

## **Leitfaden für den Datenschutz**

Eine Arbeitshilfe der

Beauftragten für den Datenschutz des Jobcenters Wuppertal

Stand: Juni 2021

## Inhaltsverzeichnis

<b>Präambel .....</b>	<b>3</b>
Daten gehören zum Alltag.....	5
Der Wert der eigenen Daten.....	5
<b>Datenschutz im öffentlichen Bereich gleicht die Asymmetrie der Kräfte zwischen Staat und Bürgern*in aus .....</b>	<b>6</b>
Das Urteil des Bundesverfassungsgerichts zur informationellen Selbstbestimmung.....	7
Datenschutz im Jobcenter allgemein .....	8
<b>Europäisches Recht ab Mai 2018.....</b>	<b>9</b>
Ein Querschnittsthema lebt vom lebendigen Austausch .....	10
Das ganzheitliche Beratungskonzept im Kontext des Datenschutzes.....	12
<b>Was man über Datenschutz wissen sollte.....</b>	<b>13</b>
Wichtige Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 DSGVO.....	16
<b>Regeln.....</b>	<b>17</b>
Datenschutz ganz praktisch.....	19
Grafik: Prozessverlauf Verarbeitung von Sozialdaten.....	22
<b>Grafiken: Datenübermittlung der Sozialleistungsträger untereinander.....</b>	<b>23</b>
Übermittlungsersuchen- in welchen Fällen darf eine Übermittlung erfolgen? .....	26
Grafik: Übermittlung für die Erfüllung sozialer Aufgaben.....	27
<b>Beispiele .....</b>	<b>28</b>
Kurzübersicht: Schutz der Sozialdaten und Übermittlungsbefugnisse .....	31
<b>Die Beauftragte für den Datenschutz .....</b>	<b>35</b>
Aufgaben der Datenschutzbeauftragten des Jobcenters.....	36
Stellung der Datenschutzbeauftragten des Jobcenters .....	38
Die zuständige Aufsichtsbehörde .....	39

## Präambel

Auf den ersten Blick scheint Datenschutz eine sehr trockene und theoretische Materie zu sein, deren Inhalte ausschließlich für Fachleute relevant sind.

Bei näherer Betrachtung wird erkennbar: **Das Thema Datenschutz betrifft uns alle jeden Tag.**

Datenschutz hat an Relevanz gewonnen, weil sich unsere Gesellschaft tiefgreifend verändert. Wir erleben aktuell den Wandel zu einer digitalisierten Informationsgesellschaft. Er vollzieht sich in rasantem Tempo und erfasst alle Alters- und Bevölkerungsgruppen. Mittlerweile stehen digitale Dienstleistungsangebote gleichrangig neben Analogangeboten; in einigen Bereichen haben digitale Angebote die analogen bereits verdrängt.

Das Besondere an digitalen Angeboten: sie funktionieren über den Austausch von Daten. Und überall dort, wo Daten ausgetauscht werden, müssen auch Vorkehrungen für ihren Schutz getroffen werden.

Mit einem Beispiel aus dem Alltag lässt sich gut verdeutlichen, wo jede\*r Einzelne in seinem/ihrer Leben eine direkte Verbindung mit dem Thema Datenschutz hat.

Ein Smartphone gehört für die meisten Menschen in unserer Gesellschaft zu ihrem Leben. Natürlich wird mit dem Smartphone auch telefoniert, aber angesichts der vielen anderen Kommunikationsmöglichkeiten eines Smartphones ist das Telefonieren –von Krisenzeiten einmal abgesehen- eher zum Randphänomen geworden.

Mit dem Smartphone tragen wir einen Rundum-Service in der Tasche, den wir -immer vorausgesetzt, es existiert eine Funkverbindung- jederzeit aktivieren können.

Mit einem durchschnittlichen Smartphone können wir:

- uns an völlig fremden Orten orientieren,
- überall auf der Welt interessante und wichtige Orte, sogenannte POI, finden,
- das nächstgelegene Restaurant finden, das zu unserem Geschmack passt,
- den Pannenservice für das liegen gebliebene Auto rufen, ohne ihn je selbst eingespeichert zu haben,
- eine Haltestelle für Bus und Bahn finden und ihre Fahrpläne einsehen, ohne physisch dort zu sein,
- ortsunabhängig ein Ticket für Bus, Bahn, Flugzeug kaufen,
- unabhängig vom eigenen Standort Waren suchen, auswählen, bestellen, an beliebige Orte liefern lassen und auf vielfältige Art bezahlen,
- Paketsendungen zu einer anderen Lieferadresse umleiten,

- überall auf der Welt Informationen suchen und finden,
- uns mit Freunden verabreden,
- auf die gespeicherten Kontaktdaten zugreifen,
- elektronisch Kontakte mit völlig Fremden knüpfen,
- unabhängig vom eigenen Standort Gruppen bilden,
- überall auf der Welt die eigenen Musikfavoriten hören oder neue Musik aussuchen,
- Blogs abonnieren,
- Über soziale Medien die eigene Meinung äußern und Beiträge anderer ansehen/ anhören und bewerten,
- Nachrichten lesen, hören und sehen,
- Podcasts erstellen und hören,
- einen YouTube-Kanal betreiben,
- fotografieren und filmen,
- Bilder und Filme versenden,
- Filme ansehen,
- Streamingdienste abonnieren,
- Gesichter beim Fotografieren erkennen,
- E-Mails erhalten, schreiben und versenden,
- mit Hilfe eines Übersetzungsprogramms in einer völlig fremden Sprache etwas zu Essen kaufen, und, und, und.



Spätestens mit dieser Auflistung der Möglichkeiten wird klar, über welche Menge an Informationen über seine\*n Besitzer\*n ein durchschnittliches Smartphone verfügt und verfügen muss, um jederzeit die Vielzahl an Diensten bieten zu können. Die Liste ist nur ein Auszug der Möglichkeiten.

Das Smartphone speichert, was wir mögen und liefert uns stets den kürzesten Weg zu unseren Favoriten. Das Lieferprinzip wird deutlich: Komfort gegen Daten.

Die Grundlage einer digitalisierten Informationsgesellschaft ist der schnelle Informationsaustausch der Menschen untereinander. Das bedeutet, eine große Menge an Daten wird gesendet und empfangen; sie wechseln den Ort, wechseln den Server.

Dass ihre persönlichen Daten dabei nicht die/den Besitzer\*in wechseln, sondern immer ihre Daten bleiben, ist die Aufgabe des Datenschutzes.

## **Daten gehören zum Alltag**

Elektronische Medien sind aus dem Alltag nicht mehr wegzudenken. Handliche Geräte in ansprechendem Design wie Smartphones, Tablets, Smartwatches, etc. können mit Apps zusätzlich zu ihren umfangreichen Grundfunktionen je nach Bedarf individuell um spezielle Funktionen für alle Lebensbereiche und Interessensgebiete erweitert werden. Die Angebote umfassen ein breites Spektrum, das von der Kalenderfunktion mit Terminplanung über unterschiedliche Kommunikationsformate, die Abwicklung von Bankgeschäften und die Lieferung medizinischer Dienstleistungen, die Buchung von Reiseverbindungen bis hin zu elektronischen Anträgen auf Geldleistungen bei Behörden reicht. Die beliebtesten Funktionen, Onlinedienste und Apps nutzen täglich weltweit Milliarden Menschen.

## **Der Wert der eigenen Daten**

Mit jeder Aktivität im Netz erzeugen Nutzer\*innen Daten. Wegen der Komplexität des Vorgangs ist es schwierig, zu durchschauen, welche Daten durch die eigenen Aktivitäten erzeugt werden, wo die eigenen Daten nach Beendigung einer Transaktion landen, von wem sie wofür genutzt werden und ob sie an Dritte weitergegeben oder gespeichert werden. Für die Nutzer\*innen haben diese Daten nach Beendigung der gewünschten Transaktion eher den Status digitaler Abfallprodukte, an die sie kaum Gedanken verschwenden.

Dass diese Daten aber keineswegs Abfall sind, wird durch die Tatsache deutlich, dass spezialisierte Analysedienste für den Ankauf der Nutzerdaten Geld zahlen. Mit Hilfe von Algorithmen gewinnen die Analysedienste aus ihnen wertvolle Nutzerprofile. Durch einen schnellen Klick auf „Cookies akzeptieren“ erlauben Nutzer\*innen den Zugriff auf personenbezogene Daten wie: den Standort ihres Servers, den genutzten Browser, das genutzte Gerät, Daten zur eigenen Mobilität (Google Maps trackt den Standort des Smartphones und generiert daraus u.a. Staumeldungen), beliebte Orte, Daten zu Absprung- und Konversionsraten (Absprungrate ist die Dauer des Verbleibs auf einzelnen Seiten, die Konversionsrate misst, wie lange es dauert, bis Interessierte zu Kunden\*innen werden), die Dauer der Onlineaktivität, die beliebtesten Websites, bevorzugte Produkte und Marken, bevorzugter Preisrahmen, bevorzugte Einkaufszeit, Entscheidungsgeschwindigkeit, etc..

In einer Marktwirtschaft, in der ein Preis durch das Verhältnis von Angebot und Nachfrage gebildet wird, hat die Person eine starke Marktposition, die besitzt, was eine andere Person gern hätte. Bezogen auf den Wert der eigenen Daten stimmt die Theorie nur zur Hälfte; denn die starke Marktposition erwächst nicht allein aus dem Besitz; sondern daraus, dass man den Wert des eigenen Besitzes kennt und die Preisverhandlung entsprechend selbstbewusst führen kann.

Vielen Menschen ist der Wert der eigenen Daten jedoch kaum bis gar nicht bewusst.

## Datenschutz im öffentlichen Bereich gleicht die Asymmetrie der Kräfte zwischen Staat und Bürger\*in aus

Daten fallen nicht nur bei Kaufprozessen und bei privatrechtlichen Aktivitäten an; auch im öffentlich-rechtlichen Bereich, beim Umgang mit Behörden und öffentlichen Einrichtungen, unterstützen IT-Systeme die Prozesse und es werden Daten verarbeitet. Immer dann, wenn Bürger\*innen ihre Rechte geltend machen, wenn sie Anträge stellen, wenn sie sich in einer Behörde beraten lassen, werden ihre Daten verarbeitet. Der **Unterschied** zu den privatrechtlichen Aktivitäten ist hier:

- die fehlende Freiwilligkeit der Bürger\*innen zur Inanspruchnahme und
- die fehlende Auswahl bei den Anbietern öffentlicher Leistungen

Wenn Bürger\*innen eine staatliche Leistung benötigen, führt ein vorgezeichneter Weg dorthin. Bürger\*innen müssen den Anspruch in der dafür zuständigen Behörde nach den dort geltenden gesetzlichen Regeln geltend machen.

