**Valkyrie IT-Solutions GmbH** für
Stefan Nagel—**TauRes Gesellschaft für Investmentberatung mbH**

04.09.2018
Band 1, Ausgabe 1

# Datenschutz für Fitnesstrainer

## WOFÜR IST DIESES INFORMATIONSSCHREIBEN?

Datenschutz spielt eine existenzielle Rolle um die eigene Sicherheit zu erhöhen.

In einem kurzen Überblick, erhalten Sie die Möglichkeit Ihre Daten, zumindest grundlegend zu schützen. Es handelt sich bei diesem Schreiben um eine Empfehlung welche wir, die Valkyrie IT-Solutions GmbH, direkt für Herrn Stefan Nagel erstellt haben.

Zielgruppe für dieses Informationsschreiben ist die Personengruppe der Fitnesstrainer und Personalcoaches, welche mit Kundendaten und Gesundheitsdaten auf Ihren eigenen Arbeitsgeräten Prozesse der Analysen und Auswertungen vollziehen.

Da es sich bei diesem Personenkreis um eine in der Regel allein agierende Unternehmerform handelt, ist die Durchführung der folgenden Schritte strikt zu empfehlen um eine mögliche Abmahnung zu vermeiden.

Bei weiteren, spezielleren Rückfragen können Sie sich gerne direkt an uns wenden, oder sprechen Sie den vortragenden Präsentationsgeber an. Dieser wird Ihre Fragen gerne weiterleiten.

Abschließend können wir Ihnen mitteilen, dass Newsletter und Informationsblätter dieser Art in unregelmäßigen Abständen neu erstellt und aktualisiert werden. Die DSGVO und der allgemeine Datenschutz sind keine Neuheiten, allerdings durch Präzedenzfälle und juristische Auslegungen immer wieder neu definiert werden. Die aktuelle Beschreibung passt dementsprechend auf die aktuelle Gesetzeslage und Definition der momentan vorhandenen Entscheidungen der Gerichtshöfe.

## WIE ERFÜLLE ICH DEN DATENSCHUTZ?

Datenschutz einzuhalten ist nur auf den ersten Blick etwas schwieriges und schwer nachzuvollziehendes.

Die letztendliche Einhaltung obliegt jeder durchzuführenden Kraft selbst und die Empfehlung einen Datenschutzbeauftragten um Hilfe zu bitten ist klar hervorzuheben.

Der Schutz der eigenen Arbeitsgeräte, insbesondere USB-Sticks, das eigene Notebook oder Tablets, mit welchen innerhalb der Coachings gearbeitet wird, ist die bindende Regel der Einhaltung dieser Richtlinien. Auf den folgenden Seiten finden Sie Tipps zur Durchführung des Datenschutzes.

## IN DIESEM HEFT



## THEMEN IN DIESER AUSGABE

- Schutz des eigenen Gerätes und Arbeitsplatzes
- Welche Maßnahmen gibt es noch zur Unterstützung?
- Benötige ich einen Datenschutzbeauftragten?
- Valkyrie IT-Solutions GmbH

## Sich selbst schützen.

Zum initialen Schutz und zur Erhöhung der Sicherheit gehört die Verschlüsselung der eigenen Windows- / Mac-Arbeitsgeräte. Unter Windows , insbesondere Windows 10, ist die Verschlüsselung der eigenen Festplatte und des BIOS ein sinnvoller und schnell durchzuführender Schritt. Diese dienen der Prävention des Diebstahls oder Fremdzugriffes auf eben diese.

*Die exakte Durchführung der Verschlüsselung entnehmen Sie bitte dem Anhang, in welchem wir Ihnen mit Screenshots Möglichkeiten für diese aufzeigen.*

Eine Verschlüsselung der Festplatte bedarf ebenfalls einem erhöhten Eigenmaß an Verantwortung, da diese einen Schlüssel generiert, welcher bis zum Austausch des Gerätes an MEHREREN Orten sicher aufbewahrt werden sollte. Ohne diesen Schlüssel, ist die Festplatte unbrauchbar!

Ein weiterer Schritt zur Erhöhung der Sicherheit ist bei unterstützenden Notebooks die Funktion des Fingerabdruckes zur Legitimierung zu nutzen. Nutzen Sie ein Kennwort, sollte Sie zur Einhaltung der Sicherheit eben dieses in einem 90-Tage-Rhythmus ändern. Dies gewährleistet einen reibungslosen Betrieb ohne Einschränkungen.

