Art. 10 Verdeckter Zugriff auf informationstechnische Systeme

(1) [1]Auf informationstechnische Systeme, die der Betroffene in der berechtigten Erwartung von Vertraulichkeit als eigene nutzt und die seiner selbstbestimmten Verfügung unterliegen, darf das Landesamt zur Abwehr einer konkretisierten Gefahr für ein in Art. 9 Abs. 1 Satz 1 genanntes Rechtsgut verdeckt mit technischen Mitteln nur zugreifen, um

1. Zugangsdaten und verarbeitete Daten zu erheben oder

2. zur Vorbereitung einer Maßnahme nach Nr. 1 spezifische Kennungen sowie den Standort eines informationstechnischen Systems zu ermitteln.

[2]Art. 9 Abs. 1 Satz 2 und 3 gilt entsprechend. [3]Die erhobenen Daten dürfen über den Anlass und Zweck hinaus, zu dem sie erhoben wurden, nur zur Abwehr einer Gefahr im Sinne des Satzes 1 oder zur Verfolgung einer Straftat, auf Grund derer eine entsprechende Maßnahme nach § 100b der *Strafprozessordnung* in der am 1. Januar 2023 geltenden Fassung angeordnet werden könnte, weiterverarbeitet werden.

(2) [1]Durch technische Maßnahmen ist sicherzustellen, dass

1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind,

2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden und

3. Daten, die den Kernbereich privater Lebensgestaltung betreffen, soweit technisch möglich nicht erhoben werden.

[2]Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. [3]Erhobene Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) [1]Die Maßnahme darf sich nur gegen die Zielperson richten und nur durch Zugriff auf deren informationstechnisches System durchgeführt werden. [2]Der Zugriff auf informationstechnische Systeme anderer ist zulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass

1. die Zielperson deren informationstechnisches System benutzt oder benutzt hat,

2. sich dadurch für die Abwehr der Gefahr relevante Informationen ergeben werden und

3. ein Zugriff auf das informationstechnische System der Zielperson allein nicht zur Erforschung des Sachverhalts ausreicht.