RECHT.NRW
Landesrecht Nordrhein-Westfalen

Ministerium des Innern
des Landes Nordrhein-Westfalen

LRMB - Landesrecht Ministerialblatt

Stammnorm
Ausfertigungsdatum: 15.08.2024

Fassung
Gültig ab: 11.10.2024

Richtlinie zur Anordnung der Auftragsverarbeitung gemäß Artikel 28 Absatz 3 der Datenschutz-Grundverordnung bei der Nutzung des IT-Verfahrens Online-Sicherheitsprüfung im Land Nordrhein-Westfalen (OSiP-Auftragsverarbeitungsrichtlinie)

Richtlinie
zur Anordnung der Auftragsverarbeitung
gemäß Artikel 28 Absatz 3 der Datenschutz-Grundverordnung
bei der Nutzung des IT-Verfahrens Online-Sicherheitsprüfung
im Land Nordrhein-Westfalen
(OSiP-Auftragsverarbeitungsrichtlinie)

Gemeinsamer Runderlass
des Ministeriums für Heimat, Kommunales, Bau und Digitalisierung,
- Aktenzeichen: 84.02.05-001003 -
des Ministeriums für Wirtschaft, Industrie, Klimaschutz und Energie,
des Ministeriums des Innern,
des Ministeriums für Kinder, Jugend, Familie, Gleichstellung, Flucht und Integration,
des Ministeriums für Arbeit, Gesundheit und Soziales,
des Ministeriums der Justiz,
des Ministeriums für Umwelt, Naturschutz und Verkehr und
des Ministeriums für Landwirtschaft und Verbraucherschutz

Vom 15. August 2024

1
Allgemeine Bestimmungen

1.1
Nutzung des IT-Verfahrens Online-Sicherheitsprüfung, im Folgenden OSiP

Für Verwaltungsverfahren zur Sicherheits- und Zuverlässigkeitsüberprüfung von Personen ist die Einholung von Informationen verschiedener Erkenntnisstellen erforderlich. Dabei erfolgt die Zulassung der zu überprüfenden Personen beziehungsweise die Entscheidung über den beantragten Verwaltungsakt abschließend durch die zuständigen Behörden auf Landes- und kommunaler Ebene.

Die Einholung der relevanten Informationen, die sämtliche Personenbezüge aufweisen und insoweit in den Geltungsbereich der Datenschutz-Grundverordnung vom 27. April 2016 (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35), und des Datenschutzgesetzes Nordrhein-Westfalen vom 17. Mai 2018 (GV. NRW. S. 244, ber. S. 278 und S. 404) in der jeweils geltenden Fassung fallen, hat über OSiP zu erfolgen. Für den datenschutzkonformen Einsatz dieses IT-Verfahrens unter der dienstleistenden Einbindung des Landesbetriebs Information und Technik Nordrhein-Westfalen, im Folgenden IT.NRW, durch die jeweils zuständige Behörde ist dieser gemeinsame Runderlass erforderlich.

1.2
Datenschutzrechtlich Verantwortliche gemäß Artikel 4 Nummer 7 der Datenschutz-Grundverordnung

Zuständige Behörden, die OSiP für die Sicherheits- und Zuverlässigkeitsüberprüfungen nutzen, sind

a) für die Luftsicherheit die Bezirksregierungen Düsseldorf und Münster als Luftsicherheitsbehörden,

b) für Verfahren nach dem Sprengstoffgesetz in der Fassung der Bekanntmachung vom 10. September 2002 (BGBl. I S. 3518), das zuletzt durch Artikel 11 des Gesetzes vom 2. März 2023 (BGBl. 2023 I Nr. 56) geändert worden ist, die Bezirksregierungen und Kreisordnungsbehörden,

c) für die Hafensicherheit die Bezirksregierung Düsseldorf,

d) für anlassbezogene Überprüfungen und Sicherheitsüberprüfungen das Landeskriminalamt,

e) für Verfahren nach dem Waffengesetz vom 11. Oktober 2002 (BGBl. I S. 3970, 4592; 2003 I S. 1957), das zuletzt durch Artikel 228 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, die Kreispolizeibehörden,

f) für den Justizvollzug sowie den Justizvollzug für Anstaltsfremde die Justizvollzugsanstalten,

g) für atomrechtliche Zuverlässigkeitsüberprüfungen das für Energie zuständige Ministerium,

h) für das Bewachungsgewerbe die zuständigen Behörden in den Kreisen und kreisfreien Städten,

i) für das Prostitutionsgewerbe die zuständigen Behörden in den Kreisen und kreisfreien Städten,