Bei der Nutzung von Mac-Geräten empfiehlt es sich alle 30-60 Tage das Apple-ID-Kennwort zu ändern, da es sich um Multi-Device-Accounts handelt!

*“Kennwortänderungen sind eine Pflicht zum Schutz der Daten, auch wenn nur Sie alleine das Kennwort kennen.”*

### WAS IST EIN CRM?

Ein CRM (Customer Relationship Model oder Contact Ressource Management) ist normalerweise ein Programm zur Verwaltung der Kundenbezogenen Daten und zur Verwaltung eines gesamten Kundenstammes.
Viele Programme dieser Art bieten ebenfalls die Möglichkeit Rechnungen und/oder angeforderte Dienstleistungen direkt in diesen abzurufen und zu speichern.

Die Verwaltung der Kundendaten wird durch neue Standards ebenfalls mit einer Exportfunktion ausgestattet sein, welche auf Anfrage eines Kunden direkte Auskunft über die genutzten und gespeicherten Stammdaten bietet.

Empfehlungen dieser Programme können Pauschal nicht gegeben werden, da jeder einzelne Unternehmer andere Anforderungen an diese hat.

## Nutzen Sie ein vertrauensvolles CRM!

Durch die Nutzung eines CRM-Programmes können Sie Ihre eigene Produktivität und Sicherheit erhöhen. Aufgrund eines LogIns mit einem Kennwort, dem speichern der Daten zum Beispiel in einer deutschen Cloud, haben Sie ebenfalls die Möglichkeit eine exakte Auskunft über den Standort Ihrer gespeicherten Daten zu geben.

Die Auskunftspflicht eines jeden „Speichernden“ auf Anfrage eines Kunden ist, wie bereits erwähnt, eine Verpflichtung und muss durchgeführt werden. Die Suche nach den Speicherorten bei der Verwaltung durch einzelne Textdokumente und Emails ist wesentlich schwieriger, als die kurze Kontrolle der Daten innerhalb des CRMs.

Es existieren wenige empfehlenswerte Alternativen zu einem gut funktionierenden Programm dieser Art. Von einer Arbeit mit Einzelsammelstellen ist jedoch von vornherein abzuraten aufgrund der schlechten Verwaltung und der niedrigeren Standhaltung gegenüber einer Prüfung.

Minimierung des Papiermanagements und Erbringung eines papierlosen Umganges mit Kundendaten wäre das Ziel einer CRM-Einführung. Eine Sammlung von Verträgen und das Verwalten sämtlicher Kundenbezogener Daten sollte der Schwerpunkt der eigenen digitalen Arbeit sein. Es stellt sicher, das Sie keine für andere Personen zugänglichen Dokumente lagern oder Gefahr laufen durch die Sichtung dritter. Für die Verarbeitung von Rechnungen und Dienstleistungsunterlagen bieten sich ebenfalls zahlreiche Möglichkeiten, welche durch Ihre branchenspezifische Nutzung jedoch einem gewissen Maß an Eigeninitiative und/oder Recherchegeschick erforderlich sind. Suchen Sie sich die für Sie passende Lösung!

Viele Dienstleister und Anbieter bewerben Ihr Produkt, verständlicher Weise, als das Beste und Einfachste auf dem Markt. Es ist jedoch empfehlenswert die Testphasen solcher Produkte zu nutzen um eben diese kennen zu lernen. Doch seien Sie vorsichtig wo und wie Sie Ihre Daten hochladen oder speichern, einige Programme weisen bereits in Ihren Vertragsgrundlagen auf die Standorte der Rechenzentren (Beispielsweise im Ausland) hin, andere geben solche Informationen nur auf Anfrage heraus!
Die Auslagerung von Kundenbezogenen Daten sollte, nach Möglichkeit, in ein in Deutschland stationiertes Rechenzentrum erfolgen, über welches das deutsche oder europäische Territorialgesetz herrscht. Anhand dieses Gesetzes sind die Daten einer gewissen Konformität unterlegen. Näheres hierzu erfragen Sie bitte bei Ihrem Datenschutzbeauftragten.

