Landeshauptstadt Hannover

Informations-
drucksache

In den Organisations- und Personalausschuss

Nr. 0088/2019

Anzahl der Anlagen 0

Zu TOP

Information über das neues Datenschutzrecht

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 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 abgekürzt.

Geltung ab 25.05.2018.

Es handelt sich um unmittelbar geltendes Recht in allen Mitgliedstaaten der EU.

Ziel: Harmonisierung des Datenschutzrechts in der EU.

Die DSGVO gilt gleichermaßen für Unternehmen und Behörden.

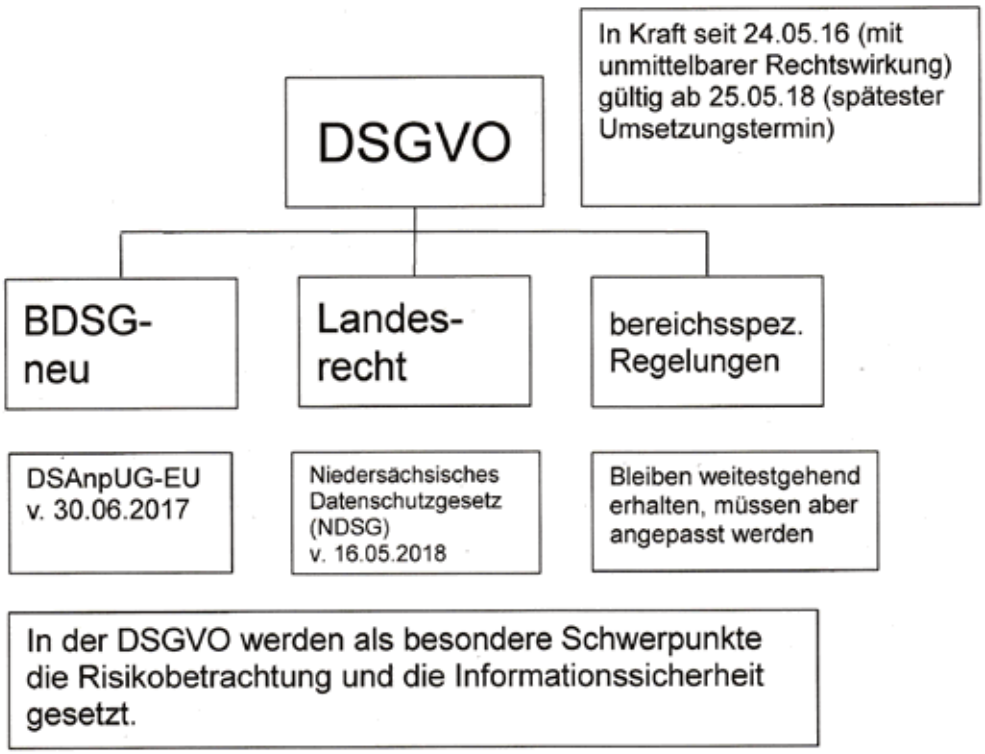
Gliederung:

I. Grundsätzliches zur DSGVO
I.1 EU-Recht, Bundes- und Landesrecht, Öffnungsklauseln
I.2 Verbindung mit Informationssicherheit
I.3 Aufbau der DSGVO

II. DSGVO - Inhalte der Verordnung
II.1 Der Verantwortliche (Art. 4 Nr. 7 DSGVO)
II.2.Der Datenschutzbeauftragte (Artt. 37 ff. DSGVO)
II.3 Betroffenenrechte (Artt. 12 ff. DSGVO)
II.4 Einige weitere neue Regelungen
II.5 Aufsichtsbehörde, Rechtsbehelfe, Haftung und Sanktionen

I. Grundsätzliches zur DSGVO

I.1
EU-Recht, Bundes- und Landesrecht, Öffnungsklauseln



Aber: insbesondere für den öffentlichen Bereich enthält die DSGVO viele Öffnungsklauseln und Regelungsaufträge für die nationalen Gesetzgeber.
Neben der DSGVO wird der Datenschutz geregelt im sonstigen EU-Recht, in neuen Datenschutzgesetzen von Bund und Ländern und bereichsspezifischen Regelungen in den Fachgesetzen wie z.B. im SGB X.