j) für aufenthaltsrechtliche Verfahren die zuständigen Behörden der Großen kreisangehörigen Städte und der kreisfreien Städte, die Kreisordnungsbehörden, die Zentralen Ausländerbehörden und die Zentralstelle Fachkräfte Einwanderung,

k) für die Einbürgerung die zuständigen Behörden in den Kreisen und kreisfreien Städten als Staatsangehörigkeitsbehörden,

l) für den Erwerb der deutschen Staatsangehörigkeit durch Erklärung die Bezirksregierungen,

m) für die erstmalige Jagdscheinerteilung, die Jagdscheinverlängerung und die Ungültigerklärung des Jagdscheins die Kreise und kreisfreien Städte als untere Jagdbehörden sowie

n) für die Umsetzung des Sprengstoffgesetzes in Betrieben, die dem Bundesberggesetz vom 13. August 1980 (BGBl. I S. 1310), das zuletzt durch Artikel 4 des Gesetzes vom 22. März 2023 (BGBl. 2023 I Nr. 88) geändert worden ist, unterliegen, die Bezirksregierung Arnsberg.

Für die Verarbeitung der erforderlichen personenbezogenen Daten ist diejenige Behörde verantwortlich, die für die Durchführung des jeweiligen Verwaltungsverfahrens zuständig ist.

Nachfolgend werden die zuständigen Behörden als datenschutzrechtlich „Verantwortliche“ bezeichnet.

1.3.
Rechte und Pflichten der Verantwortlichen

Jeder Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Bestimmungen in seinem Verantwortungsbereich, insbesondere auch für die Rechtmäßigkeit der Weitergabe der zu verarbeitenden Daten an den Auftragnehmer allein verantwortlich.

Weisungsberechtigt sind dabei die zeichnungsbefugten Angehörigen der zuständigen Organisationseinheit.

Jeder Verantwortliche führt das Verarbeitungsverzeichnis nach Artikel 30 Absatz 1 der Datenschutz-Grundverordnung.

1.4
Auftragsverarbeiter

IT.NRW wird unter Beachtung des Prinzips der Datentrennung für jeden einzelnen Verantwortlichen als Auftragsverarbeiter gemäß Artikel 28 Absatz 3 Satz 1 der Datenschutz-Grundverordnung tätig. Für die Polizeibehörden und die Justizvollzugsanstalten gilt Artikel 28 Absatz 1 bis 4 der Datenschutz-Grundverordnung über § 35 Absatz 1 Satz 1 Nummer 1 und 3 in Verbindung mit § 52 Absatz 1 des Datenschutzgesetzes Nordrhein-Westfalen entsprechend. IT.NRW hat hinreichende Garantien dafür zu bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass sie die Vertraulichkeit sicherstellen und die Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung und des Datenschutzgesetzes Nordrhein-Westfalen erfolgt sowie der Schutz der Rechte der betroffenen Personen gewährleistet ist.

IT.NRW führt das Verarbeitungsverzeichnis gemäß Artikel 30 Absatz 2 der Datenschutz-Grundverordnung.

1.5
Zweckbestimmung und Anordnung der Auftragsverarbeitung

Die Nutzung von OSiP führt dazu, dass IT.NRW im Auftrag des jeweils Verantwortlichen die erforderlichen personenbezogenen Daten der in Nummer 2 der Anlage aufgeführten Betroffenen verarbeitet. Dadurch werden IT.NRW durch die jeweils Verantwortlichen personenbezogenen Daten offengelegt, die IT.NRW nur für fremde Zwecke des jeweiligen Verantwortlichen zu verarbeiten hat. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der Datenschutz-Grundverordnung und des Datenschutzgesetzes Nordrhein-Westfalen zu konkretisieren, wird die Auftragsverarbeitung mit den in dieser Richtlinie enthaltenen Vorgaben im Sinne eines für Verantwortliche und Auftragsverarbeiter geltenden Rechtsinstruments gemäß Artikel 28 Absatz 3 Satz 1 der Datenschutz-Grundverordnung verbindlich angeordnet.

1.6
Zuständigkeit des für Digitalisierung zuständigen Ministeriums

Das für Digitalisierung zuständige Ministerium finanziert den Betrieb von OSiP für das Land Nordrhein-Westfalen und beauftragt IT.NRW mit der Bereitstellung von OSiP für die Ressorts des Landes. Eine datenschutzrechtliche Verantwortung für die einzelnen Anwendungsbereiche seitens des für Digitalisierung zuständigen Ministeriums erwächst daraus nicht. Die in Ziffer 1.2 der Richtlinie festgelegten Verantwortlichkeiten werden nicht berührt.

