



Das Strafprozessrechtsänderungsgesetz 2024 Teil 1

Mit 1.1.2025 ist mit dem StPRÄG 2024 eine umfangreiche Novelle der StPO in Kraft getreten, die gemeinhin als Novelle zur „Handysicherstellung“ bekannt ist. Vielmehr treten dabei aber zahlreiche weitere Neuerungen in Kraft, die insb auch die tägliche Arbeit von Compliance-Beauftragten beeinflussen und eine Überarbeitung diverser Compliance-Maßnahmen nach sich ziehen können.

Von [Mag. Christoph Slamanig](#)

20. Januar 2025

Diese Beitragsreihe bietet einen ersten Überblick der wichtigsten Neuerungen des StPRÄG 2024.¹ **Teil I** beschäftigt sich mit der Sicherstellung und Beschlagnahme. **Teil II** zeigt die keinesfalls zu unterschätzende Ausweitung der Beschuldigten- und Opferrechte auf, **Teil III** die Anpassungen in den Bereichen Cybercrime und Kryptowerte.

Hintergrund und Neuregelung

Bislang war die Sicherstellung sämtlicher „Gegenstände“ in der StPO gleich geregelt. Eine Tatwaffe, zB ein blutiger Hammer, konnte unter den gleichen Voraussetzungen sichergestellt werden wie ein Datenträger (zB ein Smartphone). Die Sicherstellung wurde durch die StA (Staatsanwaltschaft) angeordnet und von der KRIPO durchgeführt, eine **gerichtliche Bewilligung** war – anders als zB bei einer „Telefonüberwachung“ – **nicht notwendig**. Der VfGH² hat nunmehr die zentralen Bestimmungen der StPO zur Sicherstellung (§ 110 Abs 1 Z 1 und Abs 4 StPO sowie § 111 Abs 2 StPO) mit Ablauf des 31. Dezember 2024 wegen Verstoßes gegen das Grundrecht auf Datenschutz (§ 1 DSG) und das Recht auf Achtung des Privat- und Familienlebens nach Art 8 EMRK als verfassungswidrig aufgehoben. Mit dem StPRÄG 2024 werden die dadurch notwendig gewordenen Änderungen umgesetzt. In diesem Beitrag werden die wichtigsten Neuerungen zur Sicherstellung und Beschlagnahme aufgezeigt.

Neue Ermittlungsmaßnahme: Beschlagnahme von Datenträgern und Daten

Mit dem StPRÄG 2024 wird die neue Ermittlungsmaßnahme **Beschlagnahme von Datenträgern und Daten** aus Beweisgründen³ (§§ 115f StPO) eingeführt. Dabei muss ein begründeter Verdacht vorliegen, dass beweiserhebliche Tatsachen gewonnen werden können, die für die Aufklärung der Straftat wesentlich sind. Die Beschlagnahme von Datenträgern und Daten wird damit im Ergebnis grundsätzlich von der Sicherstellung bzw Beschlagnahme sonstiger Gegenstände getrennt. Explizit wird mit der Novelle klargestellt, dass auch Daten beschlagnahmt werden können, die nicht direkt auf einem Datenträger gespeichert sind, sondern sich an anderen **(externen) Speicherorten** (insb auf Clouds oder externen Servern) befinden, sofern ein Zugriff auf diese Daten über den Datenträger möglich ist (§ 109 Z 2a lit b StPO).

Die Beschlagnahme von Datenträgern und Daten wird von der StA nunmehr auf Grund einer **gerichtlichen Bewilligung**³ angeordnet, wobei die Durchführung selbst grundsätzlich der KRIPO zukommt (§ 115f Abs 2 StPO). Bei Gefahr im Verzug kann die KRIPO in Ausnahmefällen eine Sicherstellung auch von sich aus durchführen (§ 115f Abs 4 StPO).

Anordnungen der StA und Entscheidungen des Gerichts unterliegen fortan einer erhöhten **Begründungspflicht**. Bereits die Anordnung der StA muss eine genaue Beschreibung der **Datenkategorien** (zB Metadaten, Standortdaten, Fotos) und **Dateninhalte** („gesuchtes Beweismaterial“), die zu beschlagnahmen sind, sowie die relevanten **Zeiträume** enthalten (§ 115f Abs 3 StPO).

Die **Ergebnisse einer Auswertung** (siehe dazu unten) dürfen bei sonstiger **Nichtigkeit** nur als Beweismittel verwendet werden, sofern die Beschlagnahme rechtmäßig angeordnet und bewilligt wurde (§ 115j Abs 1 StPO).

Zur unabhängigen Aufsicht dieser Ermittlungsmaßnahmen werden die Befugnisse des **Rechtsschutzbeauftragten** der Justiz erweitert. Diesem obliegt anhand von Informations-, Auskunfts- und Akteneinsichtsrechten die Prüfung und Kontrolle der Anordnung, Genehmigung, Bewilligung und Durchführung einer Beschlagnahme von Datenträgern und Daten (§ 115l StPO).

Aufbereitung und Auswertung der beschlagnahmten Daten

Die StPO enthielt bislang grundsätzlich keine konkreten Bestimmungen zum weiteren Umgang mit sichergestellten Datenträgern und zur Auswertung der darauf befindlichen Daten. Dieser Umstand führte in der Praxis – insb bei größeren Wirtschaftsstrafverfahren – zu unbefriedigenden Ergebnissen. Mit dem StPRÄG 2024 wird die Beschlagnahme von Datenträgern und Daten nunmehr in **mehrere Phasen** gegliedert. Ziel ist es, die Transparenz anhand strenger Dokumentationspflichten zu erhöhen und den Rechtsschutz durch Informationspflichten und Beteiligungsmöglichkeiten zu stärken.

