

SIE TRAGEN DIE VERANTWORTUNG.  
WIR STEHEN IHNEN MIT SICHERHEIT ZUR SEITE.



SICHERHEIT FÜR  
FAMILY OFFICES

# 1. SICHERHEITSANFORDERUNGEN FÜR EIN FAMILY OFFICE

Das Family Office ist der verlässliche und vertrauenswürdige Partner für Vermögensinhaber. Ein professionelles Family Office kümmert sich nicht nur um die finanziellen Anlagen und Immobilien, sondern häufig auch um persönliche Belange der Familie. Sie haben deshalb umfangreiches Wissen über sensible Bereiche, persönliche Daten, Termine, Kontakte und selbstverständlich die finanziellen Angelegenheiten der Vermögensinhaber. Dieses Know-how gilt es zu schützen. Darüber hinaus ist es genauso wichtig, die Verlässlichkeit von Geschäftspartnern und Angestellten im unmittelbaren Umfeld sicherzustellen sowie die persönliche Sicherheit der Family Office Mitarbeiter, der Vermögensinhaber und aller Familienangehörigen durch entsprechende Schutzvorkehrungen zu gewährleisten.

Das Risiko für vermögende Personen ist seit jeher groß, aufgrund der finanziellen Situation und der Bekanntheit in den Focus von Kriminellen zu geraten. Dadurch entstehen auch Risiken für das Family Office, direkt oder mittelbar als Angriffsziel ausgewählt zu werden.

Durch die mediale Berichterstattung oder Veröffentlichungspflichten in Registern erhöht sich nicht nur die öffentliche Wahrnehmung, sondern auch die Verfügbarkeit von sensiblen personenbezogenen Daten. Das Internet, öffentlich zugängliche Datenbanken oder entsprechende Magazine bieten jedermann die Möglichkeit, vermögende Personen ohne großen Aufwand umfangreich aufzuklären. Dazu zählen auch Geburtsdaten, Wohn- und Geschäftsadressen, Einkommen, finanzielle Verhältnisse sowie Bilder von Personen oder Gebäuden.

Die meisten kriminellen Angriffe werden langfristig geplant und von den Tätern professionell vorbereitet. Das Risiko besteht dabei nicht nur am Sitz des Family Office bzw. dem Wohnort der Vermögensinhaber, sondern verstärkt auch bei Fahrten mit dem Pkw, regelmäßigen Terminen oder auf Reisen.

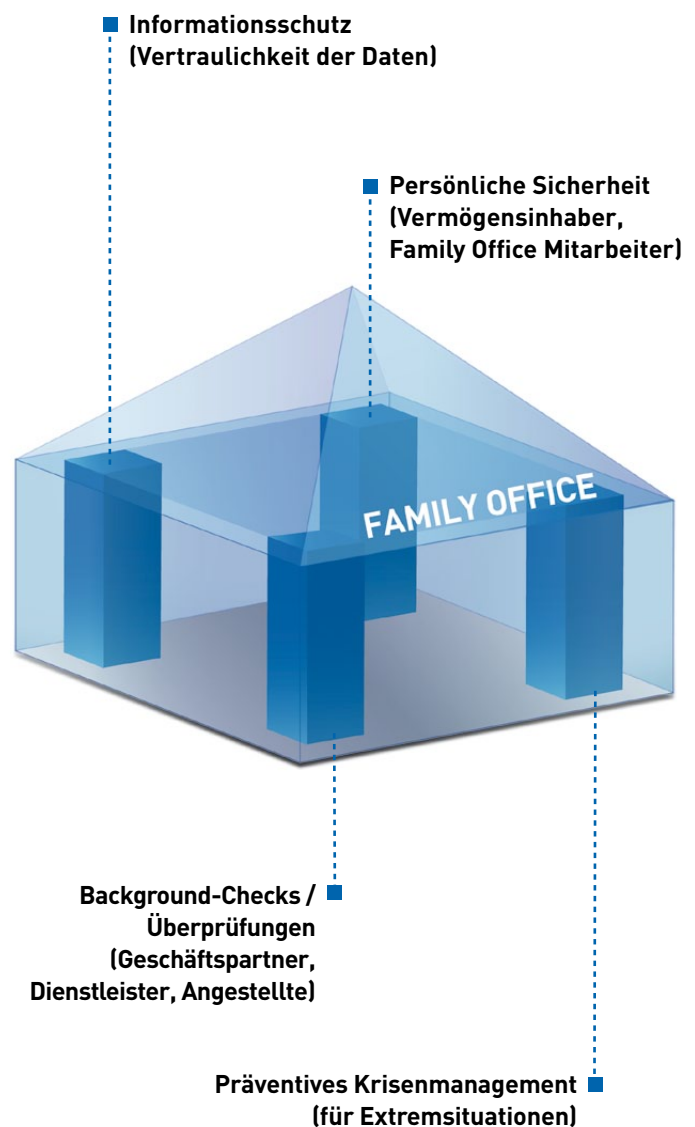
Für das Family Office und die Vermögensinhaber drohen dabei verschiedene kriminelle Angriffsformen:

