

Umgang mit der Datenschutz- Grundverordnung

Leitfaden für öffentliche Stellen in Nordrhein-
Westfalen

Stand: August 2018

Umgang mit der Datenschutzgrundverordnung

Orientierungshilfe für öffentliche Stellen in Nordrhein-Westfalen

Stand: August 2018

Herausgeber:

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Kavalleriestraße 2 – 4

40213 Düsseldorf

Tel.: 0211/38424-0

Fax: 0211/38424-10

E-Mail: poststelle@ldi.nrw.de

Dieser Leitfaden kann unter www.ldi.nrw.de abgerufen werden.

Umgang mit der Datenschutz-Grundverordnung

Orientierungshilfe für öffentliche Stellen in Nordrhein-Westfalen

Inhalt

Einleitung	4
I. Zusammenspiel von DS-GVO und nationalen Gesetzen	4
II. Zulässigkeit der Datenverarbeitung	5
1. Personenbezogene Daten	5
2. Datenverarbeitung	6
3. Rechtsgrundlage	6
4. Exkurs: Verarbeitung besonderer Kategorien personenbezogener Daten	8
III. Grundsätze der Datenverarbeitung, technische und organisatorische Maßnahmen, Dokumentations- und Rechenschaftspflicht	9
IV. Verantwortlicher	9
V. Auftragsverarbeiter	9
VI. Betroffenenrechte	10
1. Informationspflichten des Verantwortlichen	10
2. Sonstige Rechte der betroffenen Person	11
a) Auskunftsrecht	11
b) Berichtigungsrecht	12
c) Löschungsrecht	12
d) Recht auf Einschränkung der Verarbeitung	12
e) Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung	12
f) Recht auf Datenübertragbarkeit	12
g) Widerspruchsrecht	13
VII. Verarbeitungsverzeichnis	13
VII. Datenschutz-Folgenabschätzung	13
IX. Meldepflichten	14

Einleitung

Seit dem 25. Mai 2018 gilt nach zweijähriger Übergangsfrist die Datenschutzgrundverordnung (DS-GVO) in allen Mitgliedstaaten der Europäischen Union (EU), die das Ziel hat, ein einheitliches unionsweites Datenschutzniveau zu etablieren. Um die öffentlichen Stellen in Nordrhein-Westfalen (NRW) bei der Ausübung datenschutzkonformen Handelns zu unterstützen, soll diese Orientierungshilfe einen Überblick über das neue Datenschutzrecht und das Zusammenspiel der verschiedenen Gesetze geben.

Im Rahmen eines solchen Überblicks kann naturgemäß nicht auf jedes Detail und jede Ausnahme eingegangen werden; diese Orientierungshilfe erhebt deshalb keinen Anspruch auf Vollständigkeit. Insbesondere gelten die folgenden Ausführungen nicht für Behörden, soweit diese im Rahmen ihrer Zuständigkeit Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung verarbeiten. Hierfür sind nicht die DS-GVO maßgeblich, sondern eine neue Datenschutz-Richtlinie (RL 2016/680/EU) und ein spezieller Teil des neuen Datenschutzgesetzes NRW (DSG NRW) – nämlich Teil 3, §§ 35 ff. DSG NRW. Mit öffentlichen Stellen in NRW sind Stellen i.S.d. DSG NRW gemeint, also die obersten Landesbehörden, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform. Auf Stellen, für die Besonderheiten gelten, wie etwa Gerichte, der Landesrechnungshof oder der Landtag wird hier nicht eingegangen.

Eine Zusammenfassung zu den wichtigsten Punkten gibt unser 9-Punkte-Papier [„Auf dem Weg zum neuen Datenschutzrecht — Anregungen für öffentliche Stellen in NRW“](#).

I. Zusammenspiel von DS-GVO und nationalen Gesetzen

Die DS-GVO ist in jedem EU-Mitgliedstaat und damit auch in Deutschland bzw. NRW unmittelbar anwendbar. Daneben findet das DSG NRW in seiner neuen Fassung Anwendung. Es gilt für öffentliche Stellen in NRW und wurde zum 25. Mai 2018 angepasst. Es konkretisiert bzw. ergänzt einige Vorgaben der DS-GVO und macht von Spielräumen Gebrauch, die der europäische Gesetzgeber den Mitgliedstaaten vereinzelt eingeräumt hat (Öffnungsklauseln). Konzeptionell greifen DS-GVO und DSG NRW ineinander und können bzw. müssen zusammen angewendet werden.

