



---

# Agenda

1. Sieben Jahre DS-GVO - Erfahrungen
2. Die wesentlichen Regelungen des Datenschutzes
3. Betreibergesellschaft und Verein – Stolperfallen vermeiden
4. Rechenschaftspflicht der Golfanlage – Was wird benötigt?
5. Verhaltensrichtlinie für Mitarbeiter
6. Tipps für Ihre Arbeit (Veröffentlichungen, Startzeiten, Webcams, Videokameras)
7. Gefahren durch Cyberangriffe, Phishing, Beispiele
8. Fragen

## Ihr Referent

### Karl Würz

Würz Datenschutz Consulting GmbH

(equeo CompCor GmbH)

75203 Königsbach-Stein

Mobil: 0171 28 19 650

[karl.wuerz@wuedatacon.de](mailto:karl.wuerz@wuedatacon.de)



---

## Referenzen (Golfdienstleister, Verbände)

### Golfdienstleister, Verbände

- Albatros Datenservice GmbH
- GKMB GmbH
- GMVD Golf Management Verband Deutschland e.V.
- Greenkeeper Verband Deutschland e.V.
- Vereinigung clubfreier Golfspieler

---

## Referenzen (Vereine, Betreibergesellschaften)

- Golf Club St. Leon-Rot
- Wittelsbacher Golfclub
- Golfclub Dresden Elbflorenz
- Golfanlage Dresden Ullersdorf
- Golfclub Johannesthal
- Karlshäuser Hof Golf Pforzheim
- Gutperle Golfcourses (Rheintal, Heddesheim, Pfälzerwald, Kurpfalz)
- Golfclub Schloss Monrepos
- Golfclub Schönbuch
- Golfclub Domäne Niedereutin
- Hofgut Scheibenhardt
- Münchener Golf Club
- Baden Hills Golf und Curling Club
- Frankfurter Golf Club
- Golf-Club Bensheim
- Golfclub Obere Alp
- Golfclub Urloffen
- Golfpark Augsburg
- Golfclub Mangfalltal
- Golf Club Hetzenhof
- GolfRange

---

## 7 Jahre DS-GVO

- ✓ Rechtsanwendung hat sich stabilisiert.
- ✓ Mehrere wesentliche gerichtliche Entscheidungen:  
Cookie-Entscheidung EuGH/BGH; EuGH zu „privacy shield“, neue EU-Standardvertragsklauseln
- ✓ Neue gesetzliche Regelung in Deutschland zu Telekommunikation seit 01.12.2021,  
Cookie-Regelung (Einwilligung), Bußgeldandrohung für mangelhafte Cookie-Banner
- ✓ Weitere wesentliche Regelungen auf EU-Ebene (EU Data Act)
- ✓ Anhaltend hohe Belastung der Datenschutzbehörden (Beschwerden, Datenpannenmeldungen).
- ✓ Regelmäßige Bußgeldbescheide (siehe nachfolgende Folie).