- **Einbruch in Büroräume, Privatanwesen oder Fahrzeuge**
- **Überfall am /im Büro, Privatanwesen, Pkw oder auf Geschäftsreisen**
- **Datendiebstahl durch Hacker, Sniffer oder Social Engineering**
- **Datenverlust durch leichtfertigen Umgang mit Informationen bzw. dem IT-Equipment, auch bei Geschäftspartnern**
- **Erpressung mit sensiblem Wissen bzw. durch kompromittierende Informationen**
- **Entführung von Vermögensinhabern, Family Office Mitarbeitern oder Familienangehörigen**
- **Stalking**

Geschäftspartner und Angestellte im unmittelbaren Umfeld sollten in jedem Fall den hohen Ansprüchen und Erwartungen des Family Office bzw. der Vermögensinhaber an Zuverlässigkeit, Seriosität und Vertraulichkeit entsprechen. Sie sollten daher im Vorfeld von Geschäftsbeziehungen oder einer Anstellung entsprechend überprüft werden, um vor unliebsamen Überraschungen gefeit zu sein.

Um die Sicherheit der Vermögensinhaber und Family Office Mitarbeiter gewährleisten zu können, sollten die Verantwortlichen auf zuverlässige Partner mit professionellem Know-how setzen.

Die wesentlichen Säulen der Sicherheit für ein Family Office umfassen:



NIEMAND WILL EIN RISIKO EINGEHEN.  
DOCH EINER MUSS IMMER DIE VERANTWORTUNG ÜBERNEHMEN.



## 2. LEISTUNGEN



### Informationsschutz

Ein Großteil der Daten in einem Family Office sind als höchst sensibel einzustufen. Die Informationen über persönliche und finanzielle Verhältnisse könnten bei Verlust ein hohes Risikopotenzial für verschiedene kriminelle Angriffe in sich bergen und einen erheblichen Reputationsschaden bewirken. Daten können jedoch nicht nur aus Unachtsamkeit an die Öffentlichkeit gelangen, sie können auch im Focus von gezielten Angriffen stehen. Es ist deshalb wichtig, entsprechend umsichtig mit ihnen umzugehen und sie mit den optimal aufeinander abgestimmten technischen Komponenten zu schützen. Der Informationsschutz muss dabei sowohl den Schutz gegen Angriffe von außen als auch die Gewährleistung der Vertraulichkeit von Informationen intern und beim Datenaustausch mit Geschäftspartnern umfassen.

