Zu § 80 SGB X

Titel: Gemeinsames Rundschreiben zum Sozialdatenschutzrecht im SGB I und SGB X	**Normgeber:** Bund
Redaktionelle Abkürzung: RdSchr. 07s	**Gliederungs-Nr.:** [keine Angabe]
Normtyp: Rundschreiben	

Zu § 80 SGB X Rdnr. 4 bis 14 RdSchr. 07s – Zu Absatz 2 - Zulässigkeitsvoraussetzungen

4 Der stark überarbeitete Absatz 2 übernimmt zum einen das bisher geltende Recht, ordnet, in Anlehnung an § 11 Abs. 2 BDSG , die Schriftform i.S.v. § 126 BGB an und verlangt u.a. die eigenhändige Unterschrift. Da regelmäßig ein - unterschriebener - Hauptvertrag über die konkrete Dienstleistung existieren wird (z.B. EVB-IT Dienstleistungsvertrag), ist es ausreichend, wenn die Auftragsdatenvereinbarung nach § 80 SGB X eine Anlage dieses Hauptvertrages darstellt. Auch der Mindestinhalt des schriftlich zu erteilenden Auftrages wird konkretisiert:

- Gegenstand und Dauer des Auftrages,
- Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung,
- Art der Daten und Kreis der Betroffenen
- Technische und organisatorische Maßnahmen
- Berichtigung, Löschung und Sperrung von Daten
- Unterauftragsverhältnisse
- Duldungs- und Mitwirkungspflichten
- Weisungsrecht des Auftraggebers
- Prüf- Zutrittsrecht und Auskunftsrechte des AG
- Mitzuteilende Verstöße des Auftragnehmers.

5 Weiterhin sollten im Vertrag die Kosten der Durchführung der ADV, die Mitwirkung des Auftraggebers und seiner Aufsichtsbehörden, die Kündigung/Laufzeit der datenschutzrechtlichen Verpflichtungen festgehalten werden.

6 Um gemäß Nr. 2 den Umfang, die Art und den Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen festzulegen, ist eine genaue Spezifizierung des Datenschutzanteils eines IT-Projektes notwendig.

7 Satz 1 lässt eine Auftragserteilung nur dann zu, wenn der Auftragnehmer denselben Datensicherungsmaßnahmen genügt, die auch der Auftraggeber zu treffen hätte, würde er die Datenverarbeitung selbst durchführen. Das bedeutet, dass der Auftragnehmer zur Einhaltung der Datensicherungsmaßnahmen verpflichtet ist, auch wenn auf ihn das SGB X nicht anwendbar ist. Dazu ist es nicht ausreichend, dass der Auftragnehmer im Auftragsverhältnis die Einhaltung der Datensicherungsmaßnahmen zusichert. Vielmehr hat sich der Auftraggeber vor der Auftragsvergabe hiervon zu überzeugen. Die regelmäßige Nachkontrolle des Auftragnehmers durch den Auftraggeber ergibt sich nunmehr direkt aus Absatz 2 Satz 4.

8 Auskünfte, Prüfungen und Nachkontrollen können u.a. durch die Vor-Ort-Kontrolle, im Fall der regelmäßig durchzuführenden Nachkontrolle durch Selbstauskünfte, i.d.R. durch vom Auftragnehmer ausgefüllte und dem Auftraggeber übermittelte Fragebögen erfolgen.

9 Anerkannt sind vom Auftragnehmer nachgewiesene Kontrollen durch unabhängige Dritte. Diese erfolgen durch Zertifizierungen Dritter. Ein Auftragnehmer kann seine Qualität durch den von der Gesellschaft für Datenschutz und Datensicherheit zusammen mit dem Berufsverband der Datenschutzbeauftragten Deutschlands entwickelten Datenschutzstandard "DS-BvD-GDD-01" nachweisen.

10 Die Häufigkeit der regelmäßigen Nachkontrollen ist gesetzlich nicht vorgeschrieben. Sie kann zwischen den Parteien vereinbart werden und sollte sich auch nach der Schutzbedürftigkeit der Daten richten. Prüfungen bis alle 3 Jahre sollten als angemessen anerkannt sein. Prüfungen sind sowohl unangekündigt als auch häufiger möglich, in der Regel jedoch zu den üblichen Betriebszeiten, nach angemessener Ankündigungszeit.

11 Unterauftragsverhältnisse sind grundsätzlich zulässig. Sie können jedoch ausgeschlossen werden, z.B. im nichteuropäischen Ausland. Mindeststandards: Der Auftragnehmer sollte zur Beauftragung eines Subunternehmers nur berechtigt sein, wenn dem Auftraggeber im Verhältnis zum Subunternehmer vergleichbare Prüf-, Auskunfts-, und Zutrittsrechte wie gegenüber dem Auftragnehmer eingeräumt werden. Außerdem sollte der Subunternehmer seinen Sitz und seine Tätigkeit innerhalb der EU/EWR haben und erbringen. Hinsichtlich Unter-Unterauftragnehmer besteht die Gefahr der Aushöhlung der Stellung des Auftraggebers als "Herr der Daten". Zulässig sind sie - ebenfalls nur mit Durchgriff des Auftraggebers auf Unter-Unterauftragnehmer im Rahmen der Kontroll- und Weisungsrechte. Der Auftraggeber wird sich die Dokumentation der beim Unter-Unterauftragnehmer durchgeführten Kontrollen, insbesondere der Erstkontrolle zeigen lassen.

12 Sollten sich während der Auftragsdurchführung Mängel im Datensicherungskonzept des Auftragnehmers herausstellen, so ist der Auftraggeber verpflichtet, Weisungen zur Ergänzung der beim Auftragnehmer vorhandenen technischen und organisatorischen Maßnahmen zu erteilen. § 80 Abs. 2 Satz 2 SGB X sieht die Pflicht zur Festlegung des Umfangs von Weisungsbefugnissen vor. Da der Auftragnehmer nur "verlängerter Arm" des Auftraggebers ist, sind Weisungsbefugnisse nicht verhandelbar. Sie sind schriftlich zu erteilen.

13 Für den Fall von datenschutzrechtlich relevanten Leistungsstörungen oder sonstigen datenschutzrechtlich zu beanstandenden Verhaltensweisen des Auftragnehmers ist ein außerordentliches Kündigungsrecht vorzusehen.

14 Handelt es sich bei dem Auftragnehmer nicht um eine öffentliche Stelle, so hat sich der Auftraggeber schriftlich das Recht einräumen zu lassen, die in Satz 5 Nummer 1, 2 und 3 eingeräumten Maßnahmen ergreifen zu dürfen. Diese Rechte stehen unter dem Vorbehalt des Grundsatzes der Verhältnismäßigkeit, denn von Ihnen darf nur Gebrauch gemacht werden, soweit es im Rahmen des Auftrags für die Überwachung des Datenschutzes erforderlich ist. Die Voraussetzungen dieser sachlichen Eingrenzung hat der Auftraggeber im Einzelfall zu beweisen. Das Recht auf Vornahme von Besichtigungen, Prüfungen und Einsichtnahme ist auf den Ort der Grundstücke und Geschäftsräume beschränkt. Der Auftraggeber hat also nicht das Recht, die Unterlagen in seine Diensträume mitzunehmen oder deren Vorlage dort anzuordnen.