*Übergabe einer Broschüre oder eines Flyers darf nur auf Zustimmung geschehen!*

# Wie schütze ich meinen Arbeitsplatz?

Der Schutz des Arbeitsplatzes spielt eine große Rolle durch die Eventualität der öffentlichen Zugänge. Was bedeutet das für mich?
Es bedeutet, dass der eigene Arbeitsplatz ebenfalls stark geschützt werden muss. Dies vermag dem ersten Anschein nach drastisch zu klingen, ist allerdings eine klare Empfehlung zur Vermeidung von Problematiken.

Ihr Arbeitsplatz, auch wenn dieser bei Ihnen im eigenen Haus liegt, ist eine potentielle Schwachstelle für den Datenschutz. Lassen Sie keine Papiere offen liegen, betreiben Sie Ihren Drucker über eine Kabelverbindung statt über WLAN und bewahren Sie Festplatten und USB-Sticks nur in einem Abschließbaren Raum auf. Wenn Sie eine NAS nutzen, schauen Sie nach, ob Ihr Hersteller eine Festplattenverschlüsselung auf dieser unterstützt und lagern Sie sie in einem sicheren Raum. Ein Anschluss einer NAS aus einem Nebenraum ist technisch gesehen, kein großer Aufwand. Er bedarf lediglich (bei Netzwerkfähigen NAS-Speichern) eines längeren Netzwerkkabels (Cat. 5e und Cat. 6 mit RJ45-Anschlüssen) zur Verbindung..

Man sollte auch darauf achten, dass Bildschirme oder andere Geräte die Kundendaten darstellen so aufgestellt sind, dass kein Fremder diese zu sehen bekommt. Dazu zählt das Bildschirme/Beamer oder ähnliche Geräte, nicht offen am Fenster zu sehen sind wenn diese betrieben und genutzt werden. Es bietet sich hier an  Gardinen oder Vergleichbares anzubringen, welche die Sicht behindern aber dennoch Licht hindurchlassen.

Ein weiterer Schritt zur Erhöhung der Sicherheit ist die Zugangskontrolle. Stellen Sie sicher das die Tür zu Ihrem Büro immer verschlossen ist wenn Sie dieses verlassen und sperren Sie Ihren Bildschirm. Viele Fälle von Verstößen beruhen auf diesen Fehlern und sind eine stark, angreifbare Quelle.

Der Schutz des Arbeitsplatzes wird schnell zur Routine und bietet Ihnen eine ruhige Lage innerhalb der Möglichkeiten. Seien Sie gewissenhaft! Sobald Sie sich selbst an den Grundsatz des Schutzes der Daten halten, Fallen viele Probleme automatisch weg. Unser Tipp, stellen Sie sich folgende Fragen:

Habe ich offensichtlich liegende Daten auf meinem Schreibtisch?
Ist meine Dokumentenablage abschließbar?
Benötige ich dieses Dokument überhaupt in Papierform?
Ist mein Monitor sichtgeschützt? Ist er gesperrt? Habe ich einen Passwortschutz?
Wer hat Zutritt  zu meinem Büro? Müssen diese Personen Zutritt dazu haben?

## ERLAUBNIS ZUR VERARBEITUNG DER DATEN EINHOLEN

Sie verarbeiten Kundendaten in Ihrer Finanzbuchhaltungssoftware, und haben die Erlaubnis des Kunden dazu eingeholt?

Super!

Sie haben  die Erlaubnis des Kunden noch nicht eingeholt?

Abmahnung möglich!

Seit längerem, und das schon vor dem vollen Inkrafttreten der DSGVO, gilt es beim Kunden eine Erlaubnis einzuholen seine Daten auch verarbeiten zu dürfen.

Hierzu muss vom Kunden ein Dokument ausgefüllt werden, der Vertrag zur Auftragsverarbeitung.

Ein Musterformular zu diesem finden Sie unter: https://www.datenschutzzentrum.de/dsgvo/

---

Es existieren und kursieren nun vermehrt Begriffe im Unternehmerkreise, welche Double-Opt-In und Opt-In genannt werden. Diese bezeichnen die Einholung der oben beschriebenen Erlaubnis. Mit einem Double-Opt-In (Also der doppelten Bestätigung), gehen Sie, wenn zulässig, auf Nummer sicher.

Sprechen Sie Ihren Zuständigen oder Datenschutzbeauftragten auf diese Möglichkeiten an.

