

**Absender**

DATEV eG  
90329 Nürnberg

\_\_\_\_\_  
Name/Firma

\_\_\_\_\_  
Straße und Hausnummer

\_\_\_\_\_  
PLZ und Ort

**1. Gegenstand der Vereinbarung**

Hiermit erteilt der/die

\_\_\_\_\_  
Name/Firma

im Folgenden „Auftragnehmer“ genannt

der

DATEV eG  
Paumgartnerstraße 6–14  
90429 Nürnberg  
Registergericht Nürnberg, GenReg Nr. 70  
im Folgenden „DATEV“ genannt

die ausdrückliche Einwilligung, eine Überprüfung der folgenden

\_\_\_\_\_  
vorzunehmen oder durch Dritte vornehmen zu lassen. DATEV oder ihre Beauftragte werden dazu:

\_\_\_\_\_  
(nachfolgend „Sicherheitsüberprüfung“ genannt).

Die Sicherheitsüberprüfung wird im Zeitraum zwischen

und

und

jeweils von

bis

durchgeführt.

### 2. Mögliche Störungen

Die technische Sicherheitsüberprüfung der IT-Systeme durch DATEV ist mit Gefahren für die vom Auftragnehmer eingesetzten IT-Systeme verbunden. Die vorgesehene Sicherheitsüberprüfung kann während der Durchführung den normalen Betrieb der IT-Systeme in unbekanntem Umfang stören.

Generell wird bei IT-Sicherheitsüberprüfungen mit IT-Systemen und Netzwerkkomponenten auf eine Art und Weise kommuniziert und interagiert, die nicht dem normalen Verhalten der Anwender und Benutzer entspricht. Aufgrund der großen Variationsbreite von Fehlern in Software-Systemen, die unter anderem für Sicherheitsschwächen verantwortlich sind, kann nicht vorhergesagt werden, ob ein oder mehrere Systeme des Auftragnehmers mit Ausfall oder Fehlern auf ungewöhnlichen Datenverkehr reagieren.

DATEV versucht in Absprache mit dem Auftragnehmer Störungen zu vermeiden. Nach vorheriger Absprache können die Prüfungen außerhalb der Hauptgeschäftszeiten durchgeführt werden. Der Auftragnehmer stellt sicher, dass der Betriebsverantwortliche der jeweiligen Systeme zum Zeitpunkt der Sicherheitsüberprüfung telefonisch erreichbar ist und zeitnah auf mögliche Störungen reagiert. Auf Wunsch des Auftragnehmers kann die Überprüfung unverzüglich abgebrochen werden, sofern bei einer Fortführung die Gefahr eines vollständigen Systemausfalls besteht; hierzu genügt eine telefonische Mitteilung.

Vor der Sicherheitsüberprüfung müssen alle zur Wiederherstellung der IT-Systeme und der Datenbestände erforderlichen Backups durch die Verantwortlichen des Auftragnehmers erstellt worden sein.

### 3. Einsatz von Sicherheitswerkzeugen

DATEV setzt zur Ermittlung der Sicherheit (potentielle Sicherheitslücken oder Verwundbarkeiten der zu prüfenden Systeme) von Netzen und IT-Systemen Sicherheitswerkzeuge, wie z. B. sog. Security-Scanner, ein. Diese Software-Werkzeuge finden halbautomatisch erreichbare Systeme, darauf installierte Dienste und Anwendungen sowie bekannte Schwachstellen dieser Systeme einschließlich Konfigurationsfehlern. Dabei interagieren die Scanner mit den installierten Diensten und Anwendungen, beispielsweise werden Anmeldeversuche vorgenommen, Formulare ausgefüllt oder im Fall von Web-Servern Standard-Skripte ausgefüllt.

DATEV setzt je nach Bedarf als Scanner kommerziell verfügbare Werkzeuge wie z. B. nmap, curl, whoofi, Nessus, Burp suite pro und Microfocus WebInspect ein.

Darüber hinaus führt DATEV auch manuelle Tests durch.

DATEV benutzt folgende IP-Netze für den Angriff:

-----

-----

-----

## 4. Erklärung des Auftragnehmers

\_\_\_\_\_  
Vorname und Name

\_\_\_\_\_  
Abteilung

Ich bin über die Risiken einer technischen Sicherheitsüberprüfung umfassend aufgeklärt worden. Es ist mir bekannt, dass es trotz aller Sorgfalt und Vorkehrungen zu Fehlfunktionen, Ausfall betroffener Systeme sowie Datenverlust kommen kann und dass diese zu Folgeschäden, insbesondere an abhängigen oder durch Kommunikationsbeziehungen oder gemeinsame Komponenten verbundenen Systemen, führen können. Ich erlaube den Zugriff auf die Systeme und bestätige, dass der Zugriff auf die Systeme durch DATEV und / oder durch von ihr beauftragte Dritte befugt erfolgt.

Ich bin mit der folgenden Haftungsbeschränkung einverstanden:

- a. DATEV haftet für von ihr oder von ihren gesetzlichen Vertretern oder Erfüllungsgehilfen vorsätzlich oder grob fahrlässig verursachte Schäden. Bei Verletzung wesentlicher Vertragspflichten sowie bei der Verletzung von Leben, Körper oder Gesundheit tritt diese Haftung auch bei einfacher Fahrlässigkeit ein.

Bei leicht fahrlässiger Verletzung wesentlicher Vertragspflichten beschränkt sich die Haftung von DATEV auf den nach Art der Leistung vorhersehbaren, vertragstypischen Durchschnittsschaden. Dies gilt auch bei leicht fahrlässigen Pflichtverletzungen durch die ge-setzlichen Vertreter und Erfüllungsgehilfen von DATEV.

- b. Außer im Fall von Vorsatz und grober Fahrlässigkeit sowie bei Übernahme einer Garantie (Ziffer 4.4 unten) haftet DATEV nicht für mittelbare Schäden, wie z.B. Mehraufwand oder entgangenen Gewinn.
- c. Bei Datenverlust haftet DATEV nur für denjenigen Aufwand, der für die Wiederherstellung der Daten bei ordnungsgemäßer Datensicherung durch den Auftragnehmer erforderlich ist. Bei leicht fahrlässigen Pflichtverletzungen tritt diese Haftung nur ein, wenn DATEV mit der zum Datenverlust führenden Handlung gleichzeitig eine wesentliche Vertragspflicht verletzt hat.
- d. Haftungsausschlüsse oder -beschränkungen gelten nicht, soweit DATEV eine Garantie übernommen hat, die gerade den Zweck hatte, vor dem Eintritt der geltend gemachten Schäden zu schützen.
- e. Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

\_\_\_\_\_  
Ort und Datum

X

\_\_\_\_\_  
Unterschrift der zu untersuchenden Firma und Stempel

\_\_\_\_\_  
Name des/der Unterzeichnenden (in Druckbuchstaben)