Newsletter Datenschutz

Ausgabe 06 | 2024

Was ist ein „Mitarbeiter-Exzess“?

Ihr Datenschutz-Info Blatt

Liebe Leserin, lieber Leser,

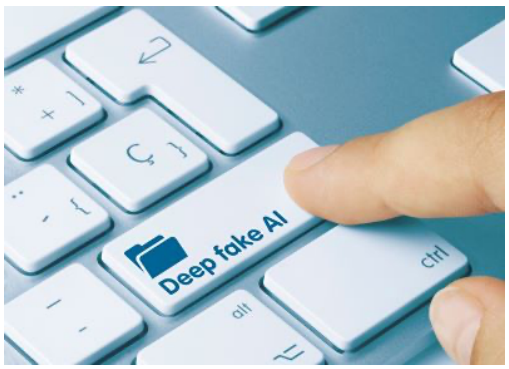
oftmals muss man für neue Erkenntnisse den Blick weiten. Das gilt auch im Datenschutz. So wird zum Beispiel viel über die Übermittlung personenbezogener Daten in die USA gesprochen, doch was ist eigentlich, wenn man personenbezogene Daten in Länder wie Andorra oder Uruguay übertragen will?

In Ihrer neuen Ausgabe finden Sie darauf die Antwort, denn ein Beitrag behandelt Fragen zu Angemessenheitsbeschlüssen für Drittstaaten. Doch es gibt weitere Themen, bei denen man die Augen weit öffnen sollte. So könnte es bald passieren, dass Sie in einem Online-Meeting mit einer gefälschten Identität sprechen, Stimme und Aussehen wurden manipuliert. Lesen Sie deshalb am besten gleich jetzt, wie Sie solche sogenannten Deepfakes erkennen können.

Neue Sichten erhalten Sie auch zu dem guten, alten Fax-Gerät und zu den virtuellen Fax-Geräten, den sogenannten Fax-Servern. Nicht zuletzt erfahren Sie auch, was man unter „Mitarbeiterexzess“ versteht.
Es gibt viel Neues zu entdecken im Datenschutz, halten Sie die Augen offen!

Ihr Frank Berns, Datenschutzbeauftragter

Vorsicht Deepfakes: Der Spion im Online-Meeting



Cyberkriminelle könnten Künstliche Intelligenz (KI) nutzen, um in Online-Konferenzen das Aussehen und die Stimme scheinbar vertrauter Personen vorzutäuschen. Die Fälschungen sind bereits extrem gut und nur schwer zu erkennen.

Den Wolf im Schafspelz gibt es nicht nur im Märchen

Wenn vertrauliche Gespräche im Internet belauscht wurden, muss kein klassischer Hackerangriff oder eine fehlende Verschlüsselung dahinterstecken. Es kann auch sein, dass der Spion unerkannt an dem

KONTAKT zu uns MAIL@Konzept17.de

Gespräch teilgenommen hat. Doch wie kann das sein, wenn doch nur vertraute Gesichter zu sehen und bekannte Stimmen zu hören waren?

Möglich macht dies KI (Künstliche Intelligenz) in Händen von Internetkriminellen. Dank KI ist es inzwischen möglich, nicht nur einzelne Bilder zu fälschen, sondern sogar Videos und Tonaufnahmen. Dies können auch Live-Videos und Live-Gespräche sein, denn die kriminell genutzte KI verwandelt das Videobild und den Ton des Spions in Aussehen und Stimme einer anderen Person, die an dem vertraulichen Online-Meeting hätte teilnehmen dürfen.

Nicht nur eine E-Mail kann im falschen Namen verschickt werden, auch Telefonate und Online-Meetings können mit gefälschter Identität geführt werden. Online-Betrug bekommt so ein ganz neues Gesicht.

Identitätsdiebstahl live und in Farbe

Der neuartige Diebstahl einer Identität wird Deepfake genannt, täuschend echt wirkende, manipulierte Bild-, Audio- oder auch Videoaufnahmen, mit Hilfe von Künstlicher Intelligenz erzeugt.

