PPP RECHTSANWÄLTE
Dres. Pittrof, Penner, Reimer & Partner
Partnerschaftsgesellschaft mbB

PPP RECHTSANWÄLTE
Dres. Pittrof, Penner, Reimer & Partner
Ungelsheimer Weg 8, 40472 Düsseldorf

Abbruchverband Nord

Unternehmerseminar

Datum	Aktenzeichen	Standort	Bei Rückfragen
26.03.2021		Düsseldorf	Dr. Groth groth@ppp-rae.de

Datenschutz Geheimnisschutz

Cybercrime

Wie die Seiten eines Dreiecksprismas können diese Stichworte auf unterschiedliche Weise einen identischen Sachverhalt ins Licht setzen.

Zunächst aber einige Fälle:

1 Ein Außendienstler nimmt beim Ausscheiden aus dem Arbeitsverhältnis seine Notizen über Namen, Anschriften, Telefonnummern, Investitionspläne seiner Messekontakte mit

2 Das Teilelager eines Baugerätevermieters wird videoüberwacht

3 Sie erhalten die Nachricht, dass Sie einen Preis gewonnen haben und werden gebeten, Namen, Anschrift, Geburtsdatum

Standort Düsseldorf
Ungelsheimer Weg 8
40472 Düsseldorf
Tel.: +49 (0)211/954336-0
Fax: +49 (0)211/954336-99
info-duesseldorf@ppp-rae.de

Rechtsanwälte

Dr. jur. Andreas Penner[1]
Lehrbeauftragter für Sozial- und Gesundheitsrecht der Juristischen Fakultät der Ruhr-Universität Bochum

Tanja Koopmann-Röckendorf, LL.M.oec[1]
Fachanwältin für Arbeitsrecht
Fachanwältin für Sozialrecht

André Bohmeier[1]
Lehrbeauftragter an der SRH Fachhochschule für Gesundheit Gera und der Ruhr-Universität Bochum

Prof. Ulf Pallme-König[3]
Kanzler der Heinrich-Heine-Universität Düsseldorf a.D.

Dr. jur. Georg Groth[3]

Benjamin Fischer[2]
Julia Zink, LL.M.[2]
Jana Junglas[2]
Pierre Finke[2]

Standort Ingolstadt
Haslangstraße 1
85049 Ingolstadt
Tel.: +49 (0)841/953565-0
Fax: +49 (0)841/953565-25
info-ingolstadt@ppp-rae.de

Rechtsanwälte

Dr. jur. Ute Pittrof[1]
Fachanwältin für Medizinrecht
Fachanwältin für Handels- und Gesellschaftsrecht
Lehrbeauftragte der FOM (München)
Akkreditierte Schiedsrichterin der Deutschen Institution für die Schiedsgerichtsbarkeit e.V. (Ärztegesellschaften)

Andrea Halbich[2]

Standort Heilbronn
Gutenbergstraße 86
74074 Heilbronn
Tel.: +49 (0)7131/797035-0
Fax: +49 (0)7131/797035-7
info-heilbronn@ppp-rae.de

Rechtsanwälte

Dr. jur. Felix Reimer[1]**, LL.M. (Medizinrecht)**
Lehrbeauftragter der FOM (München)
Fachanwalt für Medizinrecht

Standort Bergisch Gladbach
Bensberger Straße 72
51465 Bergisch Gladbach
Tel.: +49 (0)2202/251650-3
Fax: +49 (0)2202/251650-4
info-bergischgladbach@ppp-rae.de

Rechtsanwälte

Matthias Wallhäuser[1]
Fachanwalt für Medizinrecht
Certified Compliance Officer (Univ.)
Lehrbeauftragter der FOM (Köln)
Herausgeber der Zeitschrift „Der Krankenhaus-JUSTITIAR“

[1] Managing Partner am Standort
[2] Rechtsanwältin/ Rechtsanwalt in Anstellung
[3] Of Counsel

http://www.ppp-rae.de

und Bankverbindung mitzuteilen, damit Ihnen das Geld überwiesen werden kann

4 Sie erhalten eine Rechnung betreffend die gesetzlich vorgeschriebene Übermittlung bestimmter Daten Ihres Unternehmens nach dem Transparenzregistergesetz

5 Und es gibt natürlich noch die spektakulären Fälle, z.B.: Im letzten Herbst war die Universitätsklinik Düsseldorf Ziel eines Hackerangriffs, der den Klinikbetrieb für 2 Wochen lahmlegte. Anfang des Jahres erschienen die Zeitungen und Zeitschriften der Funke-Medien-Gruppe als Notausgabe und wochenlang in verkürzter Form, weil ihre EDV- Ziel eines verbrecherischen Angriffs war. Wenn schon solche Unternehmen, die über eine ständig bereite gut bezahlte IT-Abteilung verfügen, nicht sicher vor Cyber-Attacken sind, wie leichte Beute mag dann Ihr Unternehmen sein?

