Anlage 10: Muster für eine Handreichung zum Datenschutz für Beschäftigte

Datenschutz Kompakt: Handreichung für Beschäftigte

Wozu braucht es Datenschutz?

Datenschutz ist wichtig, weil natürliche Personen mit seiner Hilfe vor unrechtmäßiger oder missbräuchlicher Datenverarbeitung geschützt werden. Er kann Personen zwar nicht vor jeglicher Form der Datenverarbeitung bewahren. Datenschutz soll es aber ermöglichen, dass jede und jeder grundsätzlich selbst bestimmen kann und darüber Beschied weiß, wer was wann und bei welcher Gelegenheit mit den eigenen Daten macht.

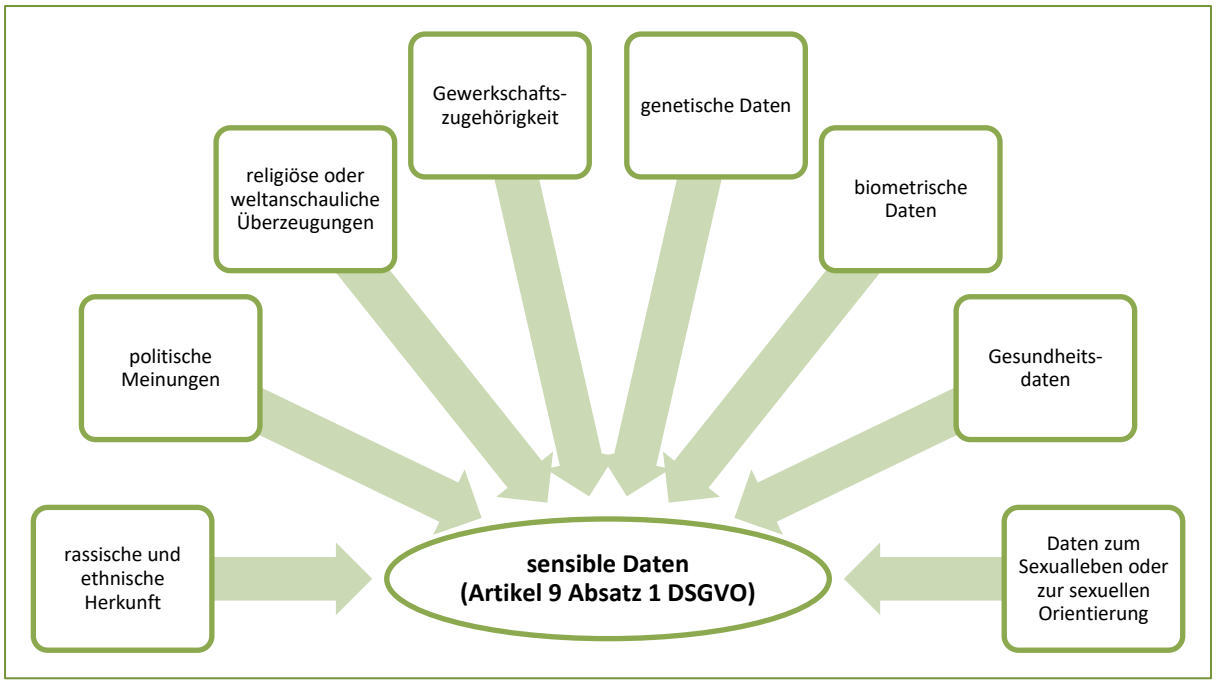
Welche Vorschriften regeln den Datenschutz?

Die wichtigste Vorschrift ist die **Datenschutz-Grundverordnung (DSGVO)**. Sie gilt seit dem 25. Mai 2018 und ist auch von den öffentlichen Stellen in Brandenburg anzuwenden. Ergänzend zur DSGVO sind das **Brandenburgische Datenschutzgesetz (BbgDSG)** und das **für den jeweiligen Verwaltungsbereich spezifische Datenschutzrecht** (zum Beispiel Vorschriften des Schulrechts, Steuerrechts, Melderechts, Sozialrechts) zu beachten.

Was sind personenbezogene Daten?

Unter personenbezogenen Daten versteht man alle Informationen, durch die sich eine Person mittelbar oder unmittelbar identifizieren lässt. Dazu gehören Informationen wie Name, Anschrift, E-Mail-Adresse, Kontonummer, Kfz-Kennzeichen, Personalausweisnummer oder auch die IP-Adresse.

Ein besonderer Schutz gilt für Daten, die in Artikel 9 Absatz 1 DSGVO genannt sind. Für diese sogenannten „sensiblen Daten“ gelten besondere Vorschriften.



Wer ist in der öffentlichen Stelle für den Datenschutz verantwortlich?