Lange Zeit war es sehr aufwändig, dynamische Medien, wie Videos oder Audiomitschnitte qualitativ hochwertig zu manipulieren, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) erklärt. Durch Methoden aus dem Bereich der Künstlichen Intelligenz (KI), durch Nutzung von tiefen neuronalen Netzen (englisch: deep neural networks) ist dies heute jedoch deutlich einfacher. Der Aufwand für Deepfakes ist für die Kriminellen entsprechend gering.

Die zunehmende Echtzeitfähigkeit der Deepfakes bewirkt, dass man in Online-Meetings womöglich nicht mehr sicher sein kann, ob man mit der realen Person, einem Angreifer oder sogar einem Avatar, also einer künstlichen Person, spricht.

So lassen sich Deepfakes am besten erkennen

Auch wenn KI-Verfahren die gefälschten Videos und Stimmen inzwischen in sehr hoher Qualität erzeugen können, gibt es gewisse Schwächen in den Deepfakes, die sich nutzen lassen, um Hinweise auf mögliche Fälschungen zu finden. Das Bundesamt für Verfassungsschutz (BfV) empfiehlt:

- Sorgen Sie für gute (Bild-)Qualität: Je höher die Auflösung beziehungsweise die Bildgröße, desto leichter lassen sich Ungereimtheiten im Bild erkennen. Videos sollten daher nicht auf dem Handy, sondern auf einem größeren Monitor geschaut werden. Gute Farbeinstellungen zeigen ebenfalls Unstimmigkeiten, zum Beispiel im Hautbild.
- Achten Sie auf die Mimik der Person: Natürliche Reaktionen, wie Blinzeln, Stirnrunzeln oder die berühmte „Zornesader“ können von einer KI ebenfalls noch nicht gut dargestellt werden. Ein genauer Blick auf die Augen und Stirn kann eine Fälschung enttarnen. Schauen Sie dafür das Bild verlangsamt, um eventuelle Verzerrungen zu erkennen.
- Prüfen Sie die Quelle: Letztlich hilft natürlich auch immer eine Quellenprüfung oder bei Unsicherheit in Videoschalten die Bitte um Rückruf, um zumindest die Gelegenheit zu bekommen, den Videoanruf oder das Video zu verifizieren.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist ebenfalls auf Anzeichen für eine Gesichtsmanipulation hin und nennt sichtbare Artefakte an der Naht rund um das Gesicht im Videobild, verwaschene Konturen bei Zähnen und Augen, eine begrenzte Mimik und eine unstimmige Beleuchtung als Warnzeichen.

Leider lernen kriminelle KI-Verfahren und die Cyberkriminellen schnell, Deepfakes werden also immer besser. Umso wichtiger ist es, vorsichtig zu sein und nicht allem einfach Glauben zu schenken, was man scheinbar sieht. Deshalb „Augen auf" bei der nächsten Online-Konferenz!

Was ist ein „Mitarbeiter-Exzess"?

Riskiere ich eine persönliche Geldbuße durch die Datenschutzaufsicht, wenn ich an meinem Arbeitsplatz gegen den Datenschutz verstoße? Die Antwort lautet: Nur wenn Ihnen ein „Mitarbeiter-Exzess" vorzuwerfen ist. Was ist damit gemeint? Und wie vermeide ich so etwas?

Beschäftigte haben bestimmte Vorgaben einzuhalten

Beschäftigte müssen sich an die Vorgaben ihres Arbeitgebers halten. So sind die Spielregeln bei einem Arbeitsverhältnis. Dass sie eingehalten werden, hat auch für den Datenschutz große Bedeutung. Denn wegen ihrer Verantwortung für den Datenschutz muss die Unternehmensleitung zu jedem Zeitpunkt sicherstellen, dass die Vorgaben des Datenschutzes beachtet werden.

Nur Beschäftigte können den Datenschutz „vor Ort" umsetzen

Papier ist bekanntlich geduldig. Der wesentliche Kern, der hinter diesem Sprichwort steckt, gilt auch im „papierlosen Büro": Auch kluge und richtige Vorgaben bewirken nur dann etwas, wenn sie tatsächlich beachtet werden. Das gilt besonders bei der Verarbeitung von Daten. Dabei kommt es auf alle Beschäftigten an. Sie – und nicht die Unternehmensleitung - haben die Daten von Kunden, Lieferanten und Kollegen unmittelbar in ihren Händen.

