Anlage zu den Teilnahmebedingungen für ZEDAL-Online-Dienste

Vereinbarung zur Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz (BDSG)

zwischen

dem ZEDAL-Nutzer (nachfolgend „Auftraggeber“)

und

der Infraserv GmbH & Co. Höchst KG (nachfolgend „Auftragnehmer“)

1. Gegenstand der Vereinbarung

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des ZEDAL-Nutzers. Der Auftrag umfasst das Speichern und Übermitteln von Daten im Sinne des § 3 Abs. 4 BDSG nach Angaben der berechtigten Benutzer der ZEDAL-Online-Dienste.

2. Art der Daten

Die Auftragsarbeiten umfassen folgende Datenarten:

- Angaben über verantwortliche Ansprechpartner für die elektronische Nachweisführung
- Angaben über die ZEDAL-Benutzer zur Benutzer-/Betriebsstättenverwaltung
- Antragsdaten der ZEDAL-Benutzers zur Erlangung einer Signaturkarte
- Stammdaten der Benutzer zur Signaturkartenverwaltung
- IT-Nutzungsdaten

3. Kreis der Betroffenen:

Der Kreis der durch den Umgang mit personenbezogenen Daten beim Auftraggeber betroffenen Personen umfasst alle Mitarbeiter des Auftraggebers, die eine Funktion im Rahmen der elektronischen Nachweisführung innehaben und diese mit oder im Zusammenhang mit ZEDAL-Online-Diensten ausführen und als solche ZEDAL-Benutzer im Sinne der vorstehenden Ziffer 2 sind.

4. Technisch-organisatorische Maßnahmen

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen des § 9 BDSG entsprechen. Dies beinhaltet insbesondere:

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),
- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
- dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und, dass personenbezogene Daten bei der Verarbeitung und Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
- dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und, dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
- dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
- dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
- dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
- dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

Die hiernach vorzusehenden Maßnahmen sind in nachfolgendem Datenschutz- und Sicherheitskonzept zusammengefasst. Das Konzept wird während der Dauer des Auftragsverhältnisses nach dem Stand der Technik hinsichtlich der Angemessenheit der festgelegten Maßnahmen geprüft und bei Bedarf angepasst. Der Auftraggeber kann jederzeit Einsichtnahme in das Konzept verlangen. Wesentliche Änderungen des Konzeptes bedürfen seiner schriftlichen Zustimmung.

Datenschutz und Sicherheitskonzept § 11 Nr. 3 BDSG

I.) Zweckbestimmung der Datenverarbeitung- und verarbeitung oder Nutzung

Die Zweckbestimmung der Datenverarbeitung ergibt sich aus der ZEDAL-Teilnahmevereinbarung.

II.) Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien

Die betroffenen Personengruppen und diesbezügliche Datenkategorien ergeben sich aus der Zweckbestimmung (Nr. 1) und umfassen folgende Personenkreise:

- Personal der ZEDAL Teilnehmer Personal Geschäftspartner der ZEDAL Teilnehmer
- Beauftragte Personen der ZEDAL Teilnehmer
- Personal des Providers.

III.) Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können

Folgenden Empfängern können die nachfolgend bezeichneten Daten übermittelt werden:

- Der Zentralen Koordinierungsstelle der Länder (ZKS) können Registrierungsanträge der ZEDAL Teilnehmer übermittelt werden.
- Dem Trustcenter der Deutschen Telekom (Telesec) können Antragsdaten zur Erlangung einer Signaturkarte übermittelt werden, wenn dies durch den Teilnehmer explizit ausgelöst wird.
- Den Geschäftspartnern der Teilnehmer sowie den Aufsichtsbehörden können Daten über verantwortliche Ansprechpartner übermittelt werden, soweit der Teilnehmer dies auslöst.

IV.) Regelfristen für die Löschung der Daten

Stammdaten (Adressen und Benutzer) werden in der ausschließlichen Hoheit der Teilnehmer gelöscht. Dies trifft auch für die Daten der Signaturkartenverwaltung zu.

Verwaltungsdaten des Teilnehmeraccounts werden unverzüglich nach Beendigung der Teilnahmevereinbarung gelöscht.

Dokumente werden gemäß den vertraglichen und gesetzlichen Aufbewahrungsfristen und unter Berücksichtigung der Rechte anderer ZEDAL Beteiligter gelöscht.