Phase I – Technische Aufbereitung der Daten

In dieser Phase wird jener reduzierte Datensatz erstellt, der dem gerichtlich bewilligten Datenumfang entspricht, wobei explizit **keine inhaltliche Auseinandersetzung** mit den Daten erfolgt. Für die Umsetzung können Hilfskräfte beigezogen oder Sachverständige beauftragt werden.

Die Phase der **Datenaufbereitung** (§ 115h StPO) umfasst insb

- das Entsperren von Speichermedien (wie Datenträger, Cloudspeicher oder Server),
- die Sicherung der Daten sowie
- gegebenenfalls die Wiederherstellung gelöschter Daten

in Form einer **Originalsicherung** (§ 109 Z 2c StPO) des gesamten Datenbestands (Kopie des Originaldatenbestandes). Im Anschluss wird eine **Arbeitskopie** (§ 109 Z 2d StPO) der Originalsicherung erstellt, die als Grundlage für die forensisch-technische Aufbereitung durch die KRIPO oder StA dient.⁵ Am Ende der Phase steht das „**Ergebnis der Datenaufbereitung**“ (§ 109 Z 2e StPO), ein der gerichtlichen Bewilligung entsprechender Datensatz, welcher den Ermittlungen inhaltlich zugrunde gelegt werden darf.

Die Umsetzung ist strikt zu dokumentieren und in einem **Aufbereitungsbericht** festzuhalten. Damit soll sichergestellt werden, dass ein deutlich kleinerer Datensatz als bisher den Ermittlungen zugrunde liegt, was den Eingriff in die Rechte der betroffenen Personen reduzieren soll. Der Aufbereitungsbericht soll zudem die Kontrolle der korrekten Umsetzung der gerichtlichen Entscheidung ermöglichen.

Phase II – Inhaltliche Auswertung der Daten

Die inhaltliche Auswertung der Daten (§ 115i und § 115j StPO) beschränkt sich in der Folge auf das **Ergebnis der Datenaufbereitung**. Die StA hat dabei nur diejenigen **Ergebnisse der Auswertung** zum Akt zu nehmen, die für das Verfahren von Bedeutung sind und als Beweismittel verwendet werden dürfen.

KRIPO und StA können bei der Durchsuchung des Datenbestandes **Suchparameter** festlegen, welche samt Ergebnissen dokumentiert werden müssen. Beschuldigte und Opfer haben das Recht, die Auswertung von Daten anhand weiterer Suchparameter zu beantragen. Wurden ihre Datenträger und Daten beschlagnahmt, ist ihnen außerdem zu ermöglichen, das Ergebnis der Datenaufbereitung einzusehen (§ 115i Abs 2 StPO).

Weitere von der Auswertung der Daten betroffenen Personen haben außerdem das Recht, das Ergebnis der Auswertung von Daten insoweit einzusehen, als ihre Daten betroffen sind. Auf Antrag oder von Amts wegen sind Daten aus dem Ergebnis der Datenaufbereitung uU auch zu vernichten (§ 115i Abs 4 und 5 StPO).

FAZIT

Das StPRÄG 2024 bringt eine umfassende Neuregelung der Sicherstellung/Beschlagnahme von Datenträgern und Daten, insb neue Ermittlungsmaßnahmen sowie entsprechende Rechte der Beschuldigten, Opfer und Betroffenen. Compliance-Beauftragten ist daher zu empfehlen, die jeweils betroffenen Compliance-Maßnahmen (zB im Rahmen der Beschlagnahme von Datenträgern bei Hausdurchsuchungen) anzupassen und Schulungen zur neuen Rechtslage anzubieten. Die konkrete Umsetzung der Novelle in der Praxis, insb das Vorgehen der Strafverfolgungsbehörden bei der Aufbereitung und Auswertung der Daten, bleibt jedenfalls mit Spannung abzuwarten. Entsprechend wichtig bleibt die proaktive Ausübung der Rechtsschutzinstrumente im Strafverfahren.

[Bleiben Sie dran für einen weiteren Teil zur Beitragsreihe "Das Strafprozessänderungsgesetz 2024".](#)

¹ Strafprozessrechtsänderungsgesetz 2024, BGBl I 157/2024.

² VfGH 14.12.2023, G 352/2021.

³ Die Sicherstellung zu anderen Zwecken als der Beweissicherung, zB der Sicherung privatrechtlicher Ansprüche und vermögensrechtlicher Anordnungen (zB Verfall) bleibt weiterhin möglich.

⁴ Kritisch zu sehen ist, dass die Möglichkeit von sog „Stampiglienbeschlüssen“, wonach die Begründung der StA von den bewilligenden Gerichten einfach übernommen werden kann, unverändert fortbesteht.

⁵ Ein späterer Zugriff auf die Originalsicherung und Arbeitskopie ist nur nach erneuter richterlicher Bewilligung zulässig (§ 115 Abs 5 StPO).

Autoren



Mag. Christoph Slamanig

Mag. Christoph Slamanig ist Rechtsanwalt und zertifizierter Compliance Officer bei DORDA Rechtsanwälte GmbH. Sein Spezialgebiet ist die Begleitung von Strafverfahren sowie die Compliance-Beratung i...