Worum geht es? Sie müssen mit den Daten, die Ihnen überlassen werden, sorgsam und rechtstreu umgehen. Sie müssen sie wie auch Ihre eigenen Daten vor kriminellen Angriffen schützen. Und Sie müssen die Informationen, die zu schützen sind, auch identifizieren, um sie schützen zu können.

250000 Cyber-Crime-Fälle in Deutschland im Jahr belegen, dass jeder, geschäftlich oder privat, Opfer sein kann. Es reicht die Nutzung irgendeines internetfähigen Gerätes. Die Täter/innen benötigen Ihren Computer oder Ihr Bankkonto (oben 3) als Mittel für kriminelle Geschäfte. Gelder oder Informationen, von denen Sie nichts ahnen, werden darüber bewegt.

Also, Grundregel beherzigen: Es gibt in diesem Leben nichts umsonst. Auf Gewinnmitteilungen wird nicht reagiert. Wer Ihnen Geld schenken will, mag es in bar vorbeibringen.

Und wie Sie Ihren Computer vor Schadsoftware schützen können, soll Ihnen Ihr IT-Provider erklären. Wichtige Informationen werden auf externen Datenträgern abgespeichert, auf die von außen nicht elektronisch zugegriffen werden kann. Stefan Richardt hat Ihnen zu diesem Thema schon einiges referiert. Falls Sie noch einmal nachschauen wollen:

Zu dem Fällen, die die Kriminalstatistik kennt, kommen die vielen weiteren, die nicht bekannt werden, weil sie niemand anzeigt. Wer gibt schon gern zu, dass er Opfer eines hinterhältigen Schlitzohres geworden ist, zumal wenn der Schaden wirtschaftlich zu verkraften ist?

Die Ermittlungsbehörden sind aber auf Anzeigen angewiesen, geben sich viel Mühe und stellen Hilfen und Informationen übersichtlich bereit:

https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html

Seien Sie sensibel! Tatsächlich gibt es (oben 4.) ein Transparenzregister (§§ 18 ff. Geldwäschegesetz) und auch eine Transparenzregistergebührenverordnung (4,80 € zahlen Sie jährlich). Es gibt aber außerdem in diesem Bereich (und einigen anderen) etwa 300 dem amtlichen „Bundesanzeiger“ bekannte unseriöse Schlingel, die Ihnen für sinnlose Tätigkeiten Beträge im Bereich von zumeist knapp unter 200.- € abverlangen wollen, dürftig getarnt als „Angebot.“

https://www.bundesanzeiger.de/pub/Alphabetische%20Uebersicht.pdf

Wenn Sie nicht jedes Mal sorgfältig prüfen (lassen) wollen, ob eine solche Forderung berechtigt ist oder nicht, sollten Sie die gute alte Kaufmannsregel beherzigen:

„Rechnung? Weglegen! Wenn es etwas Ernstes ist, zahlen wir nach der dritten Mahnung.“

Selbstverständlich schützt uns das Strafgesetzbuch durch Strafandrohungen von durchweg 2 bis 5 Jahren gegen

Ausspähen von Daten - § 202a

Abfangen von Daten - § 202b

Vorbereitungshandlungen zu solchen Taten, z. B. durch Passwortdiebstahl - § 202 c

Datenhehlerei - § 202 d

Computerbetrug - § 263 a

Fälschung beweiserheblicher Daten - § 269

Datenveränderung - § 303 a

Computersabotage - § 303 b

Aber: Wie und wo kann man der Täter/innen habhaft werden, wenn sie in Nordkorea, hinter dem Ural oder auf einer sonnigen Insel in der Südsee sitzen? Schon von einem Rechtshilfeersuchen nach Frankreich nahm in einem von mir angezeigten Fall die Staatsanwaltschaft Abstand, „weil das erfahrungsgemäß nichts bringt."

Nicht nur deshalb: Schon mal an eine Versicherung gedacht? Angesichts zahlreicher Corona-bedingter Heimarbeitsplätze haben sich die Probleme vervielfacht und der Markt der Cyber-Policen wächst. Herr Behlau wird Ihnen sicherlich eine an Ihrem Bedarf orientierte Versicherungslösung präsentieren können.