2
Anwendungsbereich

2.1
Sachlicher Anwendungsbereich

Dieser Runderlass gilt für die Verarbeitung aller personenbezogenen Daten, die im Rahmen der Sicherheits- und Zuverlässigkeitsüberprüfung mit OSiP anfallen oder IT.NRW bekannt werden, im Folgenden Daten. Nicht unter den Anwendungsbereich fallen Daten von Beschäftigten des Landesbetriebs IT.NRW, soweit sie ausschließlich das Beschäftigungsverhältnis betreffen.

2.2
Räumlicher Anwendungsbereich

Die Verarbeitung der Daten im Auftrag des Verantwortlichen findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

3
Konkretisierung des Auftragsinhalts

3.1
Datenverarbeitung

Gegenstand und Dauer der Auftragsverarbeitung sowie Umfang, Art und Zwecke der vorgesehenen Verarbeitung sowie die Art der Daten ergeben sich aus den Festlegungen in der Anlage.

3.2
Kreis betroffener Personen

Der Kreis der durch die Verarbeitung ihrer Daten betroffenen Personen ergibt sich aus den Festlegungen in Nummer 2 der Anlage.

4
Rechte und Pflichten des Auftragsverarbeiters

4.1
Einhaltung datenschutzrechtlicher Bestimmungen

IT.NRW hat sämtliche datenschutzrechtlichen Bestimmungen im Sinne der Datenschutz-Grundverordnung und des Datenschutzgesetzes NRW einzuhalten. IT.NRW führt das Verarbeitungsverzeichnis gem. Artikel 30 Absatz 2 der Datenschutz-Grundverordnung und stellt den Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 der Datenschutz-Grundverordnung niedergelegten Pflichten zur Verfügung.

4.2
Betroffenenrechte

Für die Gewährleistung der Betroffenenrechte nach den Artikeln 12 bis 22 der Datenschutz-Grundverordnung ist der jeweils Verantwortliche zuständig. Soweit sich eine betroffene Person unmittelbar an den Landesbetrieb IT.NRW wendet, leitet dieser das Ersuchen unverzüglich an den jeweils Verantwortlichen weiter. IT.NRW unterstützt den jeweils Verantwortlichen bei der Gewährleistung der Betroffenenrechte.

4.3
Datenverarbeitung auf Weisung

IT.NRW darf Daten ausschließlich im Rahmen der Weisungen des jeweils Verantwortlichen verarbeiten, sofern er nicht anderweitig zu einer anderen Verarbeitung verpflichtet ist. In einem solchen Fall teilt IT.NRW dem Verantwortlichen die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Artikel 28 Absatz 3 Satz 2 Buchstabe a der Datenschutz-Grundverordnung).

Eine Weisung ist die auf eine bestimmte Datenverarbeitung durch IT.NRW gerichtete schriftliche, elektronische oder mündliche Anordnung des Verantwortlichen. Mündliche Weisungen hat der Verantwortliche unverzüglich schriftlich zu bestätigen. IT.NRW informiert den jeweils Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung des jeweils Verantwortlichen gegen Datenschutzbestimmungen verstößt.

Der jeweils Verantwortliche kann jederzeit die Herausgabe Berichtigung, Anpassung, Löschung oder Einschränkung der Verarbeitung der Daten verlangen.

4.4
Zweckbindung

IT.NRW hat die Daten für keine anderen als die in dieser Richtlinie festgelegten Zwecke zu verwenden und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Auskünfte an Dritte oder die zu überprüfende Person darf IT.NRW nur nach vorheriger ausdrücklicher schriftlicher oder elektronischer Zustimmung durch den jeweils Verantwortlichen erteilen.

Kopien und Duplikate werden mit Ausnahme von Sicherheitskopien zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung nicht erstellt.

4.5
Datenverarbeitung durch Beschäftigte des Auftragsverarbeiters

IT.NRW gewährleistet, dass ihm unterstellte natürliche Personen, die Zugang zu Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten. Die von IT.NRW eingesetzten Personen müssen die notwendige fachliche Qualifikation und Zuverlässigkeit aufweisen. Dafür gewährleistet IT.NRW, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4.6
Gegenseitige Unterstützung

Verantwortliche und Auftragsverarbeiter haben sich gegenseitig beim Nachweis und der Dokumentation der ihnen obliegenden Rechenschaftspflicht im Hinblick auf die Grundsätze ordnungsgemäßer Datenverarbeitung einschließlich der Umsetzung der notwendigen technischen und organisatorischen Maßnahmen im Sinne von Artikel 5 Absatz 2, Artikel 24 Absatz 1 und Artikel 30 der Datenschutz-Grundverordnung zu unterstützen. Der jeweils Verantwortliche und IT.NRW stellen sich hierzu bei Bedarf entsprechende Informationen zur Verfügung.

