PRAXIS-CHECKLISTE

Durchsuchung im Unternehmen

Die ersten 60 Minuten

Für Geschäftsführung, Empfang, Rechtsabteilung und IT. Die Zeitfenster dienen der Orientierung; Maßnahmen können parallel erforderlich sein.

Nicht behindern. Sofort anwaltliche Hilfe organisieren. Keine spontanen Angaben zum Tatvorwurf. Keine Daten löschen oder verändern. Alles dokumentieren.

Minute 0 bis 5 | Ruhe und Zuständigkeit

- ☐ **Maßnahme nicht behindern.** Zutritt nicht körperlich versperren; Computer nicht abschalten und Daten nicht löschen, verschieben oder verschlüsseln.
- ☐ **Zentralen Verantwortlichen verständigen.** Geschäftsführung, Rechtsabteilung oder Krisenverantwortlicher übernimmt die Koordination.
- ☐ **Dienstausweise prüfen.** Namen, Funktion, Behörde und Einsatzbereiche der Ermittlungsbeamten dokumentieren.
- ☐ **Durchsuchungsbeschluss verlangen.** Tatvorwurf, Räume und gesuchte Beweismittel erfassen; bei fehlendem Beschluss die behauptete Gefahr im Verzug dokumentieren.

Für den Empfang: „Wir werden die Maßnahme nicht behindern. Bitte weisen Sie sich aus und übergeben Sie uns eine Ausfertigung des Durchsuchungsbeschlusses. Ich informiere jetzt die Geschäftsführung und den anwaltlichen Ansprechpartner.“

Minute 5 bis 10 | Verteidigung einschalten

- ☐ **Strafverteidiger sofort anrufen** und Beschluss übermitteln. Etwaige Einschränkungen der Kontaktaufnahme dokumentieren.
- ☐ **Um ein Abwarten bis zum Eintreffen bitten.** Grundsätzlich besteht kein Anspruch auf einen Aufschub der Durchsuchung.
- ☐ **Beschluss anwaltlich prüfen lassen.** Insbesondere Aktualität, Tatvorwurf, Räume, Gegenstände und Verhältnismäßigkeit.
- ☐ **Eigene Beistände prüfen.** Bei unterschiedlichen Interessen insbesondere für Geschäftsführung, beschuldigte Mitarbeitende und Zeugen.

Minute 10 bis 20 | Umfang kontrollieren

- ☐ **Räume und Beweismittel mit dem Beschluss abgleichen.** Bereichsverantwortliche erhalten eine Kopie; Abweichungen dokumentieren.
- ☐ **Für jedes Durchsuchungsteam einen Begleiter benennen.** Ablauf protokollieren; auf geschützte oder ersichtlich nicht relevante Unterlagen hinweisen.
- ☐ **Keine informellen Erklärungen zum Tatvorwurf.** Beschuldigte können schweigen; Zeugen sollten vor einer Aussage anwaltlichen Rat einholen. Gesetzliche Pflichten im Einzelfall klären.
- ☐ **Technische Auskünfte koordinieren.** IT erläutert Systemstruktur und Speicherorte nur abgestimmt; keine unkoordinierten Erklärungen zu Geschäftsvorgängen.

Einsatzdaten

Datum / Beginn: _____

Unternehmensverantwortlicher: _____

Behörde / Aktenzeichen: _____

Minute 20 bis 35 | Datenzugriff begleiten

- ☐ **Datenbestand nicht eigenmächtig verändern.** Auch automatische Löschroutinen nicht unkoordiniert ändern; technische Maßnahmen dokumentieren.
- ☐ **Relevante Systeme erfassen.** Server, Computer, Mobiltelefone, Datenträger, Backups, E-Mail, Cloud und Messenger.
- ☐ **Erreichbare Konten und Speicher dokumentieren.** Bei räumlich getrennten Speichermedien den Rahmen des § 110 Abs. 3 StPO anwaltlich prüfen lassen.
- ☐ **Umfang mit Verteidigung und Ermittlungsbeamten abstimmen.** Laufwerke, Konten und Zeiträume eingrenzen; pauschale Sicherung sämtlicher E-Mails hinterfragen. Keine eigenständige Datenauswahl.
- ☐ **Technische Schritte protokollieren.** Geräte, Software, Kopien, ausgelesene Konten, Datenträger und beteiligte Personen erfassen.

Minute 35 bis 45 | Herausgabe kontrollieren

- ☐ **Gesuchte Unterlagen gezielt vorlegen lassen.** Vorher rechtlich abstimmen; keine pauschale Freigabe weiterer Datenbestände.
- ☐ **Freiwillige Herausgabe gesondert prüfen.** Vorlage und Einwilligung unterscheiden. Bei ungeklärter Rechtslage Widerspruch ausdrücklich erklären und protokollieren lassen.
- ☐ **Anwaltliche Unterlagen getrennt kennzeichnen.** Schutz nach §§ 97, 160a StPO prüfen lassen; kein pauschaler Schutz sämtlicher Beratungsunterlagen.
- ☐ **Ausweitung der Suche dokumentieren.** Auf fehlenden Bezug zum Beschluss hinweisen und die rechtliche Bewertung der Verteidigung überlassen.

Minute 45 bis 55 | Bestand und Betrieb erfassen

- ☐ **Genaues Sicherstellungsverzeichnis verlangen.** Bezeichnung, Seriennummer, Benutzer, Dateipfad und Zeitraum soweit möglich erfassen.
- ☐ **Status der Mitnahme klären.** Vorläufige Mitnahme zur Durchsicht nach § 110 StPO und endgültige Beschlagnahme unterscheiden.
- ☐ **Rückgabe und Begrenzung der Auswertung verlangen.** Nicht benötigte Daten und Unterlagen benennen; Kopien geschäftskritischer Bestände beantragen.
- ☐ **Betriebliche Auswirkungen dokumentieren.** Systemausfälle, blockierte Arbeitsplätze, unterbrochene Prozesse und Dauer festhalten.

Minute 55 bis 60 | Abschluss und Rechtsschutz

- ☐ **Verzeichnis mit tatsächlich mitgenommenen Gegenständen abgleichen.** Abweichungen und offene Punkte sofort protokollieren lassen.
- ☐ **Widersprüche und Unregelmäßigkeiten festhalten.** Insbesondere betroffene Räume, Datenzugriffe und anwaltliche Unterlagen.
- ☐ **Zeitnahe Entscheidung über gesicherte Daten verlangen.** Umfang und Dauer der weiteren Durchsicht anwaltlich kontrollieren lassen.
- ☐ **Rechtsschutz prüfen.** Insbesondere Beschwerde nach § 304 StPO bzw. gerichtliche Entscheidung nach § 98 Abs. 2 Satz 2 StPO; anschließend Ablauf, IT-Protokolle und Kommunikation sichern.

Dr. Mathias Grzesiek · Rechtsanwalt | Fachanwalt für Strafrecht
Rosinus | Partner Rechtsanwälte PartG mbB · Kettenhofweg 29 · 60325 Frankfurt am Main
+49 69 8740306-0 · m.grzesiek@rosinus-partner.com
www.strafrecht-digital.com

Diese Checkliste ersetzt keine Einzelfallprüfung. Maßgeblich sind Beschluss, Tatvorwurf, betroffene Personen und IT-Infrastruktur. Bei nicht tatverdächtigen Unternehmen sind insbesondere die Voraussetzungen des § 103 StPO zu prüfen.