V.) Geplante Datenübermittlung in Drittstaaten

Eine Übermittlung an Drittstaaten ist zurzeit nicht geplant, ansonsten werden die entsprechenden gesetzlichen Voraussetzungen geschaffen.

VI.) Zugriffsberechtigte Personen

Mitarbeiter folgender Firmen bzw. deren Abteilungen haben Zugriff auf die Daten:

Fa. Infraserv, Kundenbetreuer der Abteilung Abfall- und Altlastenmanagement

Fa. Infraserv, Administratoren des Service-Center IT

Fa. Infotech, System-Administratoren

Die Zugriffsberechtigung besteht im Rahmen der Aufgabenwahrnehmung

Die Zugriffsberechtigung besteht im Rahmen der Aufgabenwahrnehmung

VII.) Sicherheitsmaßnahmen nach § 9 BDSG

1. Zutrittskontrolle

Die Verarbeitung findet an folgenden Standorten statt:

a) Rechenzentrum im Industriepark Höchst

b) Backup-Rechenzentrum im Industriepark Höchst

c) Verwaltungsgebäude im Industriepark Höchst

zu a) Chipkarte. Videoüberwachung. Einbruchmeldeanlage.
zu b) Chipkarte und PIN. Videoüberwachung. Einbruchmeldeanlage.
zu c) Empfang Zugang zum Industriepark Höchst. Bewegung im Hause nur in Begleitung eines Mitarbeiters.

2. Zugangskontrolle

- Passwortschutz der Rechner (Client Betriebssystem, Anwendung): Mindestlänge 8 Zeichen, Zeichenmix, Wechselforcierung nach 6 Monaten.
- Bildschirmsperre bei Pausen mit Passwortaktivierung
- Zugriffssperren durch zentrale Firewalls

3. Zugriffskontrolle

Für die Aufgabenwahrnehmung bestehen im Rahmen eines Berechtigungskonzeptes vergebene Zugriffsberechtigungen für Mitarbeiter folgender Firmen bzw. deren Abteilungen.

a) Fa. Infraserv, Kundenbetreuer der Abteilung Abfall- und Altlastenmanagement

Die Mitarbeiter haben Zugriff auf alle Daten des ZEDALTeilnehmers.

b) Fa. Infraserv, Administratoren des Service-Center IT

Die Mitarbeiter haben zum Zweck des Supports Zugriff auf alle Daten der Transportpapiere.

c) Fa. Infotech, System-Administratoren

Die Mitarbeiter erhalten im Einzelfall zum Zweck des Supports Zugriff auf alle Daten. Der Zugriff erfolgt auf Datenbankebene durch einen Datenbankbenutzer mit Zugriffsrechten. Er wird von demjenigen gewährt, der für die Maschinen und die Datenbanken verantwortlich ist. Dies ist der Leiter der Abteilung Business Service bzw. sein Vertreter. Er überwacht den Zugriff. Die einzelnen Datenbankzugriffe werden nicht protokolliert.

4. Weitergabekontrolle

Die Weitergabe erfolgt

- an die ZKS per verschlüsselter OSCI Nachricht
- an die Telesec per verschlüsselter Mail
- an die Geschäftspartner der Teilnehmer und Behörden per verschlüsselter OSCI Nachricht.

Der Versand wird in allen Fällen protokolliert.

5. Eingabekontrolle

Hinsichtlich der Verwaltungsdaten (Account Manager) werden Eingaben und Änderungen benutzerbezogen protokolliert.
Alle anderen Daten, bis auf die IT-Nutzungsdaten, werden ausschließlich durch den Auftraggeber selbst eingegeben und verändert. Eine Protokollierung findet hier nicht statt.

6. Auftragskontrolle

Die Auftragskontrolle spielt vor allem im Hinblick auf die Erfassung der Verwaltungsdaten eine Rolle. Sie wird dadurch sichergestellt, dass der Auftraggeber die Daten selbst online erfasst. Die online erfassten Daten werden maschinell in den Teilnehmerstamm übernommen. Änderungen werden nur aufgrund schriftlicher Beauftragung durch den Auftraggeber vorgenommen.