## Bisherige Bußgelder nach DS-GVO - Beispiele

2024	6.000 €	Online-Händler	Verspätete Meldung einer Datenpanne
2023	9.000 €	Klinik	Unterlassen der Informationspflicht über Datendiebstahl einer Mitarbeiterin
2022	16.000 €	Elektronikmarkt	Unrechtmäßige Audio- und Videoüberwachung von Beschäftigten, zu lange Speicherung, inadäquate Sicherheitsmaßnahmen.
2021	300.000 €	Betreibergesellschaft Sportverein	Fahrlässige Verletzung der datenschutzrechtlichen Rechenschaftspflicht.
2021	200 €	Privatperson	Unverschlüsselte E-Mail mit Beweismaterial zu Verkehrsverstößen an die Bußgeldabteilung der Stadt Magdeburg.
2020	8.000 €	Rechtsanwalt	Unerlaubte Verarbeitung der Daten eines mutmaßlichen Schuldners und eines unbeteiligten Ehepaars.
2020	1.240.000 €	Krankenkasse	Verwendung der Daten von 500 Gewinnspielteilnehmern für Werbezwecke.
2020	50.000 €	Unternehmen	Fehlender AV-Vertrag und Verstoß gegen Transparenz- und Verständlichkeitsgebot.
2020	12.000 €	Betreiber eines Schwimmbades	Unerlaubte Videoüberwachung in Schwimmbad, fehlender AV-Vertrag und keine Benennung eines DSB.
2020	229 €	Privatperson (LKW-Fahrer)	Betrieb einer Dashcam im Straßenverkehr und Veröffentlichung von Aufnahmen über Youtube.
2020	2.000 €	Restaurant	Unerlaubte Kameraüberwachung des Gastraumes eines Restaurants.
2020	51.000 €	Unternehmen	Unterlassene Mitteilung über den Wechsel des Datenschutzbeauftragten.
2020	20.000 €	Kommunales Unternehmen	Verspätete Meldung einer Datenpanne an betroffene Personen und Aufsichtsbehörde.
2020	100.000 €	Unternehmen	Unzureichender Schutz personenbezogener Daten in einem Bewerberportal.
2019	10.000 €	Unternehmen	Fehlende Benennung eines Datenschutzbeauftragten.
2019	80.000 €	Unternehmen	Unsachgemäße Entsorgung personenbezogener Daten.
2019	2.600 €	Privatperson	Versendung mehrerer E-Mails, in denen die (persönlichen) E-Mail-Adressen aller Empfänger sichtbar waren.
2019	20.000 €	Unbekannt	Verspätete Meldung einer Datenpanne sowie unterlassene Benachrichtigung der Betroffenen

---

## Grundsätzliches

- Datenschutz regelt den Umgang mit personenbezogenen Daten
  - persönliche oder sachliche Informationen über bestimmte oder bestimmbare natürliche Personen, wie z.B. Name, Adresse, Beruf, Geburtsdatum, Finanzdaten, Ausweisnummer usw.
- Mitglieder, Gäste, Interessenten, Eltern, Kinder, Geschäftspartner, Lieferanten, Bewerber
- **Ziele:** Vertraulichkeit – Verfügbarkeit – Integrität
  - Verhinderung von Datenverlust durch IT-Fehlverhalten, durch menschliches Fehlverhalten (bewusst/unbewusst) oder durch Angriffe von außen und innen
- **Grundsatz:**  
Sie achten auf die Einhaltung der Regelungen zum Schutz personenbezogener Daten
- Verbindliche Anforderung für alle Mitarbeiter

---

## Rechtsgrundlagen

### Keine Datenverarbeitung ohne Rechtsgrundlage

- Vertrag (Mitglieds-, Nutzungsvertrag, Spielvertrag über Greenfee-Runde)
- rechtliche Verpflichtungen (Steuerrecht, HGB)
- berechtigtes Interesse der Golfanlage, kein entgegenstehendes Interesse des Betroffenen (beachte: Abwägung)
- Einwilligung: Einwilligung NUR anwenden, wenn keine andere Rechtsgrundlage vorliegt (also im Ausnahmefall)

Datenschutzrecht: Der Betroffene ist zu informieren!

- Information im Rahmen der Datenverarbeitung (Aufnahmeantrag, Datenschutz-Richtlinie für Mitglieder und Gäste, Turnierausschreibung)

## Anforderungen des Datenschutzes an eine Golfanlage

- Auswahl und Bestellung eines Datenschutzbeauftragten oder Bestimmung einer fachlich geeigneten Person zur Umsetzung der Anforderungen
- „Datenschutz-Richtlinie für Mitglieder und Gäste“ -> Informationspflicht
- Regelung der „gemeinsamen Verantwortung“ des Vereins mit der Betreiberanlage (wer macht was?)
- Datenschutzhinweis in Turnierausschreibungen
- Prozessregeln Bildveröffentlichungen
- Aktualisierung Datenschutzerklärung Web-Seiten, Facebook, **Cookie-Banner auf Webseiten**
- Aktuelle „Verzeichnisse über Verarbeitungstätigkeiten“
- Interne Richtlinien für alle Mitarbeiter „Verhaltens-Richtlinien Datenschutz und Informationssicherheit“
- Verpflichtung zur Einhaltung der Datenschutzregelungen, regelmäßige Schulung der Mitarbeiter
- Aktualisierung der Verträge über Auftragsverarbeitung
- Regelmäßige Überprüfung der techn. und organisatorischen Sicherungen
- Regelmäßige Überprüfung des Datenbestands, ggf. Löschung von Altbeständen, Umsetzung Löschkonzept
- Festlegung interner Prozesse für Auskunftersuchen und Meldung Datenpanne (beachte Fristen)
- Dokumentation der Maßnahmen zur Erfüllung der Rechenschaftspflichten, regelmäßige Aktualisierung, Audit