Die Unternehmensleitung ist im Alltag weit weg

Natürlich ist eine Unternehmensleitung verpflichtet, die Einhaltung von Vorgaben durch Stichproben zu überprüfen. Im Alltag muss und kann sie sich jedoch darauf verlassen, dass ihre Beschäftigten korrekt handeln. Natürlich kommen auch einmal Fehler vor. Im Ernstfall muss die Leitungsebene die Dinge dann nach außen „glattziehen". Im Alltag darf sie jedoch auf ihre Beschäftigten vertrauen.

Manchmal laufen Beschäftigte aus dem Ruder

Es kann allerdings vorkommen, dass sich ein Beschäftigter nicht an die Vorgaben hält. Das wäre etwa der Fall, wenn er auf eigene Initiative unrechtmäßig die Daten von Kunden oder anderen Beschäftigten abfragt. Dieses Beispiel stammt aus einem Verfahren vor dem Europäischen Gerichtshof (EuGH). Wer Daten von Kunden ohne betrieblichen Anlass am Arbeitsplatz aufruft, verstößt bewusst gegen Vorgaben des Arbeitgebers.

Es gibt typische Beispiele für Fehlverhalten von Beschäftigten

Bei Beschäftigten mit Kontakt zu Endkunden kommt es immer wieder zum Missbrauch von Kommunikationsdaten. Beispiel: Ein Kundenberater nutzt Daten einer Kundin, um sie aus privaten Motiven zu kontaktieren. Auch bei einem Wechsel der Stelle geraten manche in Versuchung. Beispiel: Jemand nimmt aus eigener Initiative Kundendaten zu seinem neuen Arbeitgeber mit, um sie dort mit „guten Kontakten" in ein günstiges Licht zu setzen.

Vorsätzliche Regelverstöße sind als „Exzess“ zu werten

Für solche bewussten Verstöße von Beschäftigten gegen Vorgaben des Datenschutzes hat sich die Bezeichnung „Mitarbeiter-Exzess“ eingebürgert. Sie wirkt drastisch, bringt aber gut zum Ausdruck, um was es geht. Ein Exzess ist eine Verhaltensweise, die Regeln bewusst ignoriert. Verantwortung dafür trifft einen selbst, nicht den Arbeitgeber.

Ein solcher Exzess verlagert die Verantwortung

Verantwortlicher im Sinne des Datenschutzrechts ist nicht ein einzelner Beschäftigter, sondern das Unternehmen, für das er tätig ist. Dies gilt allerdings nur unter einer wichtigen Voraussetzung: Beschäftigte müssen die personenbezogenen Daten unter der Aufsicht des Verantwortlichen (also des Unternehmens) und im Einklang mit seinen Weisungen verarbeiten. Dies heißt umgekehrt: Wenn Beschäftigte bewusst gegen Weisungen verstoßen, werden sie selbst zum Verantwortlichen im Sinn des Datenschutzrechts. Ihr Arbeitgeber ist ab diesem Punkt „außen vor“.

Die Verantwortung tragen Beschäftigte dann selbst

Wer sich selbst zum „Herr der Daten“ macht und dienstliche Daten für private Zwecke verwendet, handelt außerhalb seines Arbeitsverhältnisses. Die Vorgaben des Datenschutzes muss er dann selbst erfüllen. Zu ihnen gehört etwa die ordnungsgemäße Information der betroffenen Personen über die Verarbeitung. Eine Geldbuße für Verstöße gegen den Datenschutz verhängt die Datenschutzaufsicht dann gegen den Beschäftigten persönlich.

Die Verantwortung der Unternehmensleitung endet dagegen

In Unternehmen müssen Mechanismen vorhanden sein, um Verstöße durch Stichproben aufzudecken. Mehr allerdings auch nicht. Alles andere würde auf eine Totalüberwachung am Arbeitsplatz hinauslaufen. Und die ist aus gutem Grund untersagt. Sofern Stichproben stattfinden, liegt ein Missbrauch von Daten für private Zwecke außerhalb der Verantwortung des Unternehmens.

Ein simpler Rat vermeidet Ärger

Für Daten am Arbeitsplatz gilt: Keine Verwendung der Daten für private Zwecke! Wer sich daran hält, erspart sich unnötigen Stress und Ärger.