In diesem asymmetrischen Verhältnis, in dem der öffentlich-rechtliche Leistungsträger bestimmt, welche Daten Antragstellende preisgeben müssen, hat der Gesetzgeber strukturellen Regelungsbedarf gesehen. Um das bestehende Ungleichgewicht abzufedern, musste die Position der Bürger\*innen deutlich gestärkt werden. Deshalb hat der Gesetzgeber den öffentlichen Trägern besonders strenge gesetzliche Regeln zur Sicherstellung des Datenschutzes der Bürger\*innen aufgegeben. Damit wird reglementiert, unter welchen Voraussetzungen Daten von Bürgern\*innen verlangt/ verarbeitet werden dürfen.

Eines der großen gesetzlichen Regelwerke, das sehr detailliert den Umgang des Staates mit den Daten der Bürger\*innen regelt, ist das Sozialgesetzbuch, das auch im Jobcenter Anwendung findet.

## **Das Urteil des Bundesverfassungsgerichts zur informationellen Selbstbestimmung**

In Deutschland umfasst das allgemeine Persönlichkeitsrecht auch das Recht an den eigenen Daten. Darin wird der hohe Stellenwert der Grundrechte in Deutschland sichtbar. In einem visionären Urteil des Bundesverfassungsgerichts (BVerfG) zur geplanten Volkszählung im Jahr 1983 wurde aus dem allgemeinen Persönlichkeitsrecht der Artikel 2 Abs. 1 iVm. Artikel 1 Abs.1 des Grundgesetzes das Recht auf **informationelle Selbstbestimmung** abgeleitet.

Es beinhaltet das Recht jeder\*s Einzelnen, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Das BVerfG monierte damals nicht den Fragenkatalog, der zur Volkszählung eingesetzt werden sollte. Das Gericht monierte die mögliche ungesteuerte Verknüpfung der Befragungsergebnisse der Volkszählung mit anderen, bereits bestehenden oder zukünftigen Datensammlungen und die vorsorgliche Aufbewahrung der Befragungsergebnisse (Vorratsdatenspeicherung) zur späteren Verknüpfung nach dem Motto:

**„Es gibt keine unwichtigen Daten.“**

Die Bürger\*innen konnten weder überblicken noch kontrollieren, welche ihrer Daten auf diese Weise miteinander verbunden würden und welche Schlüsse der Staat aus diesem Datenpaket ziehen würde.

Dieses Urteil ist deshalb so visionär, weil es in einer Zeit formuliert wurde, als sowohl Quantität als auch Qualität technischer Standards extrem limitiert waren. In den 1980er Jahren bedeutete Speicherung: die Speicherung von Daten auf Magnetbändern; die Verarbeitung von Lochkarten mit Großrechnern war gerade erst abgelöst worden.

Die Verfassungsrichter haben ein Urteil gesprochen, das sich nicht allein auf die Möglichkeiten der Gegenwart beschränkte. Sie haben vielmehr ein Recht abstrahiert und verfassungskonforme Regeln für eine Zukunft formuliert, die sich die meisten Menschen in ihrer Auswirkung auf Technik und Gesellschaft nicht ansatzweise vorstellen konnten.

Die Verfassungsrichter haben die Entwicklung von Künstlicher Intelligenz und Quantencomputern sicher nicht vorhergesehen. Aber sie haben in ihrem Urteil Regeln formuliert, die dazu geeignet sind, den Bürgern\*innen auch dann Privatheit zu garantieren, wenn die technischen Möglichkeiten die komplexeste Vernetzung von Daten aus unterschiedlichsten Quellen in Echtzeit und ihre nahezu unbegrenzte Speicherung erlauben.

Mit diesem Urteil haben die Verfassungsrichter den Bürgern\*innen die Möglichkeit gegeben, die Kontrolle über die eigenen Daten zu behalten. Ob wir Bürger\*innen die Möglichkeit nutzen, bleibt die Entscheidung jeder\*s Einzelnen.

Die Bedeutung des Urteils kann auch heute, fast 37 Jahre nach seiner Verkündung, kaum hoch genug geschätzt werden.

## Datenschutz im Jobcenter- allgemein

Auch im Jobcenter Wuppertal fallen täglich große Mengen personenbezogener Daten an.

Die wichtigsten Ursachen des Datenvolumens sind:

1. Die Anzahl der Alg II-Kunden\*innen in der Stadt. Sie verursacht eine große Grundmenge an Daten und zahlreiche Regel-Datenbewegungen, die für jede\*n Kunden\*in anfallen (z.B. die Anmeldung bei einer Krankenkasse).
2. Das umfangreiche gesetzliche Leistungsspektrum für alle Mitglieder der Bedarfsgemeinschaft und deren unterschiedliche Ansprüche auf schulische, berufliche und gesellschaftliche Teilhabe (z.B. durch Zahlung verschiedener BUT-Leistungen, Kostenerstattung von Fahrtkosten während einer Weiterbildung, Kostenerstattung für Teilnahme an Gesundheitskursen/ Präventionsangeboten).

Weil im Jobcenter ständig große Mengen personenbezogener Daten anfallen, ohne die die operativen Bereiche ihre Dienstleistungen nicht erbringen können, ist die Einhaltung des Datenschutzes Querschnittsthema in allen Phasen der Beratung und Fallbearbeitung.

**Das Jobcenter Wuppertal ist eine Anstalt des öffentlichen Rechts; eine Behörde. Deshalb gilt für das Jobcenter das Rechtsstaatsgebot des Art. 20 Abs. 3 GG unmittelbar; das heißt: das Jobcenter ist in seinem Handeln stets an Recht und Gesetz gebunden.**

Das schließt die einschlägigen Gesetze des Datenschutzes ein.

Ob Daten der Beschäftigten des Jobcenters, Daten der Kunden\*innen oder Betriebsdaten betroffen sind, ist unerheblich; der Datenschutz ist stets zu wahren. Je nach Personengruppe und Datenquelle ändert sich lediglich die anzuwendende Rechtsvorschrift.

## Datenschutz hat viele Gesichter



Der Klassiker: Aktentaschen



Pepper: KI



Clouds



Verschlüsselte  
Kommunikation

## Europäisches Recht ab Mai 2018

Bereits vor der Einführung der Europäischen Datenschutzgrundverordnung (DSGVO) waren die im Jobcenter anfallenden Daten der Kunden\*innen durch das im Sozialgesetzbuch I (SGB I) formulierte Sozialgeheimnis geschützt. Nicht ohne Grund haben sich die europäischen Regeln zum Datenschutz an vielen Stellen an den strengen deutschen Regelungen orientiert.

Mit Inkrafttreten der EU-Datenschutzgrundverordnung (DSGVO) am 25.05.2018 gilt in allen Mitgliedsstaaten der Europäischen Union erstmals ein gemeinsamer Standard für den Datenschutz natürlicher Personen. Die DSGVO muss nicht für jeden Mitgliedsstaat gesondert mit einem Umsetzungsakt aktiviert werden; sie ist eo ipso (Lateinisch: aus sich selbst) unmittelbar geltendes Recht für alle Mitgliedsstaaten und geht nationalem Recht vor.

Mit der DSGVO begegnen den Mitarbeitenden des Jobcenters beim Datenschutz an einigen Stellen neue Begrifflichkeiten, tatsächlich aber nur wenige neue Inhalte. **Der zentrale Begriff der DSGVO ist die Verarbeitung personenbezogener Daten, vereinfacht ausgedrückt meint Verarbeitung: jede Form des Umgangs mit personenbezogenen Daten.**

Die Begrifflichkeiten unterscheiden sich von denen des SGB und des Verwaltungsverfahrensgesetzes (VwVfG), weil die DSGVO eher grob strukturiert ist und nicht zwischen öffentlichem und privatem Bereich differenziert; ihr Kern ist der Schutz personenbezogener Daten; wo sie anfallen, ist unerheblich. Spezifika des Verwaltungsverfahrens werden weder inhaltlich noch sprachlich abgebildet; dennoch fehlt in der DSGVO nichts.

Durch sogenannte Öffnungsklauseln in der DSGVO werden den EU-Mitgliedsstaaten Möglichkeiten eröffnet, **innerhalb des Rahmens der DSGVO** spezifischere Bestimmungen einzuführen oder bestehende Bestimmungen weiter gelten zu lassen.

Für den Bereich des Sozialdatenschutzes befindet sich die Öffnungsklausel in Artikel 6 Abs.2 der DSGVO. Der deutsche Gesetzgeber hat diese Öffnungsklausel genutzt; deshalb gilt für den Sozialdatenschutz weiterhin das nationale Recht, das SGB. Es hat sich sprachlich an die DSGVO angepasst und nimmt an entscheidenden Stellen - für den Sozialdatenschutz zum Beispiel in der Begriffsbestimmung des § 67 Abs. 1 SGB X - Bezug auf die DSGVO und anerkennt den rechtlichen Vorrang des EU-Rechts vor nationalem Recht.

### Wichtig:

**Die DSGVO ist eine Verbotsvorschrift mit Erlaubnisvorbehalt.**

**Was undurchsichtig klingt, lässt sich auf einen einfachen Inhalt reduzieren:**

**Alles, was nicht ausdrücklich erlaubt ist, ist verboten.**

**Das bedeutet für den Alltag; wenn Sie keine Rechtsvorschrift finden, die Ihnen ausdrücklich die Verarbeitung, Speicherung, Weitergabe etc. personenbezogener Daten erlaubt, ist sie verboten.**

## **Ein Querschnittsthema lebt vom lebendigen Austausch**

Jeden Tag informieren Mitarbeitende Kunden\*innen über deren Rechte und Pflichten im Kontext der Grundsicherung für Arbeitsuchende. Das Ziel ist, die Kunden\*innen durch eine umfassende Beratung so in ihrer Autonomie zu stärken, dass sie reflektierte Entscheidungen für sich und ihre Familien treffen können. Mitarbeitende informieren Kunden\*innen auch über die Regeln zum Schutz ihrer Daten und achten auf deren Einhaltung.

Das ist ein wichtiger Auftrag. Die Beratung auf Augenhöhe ist die Grundlage für das Dienstleistungsverständnis einer modernen Behörde, die den Datenschutz als integrativen Bestandteil der Autonomie von Kunden\*innen begreift und achtet.

In der Regel wird Datenschutz als erlebbares Grundrecht verstanden, das entsprechend positiv konnotiert ist.

Manchmal wird Datenschutz von den Mitarbeitenden aber auch ganz anders wahrgenommen.

In diesen Fällen wirkt Datenschutz auf die Mitarbeitenden wie eine bürokratische Hürde mit schwer durchschaubaren Regeln, die gerade in besonders schwierigen oder dringenden Einzelfällen einer schnellen Lösung im Weg steht. Über diese Hürde ärgern sich die betroffenen Mitarbeitenden.

