Stellungnahme der Bundesdruckerei-Gruppe zum Konsultationsprozess zur Nationalen Rechenzentrumsstrategie

Als Technologieunternehmen des Bundes leistet die Bundesdruckerei-Gruppe mit ihrer Digital- und Sicherheitskompetenz einen Beitrag für die digitale Souveränität Deutschlands und Europas. Die Bundesdruckerei Gruppe betreibt eigene Rechenzentren an mehreren Standorten in Deutschland und arbeitet mit nationalen sowie internationalen Cloud-Partnern zusammen. Auf Basis dieser Infrastrukturen betreibt die Bundesdruckerei Gruppe insbesondere Lösungen für den öffentlichen Sektor, u.a. für das Identitätsmanagement, die digitale Verwaltung, Datenanalyse & KI sowie Verschlusssachen-Kommunikation.

Die Bundesdruckerei-Gruppe begrüßt die Initiative des BMDS, eine Nationale Rechenzentrumsstrategie zu entwickeln. Rechenzentren sind das Rückgrat der Digitalisierung und damit von zentraler Bedeutung für die Wettbewerbsfähigkeit, Souveränität und Nachhaltigkeit des Standorts Deutschland. Deutschland hat die Chance, hier gestaltend voranzugehen – eine klug ausbalancierte Strategie kann die Grundlage dafür schaffen.

Zu den Fragen nehmen wir wie folgt Stellung:

2. Welche zentralen Herausforderungen und Chancen sehen Sie für den Rechenzentrumsstandort Deutschland in den kommenden Jahren?

Herausforderungen:

Die geringe **Kosteneffizienz** deutscher Rechenzentren im Vergleich zu globalen Hyperscalern stellt ein zentrales Problem dar.

- Hyperscaler profitieren von Skaleneffekten, globaler Infrastruktur und extrem hohem Automatisierungsgrad. Nationale Anbieter müssen eine häufig lokal begrenzte Nachfrage sowie höhere Energie- und Personalkosten einkalkulieren.
  → *Politisch könnte durch gezielte Förderprogramme für nationale Betreiber sowie durch steuerliche Anreize zur Investition in Automatisierung und Energieeffizienz gegengesteuert werden.*

Die Umsetzung von **Sicherheitsanforderungen** und Mandantentrennung ist für kleinere Anbieter besonders ressourcenintensiv.

- Während Hyperscaler durch standardisierte Prozesse ein hohes Schutzniveau effizient abbilden, erfordert dies bei nationalen Anbietern eine komplexere Architektur.
  → *Gesetzliche Mindeststandards könnten stärker differenziert auf Betriebsgröße zugeschnitten werden. Zudem könnte überlegt werden, Sicherheitszertifizierungen und IT-Grundschutz durch staatliche Unterstützung zu vereinfachen.*

Die zunehmende **regulatorische Komplexität** auf nationaler und europäischer Ebene hemmt vor allem kleine und mittelgroße Anbieter.

- Neue Anforderungen wie NIS2, DORA oder der Cyber Resilience Act erfordern Ressourcen, die insbesondere für KMU schwer zu stemmen sind.
  → *Eine zentrale Beratungs-/Kompetenzeinheit könnte hier als Unterstützung dienen.*

Die **Energieinfrastruktur** ist oft ein Engpass – insbesondere der Anschluss an Mittel- und Hochspannungsnetze.

- Ohne verbindliche Fristen und transparente Netzplanung lassen sich Zeit- und Kostenpläne für neue Rechenzentren nur schwer kalkulieren.
  → *Der Gesetzgeber könnte verbindliche Anschlussfristen für Rechenzentren schaffen sowie den Netzbetreibern Berichtspflichten zur Netzkapazität und -Planung auferlegen.*

Flächenkonkurrenz und Fachkräftemangel behindern den Ausbau.

- In urbanen Räumen sind Grundstücke knapp und qualifiziertes IT-Personal ist schwer zu finden.
  → *Kommunen könnten durch Bundesprogramme zur Flächenentwicklung und Ansiedlung von RZ-Infrastruktur unterstützt werden. Parallel könnte die Aus- und Weiterbildung im Bereich RZ-Betrieb und IT-Sicherheit gezielt gefördert werden.*

Chancen:

Die **Nutzung von Abwärme** aus Rechenzentren bietet großes Potenzial für eine nachhaltige Wärmeversorgung.

- Rechenzentren liefern ganzjährig planbare Wärme, die in kommunalen Wärmeplanungen berücksichtigt werden kann.
  → Kommunen könnten verpflichtet werden, RZ-Abwärme in ihre Wärmeplanung einzubeziehen. RZ-Betreiber könnten gleichzeitig durch Investitionszuschüsse für Abwärme-Infrastruktur gefördert werden.

Der Ausbau von **europäischer Ingenieurskompetenz** – insbesondere im Bereich Hochleistungsrechenzentren – kann Innovation und Unabhängigkeit fördern.

- Durch die Förderung nationaler Kompetenzen bei Stromversorgung, Kühlung, Abwärmenutzung und RZ-Design kann ein europäischer Gegenpol zu Hyperscalern entstehen.
  → Förderprogramme für Forschung, Entwicklung und Bau von KI-RZs sowie öffentlich-private Partnerschaften mit Universitäten und Fachhochschulen könnten hier hilfreich sein.

Die **Vermeidung von Vendor-Lock-in** durch interoperable, offene Cloud-Stacks erhöht die Souveränität.