Zudem gehört zum neuen Regelungswerk noch die JI-Richtlinie 2016/680. Diese ist wie die von der DSGVO abgelöste Datenschutzrichtlinie von den Mitgliedsstaaten in nationales Recht umzusetzen. Dies ist mit Regelungen im BDSG und bezogen auf Niedersachsen im NDSG geschehen. Geregelt wird hier der Datenschutz in Zusammenhang mit Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten.

I.2
Informationssicherheit

In Zeiten fortschreitender Digitalisierung bekommt neben dem Datenschutz (Schutz der Person vor Missbrauch personenbezogener Daten) die Informationssicherheit zunehmend Bedeutung (Schutz aller Informationswerte eines Unternehmens).
Das können Informationen in Papier- oder IT-Form sein, Verträge, Urkunden, Kommunikation - aber auch das Wissen der Mitarbeiter*innen.

Die Hauptschutzziele der Informationssicherheit sind

- Vertraulichkeit (dass z.B. vertrauliche E-Mails auch vertraulich bleiben),
- Integrität (dass z.B. Kommunikation nicht verfälscht werden kann),
- Verfügbarkeit (dass wichtige Informationen jederzeit abrufbar sind).

Datenschutz und Informationssicherheit besitzen eine große Schnittmenge, haben aber u. U. im Einzelfall auch gegensätzliche Ziele.

Informationssicherheit etabliert man in der Regel in Form eines Informationssicherheits-Managementsystems (ISMS), internationaler Standard dafür ist die DIN/ISO 27001.

Ein ISMS ist eine Sammlung von Regeln und technisch-organisatorischer Maßnahmen, die auf Basis von Risikobewertungen für die zu schützenden Informationen ausgewählt, dokumentiert und zyklisch überprüft werden.

Durch ein ISMS auf Basis ISO 27001 wird erreicht

- die Erfüllung gesetzlicher Vorgaben (z.B. IT-Sicherheitsgesetz/KRITIS) – Stichwort Compliance,
- Vertrauen von Bürgern und Geschäftspartnern auf einen sicheren Umgang mit sensiblen Daten durch die LHH,
- Kostensenkungen durch risikobasierte Maßnahmen und die Etablierung von Standards.

