§ 53 SPG Zulässigkeit der Verarbeitung

SPG - Sicherheitspolizeigesetz

Berücksichtigter Stand der Gesetzgebung: 25.07.2024

1. (1)Die Sicherheitsbehörden dürfen personenbezogene Daten verarbeiten
    1. 1.für die Erfüllung der ersten allgemeinen Hilfeleistungspflicht (§ 19);
    2. 2.für die Abwehr krimineller Verbindungen (§§ 16 Abs. 1 Z 2 und 21);

    (Anm.: Z 2a aufgehoben durch BGBl. I Nr. 5/2016)
    1. 3.für die Abwehr gefährlicher Angriffe (§§ 16 Abs. 2 und 3 sowie 21 Abs. 2); einschließlich der im Rahmen der Gefahrenabwehr notwendigen Gefahrenerforschung (§ 16 Abs. 4 und § 28a);
    2. 4.für die Vorbeugung wahrscheinlicher gefährlicher Angriffe gegen Leben, Gesundheit, Sittlichkeit, Freiheit, Vermögen oder Umwelt (§ 22 Abs. 2 und 3) oder für die Vorbeugung gefährlicher Angriffe mittels Kriminalitätsanalyse, wenn nach der Art des Angriffes eine wiederholte Begehung wahrscheinlich ist;
    3. 5.für Zwecke der Fahndung (§ 24);
    4. 6.um bei einem bestimmten Ereignis die öffentliche Ordnung aufrechterhalten zu können.

    (Anm.: Z 7 aufgehoben durch BGBl. I Nr. 5/2016)
2. (2)Die Sicherheitsbehörden dürfen Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen verarbeitet haben, für die Zwecke und unter den Voraussetzungen nach Abs. 1 verarbeiten; ein automationsunterstützter Datenabgleich im Sinne des § 141 StPO ist ihnen jedoch untersagt. Bestehende Übermittlungsverbote bleiben unberührt.
3. (3)Die Sicherheitsbehörden sind berechtigt, von den Dienststellen der Gebietskörperschaften, den anderen Körperschaften des öffentlichen Rechtes und den von diesen betriebenen Anstalten Auskünfte zu verlangen, die sie für die Abwehr gefährlicher Angriffe oder für die Abwehr krimineller Verbindungen benötigen. Eine Verweigerung der Auskunft ist nur zulässig, soweit andere öffentliche Interessen die Abwehrinteressen überwiegen oder eine über die Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) hinausgehende sonstige gesetzliche Verpflichtung zur Verschwiegenheit besteht.
4. (3a)Die Sicherheitsbehörden sind berechtigt, von Betreibern öffentlicher Telekommunikationsdienste (§ 160 Abs. 3 Z 1 Telekommunikationsgesetz 2021 – TKG 2021, BGBl. I Nr. 190/2021,) und sonstigen Diensteanbietern (§ 3 Z 2 E-Commerce-Gesetz - ECG, BGBl. I Nr. 152/2001) Auskünfte zu verlangen:
    1. 1.über Stammdaten eines Nutzers gemäß § 160 Abs. 3 Z 5 lit. a bis d und g TKG 2021 oder Nutzers eines sonstigen Dienstes (§ 3 Z 1 ECG) wenn dies zur Erfüllung der ihnen nach diesem Bundesgesetz übertragenen Aufgaben erforderlich ist,
    2. 2.über die Internetprotokolladresse (IP-Adresse) zu einer bestimmten Nachricht und den Zeitpunkt ihrer Übermittlung, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr
        1. a)einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§ 19),
        2. b)eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder

3. c)einer kriminellen Verbindung (§ 16 Abs.1 Z 2) benötigen,

3. 3.über Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war, wenn sie diese Daten als wesentliche Voraussetzung zur Abwehr
    1. a)einer konkreten Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen im Rahmen der ersten allgemeinen Hilfeleistungspflicht (§19),
    2. b)eines gefährlichen Angriffs (§ 16 Abs. 1 Z 1) oder
    3. c)einer kriminellen Verbindung (§ 16 Abs. 1 Z 2) benötigen,
4. 4.über Namen, Anschrift und Nutzernummer eines bestimmten Anschlusses durch Bezugnahme auf ein von diesem Anschluss geführtes Gespräch durch Bezeichnung eines möglichst genauen Zeitraumes und der passiven Teilnehmernummer, wenn dies zur Erfüllung der ersten allgemeinen Hilfeleistungspflicht oder zur Abwehr gefährlicher Angriffe erforderlich ist.