Darüber hinaus gibt es je nach Sachgebiet auch bereichsspezifische Datenschutzvorschriften in Bundes- und Landesgesetzen, die von den Behörden der Länder oder der Kommunen in NRW anzuwenden sind. Spezielle Sachbereiche, besondere Sachverhalte, besonders einschneidende Verarbeitungsweisen und/oder die Verarbeitung bestimmter Daten etc. sind bereichsspezifisch zu regeln bzw. sind bereits geregelt. Dieses Fachrecht behält seine hohe Bedeutung, weil § 5 Abs. 6 DSG NRW vorsieht, dass besondere Rechtsvorschriften dem DSG NRW vorgehen. Dies

gilt aber nur, soweit ihr Regelungsgehalt einen speziellen Bereich auch vollständig abdeckt. Wird ein Sachverhalt, für den das DSGVO NRW gilt, nicht oder nicht abschließend durch das Spezialgesetz geregelt, sind die Lücken durch Anwendung des DSGVO NRW bzw. der DS-GVO zu füllen.

Die Anpassung der bereichsspezifischen Vorschriften an die DS-GVO erfolgt sukzessive und ist Aufgabe des Gesetzgebers. Um den Landesgesetzgeber zu unterstützen, hat die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI NRW) das sogenannte [Eckpunktepapier](#) erstellt.

II. Zulässigkeit der Datenverarbeitung

Immer wieder äußern öffentliche Stellen die Besorgnis, nunmehr nicht mehr auf vertraute Strukturen des Datenschutzrechts zurückgreifen zu können. Insbesondere in Bezug auf die Prüfung der Zulässigkeit einer Datenverarbeitung ist diese Sorge allerdings unbegründet. Zwar sind hier ggf. neue „Fundstellen“ für Legaldefinitionen und zum Teil auch für Rechtsgrundlagen zu beachten; in der Sache ändert sich diesbezüglich jedoch oft gar nicht viel, vgl. [Schema zur alten und neuen Rechtslage](#).

Die „Leitlinie“ für die Prüfung einer solchen Zulässigkeit fand sich bis zum 24. Mai 2018 in § 4 Abs. 1 DSGVO NRW alte Fassung (a.F.). Danach war die Verarbeitung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubte oder die betroffene Person eingewilligt hatte. Die Begriffe „personenbezogene Daten“, „Datenverarbeitung“ und „Einwilligung“ waren praktischerweise im DSGVO NRW a.F. selbst normiert, ebenso wie besondere und allgemeine Rechtsgrundlagen für die Datenverarbeitung. Bereichsspezifische Vorschriften galt es allerdings auch bis dato bereits zu beachten.

An diesem Prinzip des sogenannten „Verbots mit Erlaubnisvorbehalt“, das in Deutschland seit jeher dem gesamten Datenschutzrecht zugrunde liegt, hat sich mit der Anwendung der DS-GVO nichts geändert (vgl. Art. 5 Abs. 1 lit. a i.V.m. Art. 6 DS-GVO). Auch weiterhin ist eine Verarbeitung personenbezogener Daten durch eine öffentliche Stelle des Landes NRW verboten, wenn sie nicht ausnahmsweise erlaubt ist. Die entsprechenden Legaldefinitionen sowie auch der „Einstieg“ in die Prüfung finden sich nunmehr allerdings nicht mehr im DSGVO NRW, sondern in der DS-GVO.

1. Personenbezogene Daten

Kernbegriff und zwingende Voraussetzung für die Anwendbarkeit des Datenschutzrechts ist weiterhin, dass sogenannte „personenbezogene Daten“ verarbeitet werden. Darunter sind alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DS-GVO).

Jede Information kann ein personenbezogenes Datum sein, ohne dass es auf qualitative oder quantitative Kriterien zur Bestimmung des Informationsgehalts oder Informationswerts ankommt. Der Begriff ist nach wie vor sehr weit zu verstehen: Geschützt werden nicht nur unmittelbar identifizierende Informationen, sondern viel-

mehr auch Angaben, die erst durch Kombination miteinander und/oder mit Zusatzwissen auf eine konkrete Person zu beziehen sind.

2. Datenverarbeitung

Der Schutzbereich des Datenschutzrechts ist betroffen, wenn ein personenbezogenes Datum „verarbeitet“ wird.

Der Begriff „Verarbeitung“ bezeichnet gemäß Art. 4 Nr. 2 DS-GVO

- „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe
- im Zusammenhang mit personenbezogenen Daten
- wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“.