## Bestellung eines Datenschutzbeauftragten

***Ein betrieblicher Datenschutzbeauftragter für Golfanlagen ist gem. DSGVO bzw. BDSG zu bestellen, wenn sich mindestens zwanzig (20) Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.***

***Ist kein DSB bestellt, haftet der Präsident persönlich für die Einhaltung des Datenschutzes.***

„ständig“ bedeutet, dass der Umgang mit personenbezogenen Daten zum Aufgabenfeld des Mitarbeiters gehört. Hier spielt es keine Rolle, wie oft die Aufgabe anfällt (es genügt auch nur gelegentlich).

Dies umfasst also alle Personen, die mit Personendaten von Mitarbeitern, Mitgliedern, Kunden, Lieferanten befasst sind, auch wenn dies nur gelegentlich oder ehrenamtlich erfolgt (auch IT-Mitarbeiter mit Zugriffsmöglichkeiten auf Personendaten).

Somit sind folgende Personengruppe in einer Golfanlage hier mitzurechnen:

- Vorstandsmitglieder, die über einen Mitgliedsantrag entscheiden,
- alle Personen, die mit der Finanzbuchhaltung betraut sind,
- alle Personen, die bei Lieferanten oder Dienstleistern Bestellungen vornehmen (z.B. auch im Greenkeeping),
- alle Personen, die im Sekretariat einer Golfanlage tätig sind (auch in Teilzeit),
- alle ehrenamtliche Abteilungsverantwortliche, die Zugang zu den Kontaktdaten von Mitgliedern haben und beispielsweise Abteilungsturniere veranstalten, Reisen organisieren oder auch eine Abteilungskasse führen,
- alle Mannschafts-Captains, wenn diese regelmäßig die Kontaktdaten der betreffenden Spielerinnen oder Spieler erhalten, Trainings organisieren oder auch eine Mannschaftskasse führen.

---

## Betreibergesellschaft und Verein

Der Spielbetrieb auf einer Golfanlage wird oftmals von zwei verschiedenen Rechtsformen organisiert, z.B. durch eine GmbH und einen eingetragenen Verein.

In diesen Fällen werden die personenbezogenen Daten von Mitgliedern und auch Gästen in vielen Fällen von beiden Rechtsformen verarbeitet.

Grundsätzlich sind diese beiden „Rechtsformen“ eigenständige Verantwortliche.

Die DSGVO sieht in solchen Fällen nunmehr die Möglichkeit vor, dass diese verschiedenen „Rechtsformen“ dies als „gemeinsam Verantwortliche“ gem. Art. 26 DSGVO organisieren. In diesem Fall muss dies in einer Vereinbarung in transparenter Form festgelegt werden, wer von ihnen welche Verpflichtung im Sinne der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht.

### ***Empfehlung:***

Sind auf einer Golfanlage zwei (oder mehr) Rechtsformen vorhanden (z.B. Betreibergesellschaft und Verein), dann muss das „Zusammenwirken“ dieser Gebilde in einer transparenten Vereinbarung nach Art. 26 DSGVO geregelt werden. Die betroffenen Mitglieder sind darüber entsprechend in einer „Datenschutz-Richtlinie“ zu informieren.

## DDMS Golf - Dokumentation Datenschutz Management-System

Rechenschaftspflichten der DSGVO erfüllen -  
rechtssicher, praxisbewährt und einfach

### Golfdatenschutz

Benutzername  
golfdemo

Passwort  
[versteckt]

Anmelden



- Produkt von GKMB und equeo CompCor
- Unterstützt Datenschutzverantwortliche der  
Betreibergesellschaften und Golfclubs bei der Umsetzung  
der erforderlichen Maßnahmen und Richtlinien.
- Regelmäßige Informationen über Rechtsänderungen oder  
aktuelle Entwicklungen.
- Mit allen erforderlichen Mustern und Vorlagen der equeo  
CompCor GmbH.
- Preisgünstige web-basierte Lösung in einem deutschen  
Rechenzentrum; Hosting durch GKMB.