Angemessenheitsbeschlüsse für Drittstaaten

Datenübermittlungen in Staaten außerhalb der EU, also in „Drittstaaten“ sind rechtlich heikel. Für 15 Staaten, darunter Japan und die Schweiz, bieten Angemessenheitsbeschlüsse der EU-Kommission eine tragfähige Rechtsgrundlage. Sie zu kennen, kann sehr nützlich sein.

Die Ausgangslage ist schwierig

vom Grundsatz her verbietet die DSGVO Übermittlungen an Datenempfänger außerhalb der EU in „Drittstaaten“. Ausnahmen von diesem grundsätzlichen Verbot enthält die DSGVO in ihrem Kapitel V. Es besteht aus sechs größtenteils sehr umfangreichen Artikeln. Am einfachsten wird es, wenn für ein Land ein Angemessenheitsbeschluss der EU-Kommission vorliegt.

Angemessenheitsbeschlüsse vereinfachen das Leben

Art. 45 Abs.1 DSGVO hält dazu folgendes fest „Eine Übermittlung personenbezogener Daten an ein Drittland … darf vorgenommen werden, wenn die (EU-) Kommission beschlossen hat, dass das betreffende Drittland … ein angemessenes Schutzniveau bietet." Dies eröffnet gerade kleinen und mittleren Unternehmen einen gut gangbaren Weg, um personenbezogene Daten in ein Drittland zu übermitteln.

Insgesamt bestehen Beschlüsse für 18 Länder

Die Liste der Länder, für die Angemessenheitsbeschlüsse bestehen, ist inzwischen relativ lang: Andorra, Argentinien, Färöer-Inseln, Guernsey, Isle of Man, Israel, Japan, Jersey, Kanada, Neuseeland, Schweiz, Südkorea, Uruguay, Großbritannien, USA. Vielen ist nur der Angemessenheitsbeschluss für die USA bekannt, der unter dem Stichwort „Privacy Shield" große Beachtung gefunden hat. Darüber wird manchmal vergessen, dass Länder wie etwa Israel, Japan und vor allem die Schweiz zumindest für viele Branchen genauso wichtig sind wie die USA.

Großbritannien verdient einen genaueren Blick

Großbritannien gehört seit dem Brexit nicht mehr zur EU. Es ist ein Drittstaat. Ohne Angemessenheitsbeschluss hätte der Datenaustausch mit Großbritannien nicht im bisherigen Umfang fortgeführt werden können. Die drei Kanalinseln Guernsey, Jersey und Isle of Man, wichtige Standorte für den Finanzbereich, haben innerhalb des Vereinigten Königreichs einen rechtlichen Sonderstatus. Deshalb wurden für sie schon weit vor dem Brexit Angemessenheitsbeschlüsse herbeigeführt.

Angemessenheitsbeschlüsse haben große Vorteile

Wenn für ein Land ein Angemessenheitsbeschluss besteht, braucht eine Datenübermittlung dorthin keine besondere Genehmigung (siehe Art. 45 Abs. 1 Satz 2 DSGVO). Es sind auch keine Zusicherungen des Datenempfängers erforderlich, dass er irgendwelche zusätzlichen Vorgaben einhält. Sofern sich eine Datenübermittlung im Rahmen des jeweiligen Angemessenheitsbeschlusses bewegt, ist sie ohne Wenn und Aber rechtlich zulässig. Daher spricht die EU-Kommission von einer „unkomplizierten und umfassenden Lösung für die Übermittlung von Daten."

Jede Angemessenheitsbeschluss erfordert genaue Lektüre

Wer Daten in ein bestimmtes Land übermitteln will, muss zuvor den Angemessenheitsbeschluss für dieses Land genau lesen. Manchmal finden sich dort nämlich gewisse Einschränkungen. Klassisches Beispiel hierfür ist Kanada. Der Beschluss für dieses Land gilt nur für Datenempfänger in Kanada, die als kommerziell einzustufen sind. Solche Einschränkungen enthalten aber nur wenige Angemessenheitsbeschlüsse.