4.7
Mitteilungspflicht über Kontrollen durch Aufsichtsbehörden

IT.NRW informiert den oder die Verantwortlichen unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde im Rahmen ihrer Zuständigkeit bei IT.NRW anfragt, ermittelt oder sonstige Erkundigungen einzieht und stellt den Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 der Datenschutz-Grundverordnung niedergelegten Pflichten zur Verfügung.

5
Technische und organisatorische Maßnahmen, im Folgenden TOMs, und deren Kontrolle

IT.NRW hat für OSiP geeignete technische und organisatorische Maßnahmen aufzustellen. Diese Maßnahmen hat IT.NRW detailliert zu dokumentieren und den Verantwortlichen zur Kenntnis zu geben. Die Einhaltung der technischen und organisatorischen Sicherheitsmaßnahmen hat IT.NRW jederzeit zu gewährleisten.

Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Die TOMs für OSiP sind daher nach dem aktuellen Stand der Technik fortzuentwickeln. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Sämtliche Änderungen sind zu dokumentieren.

IT.NRW hat dem jeweils Verantwortlichen alle erforderlichen Informationen zur Verfügung zu stellen, die zum Nachweis der Einhaltung der in diesem Erlass getroffenen und der gesetzlichen Vorgaben erforderlich sind. IT.NRW wird insbesondere Überprüfungen und Inspektionen, die von einem Verantwortlichen oder einer oder einem anderen von diesem mit der Prüfung Beauftragten durchgeführt werden, ermöglichen und deren Durchführung unterstützen.

Auf Verlangen eines Verantwortlichen hat IT.NRW Informationen über die TOMs an diesen herauszugeben.

6
Umgang mit Verletzungen des Schutzes personenbezogener Daten durch den Auftragsverarbeiter

IT.NRW unterrichtet die Verantwortlichen umgehend nach Bekanntwerden über schwerwiegende Störungen in seinem Betriebsablauf, über den Verstoß oder den Verdacht eines Verstoßes gegen diese Vereinbarung sowie gesetzliche Datenschutzbestimmungen und über andere Unregelmäßigkeiten bei der Verarbeitung der Daten des jeweils Verantwortlichen. IT.NRW spricht sich hinsichtlich der zu treffenden Maßnahmen und des weiteren Verfahrens mit dem beziehungsweise den Verantwortlichen ab. Die Regelungen der Artikel 33 und 34 der Datenschutz-Grundverordnung bleiben davon unberührt.

7
Löschung und Rückgabe von Daten

Wird das Auftragsverarbeitungsverhältnis zwischen dem jeweils Verantwortlichen und IT.NRW beendet oder fordert ein Verantwortlicher IT.NRW dazu auf, sind sämtliche in den Besitz von IT.NRW gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigte Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem jeweils Verantwortlichen zu übermitteln oder nach vorheriger Zustimmung des Verantwortlichen datenschutzgerecht zu löschen. Die Datenlöschung ist zu dokumentieren. Ein Löschungsprotokoll ist dem Verantwortlichen auf Anforderung vorzulegen. Die Dokumentation der Löschung ist von IT.NRW zum Zweck der Datenschutzkontrolle gemäß § 52 Absatz 2 Satz 6 des Datenschutzgesetzes Nordrhein-Westfalen drei Jahre aufzubewahren.

8
Unterauftragsverhältnisse

Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter ist nur zulässig, wenn der Verantwortliche zuvor schriftlich zugestimmt hat.

IT.NRW hat sicherzustellen, dass in der Vereinbarung mit dem Subunternehmer das Datenschutzniveau diesem Runderlass entspricht und alle Vorgaben dieses Runderlasses eingehalten werden können. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Aufgaben von IT.NRW und des Subunternehmers deutlich voneinander abgegrenzt werden.

Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn dieser die Verpflichtungen nach Artikel 29 und Artikel 32 Absatz 4 der Datenschutz-Grundverordnung bezüglich seiner Beschäftigten erfüllt hat. IT.NRW hat die Einhaltung der Pflichten des Subunternehmers zu überprüfen. Das Ergebnis der Überprüfung ist zu dokumentieren und dem Verantwortlichen auf Verlangen zugänglich zu machen.

IT.NRW haftet gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Subunternehmers.

9
Inkrafttreten, Außerkrafttreten

Dieser Runderlass tritt am Tag nach der Veröffentlichung in Kraft und am 31. Dezember 2029 außer Kraft.

MBl. NRW. 2024 S. 964.

Anlagen

Anlage 1 (Anlage)
URL zur Anlage [Anlage]