichtsbehörde, die in ein Ordnungswidrigkeitenverfahren einmünden und mit einem Bußgeldbescheid enden kann.

**Bewertung:** Die im vorliegenden Fall übermittelten Daten müssen gemäß dem Schutzstufenkonzept bewertet werden. Zumindest beim Kennwort und den Kontendaten handelt es sich um besonders schützenswerte personenbezogene Daten (Schutzstufe D), weil dem Betroffenen bei unrechtmäßiger Kenntnis durch unbefugte Dritte im Rahmen der automatisierten Verarbeitung (Übermittlung) besondere Risiken für seine Rechte und Freiheiten drohen.

**Alternative:** Es ist zu prüfen, ob eine Pseudonymisierung der personenbezogenen Daten diese erheblichen Risiken verringern kann. So könnte beispielsweise die Kontonummer teilweise unkenntlich gemacht werden. Soll jedoch die Kontonummer insgesamt vom Kunden überprüft werden, bleibt nur der Postversand oder die Verschlüsselung der entsprechenden Mail unter Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

**Aufgabe des Datenschutzbeauftragten:** Datenschutzbeauftragte sollten prüfen, ob das geschilderte Verfahren in ihrem Unternehmen vorkommt. Ist das der Fall, so ist zu prüfen, ob das Verfahren in der Verfahrensübersicht, die ihm gemäß § 4g Abs. 2 zu übergeben ist, enthalten ist. Wenn nicht, ist die Verfahrensübersicht entsprechend zu ergänzen. Im Rahmen der Verfahrensbeschreibungen ist auch eine Verfahrensbeschreibung anzufertigen. Hier ist die Vertraulichkeit der Übermittlung als besondere Maßnahme mit aufzunehmen.

**Hinweis im Bericht der BFDI:** Auf diesen Sachverhalt hat im Übrigen die BFDI, Frau Andrea Voßhoff, im 25. Tätigkeitsbericht verwiesen (25. Tätigkeitsbericht BFDI vom 17. Juni 2015 S.157).

Eberhard Häcker, Ens Dorf