Praxistipp zur DSGVO: Sind E-Mail-Systeme nach dem 25.05. noch einsetzbar?

Oder widersprechen sie der Datenschutz-Grundverordnung, da sie nicht sicher sind?

Gilt dieses Tool nach Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) als sicher und darf daher weiter-verwendet werden? Was tun, wenn nicht?

In den letzten Wochen kam es verstärkt zu Diskussionen, die sich mit einem „liebgewonnenen Instrument" der täglichen Praxis, nämlich dem E-Mail-Versand, beschäftigten. Etwa:

- Darf man Kunden Angebote per Mail senden?
- Darf man Kopien von Abschlüssen betroffenen Kunden per Mail senden?
- Darf man Anträge an Versicherungen per Mail weitersenden? Etc.

Diese Frage ist in Fachkreisen noch nicht endgültig geklärt, man wird also auf eine entsprechende Information der Datenschutzbehörde (DSB) warten müssen. **Eine Anfrage bei der Behörde** hat leider **keinen Hinweis dazu ergeben,** wie die DSB das ab 26.5. beurteilen wird:

„… es wird um Verständnis dafür ersucht, dass die Datenschutzbehörde im Rahmen einer telefonischen oder schriftlichen Anfrage keine individuellen rechtlichen Beratungsleistungen erbringen kann. Die Datenschutzbehörde ist vorrangig keine Rechtsberatungseinrichtung sondern eine Aufsichts- und Rechtsschutzbehörde. Die Auskunftspflicht von Behörden umfasst nach der Rechtsprechung insbesondere nicht die Pflicht, Rechtsgutachten (etwa zur Frage einer Auslegung von Art. 32 DSGVO) zu erstatten."

Da es also **bis zum 26.5. keine klare Antwort der Behörde** zu dieser Frage geben wird, wollen wir Ihnen – nach einer kurzen Einleitung – **sichere Wege aufzeigen**, wie Sie auch künftig das Instrument E-Mail verwenden dürfen und die Unsicherheit bzw. Lücken, die sich aufgrund der Nutzung dieses Kommunikationsweges ergeben, ausschalten können.

Grundsätzlich sagen zahlreiche Datenschutz-Experten, dass das Nutzen von E-Mail-Systemen nicht Bestandteil der DSGVO ist. Das E-Mail-System ist ein Betriebsmittel wie viele andere.

ABER: **§ 54 des österreichischen Datenschutz-Anpassungsgesetzes 2018 verlangt** als Datensicherheitsmaßnahmen in Punkt 8:

8) Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle);

Und genau **diese Vorgabe können Sie mit Ihrem E-Mail-System nicht garantieren.** Denn es handelt sich hierbei um **keine sichere Kommunikationsart** und das Mitgesandte ist nicht wie in einem Brief verschlossen. Im Gegenteil! Beim Versenden einer E-Mail wird die Nachricht nicht direkt von A nach B gesandt, sondern wandert durch das Internet über viele Server. Und dort kann man – ohne besondere technische Fähigkeiten aufweisen zu müssen – den Inhalt mitlesen, so wie der Postzusteller früher jede Postkarte lesen konnte.

Verwenden Sie also ein **E-Mail-Programm wie bisher, kommen Sie in Konflikt** mit der DSGVO. Denn künftig müssen Sie für die Sicherheit der bei Ihnen gespeicherten Kunden-/Mitarbeiter- und sonstigen Daten garantieren, wenn diese unter die DSGVO fallen.

Stellen Sie sich die **berechtigte Aufregung** vor, wenn Sie einer Kundin/einem Kunden per E-Mail ein Anbot senden und darin in etwa formulieren:

„Ich bedaure, dass bei Ihnen **Krebs diagnostiziert** wurde. Ich habe Ihnen daher einige Angebote zusammengestellt, damit Sie Ihre Familie absichern können…."

Wird diese Nachricht via E-Mail-Server mitgelesen, können Sie nicht behaupten, dass Sie die personenbezogenen Daten wirklich geschützt hätten.

Was also künftig tun?

a) **E-Mails verschlüsseln.**
Das wäre die **perfekte Lösung** für eine sichere Übertragung via E-Mail.
Eine mögliche Software wäre **PGP4win** (PGP steht für pretty good privacy, also frei auf Deutsch übersetzt „wirklich guter Datenschutz"). Und außerdem brauchen Sie noch eine PGP-Erweiterung für Ihr Outlook.

Hier finden Sie eine **übersichtliche Anleitung**.

Trotz komplizierter Technik im Hintergrund ist das **Prinzip einfach.** Sie installieren diese Software bei sich. Und geben JEDEM, der seine Mails an Sie verschlüsseln möchte, IHREN eigenen Schlüssel ÖFFENTLICH bekannt. Mit diesem Schlüssel kann Ihr Partner seine Mails an Sie verschlüsseln und Sie können diese – als Einziger – entschlüsseln und lesen.