---

Häufig wird die Frage gestellt, welche Möglichkeiten zur eigenen Werbung ein Unternehmer oder eine Firma noch hat, diese Frage stellt sich als juristisch schwierig dar und sollte aufgrund der Datenverarbeitung mit einem Anwalt und/oder Datenschutzbeauftragten besprochen werden, diese können Ihnen auch Tipps zum „sauberen Direktmarketing“ geben.

## WOHER SOLL ICH WISSEN WELCHE MAßNAHMEN ICH DÜRCHFÜHREN MUSS?

Die Antwort ist kurz und knapp:
Sie können es nicht wissen!

Die aktuellen der Berichte der Rechtsanwälte und Datenschutzbeauftragten sind eindeutig:
Viele Nutzer und Firmen haben an vieles gedacht, allerdings nicht an alles.
Dies ist auch kaum möglich. Darum raten wir Ihnen an, suchen Sie sich einen Datenschutzbeauftragten zur Vermeidung von Schwierigkeiten.

---

Es ist natürlich schwierig abzuschätzen welche Maßnahmen man in seinem Unternehmen durchführen muss um DSGVO Konform zu sein.

Sie können sich aber bestmöglich vorbereiten indem Sie die Hinweise und Fragen auf folgender Website durcharbeiten:

https://
www.datenschutzzentrum.de/
artikel/1178-.html

---

Viele Behörden geben Ihnen ebenfalls Auskunft über mögliche Unterstützung und die Zahl der Datenschutzbeauftragten wächst stetig. Einen passenden zu finden, sollte kein Problem mehr darstellen.

# Der goldene Schlüssel

Es gibt zahlreiche Tools und Gadgets welche Sie dabei unterstützen können die Funktionalität zu gewährleisten. Gerade im Bezug auf die Sicherheitsaspekte sind die Hilfsmittel von großer Bedeutung. Im Folgenden erhalten Sie einen Einblick zu den kleineren Gerätschaften, welche Ihnen viel Ärger ersparen können.

Yubicos YubiKey 4—eine einfache Hilfe für LogIn und Passwortlänge.
Der YubiKey ist ein kleines, USB-Stick artiges Gerät, welches über die USB-Schnittstelle mit dem PC verbunden werden kann. Er dient der Erweiterung Ihres Sicherheitsportfolios im Bezug auf die Komplexitöt der LogIn-Passwörter. Auf dem Stick ist ein Hardware-Encrypted-Password welches 128-bit AES (dies bezeichnet die Länge und Komplexität des Kennwortes) unterstützt. Es sind Eigenschaften welche für ein sicheres Kennwort notwendig und grundlegend sind. Diese Sticks sind somit, nach korrekter Anwendung, ein notwendiges Tool für den Zugriff auf Ihr Notebook. Im Falle des Diebstahls oder eines Abhandenkommens Ihres Notebooks, ist die Verwendung einer Festplattenverschlüsselung, die Nutzung des Sticks für den Zugang zu bestimmten Programmen und das Festlegen eines BIOS Kennwortes eine hervorragende Grundausstattung!
Vorsicht: Benutzen Sie den Stick nicht für Windows-Anmeldung, separieren Sie das Kennwort von denen der Anwendungen!

*Lassen Sie Ihre Technologien nicht veralten!*

# Zwei-Faktor-Authentifizierung

Von einigen Videospielen, Internetplattformen oder besonderen Anwendungen wie Banking, kennen Sie sie vielleicht schon die Zwei-Faktor-Authentifizierung.
Dieses Verfahren zur Sicherheitssteigerung beschreibt die Einbindung eines „Key-Generator-Programms“ zur Erstellung von zeitgebundenen Kurzzeitschlüsseln für die Anmeldung und Nutzung von Programmen. Einige CRMs und Online-Anwendungen (Cloud -gelagert) unterstützen das Verfahren und steigern somit exponentiell Ihre Sicherheit. Bitte beachten Sie, dass die Wiederherstellungsschlüssel für diese „Doppel Authentifikation“ ebenfalls an mehreren Orten aufbewahrt werden sollten. Die Wenigsten bieten Ihnen die Möglichkeit einer „Passwort Wiederherstellung“ via Email oder Telefon.

Einige Möglichkeiten für dieses Verfahren:

Google Authenticator

One Identity Defender

Duo.com

Hardware Geräte

# Biometrische Authentifizierung

Der Vorteil der Biometrischen Authentifizierung liegt klar auf der Hand, Sie selbst sind der Schlüssel.