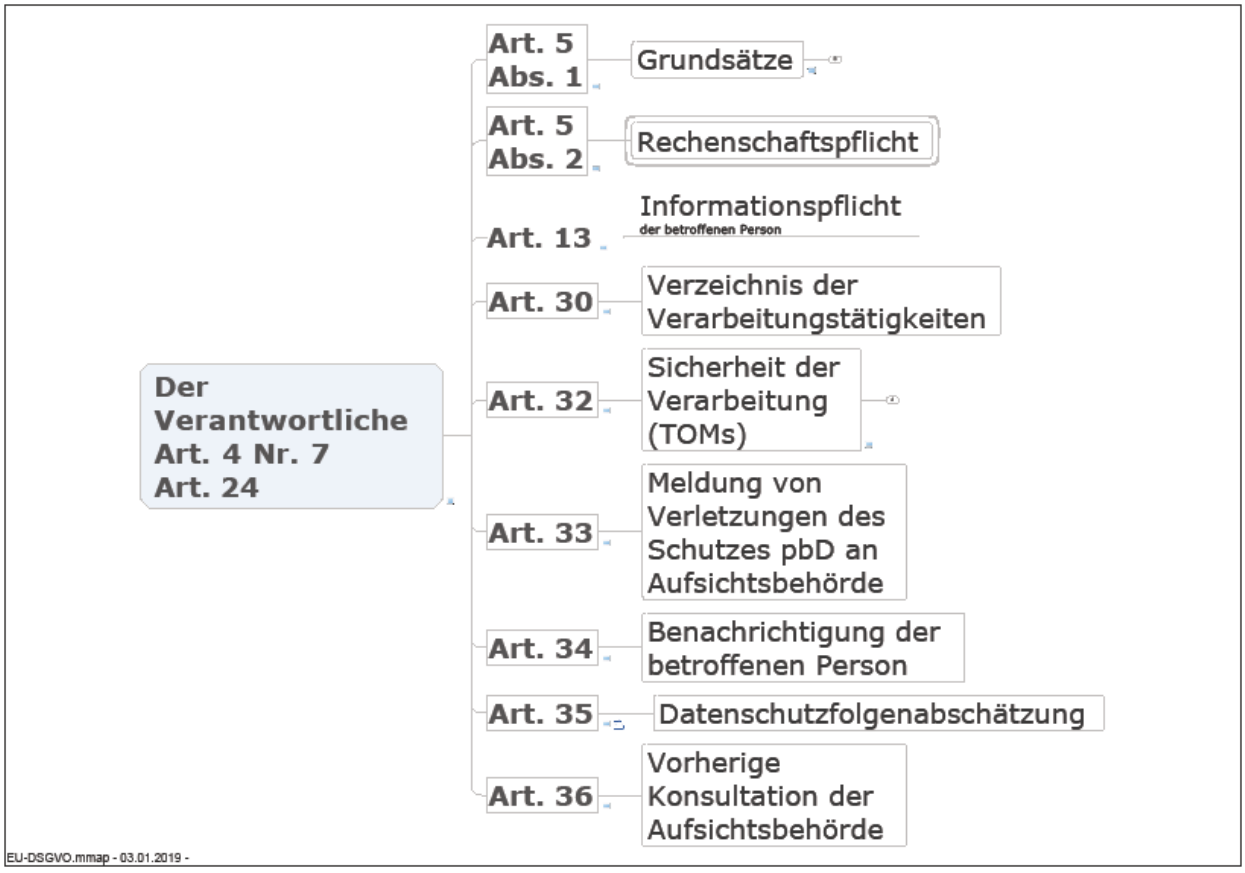
I.3
Aufbau der DSGVO

Die DSGVO ist ein Artikelgesetz mit 173 „Erwägungsgründen“ (Legal-Kommentierung des Verordnungsgebers).
EU-Verordnungen sind unmittelbar geltendes Recht.
Aber: die DSGVO enthält zahlreiche Öffnungsklauseln und ist damit teilweise „richtlinienähnlich“ konzipiert.
Ein Beispiel: die Öffnungsklausel des Art. 6 Abs. 2 u. Abs. 3 DSGVO i. V. m. Art. 6 Abs. 1 lit. c) und e)

- Möglichkeit der Konkretisierung der Datenverarbeitung (DV) zur Erfüllung einer gesetzlichen Pflicht oder öffentlichen Aufgabe.
- Bereichsspezifisches Datenschutzrecht kann weitestgehend aufrechterhalten werden.
    - Rechtsgrundlage zur DV ist wie bisher zunächst im Fachrecht zu suchen, hilfsweise Generalklausel (bisher §§ 9, 10 NDSG-alt, jetzt §3 NDSG).

II. DSGVO - Inhalte der Verordnung

II.1
Der Verantwortliche (Art. 4 Nr. 7 DSGVO)



Art. 24 Verantwortung des für die Verarbeitung Verantwortlichen

Technisch-organisatorische Maßnahmen (TOMs) **zur Sicherstellung und Erbringung des Nachweises**
dass die Verarbeitung gemäß der DSGVO erfolgt (gemeint sind alle Handlungen die dem dienen z. B.:

- die Ausrichtung technischer Systeme,
- die Instruktion des Personals (Dienstanweisungen und Dienstvereinbarungen),
- Notfallpläne.

Sie müssen geeignet sein, d.h. den konkreten Umständen unter **Abwägung des jeweiligen Risikos** (Eintrittswahrscheinlichkeit und Schwere der Risiken, siehe Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen) angemessen sein.
Es besteht die Pflicht zur regelmäßigen Überprüfung. Verhaltensregeln gemäß Art. 40 DSGVO oder ein Zertifizierungsverfahren gemäß Art. 42 DSGVO können herangezogen werden, um den Nachweis zu erbringen.

Art. 5 Abs. 1 Grundsätze für die Verarbeitung personenbezogener Daten

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und für die betroffene Person auf nachvollziehbare Weise („Transparenz“),
b) Festgelegte legitime Zwecke, Weiterverarbeitung nur in mit dem Zweck vereinbarender Weise („Zweckbindung“),
c) Angemessen und erheblich für Zweck und Beschränkung auf notwendige Maß („Datenminimierung“),
d) Sachlich richtig und erforderlichenfalls auf dem neuesten Stand („Richtigkeit“),
e) Frühestmögliche Pseudo-/Anonymisierung („Speicherbegrenzung“),
f) Integrität und Vertraulichkeit.