### **Hinter dem Ärger steht nicht selten noch etwas anderes:**

- **das Gefühl, sich nicht gut genug mit dem Thema auszukennen,**
- **die Befürchtung, nicht kompetent und sicher entscheiden zu können,**
- **die Sorge, einen Fehler zu machen, der zu Ärger führt.**

Es ist wichtig, die Mitarbeitenden, aber auch die Führungskräfte, mit ihren Fragen zum Thema Datenschutz nicht allein zu lassen, sondern den aktiven Austausch zu fördern.

Deshalb müssen solche Einzelfälle aufgegriffen und besprochen werden. Dazu sollte die verantwortliche Führungskraft den Kontakt zur Datenschutzbeauftragten suchen, die dann die Kommunikation mit den Mitarbeitenden aufnimmt.

Alle Fragen zum Umgang mit dem Datenschutz, die nicht gestellt werden, bleiben offen und verursachen oder verstärken im Alltag Handlungsunsicherheit. Außerdem wird ein Potential verschenkt, die Fragen für passende Unterstützungsangebote zu nutzen.

**Deshalb ist es wichtig, dass die Fragen gestellt werden und Diskussionen in Gang kommen.**

Die Fragen aus den operativen Bereichen sollen aufgegriffen werden und in Angebote einfließen, die zum Bedarf passen. Zum Beispiel können auf ihrer Basis FAQ, Schulungsangebote oder Leitfäden entstehen.

Damit die Bedeutung von Datenschutz als Querschnittsthema im Alltag aller Mitarbeitenden und ihrer Führungskräfte ankommen kann, braucht es eine offene, wertschätzende Kommunikation zwischen der Datenschutzbeauftragten und den operativen Bereichen.

Die Kommunikation zwischen der Datenschutzbeauftragten und den Kollegen\*innen der operativen Bereiche darf sich nicht darauf beschränken, dass die Datenschutzbeauftragte im Einzelfall Antworten auf rechtliche Fragestellungen gibt.

**Die Datenschutzbeauftragte ist Dienstleisterin für alle Beschäftigten.**

Daher muss sie:

- die Kommunikation proaktiv gestalten
- sich an alle Beschäftigten richten
- mit Widerständen konstruktiv umgehen
- einen ganzheitlichen Ansatz verfolgen
- unterschiedliche fachliche Zugänge zum Thema und Unterschiede bei den Wissensständen berücksichtigen
- kontinuierlich Fortbildungen zum Thema anbieten

Um das Thema als Querschnittsthema bei allen Beschäftigten und in der Unternehmenskultur zu verankern, macht die Datenschutzbeauftragte regelmäßig in unterschiedlichen Kreisen „das Thema zum Thema“.

Dazu eignen sich Fortbildungen, die sie selbst anbietet und die alle Mitarbeitenden regelmäßig durchlaufen, Besprechungen unterschiedlicher Hierarchieebenen, die Mitarbeiterversammlung, die Einführung neuer Verfahrensregelungen, die Vergabe der Rollen und Befugnisse für Zugriffe auf IT-Systeme und viele mehr.

Der vorliegende Leitfaden gibt grundsätzliche Informationen zum Datenschutz und zu seiner Einordnung in die Rechtssystematik. Er kann Ansätze bieten, in das komplexe Thema einzusteigen, ist jedoch nicht dazu geeignet, eine Qualifizierungsveranstaltung, die in der Regel eine ganztägige Veranstaltung ist, zu ersetzen.

Die Beauftragte für den Datenschutz des Jobcenters Wuppertal, Sandra Arnhold, steht allen Beschäftigten; Mitarbeitenden und Führungskräften gleichermaßen, aber auch den Gremien- für ihre Fragen zum Datenschutz zur Verfügung.

Nutzen Sie dazu folgende Kontaktdaten:

Sandra Arnhold

Bachstraße 2, 42275 Wuppertal

Zimmer 516

Telefon: 02 02 – 74 76 3 -910

E-Mail:

[sandra.arnhold@jobcenter.wuppertal.de](mailto:sandra.arnhold@jobcenter.wuppertal.de)

[datenschutz@jobcenter.wuppertal.de](mailto:datenschutz@jobcenter.wuppertal.de)

## Das ganzheitliche Beratungskonzept im Kontext des Datenschutzes

Für die Mitarbeitenden des Jobcenters gehören der Umgang mit Sozialdaten und der Sozialdatenschutz zu den Kerntätigkeiten ihres Berufsalltags. Deshalb steht für jede und jeden Mitarbeitende\*n die verbindliche Verpflichtung auf die Einhaltung von Amtsverschwiegenheit und Datenschutz am Beginn der Beschäftigung im Jobcenter.

Die Mitarbeitenden tragen bei ihrer Arbeit ein hohes Maß an Verantwortung. Sie erfahren von ihren Kunden\*innen sehr persönliche Dinge, müssen die erhaltenen Informationen über komplexe Lebenssachverhalte unter unterschiedliche Rechtsvorschriften subsumieren, in vernetzten Systemen arbeiten und nach einer ausführlichen Prüfung über individuelle Ansprüche entscheiden.

Je nachdem, welche Aufgabe Mitarbeitende im Jobcenter wahrnehmen; ob sie in der Eingangszone, in der Leistungsgewährung, im Vorzimmer des Vorstandsvorsitzenden, im Maßnahmebetrieb, in der Rückforderung, in der beruflichen Integration, in der Telefon-Hotline oder im Unternehmensservice tätig sind, unterscheiden sich Anlass und Ausgangspunkt für die Kommunikation mit den Menschen; im Zentrum ihrer Aktivitäten stehen jedoch immer dieselben Menschen:

Kunden\*innen des Jobcenters Wuppertal.

Die Lotsenfunktion des Jobcenters und die Bandbreite der Beratungsthemen machen die Komplexität der Aufgabe aus. Die ergänzende Beteiligung von Kollegen\*innen mit anderen fachlichen Schwerpunkten gehört zum Konzept ganzheitlicher Beratung. Um in der Komplexität sicher handeln zu können, sind klare Regelungen zur Einhaltung des Datenschutzes wichtig.



**Datenschutz ist keine Randerscheinung, sondern ein wichtiger Teil des Ganzen.**

## Was man über den Datenschutz wissen sollte:



Datenschutz ist keine Raketenwissenschaft.

Datenschutz folgt klaren Regeln, oberstes Ziel ist die Wahrung des Grundrechts auf **informationelle Selbstbestimmung**.

- Die **DSGVO ist das Dach des Datenschutzes**, keine gesetzliche Vorschrift zum Datenschutz steht über ihr.
- Die **DSGVO enthält die Prinzipien und allgemeinen Regeln** zum Umgang mit personenbezogenen Daten.
- Die **DSGVO erlaubt durch Öffnungsklauseln Spezifizierungen in nationalen Gesetzen**. Ob und in welchem Umfang die Mitgliedsstaaten davon Gebrauch machen, ist sehr unterschiedlich.
- Eine Öffnungsklausel (Artikel 6 Abs. 2 DSGVO) hat der deutsche Gesetzgeber genutzt, um die Verarbeitung personenbezogener Daten **für öffentliche Stellen und Behörden abschließend festzulegen**. Diese Öffnungsklausel führt direkt zum Sozialgesetzbuch, das mit seinen allgemeinen Vorschriften für alle Sozialleistungsträger gilt und das für jeden Sozialleistungsträger ein gesondertes Kapitel beinhaltet.
- Keine Regelung im SGB widerspricht den Grundregeln der DSGVO, anderenfalls wäre sie unwirksam.
- Die DSGVO betrachtet den **Schutz personenbezogener Daten ganzheitlich**.

- Der Schutzgedanke personenbezogener Daten ist nach der DSGVO **in allen Stadien** gleichermaßen wichtig.
- Der Schutz personenbezogener Daten beginnt nicht erst dann, wenn die Daten in der Behörde vorliegen, sondern **knüpft bereits die Erhebung der Daten an die Bedingungen der Rechtmäßigkeit**.
- Sozialdaten sind **immer** personenbezogene Daten.(§ 67 Abs.2 S.1 SGB X)
- Der Schutz personenbezogener Daten beginnt, **bevor** die Persönlichkeitsrechte konkret in Gefahr sind; z.B. bei der **Planung der technischen Infrastruktur** und ihrer operativen Rahmen.
  - Deshalb werden an **IT-Systeme** so hohe Sicherheitsanforderungen gestellt. Weil alle Daten in IT-Systemen münden, ist immanente **Datenschutzkonformität Pflicht: durch Design/Technik, Voreinstellungen, Berechtigungskonzepte und Nutzerrollen, vorgesehene Speicherfristen** und vieles mehr.
- **Sind die Daten im Jobcenter angekommen, stehen sie augenblicklich unter dem Schutz des Sozialgeheimnisses**; jede weitere Behandlung (Speicherung, Veränderung, Übermittlung, Einschränkung der Verarbeitung und Löschung) darf nur innerhalb der strengen gesetzlichen Grenzen der § 35 SGB I iVm. §§ 67 ff. SGB X erfolgen.
- Die DSGVO legt verbindlich den rechtlichen Rahmen fest. Konkrete Regelungen für Behörden finden sich in § 35 SGB I und den Vorschriften des Zweiten Buches des SGB X (§§ 67 ff SGB X). Hier wird die Verarbeitung von Sozialdaten abschließend geregelt.

## Hierarchie im Datenschutzrecht



## Wichtige Grundsätze für die Verarbeitung personenbezogener Daten aus Artikel 5 DSGVO

### Artikel 5 Abs. 1 DSGVO:

- a) **Rechtmäßigkeit**
  - Verarbeitung nach Treu und Glauben
  - Transparenz
- b) **Zweckbindung (Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke)**
- c) **Datenvermeidung und Datensparsamkeit = Datenminimierung (dem Zweck angemessen und erheblich, auf das notwendige Maß beschränkt)**
- d) **Richtigkeit (Sachlich richtig und auf dem neuesten Stand)**
- e) **Speicherbegrenzung (Identifizierung der betroffenen Person darf nur so lange möglich sein, wie es zur Erfüllung der Zwecke, für die Daten verarbeitet werden, erforderlich ist)**
- f) **Datensicherheit; Integrität und Vertraulichkeit (Systeme müssen Datensicherheit durch Voreinstellung und durch Nutzungskonzepte gewährleisten, bei Systemabstürzen Daten sichern und so schnell wie möglich wieder verfügbar sein.)**

### Artikel 5 Abs. 2 DSGVO

Der Verantwortliche muss die Einhaltung der Regeln des Abs. 1 nachweisen können. (Kontrollfunktion)

#### Rechtmäßigkeit

Daten dürfen nur verarbeitet werden, wenn es dafür eine gesetzliche Grundlage gibt und auch nur im Erlaubnisrahmen der gesetzlichen Grundlage. (Hier: § 35 SGB I iVm. §§ 67 ff. SB X)

#### Verarbeitung nach Treu und Glauben

Daten müssen nach dem Gebot der Fairness verarbeitet werden. Die Informationen für die Betroffenen über den Grund und den Umfang der Verarbeitung ihrer Daten und die Möglichkeiten der Beschwerde müssen leicht zugänglich und gut verständlich sein, damit Betroffene ihre Rechte wahrnehmen können.

