jusline®
»» Recht. Schnell

Sie können die QR Codes nützen um später wieder auf die neuste Version eines Gesetzestexts zu gelangen.

§ 9 NISG Befugnisse und Datenverarbeitung

NISG - Netz- und Informationssystemsicherheitsgesetz

Berücksichtigter Stand der Gesetzgebung:

Datenverarbeitung

1. (1)Der Bundeskanzler, der Bundesminister für Inneres, der Bundesminister für Landesverteidigung, der Bundesminister für Europa, Integration und Äußeres und die Computer-Notfallteams gemäß § 14 Abs. 1 sind berechtigt zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen bei der Wahrnehmung ihrer Aufgaben nach diesem Bundesgesetz und zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit die erforderlichen personenbezogenen Daten im Sinne des Art. 4 Z 2 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (im Folgenden: DSGVO), ABl. Nr. L 119 vom 04.05.2016 S. 1, in der Fassung der Berichtigung ABl. Nr. L 314 vom 22.11.2016 S. 72, und § 36 des Bundesgesetzes zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), BGBl. I Nr. 165/1999, zu verarbeiten und einander sowie den Mitgliedern der OpKoord zu übermitteln.
2. (2)Dies sind folgende personenbezogene Daten:
    1. 1.von Teilnehmern und ihren Organisationseinheiten, die zur Ermöglichung und im Zuge der Teilnahme an den Koordinierungsstrukturen zu organisatorischen Zwecken erforderlich sind;
    2. 2.von Personen, die in Zusammenhang mit Risiken, Vorfällen und Sicherheitsvorfällen stehen, zwecks Erörterung und Aktualisierung des vom Bundesminister für Inneres erstellten Lagebildes, zur Erörterung der Erkenntnisse, die gemäß § 13 Abs. 1 und 2 gewonnen wurden, und zur Unterstützung des Koordinationsausschusses erforderlich sind;
    3. 3.von Personen, die an einem Geschäftsfall mitwirken oder davon betroffen sind.
3. (3)Der Bundeskanzler, der Bundesminister für Inneres und der Bundesminister für Landesverteidigung sind zum Zweck der Analyse und Bewältigung von Risiken, Vorfällen und Sicherheitsvorfällen berechtigt, über die in Abs. 2 genannten Daten hinaus folgende personenbezogene Daten zu verarbeiten und einander zu übermitteln:
    1. 1.Kontakt- und Identitätsdaten sowie technische Daten des Einmelders und der Kontaktperson;
    2. 2.Kontakt- und Identitätsdaten sowie technische Daten von Personen, die mit einer Meldung zu einem Risiko, Vorfall oder Sicherheitsvorfall in Zusammenhang stehen, wie insbesondere Opfer und Angreifer.
4. (4)Der Bundeskanzler und der Bundesminister für Inneres sind zur Erfüllung ihrer Aufgaben nach §§ 4 und 5 berechtigt, über die in Abs. 2 und 3 genannten Daten hinaus folgende personenbezogenen Daten zu verarbeiten und einander zu übermitteln:
    1. 1.Kontakt- und Identitätsdaten sowie technische Daten von Betreibern wesentlicher Dienste, Anbietern digitaler Dienste, Einrichtungen der öffentlichen Verwaltung, die von der Möglichkeit gemäß § 22 Abs. 5 Gebrauch gemacht haben, Computer-Notfallteams sowie von zuständigen Behörden anderer Mitgliedstaaten;

2. 2.Kontakt- und Identitätsdaten sowie technische Daten von Personen, die mit einer Meldung zu einem Risiko, Vorfall oder Sicherheitsvorfall in Zusammenhang stehen, wie insbesondere Opfer und Angreifer;
3. 3.Kontakt- und Identitätsdaten von Teilnehmern und ihren Organisationseinheiten, die zur Ermöglichung und im Zuge der Teilnahme an EU-weiten, internationalen und nationalen Gremien für die Sicherheit von Netz- und Informationssystemen erforderlich sind;

5. (5)Der Bundesminister für Inneres ist zur Erfüllung seiner Aufgaben nach§ 5 Z 4 bis 6 berechtigt, über die in Abs. 2 bis 4 genannten Daten hinaus folgende personenbezogenen Daten zu verarbeiten:
   1. 1.Kontakt- und Identitätsdaten sowie technische Daten von qualifizierten Stellen;
   2. 2.Kontakt- und Identitätsdaten sowie technische Daten von Personen im Rahmen der Überprüfungen von Sicherheitsvorkehrungen;
   3. 3.technische Daten von Personen, die im Rahmen des§ 13 ermittelt wurden.
6. (6)Jede Abfrage, Übermittlung und Änderung personenbezogener Daten ist revisionssicher zu protokollieren. Die Protokollaufzeichnungen sind drei Jahre aufzubewahren und danach zu löschen.
7. (7)Das Recht auf Löschung und auf Widerspruch gemäß DSGVO oder § 45 DSG wird insoweit beschränkt, als durch Gesetz oder Verordnung eine Aufbewahrungspflicht oder Archivierung vorgesehen ist oder der Löschung das öffentliche Interesse der Gewährleistung eines hohen Niveaus von Netz- und Informationssystemsicherheit entgegensteht und die betroffene Person nicht Gründe nachweisen kann, die sich aus ihrer besonderen Situation ergeben und welche die Ziele der Beschränkung des Rechtes überwiegen. Der zuständige Datenschutzbeauftragte ist über die Vornahme und das Ergebnis einer solchen Abwägung in Kenntnis zu setzen.
8. (8)Das Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO oder § 45 DSG wird in Bezug auf integrierte Datenverarbeitungssysteme für die Dauer einer Überprüfung der von der betroffenen Person bestrittenen Richtigkeit ihrer personenbezogenen Daten sowie für den Zeitraum, in dem die betroffene Person ihr Recht auf Widerspruch geltend gemacht hat und noch nicht feststeht, ob die berechtigten Gründe des datenschutzrechtlich Verantwortlichen gegenüber denen der betroffenen Person überwiegen, beschränkt.
9. (9)Die datenschutzrechtlichen Pflichten nach der DSGVO und dem 3. Hauptstück DSG sind von jedem datenschutzrechtlichen Verantwortlichen hinsichtlich jener personenbezogenen Daten, die im Zusammenhang mit den von ihm geführten Verfahren oder den von ihm gesetzten Maßnahmen verarbeitet, übermittelt oder weiterverarbeitet werden, selbstständig wahrzunehmen.

In Kraft seit 29.12.2018 bis 30.09.2026

© 2026 JUSLINE
JUSLINE® ist eine Marke der ADVOKAT Unternehmensberatung Greiter & Greiter GmbH.
www.jusline.at