- Einheitliche Standards sichern die Anschlussfähigkeit ohne Innovationsfreiheit einzuschränken.
  → Staatliche IT-Vergaben könnten bevorzugt auf offenen Standards und interoperablen Architekturen basieren. Der Gesetzgeber könnte offene Schnittstellen fördern und regeln.

Die gestiegene öffentliche Aufmerksamkeit für **digitale Souveränität** bietet politisches Momentum.

- Die kritische Diskussion über die Abhängigkeit von insb. US-amerikanischen Diensten eröffnet neue Handlungsspielräume.
  → Dieses Momentum sollte durch klare politische Zielsetzungen, regulatorische Leitplanken und gezielte Förderungen für europäische Dienste – auch unter Hinnahme von teils etwas höheren Kosten – genutzt werden.

3. Welche Rahmenbedingungen sollten aus Ihrer Sicht wie verändert werden, um Rechenzentrumsinvestitionen zu fördern und Innovation zu ermöglichen?

Energieversorgung
→ Für einen wettbewerbsfähigen Rechenzentrumsstandort ist eine nachhaltige, stabile und bezahlbare Energieversorgung entscheidend. Genehmigungsverfahren für neue Stromanschlüsse müssen beschleunigt und entbürokratisiert werden. Ein modernes Netzentgeltsystem sollte netzdienliches Verhalten – etwa durch Nutzung von Speichern und Abwärme – belohnen. Der Staat sollte zudem gezielt den Einsatz regenerativer Energien für Rechenzentren fördern.

Standortpolitik
→ Der Bund sollte gemeinsam mit Ländern und Kommunen gezielt Flächen für Rechenzentren bereitstellen und kommunale Anreize für deren Ansiedlung schaffen. Eine gezielte staatliche Nachfrage – z. B. durch den Betrieb souveräner Dienste in deutschen RZs – kann Investitionen stimulieren. Außerdem ist ein flächendeckender Glasfaserausbau nötig, um auch strukturschwache Regionen zu erschließen.

Planungssicherheit und Verfahren
→ Langfristige digitale Zielbilder und Investitionssignale des Bundes können Planungssicherheit für Betreiber geben. Bundesweit einheitliche Genehmigungsverfahren mit klaren Fristen sowie die Einrichtung zentraler Koordinierungsstellen („One-Stop-Shop") auf Länderebene können Prozesse erheblich beschleunigen. Kommunale Digitalisierungsprojekte sollten transparenter und vorhersehbarer gemacht werden, um sie mit RZ-Initiativen verknüpfbar zu machen.

Förderpolitik und Innovation
→ Der Staat sollte aktiv den Transfer innovativer Technologien in den Markt unterstützen – etwa durch Reallabore oder Pilotprojekte im Bereich KI und Nachhaltigkeit. Förderprogramme für Forschung und Entwicklung sowie Fachkräftequalifizierung sind notwendig, um langfristig die Innovations- und Wettbewerbsfähigkeit nationaler Anbieter sicherzustellen.

4. Welche Rolle sollte der Staat bei der Entwicklung einer souveränen und resilienten Recheninfrastruktur einnehmen?

Der Staat sollte gezielt eigene RZ-Infrastrukturen nutzen, weiter ausbauen bzw. aufbauen, um möglichst vollständig souveräne und resiliente IT-Lösungen für Verwaltung und kritische Infrastrukturen bereitzustellen.

- Der überwiegende Anteil des Bedarfs der Verwaltung nach RZ-Leistungen kann mit eigener Betriebsinfrastruktur und ohne Rückgriff z.B. auf Hyperscaler-Angebote abgedeckt werden.
  → *Die Nutzung eigener Infrastrukturen sollte Maxime sein. Öffentliche IT-Dienstleister sollten mit den erforderlichen Mitteln ausgestattet werden, um Investitionen in eigene Infrastrukturen zu tätigen.*

Der Staat sollte Referenzmodelle definieren, die als Blaupause für den Aufbau und Betrieb souveräner **nationaler privatwirtschaftlicher RZ-Infrastruktur** dienen kann – für Anwendungsfälle in denen eigene Infrastrukturen nicht wirtschaftlich genutzt bzw. aufgebaut werden können.

- Diese Referenzmodelle sollten technische, organisatorische und regulatorische Mindestanforderungen für alle Ebenen – von der physischen Infrastruktur bis zur Servicebereitstellung – enthalten. Eine Anbindung an bestehende europäische Initiativen sollte integraler Bestandteil sein.
  → *Die Bundesregierung könnte diese Modelle gemeinsam mit Industrie, Wissenschaft und Verwaltung entwickeln und regelmäßig aktualisieren. Durch eine strategische IT-Beschaffungspolitik, die nationale Anbieter bevorzugt, sowie durch zentrale Plattformlösungen (z. B. souveräne Cloud-Angebote) kann der Staat marktgestaltend tätig werden.*

Der Staat sollte Mehrkosten für eine digitale Souveränität bewusst akzeptieren und diese in seiner Wirtschaftlichkeitsbetrachtung berücksichtigen.

- Souveräne Dienste können kurzfristig mit höheren Betriebskosten einhergehen – bieten aber langfristige Vorteile in Sicherheit, Resilienz und strategischer Unabhängigkeit.
  → *Der Gesetzgeber könnte dies durch eine angepasste Haushaltslogik und entsprechende Bewertungskriterien bei Direktvergaben oder Ausschreibungsverfahren berücksichtigen.*