#### Transparenz

Das Verfahren und die einzelnen Schritte, die die Verarbeitung der Daten auslösen und begründen, müssen für die/den Betroffene\*n klar erkennbar sein.

**Zweckbindung:** Daten dürfen nur innerhalb eines festgelegten Zwecks erhoben und (weiter-)verarbeitet werden. Die Zweckbindung beginnt bereits mit dem Zeitpunkt der Planung der Erhebung und bestimmt die gesamte Prozesskette bis zur Löschung.

### Datenminimierung

Es dürfen nur die Daten verarbeitet werden, die im Rahmen der Verhältnismäßigkeit erforderlich und geeignet sind, gesetzliche Aufgaben zu erfüllen.

### Erforderlichkeit

Es dürfen nur die Daten verarbeitet werden, ohne die eine Entscheidung nicht möglich ist.



## Regeln:

### Bei der Verarbeitung von Daten gilt:

### Weniger ist Mehr.

#### Verarbeiten Sie nur die Daten, die im Einzelfall erforderlich sind.

- Fragen Sie sich kritisch, ob Sie gerade Datenvorräte anlegen und vielleicht Daten erfragen, die für die weitere Entscheidung nicht erforderlich sind.

#### Nicht alle Informationen, die Ihnen zugänglich sind, sind auch in jedem Fall erforderlich.

- Fragen Sie sich in jedem Einzelfall kritisch, ob eine Abfrage z.B. beim Einwohnermeldeamt oder beim Ausländerzentralregister erforderlich ist.
- Die Abfrage in Datensystemen ist nur erlaubt, wenn sie im Einzelfall erforderlich ist **und** der Versuch, die Daten von der/dem Betroffenen (Kunde\*in) zu erhalten, nicht erfolgreich war.

#### Achten Sie den Ersterhebungsgrundsatz.

- Wenn Sie eine Information des/ der Kunden\* in benötigen, bitten Sie ihn/sie direkt um die Information.

**Es gilt § 67a Abs. 2 S.1 SGB X (Sozialdaten sind bei der betroffenen Person zu erheben)**

#### Sorgen Sie für Transparenz.

##### Informieren Sie den/ die Kunden\*in im Gespräch in einfachen, verständlichen Worten:

- warum Sie von ihm/ihr Daten benötigen und welche Daten genau,
- wie die Fallbearbeitung weitergeht,
- wer die nächste Ansprechperson innerhalb des Jobcenters ist
- mit wem Sie Kontakt aufnehmen werden (Bsp.: Krankenkasse, Agentur für Arbeit, Sachbearbeiter\*in der Leistungsgewährung, Integrationsfachkraft)

### **Datenschutz und Amtsverschwiegenheit gehören zusammen.**

§ 35 Abs.1 SGB I führt aus: „Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten von den Leistungsträgern nicht unbefugt verarbeitet werden.“

Das ist deutlich: Es ist verboten, personenbezogene Daten unbefugt (ohne gesetzliche Grundlage) zu erheben, zu speichern, zu verändern, zu nutzen, zu übermitteln und zu löschen.

**Ergänzend wirkt das Prinzip der Amtsverschwiegenheit, dessen Einhaltung alle Mitarbeitenden des Jobcenters bei Einstellung unterzeichnen. Einfach ausgedrückt besagt das Prinzip: Informationen über dienstliche Angelegenheiten dürfen den dienstlichen Kreis nicht verlassen. Es ist nicht erlaubt, im privaten Kreis über dienstliche Dinge zu sprechen.**

**Zu widerhandlungen haben strafrechtliche und dienstrechtliche Konsequenzen.**

- Dienstliche Angelegenheiten unterliegen **immer** der Amtsverschwiegenheit.
- Der Sozialdatenschutz geht jedoch noch weiter:  
§ 35 Abs.1 S.2 SGB I führt aus: „Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich oder nur an diese weitergegeben werden.“
- **Deshalb gilt:** Tauschen Sie sich nur mit den Kollegen\*innen über Einzelfälle aus, mit denen Sie gemeinsam an einer Gesamtstrategie für den/die Kunden\*in arbeiten und auch nur im notwendigen Rahmen.
- Der Austausch über Kunden\*innen ist kein belangloses Gespräch unter Kollegen\*innen, er untersteht den Regeln des Datenschutzes.

## Datenschutz ganz praktisch

Sie sind selbst dafür verantwortlich, dass die Ihnen anvertrauten Daten bei Ihnen sicher sind. Die Räumlichkeiten, Möbel, Material und Technikausstattung werden Ihnen durch den Arbeitgeber/ Dienstherrn gestellt; für die richtige, datenschutzkonforme Nutzung sind Sie selbst verantwortlich.

### Im Büro:

- Achten Sie darauf, dass Ihr Büro zu Dienstende so aufgeräumt ist, dass keine Papiere, die personenbezogenen Daten enthalten, (Telefonnotizen, o.ä.), offen herumliegen und Dritte sie unbefugt lesen können.
- Schließen Sie zu Dienstende alle Unterlagen, die dem Datenschutz unterliegen, ein.
- Entsorgen Sie Papiermüll, der personenbezogene Daten enthält, ausschließlich im Datenschutzmüll; in der verschließbaren, silbernen Tonne.
- Unterlagen in Papierform sichern Sie im abgeschlossenen Schrank oder Rollcontainer; elektronische Unterlagen sichern Sie durch Abspeichern in den vorgesehenen Ablagen der Fachanwendungen und Abmeldung vom Rechner.

### Tür

- Wenn Sie das Büro verlassen, schließen Sie unbedingt immer Ihre Bürotür ab.
- Kontrollieren Sie von außen durch Herunterdrücken der Klinke, dass die Tür wirklich verschlossen ist und die Klinke ohne Widerstand ist.
- Wenn die Klinke sich von außen öffnen lässt und beim Herunterdrücken ein Widerstand erkennbar ist, ist die elektronische Funktion „Dauer offen“ aktiviert; die Tür kann von außen ohne Chip geöffnet werden.
- Wenn Sie die Bürotür offen lassen, weil Sie denken: „ich bin ganz in der Nähe, was soll in der kurzen Zeit schon passieren?“ handeln Sie bereits mindestens grob fahrlässig mit allen rechtlichen Konsequenzen (Dienst- und Strafrecht, Zivilrecht/Schadenersatz). Diesen Ärger können Sie ganz einfach vermeiden, indem Sie **IMMER abschließen**.

### PC/ Notebook

- Kennworte sind der Schlüssel zu allen Daten, die sich in Ihrem PC befinden, deshalb ist der Kennwortschutz eminent.
- Deshalb nutzen Sie ein Kennwort, das den Sicherheitsregeln entspricht; die Regeln dazu finden Sie im Intranet.
- Schreiben Sie Ihr Kennwort nicht auf; wählen Sie ein Kennwort, das Sie sich gut merken können und das eine Verschlüsselung beinhaltet.
- Geben Sie Ihr Kennwort **niemals** weiter.  
Um auch unvorhergesehene Vertretungssituationen im Team gut zu bewältigen und alle notwendigen Daten vorzufinden, speichern Sie immer alle relevanten Unterlagen zu Kundenvorgängen ausschließlich in den dafür vorgesehenen Ablagen der Fachanwendungen ab; so können Zugriffe erfolgen.

### Bildschirm

- Achten Sie darauf, dass auf Ihrem Bildschirm personenbezogene Daten nicht unbefugt zugänglich sind. Der Fall des/der letzten Kunden\*in darf beim Folgegespräch nicht mehr auf dem Bildschirm zu sehen sein.
- Wenn Sie den Arbeitsplatz verlassen –auch für einen kurzen Zeitraum– sperren Sie den Bildschirm durch Drücken der Tastenkombination: **(Windows-Symbol+ L)** oder durch Betätigen der Kombination: **STRG Alt + Entfernen**; die den Task Manager aktiviert, der ebenfalls eine Sperrfunktion bietet.
- Wenn Sie ein Notebook nutzen, klappen Sie das Notebook einfach zu; damit sperren Sie automatisch den Bildschirm.

### Kunden\*innen

- Lassen Sie Kunden\*innen nicht allein im Büro. Wenn Sie zur Klärung Rücksprache mit Kollegen\*innen halten oder etwas holen müssen, bitten Sie den/die Kunden\*in, so lange vor der Tür zu warten.

## Telefonate

- Wenn Sie sich im persönlichen Gespräch mit einem/einer Kunden\*in befinden, sorgen Sie für Vertraulichkeit. Wenn Sie währenddessen Telefonate annehmen müssen, vereinbaren Sie einen Rückruf für eine Zeit, in der Sie ungestört sind.
- Klären Sie die Identität eines\*r Anrufers\*in, bevor Sie personenbezogene Daten herausgeben. Lassen Sie sich eindeutige Daten nennen, um die Identifikation vorzunehmen und erklären Sie, dass die Abfrage der Einhaltung des Datenschutzes dient.
- Name, Vorname, Geburtsdatum, Anschrift, BG-Nummer/ Kundennummer sind dazu geeignet, evtl. kann auch die Frage sinnvoll sein, bei welcher Krankenkasse die Person versichert ist.
- Wenn Sie Zweifel an der Identität haben, weil Sie den/die betreffende Kunden\*in kennen und die anrufende Person Ihnen jemand anderer zu sein scheint, vereinbaren Sie Rückruf unter den Kontaktdaten, die im System gespeichert sind; diese Angaben geben die Kunden\*innen, so dass von der Echtheit auszugehen ist.
- Auch in Telefonaten werden personenbezogene Daten ausgetauscht. Um auch hier den Datenschutz einzuhalten, schließen Sie während des Telefonats die Tür, bzw. nutzen Sie einen Arbeitsplatz, der akustisch für ein Telefonat ausgelegt ist und achten Sie auf Ihre Stimmlautstärke.
- Nutzen Sie die Freisprechfunktion nur, wenn niemand das Gespräch mithören kann
- Wenn Sie die Freisprechfunktion zur Klärung einer Frage nutzen wollen, die auch für Kollegen\*innen relevant ist, die das Gespräch mithören, fragen Sie **zuvor immer** Ihre\*n Gesprächspartner\*in um Erlaubnis, bevor sie die Freischaltung aktivieren.

## Homeoffice

Die Regeln zur Einhaltung des Datenschutzes gelten selbstverständlich auch für die Arbeit in Homeoffice; eine entsprechende Erklärung ist Teil des Antragsverfahrens für einen Arbeitsplatz in Homeoffice. Auch dann, wenn Sie in Ihren privaten Räumen arbeiten, müssen Sie die dienstlichen Daten vor unbefugten Zugriffen schützen.