Die **Behördenleitung** schafft die Rahmenbedingungen und trifft die Letztentscheidung über Zwecke und Mittel der Verarbeitung. Sie kann festlegen, wer in der öffentlichen Stelle welche datenschutzrechtlichen Aufgaben und Pflichten zu erfüllen hat.

Die **Beschäftigten** verarbeiten personenbezogene Daten auf Anweisung der Behördenleitung. Sie haben beim Umgang mit diesen Daten datenschutzrechtlichen Vorschriften einzuhalten.

Die oder der **behördliche Datenschutzbeauftragte** berät die Behördenleitung und die Beschäftigten in Sachen Datenschutz. Zudem überwacht sie oder er die Einhaltung des Datenschutzes. Sie oder er hat jedoch nicht die Aufgabe, den Datenschutz umzusetzen. Diese Aufgabe obliegt der Behördenleitung und den Beschäftigten. Die oder der behördliche Datenschutzbeauftragte ist frühzeitig bei allen mit dem Datenschutz zusammenhängenden Fragen zu beteiligen. Beschäftigte können sich bei Fragen des Datenschutzes nicht nur an ihre Vorgesetzten, sondern auch direkt an die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten wenden. In ihrer Funktion sind sie unabhängige und zur Verschwiegenheit verpflichtete Ansprechpartner. Beschäftigte können sich an sie wenden, ohne befürchten zu müssen, dass sich das nachteilig für sie auswirkt.

Welche Grundsätze sind zu beachten?

Die Grundsätze für die Verarbeitung personenbezogener Daten regelt Artikel 5 DSGVO. Zu den Grundsätzen zählen:

- **Rechtmäßigkeit der Verarbeitung:** Die Verarbeitung von personenbezogenen Daten ist nur rechtmäßig, wenn sie auf eine Rechtsgrundlage gestützt werden kann.

- **Transparenz**: Personen sollten über alle wichtigen Informationen im Zusammenhang mit der Datenverarbeitung informiert werden. Sie sind auch über ihre Betroffenenrechte zu informieren und wie sie diese geltend machen können. Alle Informationen und Mitteilungen zur Datenverarbeitung sind leicht zugänglich zu machen und verständlich sowie in einfacher Sprache abzufassen.

- **Zweckbindung:** Personenbezogene Daten dürfen nur zu eindeutigen und rechtmäßigen Zwecken verarbeitet werden. Die Zwecke müssen zum Zeitpunkt der Erhebung der Daten feststehen.

- **Datenminimierung:** Es dürfen nur die Daten verarbeitet werden, die notwendig sind.

- **Richtigkeit der personenbezogenen Daten:** Die Daten müssen sachlich richtig und auf dem neuesten Stand sein. Sind Daten im Hinblick auf die Zwecke der Verarbeitung unrichtig, sind sie unverzüglich zu löschen oder zu berichtigen.

- **Speicherbegrenzung:** Daten sind zu löschen, wenn deren Speicherung für den festgelegten Zweck nicht mehr erforderlich ist. Gesetzliche Aufbewahrungsfristen und Vorschriften zur Archivierung sind zu beachten. Um sicherzustellen, dass Daten nicht länger als nötig gespeichert werden, sind Fristen für die Löschung oder regelmäßige Überprüfungen vorzusehen.

- **Integrität und Vertraulichkeit:** Bei der Verarbeitung ist eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten. Dazu zählt der Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung.

Welche Pflichten sind zu erfüllen?

Beim Umgang mit personenbezogenen Daten sind insbesondere die folgenden Fragen zu klären und die entsprechenden Pflichten zu erfüllen.

Ist die Datenverarbeitung erlaubt?

Grundsätzlich gilt, dass die Verarbeitung personenbezogener Daten verboten ist. Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine gesetzliche Rechtsgrundlage dies erlaubt. Die zentrale Vorschrift ist der Artikel 6 DSGVO. Sie enthält in Absatz 1 sechs verschiedene Tatbestände, bei deren Vorliegen eine Verarbeitung personenbezogener Daten erlaubt ist. Auch wenn diese sechs Tatbestände grundsätzlich gleichrangig sind, kommt nicht jeder für Verarbeitungen durch öffentliche Stellen in gleicher Weise als Rechtsgrundlage in Betracht.