Das Gegenstück zum Cybercrime ist der **Datenschutz**: Wenn Sie Mitarbeiter/innen im sog. Homeoffice arbeiten lassen, dann doch hoffentlich – wie am Firmenarbeitsplatz auch - nur mit eigens hierfür zur Verfügung gestellten Firmen-Smartphones und -Computern, die NICHT privat genutzt werden dürfen, gesichert mit Passwörtern, die nur Sie kennen und ändern dürfen. Denn Sie müssen die Informationen (Daten) schützen, die Sie von Ihren Kunden und Geschäftspartnern erhalten, aber auch die Privatsphäre Ihrer Mitarbeiter respektieren, haben auf deren Datenspeicher kaum Zugriff, wenn dort Geschäftliches und Privates gemischt wird. Untersagen Sie vertraglich jede private Nutzung des Firmenrechners und des Netzes (Internetsurfen, E-Mail-Verkehr…). Behalten Sie sich das Recht vor, den Mailverkehr der Betriebsangehörigen auf dem Firmencomputer/-handy, Anruflisten, Verbindungsdaten usw. anzuschauen.

Eine ähnliche Problemlage stellt sich – oben 2. - bei der GPS-Überwachung Ihrer Fahrzeuge ein: Wenn Ihre Mitarbeiter/innen das Fahrzeug auch privat nutzen dürfen, müssen sie die Überwachung nach Feierabend ausschalten können. Also auch hier: Einfacher ist es, die Privatnutzung auszuschließen. Und in jedem Fall von Überwachung, Video, GPS oder andere, lassen Sie sich natürlich von Ihren Arbeitnehmern/innen quittieren, dass Sie sie über Grund, Art und Ausmaß der Kontrollmaßnahme informiert haben. Heimliche Überprüfungen sind nur beim konkreten Verdacht erheblicher Rechtsverstöße vertretbar.

Viele Sorgen, die beim Inkrafttreten der Datenschutzgrundverordnung geäußert wurden, haben sich glücklicherweise in Nichts aufgelöst. Weder sind massenhafte Abmahnungen noch irrwitzige Schadensersatzforderungen bekannt geworden. Aber sicher ist sicher: Haben Sie eine Musterdatenschutzerklärung?

https://www.itm.nrw/lehre/materialien/musterdatenschutzerklaerung/

Eine/n Datenschutzbeauftragte/n? Kommen Sie der Informationspflicht nach Art. 13 DSGVO bei Erhebung von personenbezogenen Daten nach?

(Daten-)schutzbedürftig sind Ihre Mitarbeiter/innen und private Auftraggeber/innen; Firmendatenschutz gibt es nicht.

„Für den Hausgebrauch“ einige Grundsätze, die Sie, wenn Sie sie beherzigen, vor größerem Ärger bewahren:

- Daten werden korrekt und sparsam erhoben.
- Es werden nur notwendige Daten erhoben.
- Daten werden gesichert, im Haus durch sichere Passwörter, Tresore…, bei aushäusiger Verarbeitung durch die Wahl zuverlässiger europäischer Unternehmen, für die die DSGVO gilt
- Daten werden gelöscht, wenn sie nicht mehr benötigt werden („Recht auf Vergessenwerden“). Die gesetzlichen z.B. steuerrechtlichen Aufbewahrungsfristen sind einzuhalten.

Das müssen Sie tun: Dokumentieren

von wem erheben Sie welche Daten wofür in welcher Form?

Wer hat auf diese Daten Zugriff?

Wie können Daten in falsche Hände geraten? Was ist dagegen zu tun?

Welche Datensicherung ist in Ihrem Unternehmen vorhanden?

Wenn das Unglück geschieht und Daten verloren gehen, weil Sie „gehackt“ worden sind oder Sie oder Mitarbeiter/innen das Smartphone verloren haben (und nicht wissen, wo es ist): Unterrichten Sie innerhalb von 72 Stunden die Aufsichtsbehörde:

https://www.datenschutz-wiki.de/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte

Wenn Sie sich vom Datenschutz gequält fühlen, weil Sie ihn aktiv ausführen müssen, dann denken Sie daran, dass es andern, die sich um *Ihren* Schutz kümmern sollen, genauso geht.

Und freuen Sie sich, dass es seit dem 26.4.2019, auch auf einer EU-Richtlinie basierend, einen verbesserten **Schutz Ihrer Geschäftsgeheimnisse** gibt.