Der Informationsschutz bei einem Family Office sollte folgende Maßnahmen umfassen:

- **Strukturierte Planung der Datensicherheit für die Gewährleistung der Vertraulichkeit von Informationen**
- **Einsatz von IT- und Telekommunikationskomponenten (Hard- und Software) mit hohem Sicherheitsstandard, zum Schutz gegen Hacker und Sniffer**
- **Gewährleistung einer sicheren Kommunikation (Verschlüsselung)**
- **Monitoring der internen Datenflüsse (Alert-System bei ungewöhnlichen Zugriffen)**
- **Awareness-Schulungen der Mitarbeiter für den Umgang mit vertraulichen Daten (Risiko durch Social Engineering, technische Angriffsmöglichkeiten oder beim Datenaustausch mit Geschäftspartnern)**
- **Regelmäßige Revision der IT- und TK-Administration unter Sicherheitsaspekten**
- **Evaluierung der Datensicherheit bei Geschäftspartnern**
  - **Vorgaben vor der Aufnahme von Geschäftsbeziehungen**
  - **Regelmäßige Audits im Laufe der Geschäftsbeziehung**
- **Regelmäßiges Monitoring der Recherchierbarkeit persönlicher bzw. personenbezogener Daten im Internet bzw. in öffentlichen Registern**
- **Maßnahmen zur Löschung bzw. Beschränkung ungewünschter Datenverfügbarkeit**



### Persönliche Sicherheit

Die Persönliche Sicherheit der Vermögensinhaber und Family Office Mitarbeiter sollte bei allen Schutzmaßnahmen an erster Stelle stehen, gerade weil das Family Office häufig nicht nur für die Betreuung des Vermögens verantwortlich ist, sondern auch für die Sicherheitsbelange der Vermögensinhaber. Auch hier müssen entsprechende Sicherheitsvorkehrungen getroffen werden. Professionelle Täter versuchen in der Regel, ihre Taten generalstabsmäßig vorzubereiten und spionieren dazu ihre Ziele lange vor der eigentlichen Tat aus. Erst wenn die Kriminellen die Gewohnheiten kennen und genau wissen, ob Alarmanlagen im Einsatz sind, welche Fahrzeuge und Strecken regelmäßig benutzt werden, zu welcher Uhrzeit Angestellte kommen oder gehen bzw. welche Regelmäßigkeiten einen Überfall, Einbruch oder eine Entführung erleichtern würden, beginnt die detaillierte Planung der Tat. Ein professionelles Aufklärungskonzept (K 106) durch Sicherheitsspezialisten, zur umfangreichen Voraufklärung genau dieser Vorbereitungsmaßnahmen, kann solche Taten verhindern. Die Family Office Mitarbeiter sollten durch entsprechende Trainings ebenfalls sensibel für Auffälligkeiten im Umfeld sein.

Die Persönliche Sicherheit ist als ganzheitliche Aufgabe zu verstehen. Der Objektschutz kann dabei eine genauso wichtige Rolle spielen, wie Schulungen zum sicherheitsgerechten Verhalten, persönliche Schutzausrüstung (z.B. Notrufdrücker) oder die entsprechenden Sicherheitsvorkehrungen bei Geschäftsreisen in kritische Länder.

Entsprechende Sicherheitsvorkehrungen zur Gewährleistung der Persönlichen Sicherheit sollten sein:

- **Schulungen / Trainings zum sicherheitsgerechten Verhalten**
- **Hoher Objektsicherheits-Standard im Family Office bzw. privaten Bereich (Zutrittssicherung, Alarmanlage, Videoüberwachung, Schlüsselmanagement etc.)**
- **Mobile Notrufdrücker für eine sofortige Alarmmeldung bei kritischen Situationen**
- **Sicherheitshinweise vor Auslandsreisen**
- **Planung von Reisen in sicherheitskritische Länder**
- **Spezielle Ortungssender und Monitoring-Systeme für Reisen**
- **Sondergeschützte Fahrzeuge im Bedarfsfalle**
- **Schutz durch Voraufklärungsmaßnahmen (K 106) im Bedarfsfalle**