Art. 5 Abs. 2: Verantwortlicher hat Rechenschaftspflicht bzgl. in Abs. 1 genannter Grundsätze

Im Rahmen der Nachweispflicht sind insbesondere folgende Unterlagen vorzulegen („Dokumentation“):

- Verzeichnis von Verarbeitungstätigkeiten,
- Datenschutz-Folgenabschätzungen, insbesondere für risikobehaftete Datenverarbeitungen,
- Leitlinien/Datenschutzkonzepte/Datenschutzrichtlinien,
- IT-Sicherheitskonzept mit Beschreibung der getroffenen technischen u. organisatorischen Datensicherungsmaßnahmen,
- Dokumentation von Einwilligungserklärungen und Schulungsmaßnahmen,
- Verträge zur Auftragsverarbeitung,
- Zertifikat/Datenschutzaudit eines unabhängigen Dritten.

Art. 13, 14 Informationspflichten, Art. 15 Auskunftsrecht

Umfängliche Informationspflichten des Verantwortlichen

- gegenüber den betroffenen Personen bei der Erhebung personenbezogener Daten sowie bei etwaigen zweckändernden Weiterverarbeitungen wie z.B.:
  - den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters,
  - gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten,
  - die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung,
  - die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer.

Ziel:

- Herstellung eines größtmöglichen Maßes an Transparenz und die betroffenen Personen sollen in die Lage versetzt werden, ihre Rechte umfassend wahrzunehmen.
  - Wird das Auskunftsrecht elektronisch geltend gemacht, sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen.

Art. 30 Verzeichnis von Verarbeitungstätigkeiten

Nach Abs. 1 S.1 sind alle (nicht nur automatisierte!) Verarbeitungstätigkeiten des Verantwortlichen zu erfassen.

- Pflicht für Verantwortliche; Mindestinhalt lit. a-g wie z.B.
  - die Zwecke der Verarbeitung,
  - eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
- Schriftform (auch elektronisch),
- Unterlagen, die auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen sind (nicht mehr das sogenannte „Jedermannverzeichnis“ gem. § 8a NDSG-alt),
- Zusätzliche Inhalte sind in der Neufassung der ADA 18/1 der LHH (Datenschutz und Datensicherheit) detailliert zu definieren.

Art. 32 Sicherheit der Verarbeitung (TOMs)

- Pseudonymisierung und Verschlüsselung,
- Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit auf Dauer sicherstellen,
- Verfügbarkeit im Schadensfall rasch wiederherstellen,
- Regelmäßige Überprüfung, Bewertung und Evaluierung der TOMs.

Dies wird im Regelfall durch das Rechenzentrum sichergestellt, aber es gibt bei der LHH auch

- dezentrale Dienstanweisungen, Dienstvereinbarungen und
- dezentrale IT-Systeme.

Art. 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

- Voraussetzung: Risiko für Rechte und Freiheiten der Betroffenen,
- Meldung unverzüglich, möglichst binnen 72 Stunden,
- Beschreibung der Datenschutzverletzung (Handlung einzelner Personen oder Schwachstellen in Verfahren?) und ungefähre Zahl der betr. Datensätze, Name und Kontaktdaten des DSB, Folgenbeschreibung, Beschreibung ergriffener oder vorgeschlagener Maßnahmen,
- Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen sind vom Verantwortlichen zu dokumentieren.

Art. 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

- Voraussetzung: hohes Risiko für Rechte und Freiheiten der Betroffenen,
- die Benachrichtigung hat unverzüglich zu erfolgen,
- sie muss Namen und Kontaktdaten der oder des DSB, Folgenbeschreibung, Beschreibung ergriffener oder vorgeschlagener Maßnahmen enthalten und zwar
- in klarer und einfacher Sprache.
- Ausnahmen: wenn geeignete technische oder organisatorische Sicherheitsvorkehrungen getroffen wurden (sodass Daten unzugänglich sind) oder andere nachfolgende Maßnahmen getroffen wurden (sodass sich aller Wahrscheinlichkeit nach Risiko nicht mehr realisiert) oder eine einzelne

Benachrichtigung einen unverhältnismäßigen Aufwand bedeutet (dann öffentliche Bekanntmachung).