Voraussetzung für den Schutz sind drei Eigenschaften, die zusammen vorliegen müssen:

Es muss sich um eine Information handeln,

a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht;

So § 2 des Gesetzes. Noch einmal in anderen Worten: Ein zu Recht geschütztes Geheimnis von wirtschaftlichem Wert.

Einen Beispielsfall (entsprechend oben 1.) löste das LAG Düsseldorf (12 SaGa 4/20 v. 03.06.2020) und erklärte:

Bei privaten Aufzeichnungen eines Arbeitnehmers über Kundenbesuche und Kundendaten und Absatzmengen kann es sich um Geschäftsgeheimnisse handeln. Voraussetzung: Angemessene Geheimhaltungsmaßnahmen des Rechteinhabers. Solche Maßnahmen können auch in hinlänglich genauen vertraglichen Vereinbarungen liegen.

Überlegen Sie, was Ihrem Unternehmen wirtschaftlich schaden würde, wenn es Ihrem Wettbewerber bekannt würde: Natürlich nicht die Preisliste, die Sie in Ihrem Internetauftritt präsentieren. Aber die Konditionen, die Ihnen Ihr Maschinenlieferant gewährt, die Preise, die Sie mit Ihren Subunternehmern vereinbart, die Gewinnmarge, mit denen Sie in Ihren Kalkulationen arbeiten … Derartige Informationen würden es Ihrem Verhandlungspartner auf Nachfragerseite erleichtern, Ihre Preise zu Lasten Ihres Gewinns zu drücken, Ihr Wettbewerber könnte seine eigenen Preise anpassen, Ihre Lieferanten würden die Preise erhöhen, wenn Sie Gewissheit über Ihre wirtschaftlichen Möglichkeiten hätten. Auch Gespräche über anstehende Projekte, erst recht Verhandlungen sind fraglos nicht für die Augen und Ohren Ihrer Wettbewerber geeignet, so wenig wie technologische/verfahrenstechnische Ausarbeitungen in schwierigen Fällen. Wir haben es in allen diesen Fällen mit vertraulichen Informationen von wirtschaftlichem Wert zu tun, an deren Geheimhaltung Sie ein berechtigtes Interesse haben. Nach LG Frankfurt 2-06 O 247/20 v. 25.08.2020 müssen Sie allerdings auch den Wert eines wirtschaftlichen Nachteils darlegen können und belegen, wie und in welchem Umfang die Offenlegung einer Information Ihnen nachteilig sein kann und wie hoch der zu befürchtende Schaden sein kann.

Es reicht nun aber nicht aus, dass Sie Ihre Geschäftsgeheimnisse also solche deklarieren, Sie müssen auch etwas zu ihrem Schutz tun. Geheimnisse, die auf allgemein zugänglichen Datenverarbeitungsgeräten oder auf Zetteln zu finden sind, die in der Kaffeeküche liegen, sind keine.

Also: Lassen Sie, wenn Ihr Betrieb groß genug ist, nicht jeden alles sehen und schließen Sie mit den wissenden Mitarbeitern/innen Geheimhaltungsvereinbarungen für die Zeit der Zusammenarbeit und darüber hinaus (sinnvollerweise mit Vertragsstrafenklauseln).

Formulierungen wie „alle Informationen, die der/m Arbeitnehmer/in während des Beschäftigungsverhältnisses in Bezug auf das Unternehmen bekannt werden“ sind wertlos.

Denken Sie aber an Geheimhaltungsabreden nicht nur mit Arbeitnehmern/innen; auch freie Mitarbeiter, Gesellschafter, externe Berater können Verräter werden.

Wenn Sie aber alles richtig gemacht haben und Opfer eines Geheimnisverrats geworden sind, haben Sie gegen den/die Rechtsverletzer/in Ansprüche auf Beseitigung/Unterlassung (schon, wenn eine Rechtsverletzung erstmalig droht!), Vernichtung/Herausgabe der im unrechtmäßigen Besitz befindlichen Datenträger, Auskunft über die Abnehmer der Information und Schadensersatz gem. §§ 6 – 14 des Gesetzes.

Außerdem kann die Verletzung von Geschäftsgeheimnissen mit Freiheitsstrafe bis zu 3 Jahren oder mit Geldstrafe geahndet werden (§ 23).

Und nun wünsche ich Ihnen ganz offen und ehrlich noch einen erfolgreichen weiteren Verlauf Ihres Seminars, danke für Ihr Interesse und hoffe, Sie alle bald endlich wieder persönlich begrüßen zu können.

Bis dann, bleiben Sie gesund!