Datenschutz ist ein Prinzip, das ortsunabhängig zu wahren ist.

Darstellung: Verarbeiten von Sozialdaten im Prozessverlauf; der **gesetzlich garantierte Schutz umfasst die gesamte Prozesskette.**

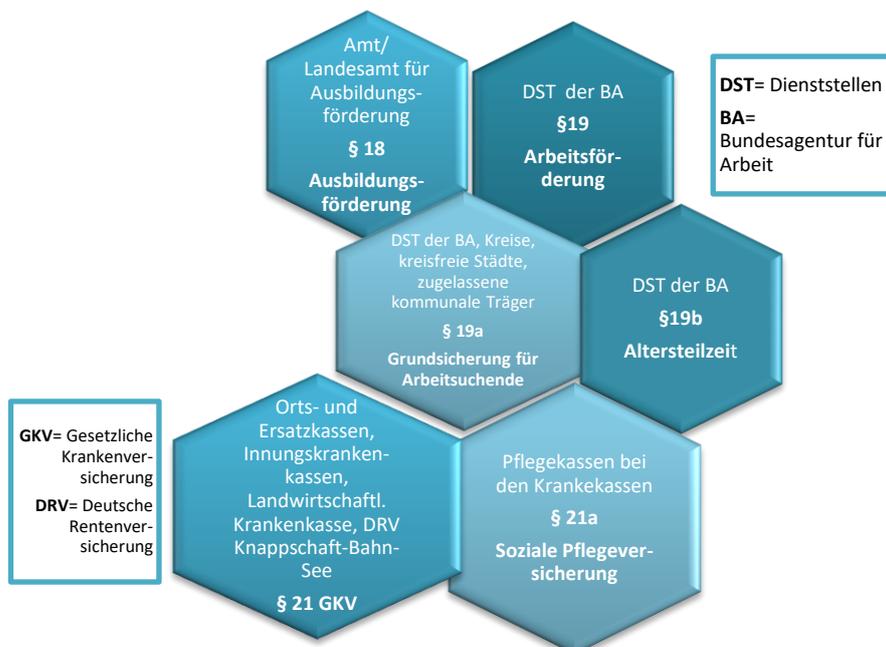


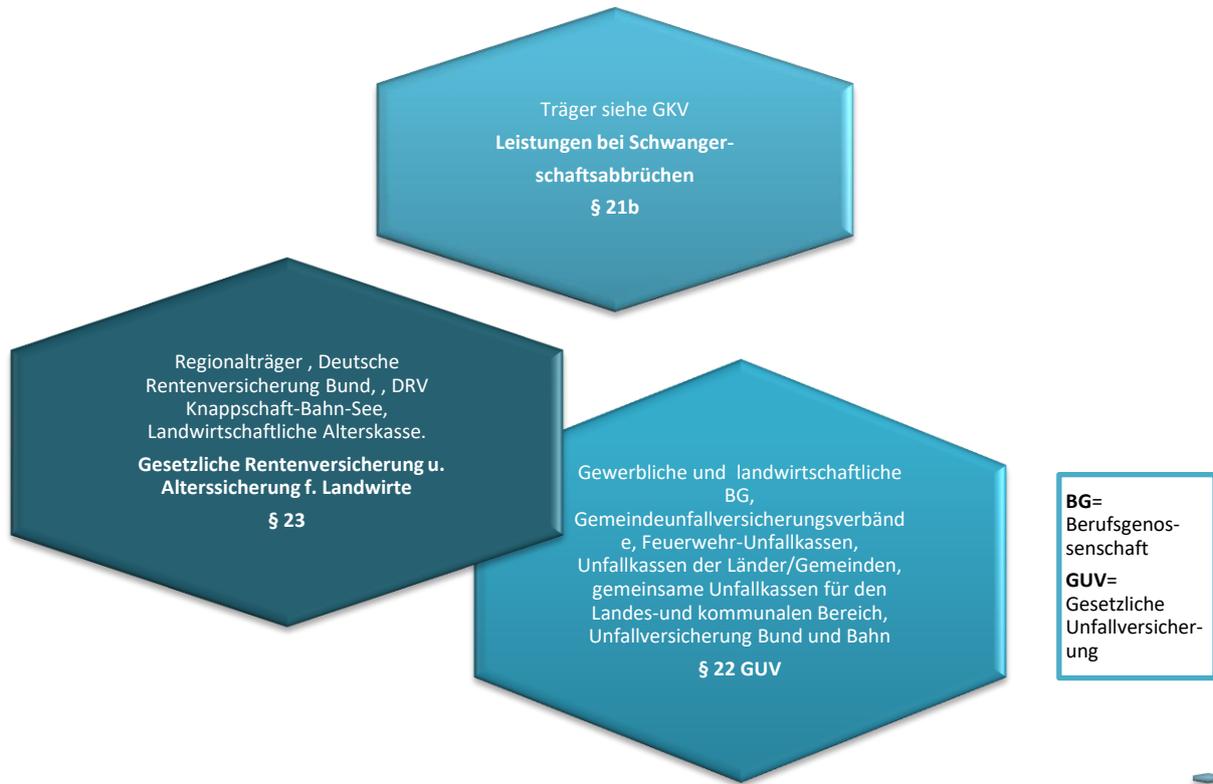
## Datenübermittlung der Sozialleistungsträger untereinander

**Sozialleistungsträger** (§§ 18-29 SGB I) dürfen einander für die Erfüllung ihrer gesetzlichen Aufgaben personenbezogene Daten im **notwendigen Umfang** (Datensparsamkeit) übermitteln, wenn die Übermittlung im Einzelfall **erforderlich** ist (Verhältnismäßigkeit= das mildeste Mittel) **und** die **Abfrage der Daten bei dem/ bei der Betroffenen** (Ersterhebungsgrundsatz) nicht erfolgreich war oder mit unverhältnismäßigem Aufwand verbunden wäre.

Wer die Sozialleistungsträger sind, sehen Sie auf den folgenden Schaubildern.

### Sozialleistungsträger §§ 18-29 SGB I







## Übermittlungsersuchen- in welchen Fällen darf eine Übermittlung erfolgen?

### Gesetzliche Aufgaben des Jobcenters

Die Jobcenter Wuppertal AöR ist gem. § 6a SGB II zugelassener kommunaler Träger der Grundsicherung für Arbeitsuchende in alleiniger Verantwortung. Das Jobcenter handelt zur Erfüllung der Aufgaben nach dem SGB II auf dem Gebiet des öffentlichen Rechts und nimmt als zuständige Fachbehörde hoheitliche Aufgaben wahr.

„Behörde im Sinne dieses Gesetzbuches ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt.“ (§ 1 Abs. 2 SGB X)

### Das Jobcenter ist ein Sozialleistungsträger

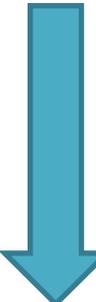
Die Sozialleistungsträger und ihre speziellen Aufgaben sind in den §§ 18 bis 29 SGB I aufgezählt, siehe Schaubild S. 23.

Die Jobcenter und ihre Aufgaben sind in § 19a SGB I benannt; die zugelassenen kommunalen Träger in § 19a Abs. 2 S. 2 SGB I.

### Welche Vorschriften zum Datenschutz finden im Jobcenter Anwendung?

In allen EU-Mitgliedsstaaten gilt die DSGVO ohne Einschränkung für alle privaten Stellen, für alle Behörden und öffentlichen Stellen.

Die DSGVO lässt Möglichkeiten zur **Spezifizierung durch nationales Recht** zu. Gemäß Artikel 6 Abs. 2 DSGVO gilt deshalb in Deutschland für den Umgang der Behörden mit personenbezogenen Daten das **Sozialgesetzbuch**.



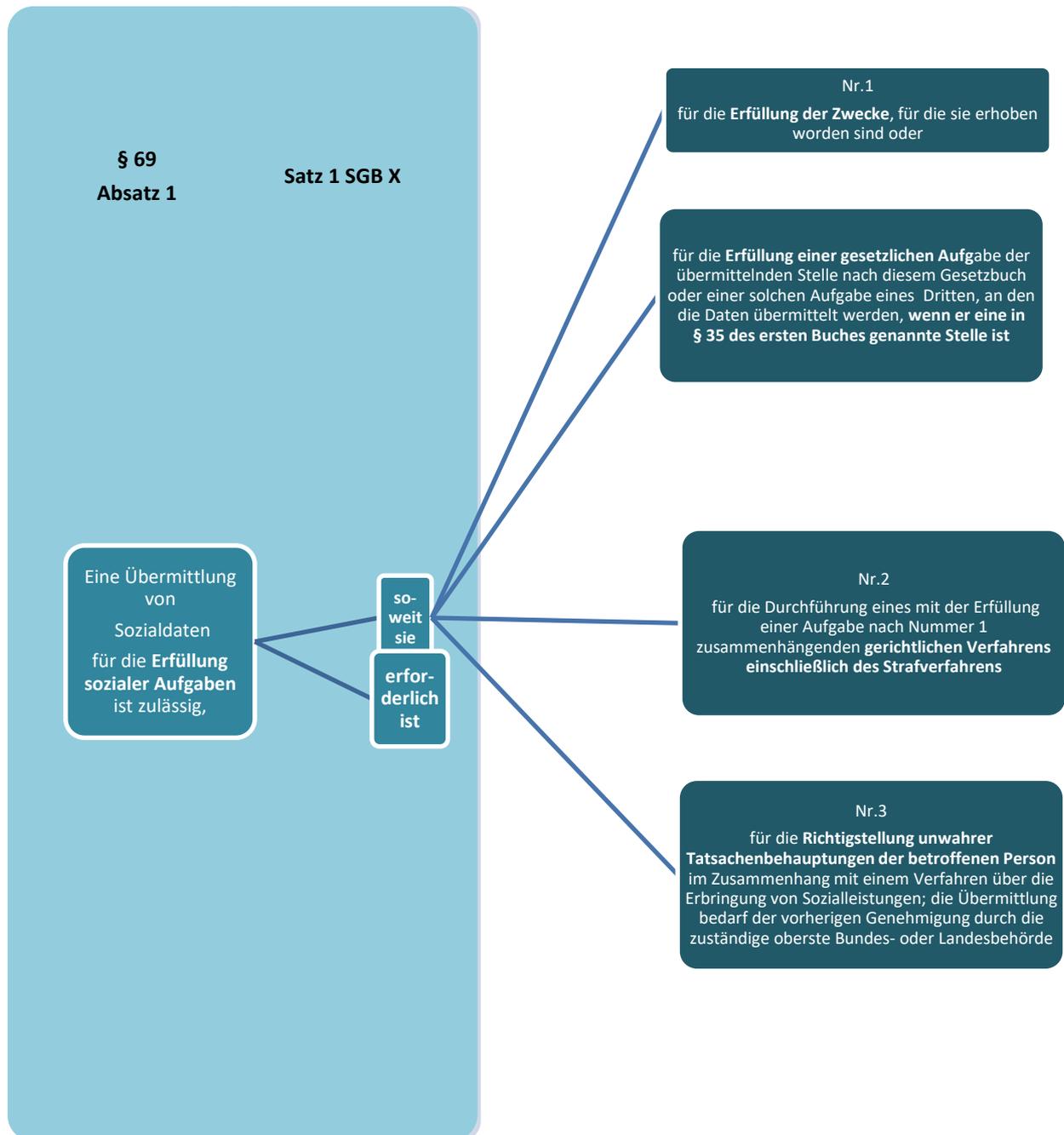
### § 35 Abs. 1 S.1 SGB I

Ist **die** zentrale Vorschrift, sie stellt Sozialdaten unter einen besonderen Schutz:

„Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs.2 Zehntes Buch) von den Leistungsträgern nicht unbefugt verarbeitet werden (**Sozialgeheimnis**).“ **Aus § 35 SGB I führt der Weg zu den speziellen Verfahrensvorschriften des SGB X, die alle Übermittlungsbefugnisse für Sozialleistungsträger enthalten.**

### Übermittlung für die Erfüllung sozialer Aufgaben

**WICHTIG:** Der Ersterhebungsgrundsatz gilt auch hier. Die Daten müssen grundsätzlich bei der betroffenen Person erfragt werden (§67a (1) SGB X). Ist dies erfolglos, oder mit unverhältnismäßigem Aufwand verbunden und sind schutzwürdige Interesse des Betroffenen nicht verletzt, (§67a (2) SGB X), greift das Verfahren.



Die überwiegende Zahl der Übermittlungsersuchen, die im Jobcenter ankommen oder das Jobcenter verlassen, gehört in diese Kategorie.

Wegen ihrer Bedeutung in der Praxis sind für diese Übermittlungsbefugnis nachstehend typische Beispiele aufgeführt.

### Beispiele, in denen eine Übermittlung nach § 69 SGB X zulässig ist:

#### Krankenkasse (KK)

- Die Krankenkasse hat Implausibilitäten bei Versicherungszeiten eines Kunden im Leistungsbezug nach dem SGB II festgestellt. Die KK hat versucht, die Informationen vom Kunden zu erhalten; dieser konnte sich jedoch nicht erinnern und verfügt auch nicht über Unterlagen. Die KK fragt nun beim JC an.
- In einer Familie sind außer einem Kind alle Kinder als familienversichert gemeldet, die KK fragt in der Sache beim JC um Informationen an und teilt in der Anfrage mit, die Anfrage bei der Familie sei nicht erfolgreich gewesen.
- Klärung der richtigen Schreibweise eines Namens; die Kundin ist mit der Anfrage einverstanden.

#### Rentenversicherungsträger

- Versicherungsverlauf einer Kundin ist unklar, die Zeiten der Arbeitslosigkeit werden beim JC erfragt. Die Abfrage bei der Kundin brachte keine Erkenntnisse, sie besitzt keine Unterlagen aus der Zeit und erinnert sich auch nicht mehr, ob sie arbeitslos oder erwerbstätig war.
- Geburtsdatum einer Kundin ist unklar; ihr Geburtsdatum wurde nachträglich geändert, dadurch ergeben sich Auswirkungen auf den Renteneintrittstermin. Kundin hat die Unterlagen aus dem Heimatland bei der DRV eingereicht und ist mit der Übermittlung an das JC einverstanden.
- Fragen zum Geburtsdatum/ Geburtsort zur Klärung der Identität; Kunde spricht kein Deutsch, die durch den bevollmächtigten Sohn vorgelegten Unterlagen konnten den Sachverhalt nicht aufklären.
- Mitteilung über den Tod eines Kunden.

#### Agentur für Arbeit

- Einem Kunden wird Insolvenzgeld bewilligt, Erstattungszeitraum und Höhe des Leistungsbezugs nach dem SGB II werden erfragt.
- Antragstellung eines Kunden auf Arbeitslosengeld I wird mitgeteilt/erfragt.

### Gesetzliche Unfallversicherung (GUV)

- ☑ Aufgrund einer bleibenden Verletzung, die während der Arbeit als ehrenamtlicher Sanitäter beim DRK entstanden ist, wird einem Kunden während der Teilnahme an einer Rehabilitation (Teilhabe am Arbeitsleben) Übergangsgeld bewilligt. Die GUV fragt an, ob sich der Versicherte im Leistungsbezug befindet.
  
- ☑ Ein Dachdecker ist in Folge eines Arbeitsunfalls schwer erkrankt und liegt seitdem im Koma. Weil die finanzielle Situation der Familie sehr angespannt ist, beantragt die Ehefrau für die Familie Alg II.  
Nach kurzer Zeit verstirbt der Ehemann an den Folgen des Arbeitsunfalls. Nach seinem Tod stellt die Witwe bei der Gesetzlichen Unfallversicherung (GUV) einen Antrag auf Hinterbliebenenrente. Die GUV erfragt beim Jobcenter schriftlich, ob die Witwe und die Kinder Leistungen nach dem SGB II erhalten.

### Landschaftsverband Rheinland/ LVR

- ☑ Dem 13-jährigen Sohn einer Familie/ Bedarfsgemeinschaft wird wegen dauerhafter gesundheitlicher Einschränkungen in Folge eines Impfschadens eine Grundrente nach dem Infektionsschutzgesetz zuerkannt. Die Angaben der Eltern im Antrag auf Alg II sind unvollständig und lassen zunächst nicht erkennen, welche Leistung gezahlt wird und warum. Auf Nachfrage des Sachbearbeiters erklären die Eltern, der Sohn sei nach einer vorgeschriebenen Impfung schwer krank geworden. Sie erhielten deshalb monatlich Geld für ihn.  
Sie legen den Kontoauszug vor, der den Überweisungsbetrag und den Namen des Leistungsträgers enthält; weitere Informationen können sie nicht liefern.  
Der Sachbearbeiter benötigt Informationen über die Rechtsgrundlage der Rente, um über eine Anrechnung nach § 11a SGB II entscheiden zu können, er schreibt den LVR an.

### Träger der öffentlichen Jugendhilfe/ Jugendamt

- ☑ Für die behinderte Tochter einer Familie im Alg II-Bezug werden Leistungen nach § 35a SGB VIII beantragt, die Tochter soll in Kürze in eine Wohngruppe aufgenommen werden. Die Eltern hatten im Gespräch zum Erstantrag darauf hingewiesen, dass der Antrag gestellt, aber noch nicht beschieden sei, der Wohngruppenplatz sei auch noch nicht vorhanden. Einen Monat später informiert das örtliche Jugendamt das Jobcenter, dass die Tochter in die Wohngruppe aufgenommen wurde und teilt die Art, Zweckbestimmung und Höhe der gewährten Leistung mit; die Eltern erhalten eine Kopie des Schreibens an das JC.

### **Träger der Grundsicherung für ältere und behinderte Menschen/ Sozialamt**

- Ein Sachbearbeiter des Sozialamts hat die Vermutung, dass ein Kunde zeitgleich mit den Leistungen nach dem SGB XII auch Leistungen nach dem SGB II beantragt hat. Der Kunde hat beim Auspacken seiner Tasche nicht nur Antragsunterlagen nach dem SGB XII auf den Tisch gelegt, sondern versehentlich auch Antragsunterlagen nach dem SGB II. Der Sachbearbeiter befragt den Kunden dazu, der Kunde äußert sich jedoch nicht. Der Sachbearbeiter richtet deshalb eine Anfrage an das JC und bittet um Informationen zum Leistungsbezug.

### **Wohngeldstelle**

- Eine Familie erhält Leistungen nach dem SGB II. Die Sachbearbeiterin stellt nach einer Berechnung fest, dass ein nicht unerheblicher Anspruch auf Wohngeld bestehen könnte. Sie informiert die Kunden\*innen schriftlich, fügt ihre Berechnung bei und fordert sie zur Antragstellung von Wohngeld auf. Zeitgleich macht sie bei der Wohngeldstelle für den Fall der Bewilligung von Wohngeld schriftlich einen Ersatzanspruch für die Familie geltend.

### **Unterhaltsvorschusskasse (UVG)**

- Die UVG-Kasse zahlt laufend Leistungen für ein minderjähriges Kind; zum Vater des Kindes besteht kein Kontakt. Die Mutter des Kindes kennt die Anschrift des Kindesvaters nicht, sie hat aber gehört, dass er Leistungen des Jobcenters erhalten soll und teilt dies der Sachbearbeiterin der UVG-Kasse mit. Die Sachbearbeiterin fragt beim Jobcenter an, ob der Kindesvater Leistungen erhalte und die Anschrift bekannt sei.

## Kurzübersicht: Schutz der Sozialdaten und Übermittlungsbefugnisse

Die Übermittlungsbefugnisse nach dem SGB X und die entsprechenden Verfahrenshinweise sind detailliert in den Vorschriften der §§ 67 bis 78 SGB X aufgeführt und werden auch in den Fortbildungsveranstaltungen ausführlich behandelt. Sie sollen hier nur kurz im Sinne einer Gesamtübersicht erwähnt werden.

### § 67 SGB X Begriffsbestimmungen.

Rechtliche Brücke zu den Begriffsbestimmungen des Artikels 4 DSGVO. Enthält in Abs. 2 S.1 die **wichtige Definition: Sozialdaten sind personenbezogene Daten**, die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden.

### § 67a SGB X Erhebung von Sozialdaten

Benennt den Kreis der zur Erhebung Berechtigten aus § 35 SGB I und enthält den wichtigen Ersterhebungsgrundsatz in Abs. 2 S.1: **Sozialdaten sind bei der betroffenen Person zu erheben**. Unter welchen Voraussetzungen vom Ersterhebungsgrundsatz abgewichen werden kann, nennt Abs. 2 S. 2 Nr. 1-2. Die Aufzählung ist abschließend.

### § 67b SGB X Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung und Löschung von Sozialdaten

Schlägt den Bogen zu den Artikeln 7 und 9 der DSGVO, in denen Zustimmung/ Einverständnis zur Verarbeitung (Art.7) und der Umgang mit besonderen Kategorien personenbezogener Daten (Art.9) geregelt sind.

Schreibt für die Träger nach § 35 SGB I die schriftliche/ elektronische Form der Einwilligung des/der Betroffenen, ihre umfassenden Information und den Nachweis darüber fest.

### § 67c SGB X Zweckbindung sowie Speicherung, Veränderung und Nutzung von Sozialdaten zu anderen Zwecken

Enthält in Abs. 1 S. 1 die wichtige Definition, die die Grundätze der DSGVO aufgreift:

Die Speicherung, Veränderung oder Nutzung von Sozialdaten durch die in § 35 des Ersten Buches genannten Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden gesetzlichen Aufgaben nach diesem Gesetz erforderlich ist und für die Zwecke erfolgt, für die die Daten erhoben worden sind.