Art. 35 Datenschutz-Folgenabschätzung

- Wenn eine Verarbeitungsform ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellt; zu beurteilen anhand: Art, Umfang, Umständen, Zwecken; zeitlich: „vorab“.

Insbesondere in folgenden Fällen:

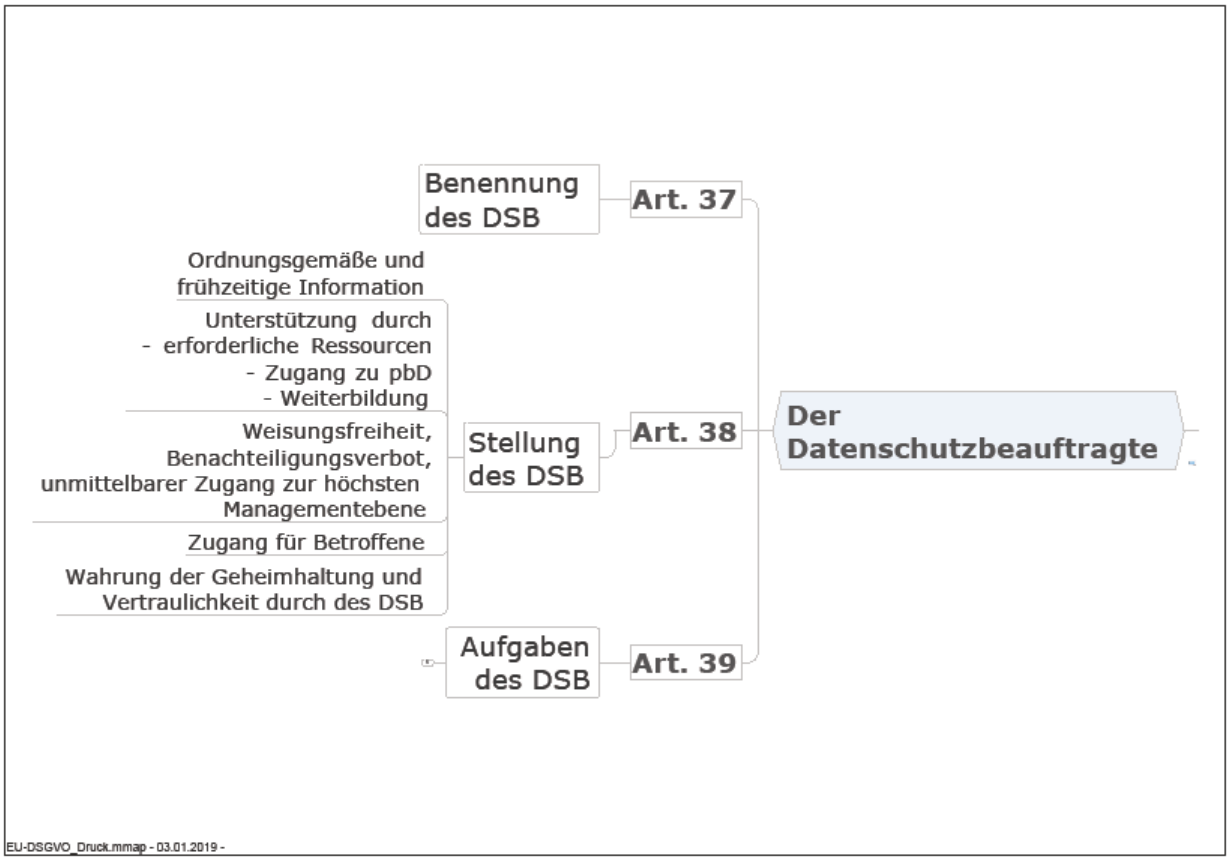
- Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen basierend auf automatisierter Verarbeitung, wenn dies Grundlage für rechtswirksame Entscheidungen ist.
- Umfangreiche Verarbeitung von Daten nach Art. 9 Abs. 1 / Art. 10.
- Systematische und umfangreiche Überwachung öffentlich zugänglicher Bereiche (Videoüberwachung).