---

# **Verhaltens-Richtlinie „Datenschutz und Informationssicherheit“**

**für die  
Geschäftsführung, Mitarbeiter,  
Vorstände und Ehrenamtliche**

**Golfanlage Musterstadt**

**über den Umgang mit personenbezogenen Daten und  
dem Schutz der Informationen und Daten**

---

## Warum benötigen Sie eine „Verhaltens-Richtlinie“?

- ✓ Eine Betreibergesellschaft und ein Verein sind verpflichtet, die gesetzlichen Anforderungen einzuhalten -> Rechenschaftspflicht.
- ✓ Deshalb Regelung der wesentlichen Verhaltensanforderungen für alle Mitarbeiter.
- ✓ Gesetzliche Regelung, alle Mitarbeiter zum vertraulichen Umgang mit personenbezogenen Daten zu verpflichten (Unterschrift).
- ✓ Schutz der personenbezogenen Daten der Mitglieder, Gäste und auch der Mitarbeiter durch technische und organisatorische Maßnahmen. -> Verhaltensregeln zur IT-Sicherheit.
- ✓ Ziel dieser Richtlinien: Verhaltensempfehlungen für alle Mitarbeiter und ehrenamtlichen Beschäftigten.

# Tipps für die tägliche Arbeit

---

## Tipps für Ihre Arbeit

### Was ist bei Foto- oder Videoveröffentlichungen zu beachten?

#### Bild- oder Video-Veröffentlichungen:

- Veröffentlichung von Ergebnissen: Veröffentlichung von Ergebnissen ist zulässig, wird vom Vereinszweck umfasst.
- Eine Veröffentlichung von Bildern ist nur mit Einwilligung der Betroffenen zulässig. Wer für ein Siegerbild „aufgestellt“ wird, stimmt der Veröffentlichung zu.
- Ausnahme: keine Einwilligung erforderlich bei „größeren Veranstaltungen“ und „Ereignissen der Zeitgeschichte“ (also größere Turnierveranstaltungen, Sponsorenturniere, sonstige Veranstaltungen), sofern kein entgegenstehendes Interesse des Betroffenen (hier Abwägung im Einzelfall „kompromittierende Bilder“)  
Beachte: bei solchen Veranstaltungen ein Hinweisschild aufstellen (Informationspflicht), siehe Muster.

#### **WICHTIG:**

**Veröffentlichung von Bildern von Personen unter 16 Jahren im Internet ausschließlich nur mit Einwilligung der Erziehungsberechtigten! (Art. 8 DS-GVO)**

---

## Tipps für Ihre Arbeit

### Videüberwachung:

- WebCam:  
Wenn ein berechtigtes Interesse vorliegt, kann eine WebCam betrieben werden. Von besonderer Bedeutung ist jedoch die Erkennbarkeit einzelner Personen. Dies sollte möglichst vermieden werden.
- Videokameras:  
Die Installation von Videokameras ist möglich, sofern entsprechende Gründe vorliegen -> berechtigtes Interesse (Einbruchgefahr, Prävention Brand etc).
- Information an die Betroffenen durch Hinweisschilder auf Videokameras.
- Zugriff auf die Aufzeichnungen (z.B. Unfallflucht, Sachbeschädigung):
  - Auswertung zulässig, wenn ein berechtigtes Interesse vorliegt (Prüfung durch DSB im Einzelfall)
  - Begründung für die Auswertung (durch DSB)
  - Information an den Betroffenen (Infoblatt durch DSB)

---

## Tipps für Ihre Arbeit

### Dürfen Daten von Turnierteilnehmern an Sponsoren übermittelt werden?

- Eine Weitergabe von personenbezogenen Daten von Turnierteilnehmern an Sponsoren ist nur mit Einwilligung des Betroffenen zulässig. Diese Einwilligung kann im Rahmen der Turnieranmeldung erhoben werden.
- Widerspricht ein Turnierteilnehmer im Rahmen der Turnieranmeldung der Weitergabe seiner Daten an den Sponsor, dann ist ein Ausschluss aus dem Turnier gesetzlich nicht zulässig.

