Verschlüsselung unter der DSGVO

Einleitung

Unter Verschlüsselung versteht man die Umwandlung eines Klartextes durch einen Schlüssel in einen Geheimtext, sodass die Ausgangsinformationen nur unter Verwendung des passenden Schlüssels wieder lesbar werden. Durch Verschlüsselungen kann die Vertraulichkeit, Integrität und Authentizität von Daten sichergestellt werden. Anknüpfungspunkt für die Pflicht zur Verschlüsselung bestimmter Informationen im Datenschutzrecht ist insbesondere Art. 32 DGSVO. Gemäß Art. 32 DSGVO müssen die für die Verarbeitung Verantwortlichen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Schwere des Risikos für die Rechte der Betroffenen geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. In Art. 32 Abs. 1 lit. a) DSGVO wird die Verschlüsselung personenbezgoener Daten ausdrücklich als eine der möglichen Schutzmaßnahmen benannt.

In Unternehmen können diverse Formen von Verschlüsselungen eingesetzt werden. Nachfolgend werden einige Fragen zur Verschlüsselung in Unternehmen erörtert.

Ist eine Festplattenverschlüsselung empfehlenswert?

Festplattenverschlüsselungen sind insbesondere für Mobilgeräte wie Handys, Tablets und Laptops empfehlenswert. Grund hierfür ist der durch die Verschlüsselung verbesserte Schutz der Daten in Fällen von Diebstahl oder bei einem Verlust des Endgeräts. Geraten die Geräte in die Hände unberechtigter Dritter, können diese bei ausreichender Verschlüsselung wenigstens nicht ohne Weiteres auf die darauf gespeicherten Daten zugreifen.

Für Unternehmen hat die Verschlüsselung von Festplatten noch einen weiteren Vorteil: Eine geeignete Verschlüsselung kann Unternehmen von der Pflicht zur Benachrichtung der Betroffenen bei Datenschutzvorfällen befreien, wie sich aus Art. 34 Abs. 3 lit. a) DSGVO ergibt. Hintergrund ist auch hier, dass Täter etwa in Fällen von geklauten Firmenlaptops zwar die Hardware in ihrem Besitz haben, aber aufgrund der Verschlüsselung die Vertraulichkeit der auf den Festplatten gespeicherten Daten sichergestellt ist. Soweit daraus keine Gefahren für die Rechte der betroffenen Personen drohen, muss auch keine Meldung an die Betroffenen gemäß Art. 34 DSGVO ergehen. Regelmäßig, aber nicht immer, entfällt in diesen Fällen auch die Meldepflicht gegenüber den Datenschutz-Aufsichtsbehörden.

Müssen E-Mails zwingend verschlüsselt werden?

Eine zwingende Vorgabe zur Nutzung von Verschlüsselungstechnologien beim Versand von E-Mails gibt es in der DSGVO nicht. Dies würde auch gegen die Systematik der DSGVO verstoßen, wonach immer abhängig von den eigenen Möglichkeiten angemessene Maßnahmen zum Schutz der Betroffenen ergriffen werden müssen. Insoweit ist die Verschlüsselung also zunächst eine von vielen möglichen technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes.

Unternehmen sollten aber darauf achten, dass bei einer Entscheidung gegen eine E-Mail-Verschlüsselung andere technische und organisatorische Schutzmaßnahmen getroffen werden müssen, z. B. indem die Dateien im Anhang einer E-Mail zuvor verschlüsselt werden.

Welche Auffassung vertreten die Datenschutz-Aufsichtsbehörden zum Thema Verschlüsselung?

Nach Ansicht der Datenschutzaufsichtsbehörde Nordrhein-Westfalen muss hinsichtlich E-Mails zwischen einer Verschlüsselung auf Inhalts- und einer Verschlüsselung auf Transportebene unterschieden werden. Für die Verschlüsselung auf Inhaltsebene, also die Verschlüsselung des Texts einer E-Mail, kommen in erster Linie die Standards S/MIME und OpenPGP in Betracht. Bei der Verschlüsselung auf Tranportebene, die von namhaften Providern standardmäßig angeboten wird, müssen die Vorgaben der Technischen Richtilnie „BSI TR-03108 Sicherer E-Mail-Transport“ erfüllt werden. Soweit besonders schützenswerte Daten, z. B. Gesundheitsdaten oder Daten, die einem Berufsgeheimnis unterliegen, übersandt werden, kann nach Auffassung der Behörde zudem eine Ende-zu-Ende-Verschlüsselung geboten sein.

Die Bayerische Aufsichtsbehörde unterscheidet ebenso zwischen einer Transport- und einer Inhaltsverschlüsselung. Als Inhaltsverschlüsselung komme insbesondere ein PDF mit Passphrase oder eine passwortverschüsselte ZIP-Datei in Betracht.

Hinsichtlich der Verschlüsselung von Festplatten stehen die Datenschutzbehörden soweit erkennbar auf dem oben beschriebenen Standpunkt, dass eine Festplattenverschüsselung eine Pflicht zur Benachrichtigung der von einem Datenschutzvorfall betroffenen Personen entfallen lassen kann.

Welche weiteren Verschlüsselungen können in Betracht kommen?

Auf Homepages kommt heute meist eine SSL- oder TLS-Verschlüsselung zur Anwendung, die eine verschlüsselte Kommunikation und Authenfikation zwischen Homepageanbieter und Nutzerbrowser ermöglicht. Es ist herrschende Meinung, dass die Einholung von Nutzerinformationen, z. B. über Kontaktformulare, nur unter Verwendung einer solchen Verschlüsselung zulässig ist.

Soweit öffentliche WLAN-Netzwerke genutzt werden, kann eine Verschlüsselung mittels eines Virtual Private Networks (VPN) aufgebaut werden. Auch Voice-over-IP-Kommunikation kann abgesichert werden, indem z. B. auf eine SRTP-Verschlüsselung zurückgegriffen wird.

Fazit und Ausblick

Unternehmen sollten regelmäßig überprüfen, ob Verschlüsselungen zu einer Verbesserung des Datenschutzniveaus führen und vor allem auch mit angemessenem Aufwand umgesetzt werden können. Die Verschlüsselung ist aber immer nur eine von vielen möglichen Schutzmaßnahmen zur Einhaltung des Datenschutzes und hat insoweit im Datenschutzrecht keine Sonderstellung. Letztlich kommt es immer darauf an, ob die Summe aller getroffenen Schutzmaßnahmen zu einem angemessenen Schutzniveau führt. Hierbei ist aber auch zu berücksichtigen, dass sich die Anforderungen an den „Stand der Technik“ stetig wandeln. So können Maßnahmen, die noch vor ein oder zwei Jahren als überobligarotisch galten, innerhalb kurzer Zeit dem Branchenstandard entsprechen.

Im Hinblick auf die vielfältigen Einsatzbereiche von Verschlüsselungstechnologien und unter Beachtung der überschaubaren Etablierungskosten ist es insgesamt verständlich, dass viele Unternehmen auf Verschlüsselungen zurückgreifen, um personenbezogene Daten zu schützen. Dass Verschlüsselungen unter Umständen auch von der Pflicht zur Meldung gegenüber Betroffenen bei Datenschutzverstößen befreien, ist dann ein zusätzlicher Vorteil.

Robert Bommel, LL.M.

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Robert Bommel, LL.M.
Wissenschaftlicher Mitarbeiter
T +49 521 96535 - 890
F +49 521 96535 - 114
M robert.bommel@brandi.net
www.brandi.net