Manche Angemessenheitsbeschlüsse sind älter als die DSGVO

Viele Angemessenheitsbeschlüsse wurden schon weit vor der DSGVO erlassen. Rechtsgrundlage hierfür war eine Bestimmung in der EG-Datenschutzrichtlinie von 1995. Die DSGVO hält ausdrücklich fest, dass solche „Alt-Beschlüsse" weiterhin gelten (siehe Art. 45 Abs. 9 DSGVO). Sie bleiben so lange in Kraft, bis die EU-Kommission sie ändert, durch einen anderen Beschluss ersetzt, oder sie aufhebt. Die Aufhebung eines solchen Beschlusses ist bisher noch nicht vorgekommen.

Die EU-Kommission sorgt für die Fortentwicklung der Beschlüsse

Zu den „Alt-Beschlüssen" gehören etwa die Angemessenheitsbeschluss für Japan und die Schweiz. Die EU-Kommission bemüht sich intensiv darum, sie dauerhaft „DSGVO-tauglich" zu machen. Dies belegt ein Bericht der EU-Kommission vom 15. Januar 2024, der sich auf 17 Seiten den „Alt-Beschlüssen" widmet. Er ist abrufbar unter https://commission.europa.eu/document/f62d70a4-39e3-4372-9d49-e59dc0fda3df_en.

Ein kurzer Blick erspart viel Arbeit

Es mag sein, dass Sie nie Daten etwa nach Uruguay übermitteln müssen. Falls es aber vorkommt, sollten Sie wissen, dass es für dieses Land einen Angemessenheitsbeschluss gibt. Eine Liste aller Angemessenheitsbeschlüsse finden Sie hier: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Das Datenrisiko FAX hat auch eine digitale Seite!

Datenschutzaufsichtsbehörden warnen nicht nur vor den Risiken durch ungeschützten Mail-Versand, sondern auch vor dem guten, altem Fax-Gerät. Dabei sollten die virtuellen Fax-Geräte nicht vergessen werden.

Viele deutsche Unternehmen faxen noch

Per E-Mail, im Chat oder in der Cloud, mittlerweile gibt es viele digitale Wege, Dokumente zu verschicken. Trotzdem halten die deutschen Unternehmen weiterhin auch an einem Klassiker der analogen Kommunikation fest, dem Faxgerät, so der Digitalverband Bitkom.

Aus Sicht des Datenschutzes ist der Fax-Versand aber nicht unkritisch: Personenbezogene Daten, die einen besonderen Schutzbedarf aufweisen, wie zum Beispiel Diagnosedaten oder Sozialdaten, dürfen grundsätzlich nicht per Fax übertragen werden, wenn keine zusätzlichen Schutzmaßnahmen bei den Versendern und Empfängern implementiert sind, wie der Hessische Beauftragte für Datenschutz und Informationsfreiheit erklärte.

In der Praxis aber findet man auch in sensiblen Bereichen wie Krankenhaus und andere Gesundheitseinrichtungen noch viele Fax-Nachrichten. Auch in anderen Branchen haben Fax-Sendungen noch nicht ausgedient, wie zum Beispiel im Einkauf und im Lager so mancher Handelsunternehmen.

Datenschützer sehen klassisches Fax kritisch

„Ein Ziel der Digitalisierung sollte immer bleiben, unkomplizierte, verlässliche und datenschutzoptimierte Kommunikationsinstrumente bereitzustellen, welche das ‚Faxen' möglichst bald überflüssig machen", so zum Beispiel der Bayerische Landesbeauftragte für den Datenschutz. Doch den Aufsichtsbehörden ist bewusst, warum viele Unternehmen bei aller Digitalisierung noch nicht auf das klassische Fax verzichten wollen: Eine schnelle, schriftliche Kommunikation bleibt im

Grundsatz möglich, auch wenn IT-Systeme des Absenders oder des Empfängers gerade nicht einsatzfähig sind.

Grundsätzlich sollte aber von der Nutzung eines Faxes abgesehen werden. Ungeachtet hiervon kann selbstverständlich in begründeten dringlichen (wie medizinischen Fällen) unter Zugrundelegung der datenschutzrechtlichen Risikoabschätzung die Datenübermittlung per Telefax genutzt werden, wie der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit klarstellte. Der Schutz der Gesundheit und die Sicherung von Leib und Leben der Betroffenen überwiegen hier gegenüber dem Risiko einer potentiellen Verletzung von Rechten und Freiheiten der Betroffenen durch unbefugte Kenntnisnahme der Daten bei der unverschlüsselten Fax-Übermittlung.