### Startzeiten-Buchungen: Wie behandle ich Buchungen von Startzeiten für weitere Mitspieler?

- Einwilligung des Betroffenen zur Veröffentlichung seiner Daten.
- Zur Abwicklung eines effizienten Startzeiten-Buchungsmoduls ist es erforderlich, dass bei Buchung einer Startzeit für den Interessenten ersichtlich ist, welche weiteren Mitspieler bereits diese mögliche Startzeit gebucht haben.
- Eine Einsicht in die Übersicht der gebuchten Personen sollte aber nicht für jedermann möglich sein, sondern erst nach einer passwortgeschützten Anmeldung am Buchungssystem. Auskunft durch Sekretariat, wenn berechtigtes Interesse des Anfragenden und Person bekannt.
- Zugriff auf Startzeitenübersicht am eigentlichen Buchungstag auf der Anlage zulässig (berechtigtes Interesse).

---

## Tipps für Ihre Arbeit

### Wie gehe ich mit dem Aushang von Start- und Ergebnislisten bei Golfturnieren korrekt um?

#### Startlisten:

Wegen der mit dem Internet verbundenen Risiken ist sicherzustellen, dass der Zugriff auf eine Startliste über das Internet nicht für jedermann möglich ist. Eine Startliste enthält sensible Daten, nämlich die Startzeiten einzelner Personen, die gleichzeitig deren Abwesenheit von zu Hause dokumentieren.

Die Veröffentlichung einer Startliste im Internet ist deshalb nur über einen passwort-geschützten Zugang möglich. Der Aushang einer Startliste am Schwarzen Brett im Golfclub ist zulässig. Über die Verfahrensweise sollte der Betroffene vorab informiert werden (z. B. durch Hinweis in einer Rahmenausschreibung oder auf der Meldeliste).

#### Ergebnislisten:

Dem Aushang von Ergebnislisten stehen keine überwiegenden schutzwürdigen Interessen der Mitglieder regelmäßig entgegen. Dies dient unmittelbar der Verwirklichung des Vereinszwecks (Sportausübung durch die Mitglieder) und ist daher zulässig, auch die Veröffentlichung der Ergebnisliste im Internet. Es sollte jedoch auch hier bereits bei der Datenerhebung (Meldung zum Wettspiel) oder gar schon in der (Rahmen-) Ausschreibung deutlich darauf hingewiesen werden, dass eine Veröffentlichung der Ergebnisliste im Internet erfolgt. Widerspricht ein Betroffener der Veröffentlichung seiner Daten im Rahmen der Ergebnisliste, so wäre sein Name im Internet „zu schwärzen“.

# Phishing, SPAM - Gefahrenpotential

## Phishing, SPAM, CEO-Fraud – Was ist das eigentlich ?

### Phishing

Phishing-Mails sind gefälschte Mails, mit denen Cyber-Kriminelle nach Passwörtern, Kontodaten oder sonstigen Zugangsdaten „fischen“, um mit diesen Daten kriminelle Taten zu begehen  
(Bestellung von Waren, CEO-Fraud, Zugriff auf Bankkonten)

#### Beispiele:

Gefälschte Mails von Banken oder Kreditkartenfirmen:  
„Ihr Konto wurde gesperrt ....“ oder ähnliches

Gefälschte Rechnungen mit Links zu Webseiten mit Abfrage von Login-Daten

### SPAM

SPAM steht als Sammelbegriff für alle Formen von massenhaft versandten, unerwünschten E-Mails, elektronischen Kettenbriefe oder Werbeposts in sozialen Netzwerken.  
Ziel: Verbreitung von Schadsoftware oder Kombination mit Phishing-Angriff

#### Beispiele:

Initiativbewerbung mit Dateianhang (Virus in Anhang)  
Gewinnspiel: „Sie haben gewonnen ...“

Gefälschte Rechnung mit Dateianhang:  
Amazon Bestellbestätigung mit Anhang (Virus in Anhang).

### CEO-Fraud

Gefälschtes E-Mail, das scheinbar von der Geschäftsführung kommt.

Darin wird unter vermeintlich berechtigten Gründen die Überweisung eines hohen Geldbetrages auf ein ausländisches Konto angewiesen.