### § 67d SGB X Übermittlungsgrundsätze

Regelt die Verantwortlichkeit für die Übermittlung von Daten; verantwortlich ist gem. Abs. 1 S. 1 die übermittelnde Stelle

### **§ 67e SGB X Erhebung und Übermittlung zur Bekämpfung von Leistungsmissbrauch und illegaler Ausländerbeschäftigung**

Legt fest, welche ergänzenden Daten bei der überprüften Person zusätzlich erfragt werden dürfen.

### **§ 68 SGB X Übermittlung für Aufgaben der Polizeibehörden, der Staatsanwaltschaften, Gerichte und der Behörden zur Gefahrenabwehr**

Greift auch für die Behörden außerhalb des Kreises des § 35 SGB I die bekannten Grundsätze der Zweckbindung (zur Erfüllung ihrer Aufgaben) und Ersterhebung (.. wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen kann) sowie die Verpflichtung zur Abwägung der Schutzwürdigkeit des Interesses des/der Betroffenen auf und nennt in einer abschließenden Aufzählung die Daten, die im Einzelfall übermittelt werden dürfen.

#### **WICHTIG:**

- **Über das Übermittlungsersuchen entscheidet der/die Leiter\*in der ersuchten Stelle; im Jobcenter der Vorstandsvorsitzende. (Abs. 2)**
- Die Verantwortung für die Zulässigkeit der Übermittlung trägt ausnahmsweise die anfragende Stelle, die übermittelnde Stelle trägt nur die Verantwortung für die Prüfung, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten liegt. (Abs. 3)

**§ 69 SGB X ist mit Beispielen ausführlich illustriert.**

### **§ 70 SGB X Übermittlung für die Durchführung des Arbeitsschutzes**

Aufgreifen des Grundsatzes der Zweckbindung für Behörden außerhalb des § 35 SGB I (zur Durchführung des Arbeitsschutzes). Auch hier ist eine Abwägung der Rechte der Betroffenen mit dem öffentlichen Interesse vorzunehmen.

### **§ 71 SGB X Übermittlung für die Erfüllung besonderer gesetzlicher Pflichten und Mitteilungsbefugnisse**

Enthält in Abs. 1 eine abschließende Aufzählung, zur Erfüllung welcher Aufgaben Dritter die Übermittlung von Sozialdaten zulässig ist.

In Abs. 2 wird ergänzend der Rahmen für die Zulässigkeit der Übermittlung von Sozialdaten eines Ausländers im Einzelfall geregelt.

### § 72 SGB X Übermittlung für den Schutz der inneren und äußeren Sicherheit

Abs. 1 legt die Behörden fest, an die grundsätzlich im Rahmen dieser Vorschrift übermittelt werden kann und grenzt die zu übermittelnden Daten ein.

#### **WICHTIG:**

**Auch in diesen Fällen entscheidet der/die Behördenleiter\*in (hier: der Vorstandsvorsitzende des Jobcenters) über das Übermittlungsersuchen. (§ 72 Abs. 2 SGB X)**

#### **Behörden, die in § 72 SGB X genannt sind:**

- Verfassungsschutzbehörden
- Bundesnachrichtendienst
- Militärischem Abschirmdienst
- Bundeskriminalamt

#### **Die zu übermittelnden Daten beschränken sich auf:**

- Name
- Vorname
- früher geführte Namen
- Geburtsdatum
- Geburtsort
- derzeitige und frühere Anschriften der betroffenen Person
- Namen und Anschriften ihrer derzeitigen und früheren Arbeitgeber

### § 73 SGB X Übermittlung für die Durchführung eines Strafverfahrens

Unterscheidet zwischen Verbrechen und sonstigen Straftaten (Abs. 1).

**Das Ermittlungsersuchen erfolgt immer durch einen richterlichen Beschluss. (Abs. 3)**

### § 74 SGB X Übermittlung bei Verletzung der Unterhaltspflicht und beim Versorgungsausgleich

Nennt die Fälle, in denen Sozialdaten für die Durchführung des Verfahrens über Unterhaltsansprüche und den Versorgungsausgleich (Abs. 1 S. 1 Nr.1) als auch für deren Geltendmachung (Abs. 1 S. 1 Nr. 2 u.3) zulässig sind. Der Ersterhebungsgrundsatz ist zu achten (Abs. 1 S.2).

### § 74a SGB X Übermittlung zur Durchsetzung öffentlich-rechtlicher Ansprüche und im Vollstreckungsverfahren

Regelt die Übermittlung von Sozialdaten zur Durchsetzung von Forderungen in Höhe von mindestens 500 Euro. Die Einhaltung des Ersterhebungsgrundsatzes muss nachgewiesen sein; die Abwägung der Schutzwürdigkeit des Interesses des/der Betroffenen mit den Interessen der Allgemeinheit an der Herstellung eines rechtmäßigen Zustands muss erfolgen.

### **§ 75 SGB X Übermittlung von Sozialdaten für die Forschung und Planung**

Die Übermittlung ist zulässig für ein konkretes Vorhaben (Abs. 1 S. 1)

1. der wissenschaftlichen Forschung im Sozialleistungsbereich oder der wissenschaftlichen Arbeitsmarkt- und Berufsforschung (Abs. 1 S. 1 Nr.1) oder
2. der Planung im Sozialleistungsbereich durch eine öffentliche Stelle im Rahmen ihrer Aufgaben.

Schutzwürdige Interessen sind zu achten, die Einwilligung der betroffenen Personen ist einzuholen; ohne Einwilligung dürfen die Daten nicht übermittelt werden.(Abs. 1 S.2) Die Behörde, die ein Forschungs- oder Planungsvorhaben durchführen möchte, muss zwingend auch ein Datenschutzkonzept erstellen und der obersten Landes- oder Bundesbehörde vorlegen. (Abs. 1 S. 4)

### **§ 76 SGB X Einschränkung der Übermittlungsbefugnis bei besonders schutzwürdigen Sozialdaten**

Regelt verbindlich die Übermittlung von Gesundheitsdaten für alle Sozialleistungsträger; die Zustimmung des /der Betroffenen ist einzuholen. Die Einwilligung kann widerrufen werden.

### **§ 77 SGB X Übermittlung ins Ausland und an internationale Organisationen**

Regelt die Fälle, in denen Sozialdaten an Mitgliedsstaaten der Europäischen Union und die ihnen nach § 35 Abs. 7 SGB I gleichgestellten Staaten übermittelt werden dürfen.

Die Zweckbestimmung ist auch hier nachzuweisen (Abs. 1 S.1 Nr.1), darüber hinaus muss zuvor die Vergleichbarkeit der Aufgaben (Abs.1 S.1 Nr.2) und die Vergleichbarkeit der Ansprüche (Abs. 1 S.1 Nr.3) nachgewiesen werden. Eine Übermittlung ist außerdem zulässig bei Verletzung der Unterhaltspflicht zur Durchführung des Versorgungsausgleichs (Abs. 1 S. 1 Nr.3) und zur Durchführung eines Strafverfahrens (Abs. 1 S.1 Nr.4).

Die Schutzwürdigkeit der Interessen Betroffener ist abzuwägen. (Abs. 4)

### **§ 78 SGB X Zweckbindung und Geheimhaltungspflicht eines Dritten, an den Daten übermittelt werden**

Wenn Stellen, die nicht Sozialleistungsträger sind, Sozialdaten übermittelt werden, gelten für sie dieselben strengen Datenschutzregeln, die auch für die Träger nach § 35 SGB I gelten. Darüber hinaus ist eine Erklärung erforderlich, dass die Dritten die Daten nur zu dem Zweck verarbeiten, zu dem sie übermittelt wurden. (Abs. 1 S.2)

## Die Beauftragte für den Datenschutz

Der europäische Gesetzgeber nimmt die Stärkung der Grundrechte der Bürger\*innen sehr ernst. Bereits Ende des Jahres 2000 wurde die Charta der Grundrechte der Europäischen Union verabschiedet; sie enthält die Grundrechte, die für alle Bürger\*innen der Mitgliedsstaaten gelten sollen.

Sie enthält auch bereits eine Herleitung zum heute geltenden Datenschutzrecht einschließlich der unabhängigen Aufsichtsbehörden.

Kapitel II der Grundrechtecharta enthält die Freiheitsrechte.

**In Artikel 8 Abs. 1 heißt es: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“**

**Artikel 8 Abs. 3 ergänzt: „Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“** Der gemeinsame Wille war formuliert; die Notwendigkeit der unabhängigen Kontrolle erkannt.

Danach folgten Phasen des Gesetzgebungsverfahrens, die wegen des großen Kreises Stimmberechtigter einige Zeit in Anspruch nahm.

Im Jahr 2018 war es dann so weit; am 25.05.2018 trat nach einer zweijährigen Übergangsphase in allen Mitgliedsstaaten der Europäischen Union die EU-Datenschutzgrundverordnung (DSGVO) in Kraft.

Damit galt erstmals ein gemeinsamer, rechtlich verbindlicher Standard für den Datenschutz.

Das Datenschutzrecht aller EU-Mitgliedsstaaten wurde in den Kontext gemeinsamer europäischer Werte gesetzt und harmonisiert. Seitdem gelten für den Umgang mit personenbezogenen Daten EU-weit dieselben Grundregeln, die jeder Mitgliedsstaat aufgrund der Möglichkeiten in den Öffnungsklauseln der DSGVO konkretisieren und präzisieren kann.

### Wer kontrolliert die Einhaltung der DSGVO?

Weil gesetzliche Regelungen nicht selbst für ihre Einhaltung sorgen können, legt die DSGVO verbindlich fest, wer im Einzelfall sicherstellt, dass im Umgang mit personenbezogenen Daten die DSGVO eingehalten wird. Verantwortlich sind der/die Datenschutzbeauftragte der privaten und öffentlichen Stellen und der Behörden sowie die Aufsichtsbehörden. Die einschlägigen rechtlichen Bestimmungen für die Datenschutzbeauftragten finden sich in den Artikeln 37 bis 39 der DSGVO, die Aufgaben der Aufsichtsbehörde werden später detailliert beschrieben.

Die DSGVO gilt gleichermaßen für den öffentlichen und den privaten Bereich, deshalb sieht die DSGVO auch für beide Bereiche die Bestellung eines\*r Datenschutzbeauftragten vor. Der Unterschied liegt in der Verbindlichkeit, eine\*n Datenschutzbeauftragte\*n unabhängig von der Größe des Unternehmens zu bestellen.

### Wer ist der Verantwortliche nach der DSGVO?

Die DSGVO nennt im Kontext mit der rechtskonformen Umsetzung neben dem/der Datenschutzbeauftragten immer wieder den Begriff des **Verantwortlichen**; erstmals in Artikel 4 der DSGVO, in dem sich die Begriffsbestimmungen befinden.