Zulässigkeits-tatbestand	Rechtsgrundlage: Artikel 6 Absatz 1…	Anmerkungen und Hinweise
Erfüllung einer rechtlichen Verpflichtung	Buchstabe c	Eine solche rechtliche Verpflichtung kann sich aus Vorschriften des Unionsrechts oder des nationalen Rechts ergeben (Gesetze, Verordnungen, Satzungen, Dienstvereinbarungen, Verwaltungsvorschriften, Geschäftsordnungen). Beispiel: Für Arbeitgeber gelten Aufbewahrungspflichten für bestimmte Daten von Beschäftigten aufgrund von Bestimmungen im Arbeits-, Sozialversicherungs-, und Steuerrecht.
Wahrnehmung öffentlicher Aufgaben oder Ausübung hoheitlicher Gewalt	Buchstabe e	Auch hier muss sich die öffentliche Aufgabe aus Vorschriften des Unionsrechts oder des nationalen Rechts ergeben. Beispiel: Zur Erfüllung ihres Erziehungs- und Bildungsauftrags verarbeiten Schulen Daten von Schülerinnen und Schülern auf der Grundlage von § 65 Brandenburgisches Schulgesetz.
Einwilligung	Buchstabe a	In der Regel besteht ein klares Ungleichgewicht zwischen öffentlichen Stellen als Verantwortlichen und der betroffenen Person, sodass nach Erwägungsgrund 43 DSGVO eine Einwilligung als Rechtsgrundlage oft ausscheidet. Im Ausnahmefall kann eine Einwilligung aber als Rechtsgrundlage dienen, sofern den betroffenen Personen keine Nachteile bei einer Verweigerung der Einwilligung entstehen. Beispiel: Newsletter oder Presseverteiler.
Schutz lebenswichtiger Interessen	Buchstabe d	Es handelt sich um eine Ausnahme, die nur dann greift, wenn es um den Schutz höchstpersönlicher Rechtsgüter wie Leben oder körperliche Unversehrtheit geht und eine andere Rechtsgrundlage nicht in Betracht kommt.
Erfüllung eines Vertrags oder vorvertraglicher Verpflichtungen	Buchstabe b	Üblicherweise schließen öffentliche Stellen keine Verträge mit Bürgerinnen und Bürgern ab, sondern sind hoheitlich tätig. Für diese Fälle kommt Buchstabe b nicht in Betracht. Bei nicht hoheitlichen Tätigkeiten (im Rahmen des fiskalischen Handelns) kann eine Verarbeitung jedoch, je nach Einzelfall, auf Buchstabe b gestützt werden. Beispiel: Kauf von Büromaterial oder Dienstwagen.
überwiegende berechtigte Interessen	Buchstabe f	Diese Rechtsgrundlage kommt für öffentliche Stellen grundsätzlich nicht in Betracht.

Bei der **Verarbeitung von sensiblen Daten ist Artikel 9 DSGVO** die zentrale Vorschrift. Dort sind Tatbestände in Absatz 2 Buchstaben a bis j geregelt, die eine Verarbeitung solcher besonders ge-

schützten Daten erlaubt. In der Regel bedarf es einer nationalen Rechtsvorschrift, auf die Verarbeitung gestützt werden kann.

Ist die betroffene Person über die Datenverarbeitung informiert?

Es ist nicht ausreichend, dass eine Datenverarbeitung erlaubt ist. Die betroffene Person muss auch Kenntnis von der Existenz der Verarbeitung haben. Nur so kann sie informiert über die Verarbeitung ihrer Daten entscheiden. Zur Erfüllung des Grundsatzes einer fairen und transparenten Verarbeitung sehen die Artikel 13 und 14 DSGVO daher die Information der betroffenen Personen vor.

Checkliste: Betroffene Personen sind zu informieren über

- ☐ Namen und Kontaktdaten der öffentlichen Stelle,
- ☐ Kontaktdaten der oder des behördlichen Datenschutzbeauftragten,
- ☐ Zwecke und Rechtsgrundlagen der Verarbeitung,
- ☐ Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (hierzu zählen auch Auftragsverarbeiter wie zum Beispiel Betreiber von Webservern und Rechenzentren),
- ☐ (sofern zutreffend) Datenübermittlungen an Länder außerhalb des europäischen Wirtschaftsraums,
- ☐ Dauer der Datenspeicherung,
- ☐ Betroffenenrechte: Auskunft, Berichtigung oder Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit und bei Einwilligungen Informationen zum Widerrufsrecht,
- ☐ Beschwerderecht bei datenschutzrechtlichen Verstößen bei der Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht Brandenburg und
- ☐ Pflicht oder Erforderlichkeit zur Bereitstellung der Daten.

Werden die Daten nicht bei der betroffenen Person selbst erhoben, sondern bei Dritten, ist zudem zu informieren über:

- ☐ Kategorien der verarbeiteten personenbezogenen Daten und
- ☐ Herkunft oder Quelle der Daten.

Erfolgt die Datenverarbeitung sicher?