Oftmals Kombination mit Phishing-Angriff, mit dem zuerst die Zugangsdaten zu E-Mail-Konten erlangt werden.

CEO-Fraud-Mail kommt dann von Innen.

# Konkrete Beispiele aus der Branche

---

## Fallbeispiel einer Datenpanne (1) - Ransomware

### Sachverhalt:

An einem Sonntag Morgen will die Mitarbeiterin im Sekretariat den Rechner einschalten und stellt fest, dass die gesamten Daten verschlüsselt sind. Es ist nur noch eine Datei lesbar mit der Erpressungsaufforderung: „Ihre Daten wurden verschlüsselt. Überweisen Sie XXXX US-Dollar in Bitcoins auf ...“

### Vorgehensweise/Feststellungen:

Meldung einer Datenpanne.

Die Daten der Golfanlage wurde von einem Verschlüsselungstrojaner angegriffen und vollständig verschlüsselt (Ransomware), auch der „Spiegelserver“ für Datensicherung. Der konkrete Angriff konnte nicht mehr rekonstruiert werden, da alle Daten verschlüsselt sind.

Es waren Datensicherungen der Mitgliederdaten und Buchhaltungsdaten extern vorhanden, so dass diese wiederhergestellt werden konnten. Die sonstigen „Bewegungsdaten“ sind verschlüsselt und nicht mehr zugänglich.

Ob der Angreifer Daten ausgelesen hatte, konnte nicht festgestellt werden. IT musste vollständig ausgetauscht werden (hoher Schaden).

Datenschutzbehörde verlangte Warnmeldung an alle Mitglieder (Überwachen Sie die Kontobewegungen auf Ihren Privatkonten – erhebliche Unruhe).

---

## Fallbeispiel einer Datenpanne (2) – Phishing-Angriff

### Sachverhalt:

Ein Mitarbeiter eine Golfanlage erhält ein Mail mit dem Inhalt: „Sie haben ein e-Fax erhalten“ mit einem Link zu dem Fax. Der Mitarbeiter ruft den Link auf und gelangt auf eine (gut aussehende) Internetseite. Hier wird er aufgefordert, seine Windows-Zugangsdaten einzugeben. Der Mitarbeiter macht dies, erhält danach eine Störungsmeldung.

Kurze Zeit später meldet sich der Angreifer mit den erbeuteten Zugangsdaten im Mailprogramm des Mitarbeiters an, liest seine Kontakte aus und sendet vom Mailaccount des Mitarbeiters 500 Phishing-Mails an Kontakte des Mitarbeiters (intern und extern). Der Mailserver erkennt aufgrund seiner Sicherheitseinstellungen diese Serien-Mail und unterbricht nach 500 Mails die Sendung. Mailserver sperrt den Account automatisch und sendet Alert-Meldung an IT-Admin.

### Vorgehensweise/Feststellungen:

Meldung einer Datenpanne. Die IT-forensische Untersuchungen (Kosten !) ergaben, dass keine Daten ausgelesen wurden, sondern „nur“ Phishing-Mails versandt wurden. Ein direkter Schaden entstand nicht. Warnmeldung an die 500 Empfänger (intern und extern).  
Reputationsschaden!

# Allgemeine Beispiele

## Beispiel:

## Phishing-Mail (1)

mit Link zu einer  
URL „push-tan-de.app“

Sehr geehrter Kunde,

Aus unseren Kundenunterlagen geht hervor, dass Ihre S-PushTAN App-Registrierung bald abläuft. Aus Sicherheitsgründen müssen Sie ihre S-pushTAN-Verbindung regelmäßig aktualisieren. Nach der Aktualisierung können Sie wieder problemlos und sicher Ihre TANs empfangen. Ihre S-PushTAN App wird nach dem 06.03.2021 gesperrt und Sie müssen den Registrierungsvorgang erneut durchführen.

### Wie erneuere ich meine S-PushTAN App-Registrierung?

Erneuern Sie Ihre S-PushTAN App sofort, indem Sie den QR-Code rechts mit der Kamera Ihres Smartphones scannen. Gehen Sie dann die Schritte durch und schließen Sie die Registrierung ab. Sie können auch [hier](#) klicken!