## Background-Checks / Überprüfungen

Seriosität und Zuverlässigkeit sind elementare Grundvoraussetzungen einer erfolgreichen Geschäftsbeziehung. Daher gehört auch die präventive Abklärung von neuen Geschäftspartnern zu den Sicherheitsaufgaben eines Family Office. Nicht nur im Vorfeld von Geschäftsreisen ins Ausland sollten potenzielle Kontaktpartner überprüft werden, sondern generell bei allen Engagements mit neuen, bisher unbekanntem, Unternehmen. Ein Background-Check sollte sich sowohl auf das Unternehmen selbst als auch auf die Verantwortlichen erstrecken, um unliebsamen Überraschungen aus dem Weg zu gehen. Für eine umfangreiche Due Diligence im Vorfeld einer Akquisition oder eines finanziellen Investments können Überprüfungen durch Sicherheitsspezialisten wertvolle Hinweise auf das Unternehmen oder die handelnden Personen liefern. Background-Checks sollten auch bei neuen Bewerbern für das Family Office sowie bei Angestellten im unmittelbaren Umfeld der Vermögensinhaber, also auch bei Hausangestellten oder externen Beratern, durchgeführt werden.

Damit gewährleistet werden kann, dass nur eine Geschäftstätigkeit mit zuverlässigen Geschäftspartnern aufgenommen wird bzw. nur loyale und unbescholtene Personen im engeren Umfeld tätig sind, sollten folgende Überprüfungen bzw. Background-Checks durchgeführt werden:

- **Sicherheitsrelevante Überprüfung im Vorfeld von neuen Geschäftsbeziehungen**
- **Intensive Abklärung der Unternehmung bzw. Gesellschaft**
- **Background-Check zu den handelnden Personen**
- **Spezielle Prüfung der Zuverlässigkeit von eingesetzten Dienstleistern**
- **Psychologischer Integritätstest bei der Auswahl von neuen Mitarbeitern**
- **Background-Check bei Angestellten im direkten Umfeld der Vermögensinhaber**



## Präventives Krisenmanagement

Sämtliche Sicherheitsvorkehrungen sind dazu gedacht, einen möglichst dezenten und unauffälligen Schutz für das Family Office sowie die Vermögensinhaber zu errichten. Für den Ernstfall eines kriminellen Übergriffs sollten jedoch entsprechende Vorkehrungen getroffen worden sein, um schnell reagieren zu können. Für solche Krisenfälle ist es erforderlich, dass es bereits Handlungsanweisungen für realistische Schadensszenarien gibt, eine Krisen-Hotline zu Sicherheitsspezialisten besteht, ein Krisenstab etabliert wurde und entsprechende Datenblätter oder persönliche Dossiers angelegt wurden. So treffen Sie die beste Vorsorge, dass ein Übergriff ohne Schaden für Leib oder Leben der betroffenen Personen endet.

Für ein Präventives Krisenmanagement empfiehlt Corporate Trust:

- **Krisen-Hotline für die permanente Erreichbarkeit von Sicherheitsspezialisten (24/365)**
- **Handlungsanweisungen für entsprechende Sofortmaßnahmen bei realistischen Krisen-Szenarien (Überfall, Datenklau, Illoyaler Geschäftspartner, Durchsuchung, Entführung, Erpressung etc.)**
- **Informationsaufbereitung im Vorfeld (Persönliche Dossiers, Erreichbarkeiten, Kontakt- bzw. Ansprechpartner, etc.)**
- **Aufbau und Training eines Krisenstabs**

## 3. TYPISCHE VORGEHENSWEISE

Um den Sicherheitsanforderungen eines Family Offices effektiv und professionell gerecht werden zu können, braucht es einen leistungsstarken Sicherheitspartner, der sich flexibel auf die jeweiligen Geschäftsprozesse einstellt und die Maßnahmen individuell anpasst – nicht umgekehrt. Die Optimierung der Sicherheitsvorkehrungen beginnt damit, dass wir Ihr Family Office und die Geschäftsprozesse verstehen lernen. Aus Ihrem individuellen Bedarf an Sicherheit ergeben sich die Ziele und Maßnahmen.