Diese denkbar weite Auflistung von Verarbeitungsvorgängen zeigt deutlich, dass quasi jeder Umgang mit personenbezogenen Daten eine Verarbeitung darstellt und damit dem Datenschutzrecht unterliegt. Die DS-GVO selbst enthält zwar eine Einschränkung, da sie für automatisierte Verarbeitungen sowie in einem Dateisystem gespeicherte oder dafür bestimmte Daten gilt. Wann genau von einer solchen automatisierten Verarbeitung oder einem Dateisystem auszugehen ist, ist für öffentliche Stellen jedoch unerheblich, weil das DSG NRW – wie auch schon bisher – eine solche Einschränkung nicht vorsieht und öffentliche Stellen auch bei nichtautomatisierten Verarbeitungen an das Datenschutzrecht bindet (vgl. § 5 Abs. 8 DSG NRW). Dies umfasst sogar beispielsweise den mündlichen Datenaustausch.

Im Hinblick auf diese Grundvoraussetzungen für die Anwendbarkeit des Datenschutzrechts bringt die DS-GVO keine wesentlichen Veränderungen im Vergleich zur bisherigen Rechtslage mit sich.

3. Rechtsgrundlage

Wie oben bereits ausgeführt ändert auch die DS-GVO an dem seit jeher geltenden Prinzip eines „Verbots mit Erlaubnisvorbehalt“ nichts (vgl. Art. 5 Abs. 1 lit. a i.V.m. Art. 6 DS-GVO). Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist immer dann verboten, wenn sie nicht ausnahmsweise nach Art. 6 Abs. 1 DS-GVO erlaubt ist.

Art. 6 Abs. 1 Satz 1 DS-GVO benennt sechs Konstellationen, in denen eine solche Erlaubnis gegeben ist:

- a) Einwilligung der betroffenen Person;
- b) Erforderlichkeit der Verarbeitung zur Erfüllung eines Vertrags, den der Betroffene geschlossen hat;

- c) **Erforderlichkeit zur Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt;**
- d) Erforderlichkeit, um lebenswichtige Interessen einer natürlichen Person zu schützen;
- e) **Erforderlichkeit für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;**
- f) Erforderlichkeit zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (sofern keine überwiegenden Interessen/Grundrechte/Grundfreiheiten der betroffenen Person gegeben sind).

Zu beachten ist, dass für Behörden im Rahmen ihrer hoheitlichen Tätigkeit **Buchstabe a)** – Einwilligung – nur eingeschränkt zur Verfügung steht. Eine Einwilligung können Behörden im Rahmen ihrer hoheitlichen Tätigkeiten nicht heranziehen, sofern aufgrund eines bestehenden Über-/Unterordnungsverhältnisses zwischen Staat und Bürgerin bzw. Bürger eine Freiwilligkeit der Einwilligung nicht gewährleistet werden kann (Erwägungsgrund 43). Deshalb wird die Einwilligung nur in den Fällen als Grundlage für eine Datenverarbeitung in Betracht kommen, in denen sich die öffentliche Stelle und die Bürgerin bzw. der Bürger quasi auf Augenhöhe begegnen und die betroffene Person keinerlei Nachteile befürchten muss, wenn sie die Einwilligung verweigert. Dabei muss ihnen zudem eine echte Handlungsalternative zur Verfügung stehen. Eine Legaldefinition der „Einwilligung“ enthält Art. 4 Nr. 11 DS-GVO; weitere Vorschriften finden sich insbesondere in Art. 7 f. DS-GVO.

In der alltäglichen Behördenarbeit wird der Schutz lebenswichtiger Interessen – **Buchstabe d)** – als Erlaubnisgrundlage eher selten in Betracht kommen. Auch Verträge mit betroffenen Personen – **Buchstabe b)** – sind zumindest nicht das primäre Handlungsinstrument öffentlicher Stellen.

Die wesentlichen Erlaubnistatbestände für öffentliche Stellen sind deshalb Art. 6 Abs. 1 Satz 1 lit. **c und e** DS-GVO. Die jeweiligen rechtlichen Verpflichtungen oder Aufgabenzuweisungen müssen dabei auf EU-Recht oder nationalem Recht beruhen (Art. 6 Abs. 3 DS-GVO). Der maßgebliche Unterschied zwischen Buchstabe c und Buchstabe e besteht darin, dass die rechtliche Verpflichtung bei Buchstabe c gerade in der Datenverarbeitung bestehen muss. Dies kann beispielsweise der Fall sein, wenn ein Gesetz eine öffentliche Stelle dazu verpflichtet, ein Register zu führen. Bei Buchstabe e dagegen ist Gegenstand der zugewiesenen Aufgabe nicht die Datenverarbeitung, sondern jede andere denkbare Handlung, bei deren Vornahme aber zwangsläufig auch personenbezogene Daten verarbeitet werden müssen.