Wem vertraut man mehr als sich selbst? Aufgrund dieser Frage und der Unikat-Lösung des biologischen Prinzips sind die Biometrischen Authentifizierungen eine sichere Möglichkeit für die Anmeldung und Nutzung Ihres Arbeitsgerätes. Ob Sie sich mit Ihrem Fingerabdruck registrieren, Ihr Notebook oder Ihr Smartphone mit dem Gesicht entsperren, oder mehrere tausend Euro für einen Retina-Scanner benutzen möchten, ist sicher Ihre eigene Entscheidung, aber die Möglichkeiten für eine Körperbasierte Entsperrung sind sehr vielfältig.

Viele Sicherheitsfirmen und Labore nutzen diese Zugangsmethoden zur Vermeidung von Fehlzutritten oder dem allgemeinen Ausschließen von Unbefugten. Es schenkt einem eben nichts mehr Sicherheitsgefühl, als zu wissen, dass der Schlüssel nicht verloren gehen kann. Außer Ihr Fingerabdruck geht bei fehlerhafter Gartenarbeit verloren—davon ist abzuraten.

Dennoch gilt, seien Sie sich nicht zu sicher! Die Änderung von Kennwörtern und der Wechsel des Fingerabdruckes nach einer ausreichenden Zeit ist immer zu empfehlen um Fälschungen zu vermeiden. Die Kriminologie hat gezeigt, das Fälschen eines Fingerabdruckes wird immer leichter!

# Musterentsperrung und Smartphone-Schutz

Man kann es nicht bestreiten, die Smartphones sind unser ständiger Begleiter und der mit Abstand wichtigste Helfer im Alltag. Bereits im Jugendalter erhält der Nachwuchs heutzutage ihr erstes Gerät, welches Stück für Stück immer mehr integriert wird. In die allgemeine Kommunikation, den Zeitvertreib mit Spielen oder zum Austausch von Daten und Dateien.
Diese Geräte zu schützen und vor fremden Zugriffen zu sichern ist also zwingend notwendig und ein sehr oft vernachlässigtes Thema.

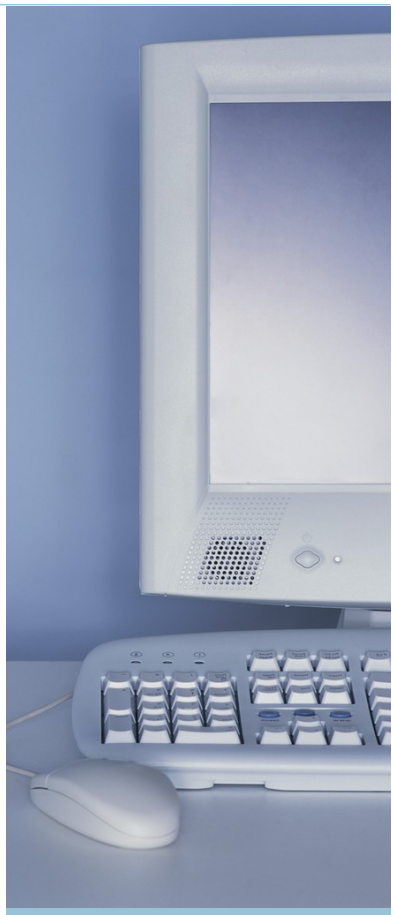
Welche Methode zur Entsperrung meines Gerätes sollte ich nutzen?

Diese Frage ist einfach und schwer zugleich!
Pauschal gilt allerdings:
Nutzen Sie ein langes und komplexes Kennwort zur Anmeldung am Gerät (nicht die SIM-PIN)
Nutzen Sie KEINE Musterentsperrung, diese sind schnell nachzuvollziehen durch Spuren
Nutzen Sie Biometrische Möglichkeiten wenn Ihr Smartphone diese unterstützt
Nutzen Sie Kombinationsmöglichkeiten aus mehreren Schichten der Sicherheit.

Erläuterung zu den Schichten:
Wenn Sie beispielsweise eine Gesichtserkennung nutzen, richten Sie zusätzlich ein Passwort ein.