Problem: Kaum Nutzerinnen und Nutzer!
Der Grund, warum das aber niemand tut, ist der, dass das nur dann funktioniert, wenn viele/alle ihre Mails verschlüsseln. Da das Verschlüsseln nicht verbreitet ist, macht es keinen Sinn, wenn Sie verschlüsseln möchten, aber niemand anderen tut das, wodurch Sie keinen Schlüssel von den anderen zum Verschlüsseln erhalten … Damit beißt sich die Katze in den Schwanz. Weil das Verschlüsseln komplett unüblich ist, gibt es kaum Anwender. Das wird sich vielleicht durch die DSGVO ändern, aber kein Massenphänomen werden …

Auf jeden Fall **empfehlen Expertinnen und Experten,** dieses Service zur Verfügung zu stellen und damit zu beweisen, dass man alles versucht hat, einen sicheren Übertragungsweg anzubieten (auch wenn das kaum genutzt wird).

b) **Unterlagen zum Download anbieten**
Was immer Sie per Mail versenden wollten, stellen Sie auf einer **Passwort-geschützten Unterseite Ihrer Homepage zur Verfügung** (Mitglieder-, Mitarbeiter-, Partner-Bereich etc.) und senden dem Empfänger einen **Link zu der Stelle, wo er sich einloggen soll** (sofern noch nicht bekannt).
Benutzername und Passwort dürfen aber nicht in den Link eingebettet werden (wäre für den Nutzer bequem, doch dann könnte erst wieder jeder, der die Mail liest, auch auf den geschützten Bereich zugreifen) und auch nicht via E-Mail gesendet werden.
Wie beim E-Banking müssen Sie die Zugangsdaten auf einem zweiten Wege übermitteln (SMS, Anruf). Das erhöht die Sicherheit.

c) **Anhänge zippen und ein Passwort vergeben.**
Manchmal sind die einfachsten Lösungen die besten.
Früher waren Zipp-Programme üblich, weil Platz auf Festplatten beschränkt bzw. die Internetverbindung zu langsam war. Damals wären E-Mails mit 10 MB großen Anhängen undenkbar gewesen. Also zippte, d.h. verkleinerte, man die Dateien.
Diese Methode könnte nun ein Comeback feiern, da man mit diesem Verfahren das Dokument auch mit einem Passwort schützen kann.

Damit wäre also das Anbot praktisch verschlüsselt unterwegs.
Sie müssten dann allerdings Ihre Kundin/Ihren Kunden anrufen – Motto: Haben Sie mein Anbot erhalten? – und ihr/ihm **telefonisch das Passwort mitteilen**. Oder Sie senden ihr/ihm – wie vom Online-Banking bekannt – das Passwort **als SMS** und nutzen damit die Sicherheit der 2-Wege-Authentifizierung.
Der Arbeitsaufwand dafür scheint doch erheblich, dafür ist dieses Vorgehen kostenlos und trotzdem sicher.

d) **Eher „Hände weg" von Tunnel-Software – sogenanntes VPN (virtual private network)**
Hier gibt es Anbieter, die für wenige Euro im Monat versprechen, dass Ihre E-Mails auf geschützte und anonyme Weise versendet werden. So als ob man für Sie einen Tunnel durch das Internet graben würde. VPN ist der technische Begriff dazu, das steht für virtual private network, also virtuelles privates Netzwerk.

Wie so eine Tunnelsoftware funktioniert, können Sie sich in diesem Video ansehen.

Ob die kostenlosen VPN-Angebote etwa von Avira, Kaspersky & Co **wirklich die Übertragung schützen, ist schwierig zu beurteilen.** Ganz sicher verschleiern sie den Absender, in dem sie die Mail anonymisieren.

EDV- und Datenschutz-Experten wie Mag. Georg Markus Kainz halten nur die unter a) und b) genannten Varianten für topsicher und empfehlenswert. Variante c) ist auch sicher, aber mühsam.

Einschub: Technischer **Tipp zu VPN:** (der zwar nichts mit E-Mail-Versand zu tun hat, für Ihr Unternehmen aber weitere riskante Zugriffe vermeiden hilft):

Firewall erlaubt nur VPN-Zugriffe:
Firmennetzwerke sind den täglichen Angriffen aus dem Internet ausgeliefert. Gleichzeitig erlaubt man es den Mitarbeitern (aus Bequemlichkeit) von überall aus, auf personenbezogene, eventuell sogar sensible Kundendaten zuzugreifen.

Um die Sicherheit enorm zu erhöhen, sollte man die Firewall so einstellen, dass – wenn Personen von außen auf Firmendaten zugreifen (via Handy, iPad, Laptop, Heim-PC) – Zugriffe nur dann erlaubt werden, wenn über eine VPN-Verbindung gearbeitet wird.

D.h.: Verwende ich das kostenlose WLAN eines Restaurants, der Abflugshalle usw., darf mich der Firmenserver nicht reinlassen.
Diese **gesicherten VPN-Zugänge** nutzt man dann gleich auch, um eine Datensicherung außer Haus auf einen Server, in einer Cloud abzulegen.
Dies ist im Rahmen der Risikoanalyse zu klären bzw. sicherzustellen.

Für welche Variante man sich entscheidet, hängt wohl von den individuellen Vorlieben ebenso ab, wie von den Wünschen/Vorgaben der Kunden und Partner.
Wer bisher ein E-Mail-Programm und die zahlreichen Vorteile davon intensiv genutzt hat, wird dieses wohl auch künftig nutzen wollen. Aber muss danach trachten, die **Datenübertragung sicher zu gestalten, um die Strafandrohungen der DSGVO zu verhindern.**

Recherche-Quellen: Mag. Georg Markus Kainz, Quintessenz und RA Mag. Stephan Novotny (Spezialgebiet Versicherungen & Datenschutz-Grundverordnung)