Die Handhabung des Art. 6 Abs. 1 Satz 1 lit. c DS-GVO – Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung – dürfte keine besonderen Schwierigkeiten aufwerfen. Hierfür bedarf es nämlich einer anderen Rechtsvorschrift, die klar regelt, welche Daten zu welchem Zweck und in welcher Weise von der öffentlichen Stelle verarbeitet werden dürfen. An diesen spezialgesetzlichen Regelungen muss sich die öffentliche Stelle orientieren.

Art. 6 Abs. 1 Satz 1 lit. e DS-GVO – Wahrnehmung öffentlicher Aufgaben – wird durch § 3 Abs. 1 DSG NRW konkretisiert. Danach ist für öffentliche Stellen eine Datenverarbeitung zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe der verarbeitenden Stelle erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Gibt es bereichsspezifische Regelungen, gehen diese allerdings vor.

§ 3 Abs. 1 DSG NRW ist im Übrigen auch für die Weitergabe personenbezogener Daten innerhalb eines Verantwortlichen, z.B. zwischen zwei Ämtern einer Kommune, anzuwenden. Sah das alte Recht in § 14 Abs. 4 DSG NRW a.F. vor, dass die Vorschriften zur Übermittlung an eine andere öffentlichen Stelle auch für die Weitergabe personenbezogener Daten innerhalb einer öffentlichen Stelle anwendbar waren, fehlt eine solche Regelung im jetzigen DSG NRW. Das bedeutet aber nicht, dass eine Weitergabe innerhalb einer öffentlichen Stelle unbeschränkt erfolgen darf (Grundsatz der informationellen Gewaltenteilung; weite Definition der Verarbeitung (Art. 4 Nr. 2 DS-GVO)).

Das Kriterium der Erforderlichkeit ist nicht neu. Es ist Ausfluss des Gebots der Datensparsamkeit und Datenminimierung und sowohl qualitativ als auch quantitativ zu verstehen. Es ist stets zu prüfen, ob überhaupt personenbezogene Daten verarbeitet werden müssen und wenn ja, wie viele, welche, in welcher Form, wie lange etc. Ob die Verarbeitung eines Datums erforderlich ist, hängt davon ab, ob sie für die Erreichung des Zwecks (Wahrnehmung der Aufgaben oder Erfüllung der rechtlichen Verpflichtungen) geeignet ist und kein milderer gleich geeignetes Mittel zur Verfügung steht. Im Ergebnis wird diese Prüfung auf eine Interessenabwägung im Sinne einer Verhältnismäßigkeitsprüfung hinauslaufen, die generell Maßstab staatlichen Handelns ist und bei der festzustellen ist, ob die Aufgabenerfüllung auch genauso gut ohne Verarbeitung des betroffenen personenbezogenen Datums möglich ist. Je sensibler das betroffene Datum ist, desto höher ist sein Schutzbedarf und desto weniger entbehrlich darf es für die Wahrnehmung der Aufgaben sein.

Unbedingt zu beachten ist, dass für Behörden im Rahmen ihrer hoheitlichen Tätigkeit **Buchstabe f** – Wahrung berechtigter Interessen – als Erlaubnistatbestand nicht zur Verfügung steht. Nach der Regelung in Art. 6 Abs. 1 Satz 2 DS-GVO gilt diese Variante ausdrücklich nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Datenverarbeitung.

4. Exkurs: Verarbeitung besonderer Kategorien personenbezogener Daten

Zur Verarbeitung besonderer Kategorien personenbezogener Daten wird auf das [Kurzpapier Nr. 17 der Datenschutzkonferenz \(DSK\) „Besondere Kategorien personenbezogener Daten“](#) verwiesen.

Wie dort ausgeführt können einige der in Art. 9 Abs. 2 DS-GVO genannten Erlaubnistatbestände nur eingreifen, wenn dies im mitgliedstaatlichen Recht vorgesehen ist. Dies wird durch § 16 DSG NRW aufgegriffen. Zusätzlich schreibt § 15 DSG NRW vor, welche Maßnahmen eine öffentliche Stelle zum Schutz des Betroffenen

ergreifen muss, wenn sie besondere Kategorien personenbezogener Daten verarbeitet.