**Einige typische Vorgehensweisen bei der Implementierung von Maßnahmen sind:**

### ■ Gewährleistung der Datensicherheit im Family Office

Analog einem Chief Information Security Officer (CISO) bei großen Unternehmen planen und überwachen wir die Einhaltung der IT- und Telekommunikationssicherheit im Family Office. In einem speziell darauf zugeschnittenen Audit erfassen wir detailliert die Schwachstellen für Informationsabflüsse. Dabei sind wir in der Regel drei Tage vor Ort und analysieren die eingesetzten technischen Komponenten, die Prozesse für das Daten-Handling, die bauliche Sicherung und die Vorkehrungen beim Datenaustausch mit Geschäftspartnern. Auf Grundlage dieses Audits erstellen wir dem Family Office ein strukturiertes Konzept für die Sicherung der sensiblen Daten. Dies beinhaltet, dass wir die Implementierung von entsprechenden baulichen und/oder technischen Komponenten für einen hohen IT-Sicherheitsstandard planen und umsetzen, uns um die Verschlüsselung der sensiblen Kommunikation (Email, Fax, Telefon) kümmern und in einem 1-Tages-Training die Mitarbeiter zu gesteigerter Awareness für Informationsschutz schulen. Außerdem werden regelmäßig die IT- und Telefonanlagen-Konfigurationen nach Auffälligkeiten überprüft (Revision der eingesetzten Dienstleister / Administratoren).

### ■ Sicherheit beim Datenaustausch mit Geschäftspartnern

Wir erstellen Ihnen ein Regelwerk für die Datenverarbeitung zur Vorgabe für Geschäftspartner. Dies beinhaltet nicht nur Vorgaben zur Kommunikation, sondern auch zur Speicherung und der internen Weitergabe von Daten. Um die Sicherheit der sensiblen Informationen gewährleisten zu können, überprüfen wir bei Bedarf im Vorfeld der neuen Geschäftsbeziehung mit einem Kurz-Audit den Partner zu seinen Sicherheitsvorkehrungen. Im Laufe der Geschäftsbeziehung gibt es standardisierte und regelmäßige Prüfungen beim Partner, ob die Standards eingehalten werden. Diese Audits nützen auch dem Geschäftspartner, nachhaltig eine hohe Daten- und Informationssicherheit zu erlangen.

### ■ Objektsicherheit

Die Sicherheit im Gebäude (Family Office, Privatanwesen) stellt einen wesentlichen Baustein für die Persönliche Sicherheit dar. Deshalb sollten alle technischen Komponenten einwandfrei funktionieren und die Alarmprozesse stimmig sein. Wir überprüfen in einem ersten Schritt die Alarmanlagen und sonstigen baulichen Sicherheitsvorkehrungen. Dann werden anhand eines Gebäudegrundrisses die Schutzbereiche definiert und entsprechend sinnvolle Sicherheitsmaßnahmen vorgeschlagen. Wir übernehmen für das Family Office die Planung aller Objektsicherheitskomponenten, erstellen ausschreibungsfertige Unterlagen, überwachen den Einbau und nehmen die Endabnahme vor. Darüber hinaus kümmern wir uns um die Struktur für die sofortige Intervention. Durch eine regelmäßige Überprüfung der vorhandenen Alarmanlagen, mindestens einmal im Quartal, wird sichergestellt, dass alle Bauteile bei einem Ernstfall zuverlässig ihren Zweck erfüllen.

### ■ Background-Check

Bei der Aufnahme von Geschäftsbeziehungen wird im Rahmen der Due Diligence auch ein Background-Check zum Unternehmen bzw. den handelnden Personen durchgeführt. Hier geht es vor allem um die Abklärung harter Negativ-Merkmale für eine Zusammenarbeit mit dem Unternehmen. Die Recherche zur Seriosität einer Person beinhaltet auch Hinweise zu kritischen Verhaltensweisen. Je nach Anforderung und Detailgrad der Überprüfung kann ein Background-Check in der Regel innerhalb von 5 bis 10 Tagen durchgeführt werden. Darüber hinaus findet auch eine umfassende Überprüfung von Personen bei der Auswahl von neuen Mitarbeitern statt. Corporate Trust screen die potenziellen Bewerber nach Auffälligkeiten und führt auch entsprechende psychologische Tests durch. Damit wird sichergestellt, dass nur zuverlässige und vertrauenswürdige Personen Zugang zu den höchst sensiblen Informationen sowie in das persönliche Umfeld der Vermögensinhaber haben.