<u>Mindestanforderungen:</u>

- systematische Beschreibung der Verarbeitungsvorgänge und -zwecke (ggf. berechtigtes Interesse des Verantwortlichen darlegen),
- Bewertung von Notwendigkeit und Verhältnismäßigkeit in Bezug auf den Zweck,
- Bewertung der Risiken für Rechte und Freiheiten gem. Abs. 1,
- geplante Abhilfemaßnahmen einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren zur Bewältigung der Risiken,
- ggf. Einholung Standpunkt Betroffener.

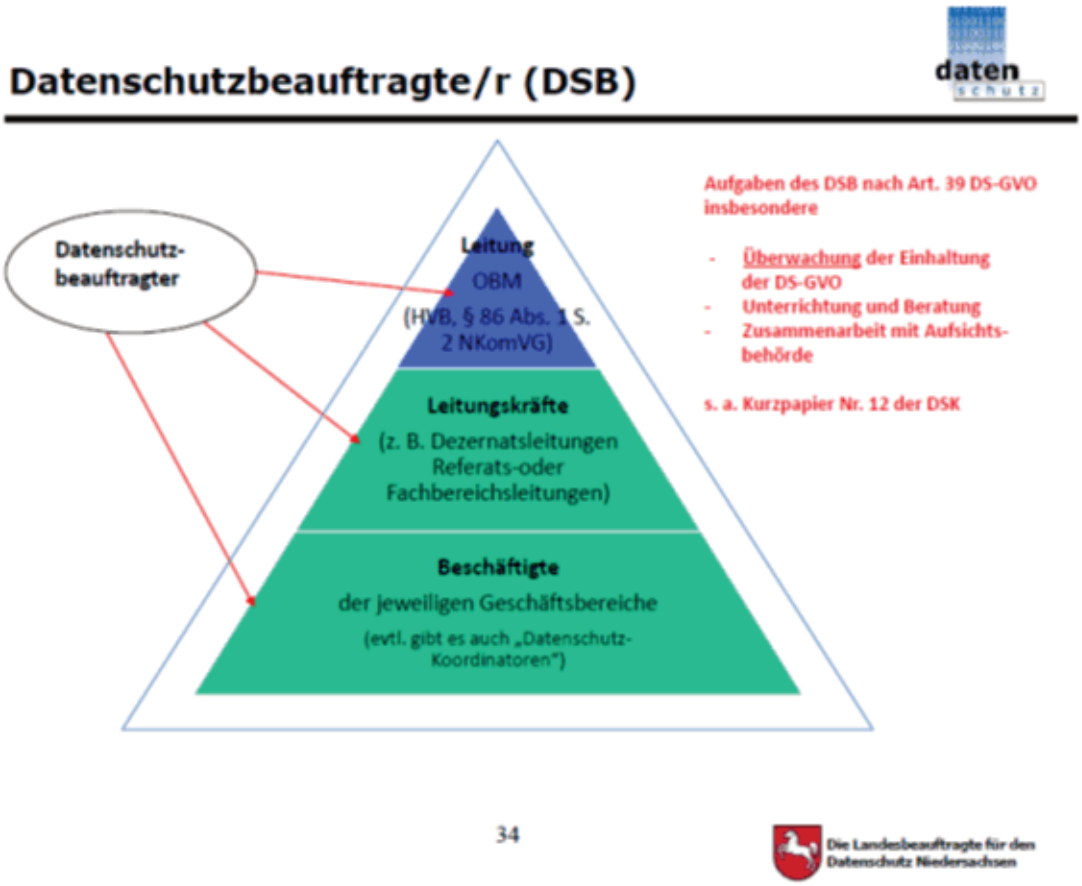
Die Datenschutz-Folgeabschätzung ist vom **Verantwortlichen** vorzunehmen, der Rat der/des Datenschutzbeauftragten **ist** einzuholen.