Beschäftigte müssen darauf achten, dass personenbezogene Daten nicht verlorengehen und dass sie nicht von Unbefugten eingesehen oder verändert werden können. Ist eine Weitergabe von Daten erforderlich, ist darauf zu achten, dass diese sicher erfolgt. Die Informationen über natürliche Personen sind daher von Beschäftigten vor unerlaubter Weitergabe, Kenntnisnahme und Verfälschung zu schützen. Sie müssen sich an entsprechende Vorgaben ihrer Behörde halten. Insbesondere sind folgende wichtige Sicherheitsregeln zu beachten:

- **Datenerhebung:** Erhoben werden dürfen nur für den Zweck erforderliche Informationen. Daten, die nicht gebraucht werden, sind zu schwärzen oder gar nicht erst zu erheben bzw. zu speichern.

- **Entsorgung von Unterlagen:** Dokumente mit personenbezogenen Daten dürfen nicht im normalen Müll oder Altpapiercontainer entsorgt werden. Es sind entweder gesonderte Datenabfallbehälter oder Aktenvernichter zu benutzen.

- **Weitergabe von Daten:** Achten Sie stets darauf, dass Daten nur an berechtigte Empfänger weitergegeben werden. Überprüfen Sie, ob die Kontaktdaten der Empfänger richtig sind (zum Beispiel richtige E-Mail-Adresse oder Faxnummer).

- **Datentransport:** Außerhalb der Behörde sind personenbezogene Daten stets auf verschlüsselten Datenträgern zu transportieren.

- **Passwortschutz:** Informieren Sie sich über die in Ihrer Behörde geltenden Anweisungen zum Passwortschutz. Verwenden Sie keine leicht zu erratenden Passwörter und geben Sie Ihre Passwörter nicht an andere weiter. Wenn Sie Ihren Arbeitsplatz verlassen, sperren Sie Ihren Computer mit der Tastenkombination „Windows-Taste“ + „L“.

Wann sind personenbezogene Daten zu löschen oder deren Verarbeitung einzuschränken?

Wann personenbezogene Daten zu löschen sind, regelt Artikel 17 DSGVO. Daten sind insbesondere zu löschen, wenn sie für die Zwecke, zu denen sie erhoben wurden, nicht mehr notwendig sind. Dem gegenüber stehen in der Regel jedoch gesetzliche Aufbewahrungspflichten, die zu beachten sind. Ebenso sind die Daten zuvor dem zuständigen öffentlichen Archiv anzubieten (§ 9 BbgDSG). Der Zugriff auf Daten ist unter den Maßgaben von Artikel 18 DSGVO einzuschränken. Die Einschränkung der Verarbeitung bedeutet, dass die Daten der Person technisch markiert und zukünftig nur beschränkt genutzt werden können.

Für Beschäftigte gilt, dass sie die Vorgaben ihrer Behörde zur Löschung und Einschränkung von Daten zu beachten haben. Daten dürfen nicht willkürlich gelöscht werden.

Was ist bei Datenschutzverletzungen zu tun?

Artikel 4 Nummer 12 DSGVO definiert eine Verletzung des Schutzes personenbezogener Daten (auch als „Datenschutzverletzung“ bezeichnet) als eine Verletzung der Sicherheit der Verarbeitung, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten bzw. zum unbefugten Zugang zu personenbezogenen Daten führt. Dies gilt unabhängig davon, ob es unbeabsichtigt oder unrechtmäßig zu einer Datenschutzverletzung kommt. Zudem bezieht sich dies nicht nur auf sensible Daten (Artikel 9 DSGVO), sondern auf alle personenbezogenen Daten.

Eine Dienstanweisung zum Datenschutz oder ein Datenschutzkonzept der öffentlichen Stelle sollte die Meldewege und den Umgang mit Datenschutzverletzungen innerhalb der Stelle regeln. Wenn Sie eine Verletzung erkennen, wenden Sie sich an Ihren Vorgesetzten und an die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten, sofern in Ihrer Behörde keine gesonderten Meldewege geregelt sind.

Wo finde ich weitere Informationen?

Umfangreiches Informationsmaterial, praktische Hinweise und Vorlagen sowie Muster können Sie auf den folgenden Seiten finden und herunterladen:

- Internetseite des Europäischen Datenschutzausschusses: https://edpb.europa.eu/edpb_de,
- Internetseite der Datenschutzkonferenz des Bundes und der Länder: https://www.datenschutzkonferenz-online.de,
- Infothek des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit: https://www.bfdi.bund.de/DE/Infothek/Informationsmaterial/informationsmaterial-node.html (die Texte zur DSGVO mit Erläuterung können als Druckexemplar bestellt oder heruntergeladen werden),
- Internetseite der Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht Brandenburg: https://www.lda.brandenburg.de,
- Praxishilfen der Stiftung Datenschutz: https://stiftungdatenschutz.org/dsgvo-info/praxishilfen/ und
- Anwendungshinweise des Ministeriums des Innern und für Kommunales Brandenburg: https://mik.brandenburg.de/mik/de/ministerium/akteneinsicht-und-datenschutz/.