### ■ Reisesicherheit

Corporate Trust erstellt einen Handlungsleitfaden für die Vorbereitung von Reisen in kritische Länder. Darin sind sowohl Verhaltensregeln als auch Sicherheitshinweise und Möglichkeiten zur Wahrung der Vertraulichkeit im Reiseland enthalten. Das Family Office erhält den Zugang zu einer speziellen Länderinformations-Datenbank, mit Sicherheitshinweisen für alle Länder und die meisten Business-Metropolen. Dort kann vor jeder Reise in Länder mit erhöhtem Gefährdungspotential die aktuelle Sicherheitslage abgeklärt und die entsprechenden Maßnahmen geplant werden. Die Geschäftsreisenden erhalten bei Bedarf einen Ortungssender, über den ein Monitoring der Reiseroute stattfinden und jederzeit ein Alarm abgesetzt werden kann. Einmal jährlich werden die Family Office Mitarbeiter zum sicherheitsgerechten Verhalten bei kritischen Situationen geschult. Im Einzelfall prüfen wir vor Ort die Sicherheit der Hotels, Reiserouten, Aufenthaltsorte und beschaffen sondergeschützte Fahrzeuge. Bei Bedarf gewährleisten wir die Sicherheit durch direkten Personenschutz.

### ■ Präventives Krisenmanagement

Die präventive Vorbereitung auf einen Ernstfall ist unumgänglich. Um bei unerwarteten Ereignissen mit hohem Schadenspotenzial schnell und angepasst reagieren zu können, steht Corporate Trust deshalb mit seinen erfahrenen Krisenmanagern rund um die Uhr (24/365) über eine Hotline zur Verfügung. Als Vorbereitung auf Extremsituationen, erheben wir im Vorfeld alle nötigen Daten und erstellen den Basis-Krisenplan für das Family Office. Bei einem Kick-off-Meeting mit den Verantwortlichen werden dazu die realistischen Krisen-Szenarien definiert. Für die Persönliche Sicherheit ist es wichtig, für gefährdete Personen (Vermögensinhaber und Family Office Mitarbeiter) persönliche Dossiers anzulegen, in denen z.B. Lebensbeweisefragen und persönliche Merkmale umfangreich dokumentiert sind. Diese stehen bei einer Extremsituation dem Krisenstab zur Verfügung und können helfen, das Leben des Opfers zu retten. Außerdem wird anhand eines realistischen Schadensfalls einmal jährlich ein Training mit dem Krisenstab durchgeführt. Dabei werden die Mitglieder des Krisenstabs auf die verantwortungsvolle Rolle und die Dynamik in einer Krise optimal vorbereitet.

MENSCHEN, DIE IMMER HOCH HINAUS WOLLEN,  
SICHERN SICH NUR EXPERTEN ALS BEGLEITER.



# SICHERHEIT FÜR FAMILY OFFICES

Ein Dienstleistungsangebot von

**CORPORATE TRUST**

BUSINESS RISK & CRISIS MANAGEMENT GMBH

Graf-zu -Castell-Straße 1

D-81829 München

Tel.: +49 89 599 88 75 80

Fax: +49 89 599 88 75 820

[info@corporate-trust.de](mailto:info@corporate-trust.de)

[www.corporate-trust.de](http://www.corporate-trust.de)



SIE TRAGEN DIE VERANTWORTUNG.  
WIR STEHEN IHNEN MIT SICHERHEIT ZUR SEITE.



SICHERHEIT FÜR  
FAMILY OFFICES