II.2
Der Datenschutzbeauftragte (Artt. 37 ff. DSGVO)



Art. 38 Stellung des Datenschutzbeauftragten

- Ordnungsgemäße und frühzeitige Einbindung des DSB-Teams in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen,
- Unterstützungspflicht des Verantwortlichen, u.a. durch
  - erforderliche Ressourcen,
  - Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen (Es gibt keine kontrollfreie Datenverarbeitung, Kühling/Buchner, DSGVO, Art. 38, Rn. 18; Der Zugang zu personenbezogenen Daten umfasst auch Daten, die einem Geschäfts- oder Berufsgeheimnis unterliegen, Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 38 Rn. 27, 28, beck-online),
  - Zutritt zu allen Räumlichkeiten in denen personenbezogene Daten verarbeitet werden oder werden könnten (Kühling/Buchner, DSGVO, Art. 38, Rn. 19),
- Weisungsfreiheit, unmittelbarer Zugang zur höchsten Managementebene,
- Abberufungs- und Benachteiligungsverbot,
- Wahrung der Geheimhaltung und Vertraulichkeit durch den DSB.



Art. 39 Aufgaben des Datenschutzbeauftragten

- Unterrichtung und Beratung des Verantwortlichen,
- Überwachung
  - der Einhaltung der DSGVO,
  - anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten,
  - der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Beschäftigten und der diesbezüglichen Überprüfungen.
- Beratung und Überwachung in Zusammenhang mit der Datenschutz-Folgenabschätzung,
- Anlaufstelle für die Aufsichtsbehörde.
- Der Datenschutzbeauftragte erfüllt seine Aufgaben entsprechend einer Risikoabwägung bei den Verarbeitungsvorgängen.

II.3
Betroffenenrechte (Artt. 12 ff. DSGVO)

Recht auf Information (Artt. 13, 14 DSGVO)
Der Verantwortliche muss zum Zeitpunkt der Datenerhebung dem Betroffenem u.a. den Zweck der Verarbeitung, die Rechtsgrundlage, die Kategorien der verarbeiteten Daten und die Speicherdauer mitteilen.

Recht auf Auskunft
Der Betroffene kann Auskunft über seine verarbeiteten personenbezogenen Daten verlangen (Art. 15 DSGVO).

Recht auf Berichtigung
Der Betroffene kann die Berichtigung oder Vervollständigung seiner Daten verlangen (Art. 16 DSGVO).

Recht auf Löschung
Der Betroffene kann unter den Voraussetzungen des Art. 17 DSGVO die Löschung seiner personenbezogenen Daten verlangen (sofern nicht rechtliche Gründe wie z.B. gesetzliche Aufbewahrungsfristen dem entgegenstehen). Das Recht auf Vergessenwerden erweitert dieses Betroffenenrecht auf Inhalte, die im Internet veröffentlicht worden sind.

Recht auf Einschränkung der Verarbeitung
In den in Art. 18 DSGVO genannten Fällen (z.B. wenn die Richtigkeit der gespeicherten Daten bestritten wird) hat der Betroffene das Recht, eine Einschränkung der Verarbeitung der ihn betreffenden Daten zu verlangen.

Recht auf Datenübertragbarkeit
Der Betroffene kann verlangen, dass seine personenbezogenen Daten einem anderen „Anbieter“ übertragen werden (Art. 20 DSGVO). Dies gilt nicht, soweit die Verarbeitung in Wahrnehmung öffentlicher Aufgaben erfolgt(e).

Recht auf Widerspruch
Der Betroffene hat ein Widerspruchsrecht gegen die Verarbeitung seiner personenbezogenen Daten, soweit dafür Gründe vorliegen, die sich aus seiner besonderen Situation ergeben, und sofern an der Verarbeitung kein überwiegendes öffentliches Interesse besteht oder eine Rechtsvorschrift die Verarbeitung dieser Daten vorschreibt (Art. 21 DSGVO).

Widerrufsrecht bei Einwilligung
Beruht die Verarbeitung personenbezogener Daten auf einer Einwilligung, kann der Betroffene diese jederzeit mit Wirkung für die Zukunft widerrufen.

II.4
Einige weitere neue Regelungen

- **Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO)**
  Die Verarbeitung besonders sensibler Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder welt-anschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt – es sei denn es liegen ausdrücklich geregelte Ausnahmen vor (Art. 9 Abs. 2 DSGVO). Diese sind im Vergleich zu Art. 6 DSGVO strenger.
- **Privacy by Design - Privacy by Default (Art. 25 DSGVO)**
  Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen stellt Anforderungen an die Produktentwicklung und -implementierung, um eine wirksame Umsetzung der Datenschutzgrundsätze zu erreichen.
  Dazu zählen angemessene technische und organisatorische Maßnahmen wie z. B. Verschlüsselung oder Pseudonymisierung.