III. Grundsätze der Datenverarbeitung, technische und organisatorische Maßnahmen, Dokumentations- und Rechenschaftspflicht

Besonders wichtig ist es auch zu gewährleisten, dass die in Art. 5 Abs. 1 DS-GVO normierten Grundsätze der Datenverarbeitung umfassend eingehalten werden. Dies gilt sowohl in rechtlicher als auch in technischer und organisatorischer Hinsicht. Der Verantwortliche muss die Einhaltung dieser Grundsätze gemäß Art. 5 Abs. 2 DS-GVO nachweisen können („Rechenschaftspflicht“). Nach Maßgabe des Art. 24 Abs. 1 Satz 1 DS-GVO hat er durch geeignete technische und organisatorische Maßnahmen sicherzustellen und den Nachweis zu erbringen, dass die Verarbeitung gemäß der Verordnung erfolgt. Es bedarf also insgesamt geeigneter und umfassender Dokumentationen. Bestandteil der Dokumentation sollte – wie bisher – auch ein Datensicherheitskonzept sein.

In diesem Zusammenhang sei erwähnt, dass Art. 25 DS-GVO zudem bestimmte Rahmenbedingungen für die Art und Weise enthält, wie die Anforderungen der DS-GVO schon bei der Technik- bzw. Prozessgestaltung („Privacy-by-Design“) und durch Voreinstellungen („Privacy-by-Default“) umzusetzen sind. Diese Vorgaben sind auch durch öffentliche Stellen in NRW zu beachten.

IV. Verantwortlicher

Verantwortlicher für die Datenverarbeitung ist gemäß Art. 4 Nr. 7 DS-GVO jede Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Regelfall ist deshalb zumindest nach außen hin bei öffentlichen Stellen die Behörde, vertreten durch den Behördenleiter, Verantwortlicher. Gemeinden und Gemeindeverbände sind grundsätzlich „als Ganzes“ Verantwortliche (vgl. § 5 Abs. 1 Satz 1 DSGVO NRW; Ausnahmen, soweit besonders gesetzlich geregelt). Dies ändert aber nichts daran, dass im Innenverhältnis jeder Behördenmitarbeiter zur Einhaltung des Datenschutzrechts verpflichtet ist.

Weiterhin gibt es noch die Möglichkeit einer gemeinsamen Verantwortung gemäß Art. 26 DS-GVO, wenn mindestens zwei Verantwortliche gemeinsam Mittel und Zwecke der Verarbeitung festlegen. Hierzu finden sich nähere Informationen im [Kurzpapier Nr. 16 der DSK „Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DS-GVO“](#).

V. Auftragsverarbeiter

Nimmt eine Stelle fremde Dienstleistungen in Anspruch, in deren Rahmen personenbezogene Daten an den dritten Dienstleister weitergegeben und von diesem fremdnützig für die auftraggebende Stelle verarbeitet werden, ist dieser Dritte möglicherweise „Auftragsverarbeiter“. Auch dieser ist unter der DS-GVO in gewisser

Weise verantwortlich, obwohl sich der Auftraggeber seiner Verantwortung für die Rechtmäßigkeit der Datenverarbeitung dadurch nicht entledigen kann. Beim Einsatz von Auftragsverarbeitern sind gemäß Art. 28 DS-GVO viele Aspekte zu beachten, mit denen die Rechtmäßigkeit und Sicherheit der Verarbeitung durch den Auftragsverarbeiter sichergestellt werden sollen.

Nähere Informationen zum Thema Auftragsverarbeitung finden sich im [Kurzpapier Nr. 13 der DSK „Auftragsverarbeitung, Art. 28 DS-GVO“](#).

VI. Betroffenrechte

Ein Schwerpunkt der DS-GVO liegt in der qualitativen und quantitativen Ausweitung der Betroffenenrechte gegenüber dem bisherigen Rechtszustand. Zu nennen sind hier die Informationspflichten bei Datenerhebung sowie die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit sowie das Widerspruchsrecht. Generell gilt im Rahmen der Erfüllung dieser Betroffenenrechte, dass Informationen und Mitteilungen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen müssen. Einer bürgernahen, verständlichen Ausdrucksweise und serviceorientierten Arbeitsweise kommt deshalb besondere Bedeutung zu.