7. Verfügbarkeitskontrolle

Folgende Maßnahmen zum Schutz gegen zufällige Zerstörung oder Verlust wurden getroffen:

- Einsatz von RAID-Systemen
- Einsatz von Spiegelplatten -Einsatz redundanter Datenbanken
- Tägliche Datensicherung
- Einsatz von Firewalls der Fa. Infraserv Höchst

8. Trennungskontrolle

Die Trennungskontrolle ist wie folgt realisiert:

- es gibt Produktivinstanzen und Testinstanzen
- die Daten sind kundenbezogen (teilnehmerbezogen) separiert
- die Erfassung, Veränderung, Löschung und Übermittlung erfolgt durch jeweils eigenständige Funktionen.

VIII.) Ort der Datenverarbeitung

An folgenden Orten werden Daten verarbeitet:
Rechenzentrum C 584 und K 705
Industriepark Höchst
65926 Frankfurt am Main

5. Sonstige Pflichten des Auftragnehmers

Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher aufbewahrungspflichten erforderlich sind.

Der Auftragnehmer stellt die auftragsgemäße Abwicklung der Datenverarbeitungsaufgaben durch die regelmäßige Überwachung und Prüfung der Wirksamkeit der getroffenen Regelungen und Maßnahmen sicher. Die Durchführung der

Auftragskontrolle durch den Auftragnehmer erfolgt mittels regelmäßiger Prüfungen im Hinblick auf die Vertragsausführung und – erfüllung.

Der Auftragnehmer ist zur Wahrung des Datengeheimnisses gemäß § 5 BDSG verpflichtet. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, werden auf das Datengeheimnis verpflichtet und über dies sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- und Zweckbindung belehrt. Die Verpflichtung zur Wahrung des Datengeheimnisses besteht auch nach Beendigung der Tätigkeit fort.

Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt, der seine Tätigkeit gemäß §§ 4f, 4g BDSG ausüben kann.

Der Auftragnehmer stellt dem Auftraggeber auf Anforderung die für die Übersicht nach § 4g Abs. 2 S. 1 BDSG notwendigen Angaben zur Verfügung.

6. Unterauftragsverhältnisse

Hinsichtlich der Bereitstellung der technischen Infrastruktur erfolgt die Erfüllung der vertraglich vereinbarten ZEDAL-Leistungen unter Einschaltung der INFOTECH GmbH, Holthoffstraße 122a, 45659 Recklinghausen.

Darüber hinaus ist der Auftraggeber mit der Einschaltung weiterer Subunternehmer zum Zwecke der Auftragserfüllung einverstanden. Der Auftragnehmer stellt hierbei Folgendes sicher:

- Die Unterauftragnehmer werden mit der gebotenen Sorgfalt ausgesucht.
- Die vertraglichen Regelungen mit den Unterauftragnehmern werden so gestaltet, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer entsprechen.
- Der Auftragnehmer lässt sich von dem Unterauftragnehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung und des § 11 BDSG i.V.m. Nr. 6 der Anlage zu § 9 BDSG einräumen. Dies umfasst auch das Recht des Auftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrechtlichen Verpflichtungen im Unterauftragsverhältnis, zu erhalten.

Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt, z.B. Telekommunikationsleistungen.

7. Kontrollrechte des Auftraggebers

Für die Beurteilung der Zulässigkeit der Datenverarbeitung/-erhebung/-nutzung sowie die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich.

Der Auftraggeber hat das Recht, die in Nr. 6 der Anlage zu § 9 BDSG vorgesehene Auftragskontrolle im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen.

Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach § 11 Abs. 2 S. 4 BDSG vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß § 9 BDSG und der Anlage nach.

8. Mitteilung bei Verstößen

Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind. Dies gilt vor allem auch im Hinblick auf eventuelle Informationspflichten des Auftraggebers nach § 42a BDSG. Der Auftragnehmer wird Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, wird der Auftragnehmer ihn hierbei unterstützen.

9. Weisungsbefugnis des Auftraggebers

Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftragnehmer hat nur nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich bestätigen.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

10. Löschung von Daten und Rückgabe von Datenträgern

Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- oder Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial . Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Ort der Datenverarbeitung

Die Verarbeitung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

12. Haftung

Die Haftung des Auftragnehmers richtet sich nach den Bestimmungen der Leistungsvereinbarung.

Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem BDSG oder anderen Vorschriften für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff beim Auftragnehmer vorbehalten.