Die Lösung kann das „digitale" Fax sein

Die Aufsichtsbehörden haben einen weiteren, wichtigen Hinweis: Es gibt nicht nur klassische, physische Fax-Geräte. Ein Fax-Server ersetzt ein „althergebrachtes" Faxgerät durch eine Software, welche ein echtes Faxgerät simuliert. Damit können über ein analoges Faxgerät gesendete Dokumente als PDF-Datei auf einem PC empfangen werden. Umgekehrt kann von dem betreffenden PC ein PDF-Dokument über die Faxnummer an ein analoges Faxgerät gesendet werden.

Auch das Senden eines „digitalen" Faxes von Fax-Server zu Fax-Server ist möglich. Damit sind die Datenrisiken des Faxes nicht verschwunden, aber es stehen Schutzmöglichkeiten zur Verfügung, die ein Unternehmen bereits für den E-Mail-Versand verfügbar haben müsste. Dazu gehören insbesondere Verschlüsselung, Nutzerauthentifizierung, verschiedene Nutzerrollen, Festplattenverschlüsselung, sicheres Löschen, Netzwerksegmentierung, Virenscanner und Firewalls.

Dann aber wird das Fax wirklich digitalisiert. Für den Bayerischen Landesbeauftragten für den Datenschutz ist klar: Wenn das Versenden verschlüsselter E-Mails so unkompliziert möglich ist wie das Versenden eines Faxes, und wenn in die Stabilität der dafür benötigten IT-Systeme so vertraut werden kann wie in die Verfügbarkeit von Telefax-Diensten, wird das klassische Fax auch das Ende seines Lebenszyklus erreicht haben.

Es zeigt sich: Mit der digitalen Seite des Faxes kommen zunehmend die bereits vorhandenen digitalen Kommunikationsverfahren wie E-Mails zum Zuge, das Fax wird zur Mail mit Anhang. Aber auch dieses „digitale Fax" brauchen den richtigen Schutz. Nicht das Fax ist also das Risiko, sondern das Fehlen von Schutzmaßnahmen.

Kennen Sie die Risiken durch den Fax-Versand? Machen Sie den Test!

Frage: Der Fax-Versand kann nicht abgehört werden, die Inhalte bleiben vertraulich, wenn der Fax-Ausdruck nicht abhandenkommt. Stimmt das?

1. Nein, der Fax-Versand ist unverschlüsselt und kann deshalb durch Dritte abgefangen und belauscht werden.
2. Ja, nur Sender und Empfänger haben Zugang zu den Fax-Inhalten wie bei verschlüsselten E-Mails.

Lösung: Die Antwort 1. ist richtig. Das klassische Fax ist unverschlüsselt. Eine Verschlüsselung ist aber möglich, wenn Fax-Server genutzt und entsprechend abgesichert werden. Dann aber wandelt sich das Fax in Richtung E-Mail mit PDF-Anhang.

Frage: Wenn es eilig ist, kann man auf alle Fälle einen Brief per Fax verschicken. Stimmt das?

1. Ja, in solchen Ausnahmefällen hat der schnelle Versand Vorrang.
2. Nein, man kann nur eine Ausnahme machen, wenn es wirklich dringend ist und kein alternatives, datenschutzkonformes Kommunikationsmittel genutzt werden kann.

Lösung: Die Antwort 2. ist richtig. In bestimmten Ausnahmefällen, wenn die besondere Eilbedürftigkeit dies erforderlich macht und sichergestellt ist, dass die Sendung nur dem richtigen Empfänger zugeht, kann auch die Versendung besonders schutzbedürftiger personenbezogener Daten mittels Fax rechtmäßig sein. Dies gilt aber nur dann, wenn kein alternatives, datenschutzkonformes Kommunikationsmittel genutzt werden kann und dem Verantwortlichen insofern kein alternatives Kommunikationsmittel zur Verfügung steht.

Impressum

Redaktion:
Frank Berns, Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de