1. Informationspflichten des Verantwortlichen

Um den Betroffenen von Anfang an das nötige Wissen über die Verarbeitung ihrer Daten zu verschaffen, sehen Art. 13 und 14 DS-GVO umfangreiche Informationspflichten der Stelle vor, die Daten erhebt. Dabei wird unterschieden zwischen einer Datenerhebung bei der betroffenen Person selbst und einer sonstigen Datenerhebung. Werden Daten direkt beim Betroffenen erhoben, sieht Art. 13 DS-GVO vor, dass die Information „zum Zeitpunkt der Erhebung“ erfolgen soll, was ein unmittelbares Tätigwerden erfordert. Werden die Daten dagegen nicht beim Betroffenen, sondern aus anderer Quelle erhoben, soll die Information innerhalb einer angemessenen Frist, längstens jedoch innerhalb eines Monats, bzw. zum Zeitpunkt der ersten Kommunikationsaufnahme oder der ersten Weitergabe der Daten an eine andere Stelle erteilt werden. Eine „Erhebung“ ist jede Handlung, mit der auf bestimmte personenbezogene Daten zielgerichtet zugegriffen wird. Dies gilt auch, wenn einer Stelle Daten übermittelt werden, die sie zielgerichtet zur weiteren Verarbeitung entgegennimmt. Werden einer Stelle dagegen unaufgefordert Daten übermittelt, beispielsweise per Post oder per Mail, liegt in der bloßen Annahme der Nachrichten noch keine Erhebung. Schließt sich dem aber eine weitere Verarbeitung an, wofür schon eine zielgerichtete Speicherung ausreicht, ist eine Erhebung gegeben. Werden die Daten dagegen sofort gelöscht, liegt keine Erhebung vor, obwohl auch das Löschen grundsätzlich dem Verarbeitungsbegriff unterfällt.

Wegen der Einzelheiten, insbesondere des Umfangs der zu erteilenden Informationen, wird auf das [Kurzpapier Nr. 10 der DSK „Informationspflichten bei Dritt- und Direkterhebung“](#) verwiesen.

Erfolgt die Dritterhebung bei einer nicht-öffentlichen Stelle oder sonstigen dritten natürlichen Personen, sieht § 7 DSGVO eine weitere Informationspflicht vor, die jedoch nicht gegenüber der Person gilt, auf die sich die Daten beziehen, sondern gegenüber der Stelle, von der die Daten erhoben werden: Auf deren Verlangen muss sie über den Zweck der Erhebung informiert werden, sofern nicht schutzwürdige Belange des Betroffenen entgegenstehen. Wird diese dritte Stelle aufgrund einer gesetzlichen Auskunftspflicht für die Erhebung herangezogen, muss ihr die Vorschrift mitgeteilt werden, aus der sich diese Auskunftspflicht ergibt. Anderenfalls muss ein Hinweis auf die Freiwilligkeit ihrer Angaben durch die öffentliche Stelle erfolgen.

Art. 13 und 14 DSGVO enthalten zudem Ausnahmen von der Informationspflicht, welche noch durch § 11 Abs. 1 DSGVO ergänzt werden. Betroffen sind dabei Fälle, in denen durch die Erteilung der Information eine etwaige Strafverfolgung gefährdet würde, Geheimhaltungsvorschriften bestehen oder die Verfolgung zivilrechtlicher Ansprüche beeinträchtigt würde. Außerdem verankert § 11 Abs. 2 DSGVO noch einen Zustimmungsvorbehalt zugunsten dort genannter Sicherheits- und Strafverfolgungsbehörden, falls Daten der betroffenen Person an diese Stellen übermittelt werden und der Betroffene aufgrund der Informationspflicht darüber informiert werden müsste. Auch gelten gemäß § 5 Abs. 9 DSGVO Art. 13 und 14 DSGVO nicht für Verarbeitungen, die nicht dem Anwendungsbereich von Art. 2 Abs. 1 DSGVO unterfallen, also beispielsweise für Telefongespräche ohne weitere Verarbeitung der Daten.

2. Sonstige Rechte der betroffenen Person

Die übrigen Rechte bedürfen zu ihrer Geltendmachung eines Antrags. Ist ein solcher gestellt, sind die beantragten Informationen gemäß Art. 12 Abs. 3 DSGVO unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen. Sollte es in Anbetracht der Anzahl der Anträge oder deren Komplexität erforderlich sein, kann diese Frist um zwei Monate verlängert werden. In diesem Fall muss die betroffene Person noch innerhalb des ersten Monats nach Eingang des Antrags über eine Fristverlängerung und die Gründe für die Verzögerung unterrichtet werden. Bei elektronischer Antragstellung soll auch die Unterrichtung möglichst auf elektronischem Wege erfolgen.

a) Auskunftsrecht

Informationen zum Auskunftsrecht sind in [Kurzpapier Nr. 6 der DSK „Auskunftsrecht der betroffenen Person, Art. 15 DSGVO“](#) enthalten.