  Der Verantwortliche muss darüber hinaus sicherstellen, dass Standardeinstellungen darauf ausgerichtet sind, nur personenbezogene Daten zu verarbeiten, die für den konkreten Zweck auch erforderlich sind. Das betrifft den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

- **Auftragsverarbeiter (Art. 28 DSGVO)**
  - Anforderungen festlegen
    (z. B. Erstellung Lastenheft, Art. 25 DSGVO beachten),
  - Hinweise für Bieter im Vergabeverfahren/Ausschreibung aufnehmen, dass Auftragsverarbeitung den Anforderungen der DSGVO entsprechen muss,
  - Eignung des Auftragsverarbeiters prüfen,
  - Geeignete Garantien/Nachweise wie z. B. Zertifizierungen des Auftragsverarbeiters anfordern und prüfen, s. u. a. Regelungen zu genehmigten Zertifizierungsverfahren nach Art. 42 DSGVO

Haftung und Recht auf Schadenersatz (Art. 82 DSGVO) richten sich nunmehr auch direkt gegen den Auftragsverarbeiter.

II.5
Aufsichtsbehörde, Rechtsbehelfe, Haftung und Sanktionen

Art. 58 Befugnisse der Aufsichtsbehörde (Auszug)

Jede Aufsichtsbehörde verfügt über Untersuchungsbefugnisse,

- den Verantwortlichen, anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind,
- Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen.

Jede Aufsichtsbehörde verfügt über Abhilfebefugnisse,

- den Verantwortlichen anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,
- eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen.

Die Befugnis, Geldbußen zu verhängen (Art. 83 DSGVO), steht der Aufsichtsbehörde gegenüber öffentlichen Stellen nur zu, soweit diese als Unternehmen am Wettbewerb teilnehmen (§ 20 Abs. 5 NDSG):

Art. 77 Recht auf Beschwerde bei einer Aufsichtsbehörde

- Jede betroffene Person hat das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.

Art. 79 DSGVO Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter.

- Jede betroffene Person hat das Recht auf einen wirksamen gerichtlichen Rechtsbehelf.

Art. 82 DSGVO Haftung und Recht auf Schadenersatz

- Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Auszug aus dem NDSG:

§ 59 NDSG Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer
als Person, die bei einer öffentlichen Stelle oder deren Auftragsverarbeiter dienstlichen Zugang zu nicht allgemein zugänglichen personenbezogenen Daten hat oder hatte, diese Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck

a. speichert, verändert oder übermittelt,
b. zum Abruf bereithält,
c. abruft oder sich oder einem anderen verschafft oder
d. in anderer Weise verarbeitet

oder

personenbezogene Daten, die in dem Anwendungsbereich dieses Gesetzes verarbeitet werden und nicht allgemein zugänglich sind, durch Vortäuschung falscher Tatsachen sich oder einer anderen Person verschafft oder sich oder einer anderen Person durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung offenlegen lässt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50 000 Euro geahndet werden.

§ 60 NDSG Straftaten

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, eine in § 59 Abs. 1 genannte Handlung begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person zusammenführt und dadurch wieder bestimmbar macht.

(2) Der Versuch ist strafbar.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, der Auftragsverarbeiter und die von der oder dem Landesbeauftragten geleitete Behörde.

Quellenangabe

- Die Bundesbeauftragte für den Datenschutz und die Informationssicherheit, Datenschutz-Grundverordnung
- Die Landesbeauftragte für den Datenschutz Niedersachsen, Umsetzung der EU-Datenschutz-Grundverordnung (DSGVO) bei Behörden und sonstigen öffentlichen Stellen in Niedersachsen
- Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Kurzpapiere
- Artikel-29-Datenschutzgruppe, WP 243 rev.01 de, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“)
- Kühling/Buchner: DSGVO, 1. Auflage 2017, München: C. H. Beck
- Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO, beck-online

Berücksichtigung von Gender-Aspekten
Gender-Aspekte werden durch diese Info-Drucksache nicht berührt.

Kostentabelle
Es entstehen keine finanziellen Auswirkungen.

18DS
Hannover / 09.01.2019