Wir vertrauen darauf, dass wir Sie ausreichend informiert haben.

Mit freundlichen Grüßen  
Ihre Sparkasse

Domain oder IP-Adresse:

whois-Abfrageserver:

Abfrage starten

Gefundener whois-Eintrag von push-tan-de.app:

```
Using server whois.nic.app.  
Query string: "push-tan-de.app"  
  
Domain Name: push-tan-de.app  
Registry Domain ID: 45BB66898-APP  
Registrar WHOIS Server: whois.nic.google  
Registrar URL: http://www.key-systems.net  
Updated Date: 2021-02-22T21:40:40Z  
Creation Date: 2021-02-17T21:40:40Z  
Registry Expiry Date: 2022-02-17T21:40:40Z  
Registrar: Key-Systems LLC  
Registrar IANA ID: 1345  
Registrar Abuse Contact Email: abuse@key-systems.net  
Registrar Abuse Contact Phone: +49.68949396850  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferPr  
Registry Registrant ID: REDACTED FOR PRIVACY  
Registrant Name: REDACTED FOR PRIVACY  
Registrant Organization: Private Person  
Registrant Street: REDACTED FOR PRIVACY  
Registrant City: REDACTED FOR PRIVACY  
Registrant State/Province: Moscow  
Registrant Postal Code: REDACTED FOR PRIVACY  
Registrant Country: RU  
Registrant Phone: REDACTED FOR PRIVACY  
Registrant Fax: REDACTED FOR PRIVACY
```

## Recherche zu

## Phishing-Mail (1)

## Maileingang:

## Wie verhalten Sie sich?

Antworten Allen antworten Weiterleiten

Mi 10.03.2021 15:21



customer service <customer\_service@freightquote.com>

New Invoice(s) for C386493457 are Available to be Viewed

An Karl Wuerz



Your new Invoice(s) are available to be viewed.

The Attachments include the following Invoice(s):

Invoice Number	CHR Load Number
6076989103	386493457

Thank you for your business, if there are any issues with your Invoice(s) please contact your Sales Rep

\*\*\*\*\*  
This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this e-mail by mistake you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. Please note that any views or opinions presented in this email are solely those of the sender and do not necessarily represent those of the sender of the e-mail. The sender of the e-mail accepts no liability for any damage caused by the use of the e-mail transmitted by this email. (IP)  
\*\*\*\*\*

## Prüfung des Dateianhangs mit „virustotal.com“

The screenshot shows the VirusTotal interface for a file. A circular progress indicator shows 6 engines detected the file out of 62. The file hash is 555737271a58f1b566e2d15afb128ae37c8475923ef73d69480d047f40ed098e. The file size is 36.78 KB and it was scanned on 2021-03-10 at 14:34:46 UTC, 11 minutes ago. The file is identified as an attachment, download, macros, run-dll, and xlsx. The detection results are as follows:

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY <b>1</b>
Elastic		Malicious (high Confidence)		Fortinet VBA/Agent.VQX!tr
Ikarus		Win32.Outbreak		K7AntiVirus Trojan ( 00577a091 )
K7GW		Trojan ( 00577a091 )		McAfee-GW-Edition Artemis!Trojan

---

## Was sollten Sie unternehmen?

- Schulung aller Mitarbeiter: Vorsicht vor „kritischen“ Mails.  
Unbekannte Mail sofort löschen, ggf. IT-Beauftragten über Angriff informieren.
- IT-Sicherheitsstruktur auf aktuellem Stand halten!  
(Firewall, Virenschanner, Software für Server und Clients, Telefonanlage)
- Notfallkonzept erarbeiten und regelmäßig üben.
- Regelmäßige Datensicherungen des gesamten Bestandes.  
Eine Datensicherung sollte physikalisch vom Netz getrennt sein.
- Versicherung gegen Cyber-Angriff prüfen.
- **Anweisung an alle Mitarbeiter:**
  - Keinen unbekanntem Dateianhang öffnen.
  - **NIEMALS** Zugangsdaten oder Kontodaten eingeben.
  - Bei verdächtigen Zahlungsanweisungen telefonische Rückfrage bei der verantwortlichen Person.

## Fragen oder Anregungen?