Eine gewisse Erleichterung hinsichtlich der Erfüllung des Auskunftsrechts sieht § 12 Abs. 1 DSGVO für den Fall vor, dass die öffentliche Stelle große Mengen von Daten über den Betroffenen verarbeitet, der Auskunft begehrt. In diesem Fall darf von dem Antragsteller gefordert werden, dass er präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich sein Auskunftsersuchen bezieht. Dies gilt in besonderem Maße für Kommunen, da ansonsten bei allen Ämtern nach Daten

des Betroffenen geforscht werden müsste. Ausreichend ist allerdings eine Angabe der in Betracht kommenden Ämter. Darüber hinaus enthält § 12 Abs. 2 und 3 DSGVO NRW Ausschlussgründe für den Auskunftsanspruch, die weitgehend den oben zu § 11 DSGVO NRW erläuterten entsprechen (also insbesondere Gefährdung von Strafverfolgung oder der öffentlichen Sicherheit, Geheimhaltungspflichten und Zustimmungsvorbehalt bei Auskunft über Übermittlung von Daten an Strafverfolgungs- und Sicherheitsbehörden).

b) Berichtigungsrecht

Das Recht auf Berichtigung unrichtiger Daten aus Art. 16 DSGVO war auch zuvor schon im DSGVO NRW a.F. enthalten.

c) Löschungsrecht

Ausführungen zum Löschungsrecht des Art. 17 DSGVO finden sich in [Kurzpapier Nr. 11 der DSK „Recht auf Löschung / „Recht auf Vergessenwerden“](#).

d) Recht auf Einschränkung der Verarbeitung

Das Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO weist zum Teil Parallelen zur früheren Sperrung von Daten auf. Als mögliche Maßnahmen zur Umsetzung der Einschränkung der Verarbeitung benennt Erwägungsgrund 67 beispielsweise die vorübergehende Übertragung von Daten auf ein anderes Verarbeitungssystem, die Sperrung der Daten für Nutzer oder die vorübergehende Entfernung veröffentlichter Daten von einer Webseite.

e) Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung

Um die Effektivität der soeben dargestellten Betroffenenrechte der Art. 16 - 18 DSGVO auch in den Fällen sicherzustellen, in denen die Daten an dritte Stellen weitergegeben worden sind, erlegt Art. 19 DSGVO dem ursprünglichen Verarbeiter die Pflicht auf, den jeweiligen Empfängern diese Maßnahmen mitzuteilen. Dies erfordert praktisch einen Rückgriff auf die sorgfältig erstellte Dokumentation, an wen Daten weitergegeben worden sind. Ausgeschlossen ist die Mitteilungspflicht, wenn ihre Erfüllung unmöglich oder nur mit unverhältnismäßigem Aufwand möglich ist.

f) Recht auf Datenübertragbarkeit

Das Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO, mit dessen Hilfe Betroffene einen digitalen Auszug ihrer Daten erhalten können sollen, wird bei öffentlichen Stellen weitgehend nicht bedeutsam sein, weil es nur gilt, wenn die Datenverarbeitung auf einer Einwilligung beruht oder sie zulässig ist, weil sie für die Erfüllung eines Vertrages erforderlich ist. Bei Verarbeitungen, die hingegen zur Aufgabenerfüllung einer öffentlichen Stelle erforderlich sind oder auf einer rechtlichen Verpflichtung beruhen, kommt dieses Recht nicht zur Anwendung.

g) Widerspruchsrecht

Schließlich ist noch das Widerspruchsrecht des Art. 21 DS-GVO zu erwähnen. Für öffentliche Stellen ist dies relevant, wenn sie die Datenverarbeitung darauf stützen, dass sie für ihre Aufgabenwahrnehmung nach Maßgabe des Art. 6 Abs. 1 lit. e DS-GVO erforderlich ist. In diesen Fällen darf der Betroffene jederzeit Widerspruch gegen die Verarbeitung einlegen, sofern dieser auf Gründen beruht, die sich aus seiner besonderen Situation ergeben. Damit wird dem Umstand Rechnung getragen, dass Datenverarbeitungen im konkreten Fall für eine Person ausnahmsweise deutlich belastender und schädlicher sein können, als dies üblicherweise in vergleichbaren Situationen der Fall ist. Legt der Betroffene einen solchen Widerspruch ein und ist dieser begründet, muss die ihn betreffende Datenverarbeitung eingestellt werden. Eine Ausnahme gilt jedoch, wenn die öffentliche Stelle zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient. Darüber hinaus schließt § 14 DSGVO NRW dieses Widerspruchsrecht aus, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