5. (3b)Ist auf Grund bestimmter Tatsachen anzunehmen, dass eine gegenwärtige Gefahr für das Leben, die Gesundheit oder die Freiheit eines Menschen besteht, sind die Sicherheitsbehörden zur Hilfeleistung oder Abwehr dieser Gefahr berechtigt, von Betreibern öffentlicher Telekommunikationsdienste Auskunft über Standortdaten und die internationale Mobilteilnehmerkennung (IMSI) der vom Gefährder oder von dem gefährdeten oder diesen begleitenden Menschen mitgeführten Endeinrichtung zu verlangen sowie technische Mittel zur Lokalisierung der Endeinrichtung einschließlich der Feststellung der dazugehörenden IMSI zum Einsatz zu bringen.
6. (3c)In den Fällen der Abs. 3a und 3b trifft die Sicherheitsbehörde die Verantwortung für die rechtliche Zulässigkeit des Auskunftsbegehrens. Die ersuchte Stelle ist verpflichtet, die Auskünfte unverzüglich und im Fall des Abs. 3b gegen Ersatz der Kosten nach der Überwachungskostenverordnung – ÜKVO, BGBl. II Nr. 322/2004, zu erteilen. Im Falle des Abs. 3b hat die Sicherheitsbehörde dem Betreiber überdies unverzüglich, spätestens innerhalb von 24 Stunden eine schriftliche Dokumentation nachzureichen.
7. (3d)Die Sicherheitsbehörden sind zur Vorbeugung und Abwehr gefährlicher Angriffe gegen die Umwelt berechtigt, von Behörden des Bundes, der Länder und Gemeinden Auskünfte über von diesen genehmigte Anlagen und Einrichtungen zu verlangen, bei denen wegen der Verwendung von Maschinen oder Geräten, der Lagerung, Verwendung oder Produktion von Stoffen, der Betriebsweise, der Ausstattung oder aus anderen Gründen besonders zu befürchten ist, dass im Falle einer Abweichung der Anlage oder Einrichtung von dem der Rechtsordnung entsprechenden Zustand eine Gefahr für das Leben, die Gesundheit mehrerer Menschen oder in großem Ausmaß eine Gefahr für Eigentum oder Umwelt entsteht. Die ersuchte Behörde ist verpflichtet, die Auskunft zu erteilen.
8. (4)Abgesehen von den Fällen der Abs. 2 bis 3b und 3d sind die Sicherheitsbehörden für Zwecke des Abs. 1 berechtigt, personenbezogene Daten aus allen anderen verfügbaren Quellen durch Einsatz geeigneter Mittel, insbesondere durch Zugriff etwa auf im Internet öffentlich zugängliche Daten, zu verarbeiten.
9. (5)Die Sicherheitsbehörden sind im Einzelfall berechtigt, für die Zwecke des Abs. 1 personenbezogene Bild- und Tondaten zu verarbeiten, die Rechtsträger des öffentlichen oder privaten Bereichs mittels Einsatz von Bildaufnahmegeräten rechtmäßig verarbeitet und der Sicherheitsbehörde freiwillig übermittelt haben. Nicht zulässig ist die Verarbeitung von personenbezogenen Bilddaten über nichtöffentliches Verhalten. Die Rechtsträger des öffentlichen oder privaten Bereichs, sofern letzteren ein öffentlicher Versorgungsauftrag zukommt, die zulässigerweise einen öffentlichen Ort mit Bildaufnahmegeräten überwachen, sind im Einzelfall für die Zwecke der Vorbeugung wahrscheinlicher oder Abwehr gefährlicher Angriffe, der Abwehr krimineller Verbindungen sowie der Fahndung verpflichtet, die auf diese Weise erlangten Bild- und Tondaten auf Verlangen unverzüglich der Sicherheitsbehörde in einem üblichen technischen Format weiterzugeben oder Zugang zur Bildaufnahme zu gewähren, um sie für die genannten Zwecke zu verarbeiten. Ab dem Zeitpunkt der Kenntnis von einem solchen Verlangen darf der verpflichtete Rechtsträger die verlangten Bild- und Tondaten nicht löschen. Bei jeder Verarbeitung von Bild- und Tondaten ist besonders darauf zu achten, dass Eingriffe in die Privatsphäre der Betroffenen die Verhältnismäßigkeit (§ 29) zum Anlass wahren.

In Kraft seit 23.07.2024 bis 31.12.9999