Man findet den Verantwortlichen unter anderem im Impressum der Websites und auf den Aushängen zur Videoüberwachung. Verantwortliche\*r ist der Regel der/die Behördenleiter\*in; im Jobcenter ist der Vorstandsvorsitzende der Verantwortliche.

### Datenschutzbeauftragte in Behörden

Nach Artikel 37 Abs. 1 lit.a) der DSGVO muss jede Behörde oder öffentliche Stelle eine\*n Datenschutzbeauftragte\*n bestellen.

Auf diesem Wege wird die asymmetrische Kräfteverteilung zwischen einzelnen Bürgern\*innen und dem Staat bezogen auf den Schutz der eigenen Daten angeglichen.

Durch die Bestellung eines\*r Datenschutzbeauftragten wird das Grundrecht auf informationelle Selbstbestimmung systematisch und dezentral gestärkt. Mit der Benennung eines\*r Datenschutzbeauftragten erhält der Datenschutz in allen Behörden und öffentlichen Stellen einen herausgehobenen Stellenwert; keine öffentliche Stelle darf das Thema unbearbeitet lassen.

Die Benennung des/der Datenschutzbeauftragten muss der zuständigen Aufsichtsbehörde namentlich gemeldet werden, weil der/die Datenschutzbeauftragte die Ansprechperson der Aufsichtsbehörde ist.

### Aufgaben der Datenschutzbeauftragten des Jobcenters

Die Datenschutzbeauftragte ist für Betroffene und Beschäftigte in Fragen des Datenschutzes die erste Ansprechpartnerin. Sie nutzt Gespräche mit Führungskräften und Mitarbeitenden, Hospitationen, Datenstichproben, Feedbacks und Beschwerden, um die Einhaltung des Datenschutzes systemisch zu beleuchten und auch kritisch zu hinterfragen.

Dazu ist es wichtig, die internen Strukturen organisatorisch und operativ gut zu kennen, um auf die Bandbreite an Aufgaben und Kerntätigkeiten innerhalb des Jobcenters mit entsprechenden Angeboten zu reagieren. Die Grundprinzipien des Datenschutzes gelten für alle -Führungskräfte wie Mitarbeitende- deshalb müssen diese Prinzipien für alle verständlich und regelmäßig kommuniziert werden. Danach öffnet sich jedoch eine Bandbreite dessen, was Einzelne für ihren Alltag benötigen; deshalb sind die Qualifizierungen inhaltlich verschieden.

Sie tauscht sich regelmäßig mit dem Vorstandsvorsitzenden aus und legt zum Jahresende einen Tätigkeitsbericht mit den Schwerpunkten der Arbeit des abgelaufenen Jahres vor. Sie stößt Änderungen an und überwacht deren Einhaltung.

#### Der Auftrag der Datenschutzbeauftragten ist es:

**Datenschutz als Querschnittsthema im Unternehmen zu verankern und sowohl die Führungskräfte als auch die Mitarbeitenden mit den Alltagskompetenzen zum Thema Datenschutz auszustatten, die sie benötigen, um ihre Aufgabe kompetent und gut erledigen zu können.**

Die Datenschutzbeauftragte berät den Vorstandsvorsitzenden sowie den Vorstand insgesamt in allen Fragen des Datenschutzes und arbeitet darüber hinaus vertrauensvoll mit den Führungskräften und auch mit den Gremien zusammen.

Neben den Aufgaben, die in Artikel 39 der DSGVO als gesetzlicher Mindeststandard verbindlich festgelegt sind und die noch genannt werden, hat die Datenschutzbeauftragte eigene Aufgabenschwerpunkte. Sie richten sich nicht zuletzt danach,

- welche Kernaufgaben das Unternehmen wahrnimmt
- an welchen Schnittstellen innerhalb des Unternehmens personenbezogene Daten verarbeitet werden
- in welcher Qualität IT-Verfahren eingesetzt werden und
- mit welchen Sicherheitsstandards
- wie groß die Anzahl der Beschäftigten ist
- in welcher Größenordnung personenbezogene Daten regelmäßig und systematisch verarbeitet werden und
- in welchem Umfang besondere Kategorien von Daten nach Art. 9 DSGVO (Biometrie, Gesundheit, religiöses Bekenntnis, sexuelle Orientierung, etc.) betroffen sind.

Im Jobcenter steht aufgrund der gesetzlich festgelegten Aufgabe in der Regel ein\*e Kunde\*in mit individuellen Bedarfen im Zentrum der Aufgaben der operativen Teams; daraus ergeben sich jedoch auch wichtige Auswirkungen für die zentralen, übergeordneten Aufgaben, die im Fachbereich Personal und Zentrale Dienste wahrgenommen werden.

Aus der Kernaufgabe des Jobcenters erwächst ein Arbeitsschwerpunkt der Datenschutzbeauftragten:

Die Einhaltung des Datenschutzes in den Bereichen zu beleuchten und zu unterstützen, in denen Mitarbeitende und beauftragte Dritte (z.B. Träger) regelmäßig mit Kundendaten umgehen.

Die Formulierung in Artikel 39 Abs. 1 S.1: „Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben“ macht deutlich, dass der Gesetzgeber bewusst Luft für die adäquate Behandlung unterschiedlicher Verhältnisse vor Ort gelassen hat; dass er aber den Mindeststandard nicht verhandelt.

### Die Mindeststandards in Artikel 39 DSGVO umfassen folgende Aufgaben:

#### **Absatz 1 lit.**

- a. Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedsstaaten;
- b. Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedsstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- c. Beratung- auf Anfrage- im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gem. Artikel 35;
- d. Zusammenarbeit mit der Aufsichtsbehörde;
- e. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gem. Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

### **Stellung der Datenschutzbeauftragten**

Auch dazu enthält die DSGVO in Artikel 38 Hinweise. Die Datenschutzbeauftragte untersteht als Stabsstelle direkt dem Verantwortlichen (hier: dem Vorstandsvorsitzenden des Jobcenters). Er stellt sicher, dass die Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

Dienstrechtlich finden für die Datenschutzbeauftragte dieselben Regelungen Anwendung wie für alle anderen Beschäftigten.

In der Erledigung ihrer Fachaufgabe jedoch ist sie weisungsfrei und unabhängig. Damit ist die gesetzliche Voraussetzung geschaffen, als Datenschutzbeauftragte wirkungsvoll tätig werden zu können. Nur so ist sichergestellt, dass der Datenschutz sachorientiert und frei von hierarchischen Zwängen umgesetzt werden kann. Um alle Datenschutzbeauftragten davor zu schützen, wegen der Ausführung ihrer Tätigkeit benachteiligt zu werden, hat der Gesetzgeber für sie einen besonderen Schutz verfügt.

Die Datenschutzbeauftragten dürfen wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden. (Art. 38 Abs. 3 DSGVO)

Die Datenschutzbeauftragten unterliegen natürlich auch selbst dem Datenschutz.

Dazu regelt Art. 38 Abs. 5 DSGVO: Der/ die Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedsstaaten bei der Erfüllung seiner/ihrer Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.

### **Die zuständige Aufsichtsbehörde**

Die zuständige Aufsichtsbehörde für das Jobcenter, die Landesbeauftragte für den Datenschutz und die Informationsfreiheit NRW, (LDI), überprüft gegenüber den öffentlichen und nicht öffentlichen Stellen des Landes die Einhaltung der DSGVO, des Datenschutzgesetzes NRW, des BDSG und anderer Vorschriften des Datenschutzes. Ihre Rechtsstellung und ihre Aufgaben sind in den Artikeln 51 ff. der DSGVO festgeschrieben. Sie bewertet Verfahren/ Strukturen auf Kompatibilität mit der DSGVO und kann verbindlich deren Abänderung verlangen.

**Die zuständigen Aufsichtsbehörden sind auch berechtigt, bei Verstößen gegen den Datenschutz Bußgelder zu verhängen, allerdings gilt dies nur für Unternehmen der Privatwirtschaft; im öffentlichen Bereich wird auf Bußgelder verzichtet. Aufgrund der Finanzierungsströme über Steuern, Abgaben und Pflichtbeiträge Versicherter würde ein Bußgeld indirekt die Bürger\*innen treffen.**

Die Aufsichtsbehörde kann sich auf vielfältige Art einen Überblick über die Qualität der Arbeit des Jobcenters verschaffen.

Dies kann durch Sichtung der frei zugänglichen Medien geschehen. Ein Beispiel ist die Prüfung der Website bezüglich der Datenschutzkonformität der dort veröffentlichten Materialien (Datenschutzhinweise, Hinweise zur Videoüberwachung). Sie kann außerdem die technischen Einstellungen prüfen. (Bsp.: Einsatz von Cookies im vorgeschrieben Opt-In-Verfahren, Einsatz unerlaubter Tracking-Tools). Darüber hinaus lassen auch die Konsultationsverfahren, die allen Datenschutzbeauftragten für die Klärung rechtlicher Zweifelsfragen bei der Aufsichtsbehörde offen stehen, Rückschlüsse auf die Arbeit vor Ort zu; außerdem die Tätigkeitsberichte der Datenschutzbeauftragten, interne Datenschutzmanagementsysteme und ihre Überprüfung anlässlich einer Zertifizierung oder Re-Zertifizierung. Nicht zuletzt reflektiert die Art und die Anzahl der bei der Aufsichtsbehörde gemeldeten Datenschutzverstöße und der Beschwerden die Art des Umgangs mit dem Thema Datenschutz.

Die LDI ist auch die zuständige Stelle, **bei der sich Betroffene beschweren können**, die sich durch das Jobcenter Wuppertal grundsätzlich oder speziell durch eine Entscheidung der Datenschutzbeauftragten des Jobcenters in ihren Datenschutzrechten verletzt fühlen.

Für öffentlich-rechtliche Stellen des Landes und damit auch für die Kommunen und ihre Tochterunternehmen ist die zuständige Aufsichtsbehörde die:

**Beauftragte für den Datenschutz und die Informationsfreiheit des Landes Nordrhein-Westfalen**

**Bettina Gayk**

**Kavalleriestr. 2-4**

**40213 Düsseldorf**

**Tel.: 0211/ 384 24 0**

**E-Mail: [poststelle@ldi.nrw.de](mailto:poststelle@ldi.nrw.de)**

**<https://www.ldi.nrw.de>**

Darüber hinaus gibt es eine weitere, wichtige Aufsichtsbehörde für Bundesbehörden und bundesweit tätige Stellen (Post, Telekommunikation, Rentenversicherung); den

**Bundesbeauftragten für den Datenschutz und die Informationsfreiheit**

**Prof. Ulrich Kelber**

**Graurheindorfer Str. 131**

**53117 Bonn**

**E-Mail: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)**

**<https://www.bfdi.bund.de>**