VII. Verarbeitungsverzeichnis

Galt für öffentliche Stellen bisher gemäß § 8 DSGVO NRW a.F. die Pflicht, ein sogenanntes „Verfahrensverzeichnis“ zu erstellen, welches eine Art Übersichtsdokumentation über alle automatisierten Datenverarbeitungen der betreffenden Stelle war, sieht nun Art. 30 Abs. 1 DS-GVO vor, dass jeder Verantwortliche ein „Verarbeitungsverzeichnis“ erstellen muss. Die Anforderungen der DS-GVO an das Verarbeitungsverzeichnis sind zum Teil strenger als die an das frühere Verfahrensverzeichnis. Der Verantwortliche ist auch für die Erstellung und Führung dieses Verarbeitungsverzeichnisses verantwortlich. Mittels dieses Verzeichnisses soll er nachweisen können, dass er die Anforderungen der DS-GVO erfüllt. Es ist also Bestandteil der erweiterten Dokumentations- und Rechenschaftspflichten, die die DS-GVO vorsieht. Auch Auftragsverarbeiter haben die Pflicht, ein Verarbeitungsverzeichnis zu führen (Art. 30 Abs. 2 DS-GVO).

Informationen zu den konkreten Anforderungen finden sich in [Kurzpapier Nr. 1 der DSK „Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO“](#).

Muster und weitere Hinweise für Verantwortliche und Auftragsverarbeiter finden sich auf unserer [Internetseite](#).

VII. Datenschutz-Folgenabschätzung

Besteht bei Datenverarbeitungsvorgängen voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen, muss der Verantwortliche vorab eine Abschätzung der Folgen der vorhergesehenen Verarbeitungsvorgänge für den

Schutz personenbezogener Daten durchführen. Das bisherige Instrument der Vorabkontrolle entfällt.

Die Datenschutz-Folgenabschätzung ist also ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Ihr Ziel besteht darin, die Folgen der Datenverarbeitung möglichst umfassend zu erfassen und Maßnahmen zur Eindämmung der Risiken zu prüfen. Auf jeden Fall ist vor den Datenverarbeitungsvorgängen eine Schwellwertanalyse durchzuführen, ob in diesem Sinn ein hohes Risiko besteht; das Ergebnis ist zu dokumentieren. Ergibt diese ein voraussichtlich hohes Risiko, muss eine Datenschutz-Folgenabschätzung erfolgen und ebenfalls dokumentiert werden.

Näheres ist nachzulesen im [Kurzpapier Nr. 5 der DSK „Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO“](#) sowie im [Kurzpapier Nr. 18 der DSK „Risiko für die Rechte und Freiheiten natürlicher Personen“](#).

Die verbindliche, aber nicht abschließende Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO für den öffentlichen Bereich, für die immer eine Datenschutzfolgenabschätzung durchgeführt werden muss, ist auf unserer [Internetseite](#) veröffentlicht.

IX. Meldepflichten

Neu ist für öffentliche Stellen in NRW, dass es nunmehr bei der Verletzung des Schutzes personenbezogener Daten Melde- bzw. Benachrichtigungspflichten gibt, die das DSG NRW a.F. noch nicht vorsah.

Unter einer Verletzung des Schutzes personenbezogener Daten ist nach Art. 4 Nr. 12 DS-GVO „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“ zu verstehen. Ihre Grundlage finden diese neuen Pflichten in Art. 33 und 34 DS-GVO. Je nach Schwere der Verletzung und Risiko für den Betroffenen ist entweder nur eine unverzügliche Meldung bei der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW (LDI NRW) oder aber auch zusätzlich eine unverzügliche Benachrichtigung der Betroffenen vorgesehen.

Für Art, Umfang und Ausnahmen von diesen Meldepflichten sei auf die Ausführungen der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im Leitfaden [„Die DSGVO in der Bundesverwaltung“](#) (S. 19 ff.) verwiesen. Für öffentliche Stellen in NRW werden die bestehenden Ausnahmen für die Benachrichtigung des Betroffenen noch durch § 13 DSG NRW ergänzt, der ein Absehen von der Benachrichtigung aus Gründen der öffentlichen Sicherheit, wegen Geheimhaltungspflichten oder wegen der Gefährdung der Sicherheit von IT-Systemen erlaubt.

X. Behördliche Datenschutzbeauftragte

Auch weiterhin müssen öffentliche Stellen behördliche Datenschutzbeauftragte bestellen, Art. 37 Abs. 1 lit. a DS-GVO. Eine Ausnahmeregelung für kleinere Organisationseinheiten gibt es für öffentliche Stellen nicht.

Antworten auf häufig gestellte Fragen geben wir auf unserer [Internetseite](#).

Die Kontaktdaten der Datenschutzbeauftragten sind nach Art. 37 Abs. 7 DS-GVO der Aufsichtsbehörde mitzuteilen.

Die LDI NRW hat hierfür ein [Meldeportal](#) eingerichtet, welches auch über unsere [Internetseite](#) zu erreichen ist.