*“Die Durchführung des allgemeinen Datenschutzes ist nicht als Problem zu betrachten, sondern als Präventionsmaßnahme mit ständiger Eigenkontrolle.”*

# Warum also noch einen Datenschutzbeauftragten?



Alle Informationen die Sie diesem Schreiben entnehmen können, sind reine Empfehlungen. Die Durchführung dieser Schritte sollte dennoch immer durch einen, für Ihren Bereich geeigneten Datenschutzbeauftragten geprüft und genehmigt werden.
Der Datenschutz ist eine auf Prüfungen basierende Angelegenheit, welche in der Verpflichtung der Einhaltung begründet ist. Nur ein solcher, welcher mit seiner eigenen Person und seinem Unternehmen haftet, hat die Befugnis Ihnen die Bestätigung der Einhaltung zu geben. Eine Befragung und/oder Beauftragung eines Datenschutzbauftragten ist also gerade im Bereich des Gesundheitswesens und dem häufigen Umgang mit Kunden eine empfehlenswerte Unternehmung.

Bei Fragen diesbezüglich oder dem Wunsch nach einem Kontakt hilft Ihnen die zuständige Behörde oder ein vertrauter Rechtsanwalt. Gerne können wir Sie ebenfalls bei der Suche nach einem geeigneten Partner unterstützen. Durch zahlreiche Kontakte und ein ausgiebiges Netzwerk haben wir die nötigen Mittel Sie zu beraten.

Verlassen Sie sich nicht ausschließlich auf unsere Tipps und Empfehlungen zur Vermeidung einer Abmahnung!

Durch die DSGVO werden lediglich bereits existierende Regelungen erneut bekräftigt und die Durchführung gefördert. Die Datenschutzregelungen sind bereits seit mehreren Jahren in Kraft und eine „neue Gesetzeslage“ ist es im Grunde genommen nicht.

Aufgrund dieser Fakten und Tatsachen sollten Sie bei der Suche nach einem geeigneten Datenschutbeauftragten ebenfalls auf einen Ihnen zusagenden Partner zählen. Die Häufigkeit der Prüfung und Unterstützung eines Beauftragten obliegt der Komplexität Ihres Unternehmens und der Häufigkeit der von Ihnen getätigten kundenbezogenen Tätigkeiten.

**Was kann ich tun wenn ich mich falsch aufgehoben fühle?**

Der Wechsel eines Datenschutzbeauftragten ist ohne Probleme möglich! Sie können sich jederzeit neu orientieren .

**Gibt es Zuschüsse vom Staat?**

Ja! Es gibt zahlreiche Möglichkeiten Zuschüsse zu erhalten und auch kostenlose Unterstützung zu erlangen. Informieren Sie sich diesbezüglich bei Ihrer zuständigen Behörde.

## Valkyrie IT-Solutions GmbH

Nah, regional und verständlich. Wir sprechen eine klare Sprache der IT und unterstützen klein- und mittelständische Unternehmen. Interesse geweckt? Dann kontaktieren Sie uns gerne! Wir sind für Sie erreichbar!

Mit unseren zahlreichen und starken Partnern können wir Ihnen bei Ihren Datenschutzfragen behilflich sein und unterstützen Sie gerne bei der Suche nach einem passenden Partner!

Sollten Sie ebenfalls Fragen haben zum Aufbau einer modernen IT-Struktur, der Modernisierung Ihrer IT-Einrichtung oder der Betreuung durch ein professionelles IT-Unternehmen haben, sprechen Sie uns gerne an.

# Unsere Leistungen

- Server und Client Betreuung
- Einrichtung von Backuplösungen
- Erstellung von Storagelösungen
- Support von VOIP – Telefonanlagen
- Support von Microsoft Office Lösungen
- Wartung und Erneuerung von Netzwerken
- Einrichtung von Firewalls
- Support von Konferenzsystemen
- Verkauf von Hard- und Softwarelösungen
- Beratung und Schulung von Mitarbeitern
- Erstellung und Pflege von Dokumentationen
- Beratung bei Netzwerk-Infrastruktur


## Valkyrie IT-Solutions GmbH

Oststraße 86
22844 Norderstedt

Telefon: 0171 16 555 00
E-Mail: info@valkyrie-it.de
Website: www.it-norderstedt.de

Ansprechpartner:
**Cedric Rahlff** (Geschäftsführung)
**Patrick Oswald** (Geschäftsführung)


**WIR FREUEN UNS AUF IHRE KONTAKT-ANFRAGE!**

VALKYRIE

IT-SOLUTIONS