Vereinbarung zur Auftragsverarbeitung zum Einzelabruf und technisch-organisatorische Maßnahmen

betreffend EfA-Online-Dienst::

„Sportstättenbelegungsmanagement“

Zwischen dem Leistungsbezieher (Auftraggeber / nachnutzende Kommune) und dem Leistungserbringer (Auftragnehmer / Kommunalvertreter NRW, d-NRW AöR) wird mit Abschluss des Einzelabrufs die folgende dienstspezifische Einzel-Auftragsverarbeitungsvereinbarung (nachfolgend „Einzel-AV“) für den Online-Dienst „Sportstättenbelegungsmanagement“ (SBM) geschlossen.

Präambel

Der Gegenstand des Auftrags ergibt sich aus dem Einzelabruf für den Bezug einer OZG-Verwaltungsleistung (094-26-141) für den EfA-Onlinedienst Sportstättenbelegungsmanagement mit der Vertragsnummer (094-26-141). Der Auftrag umfasst die Verarbeitung und Nutzung von personenbezogenen Daten bei der Durchführung folgender Aufgaben durch den Auftragnehmer: Im Rahmen des Sportstättenbelegungsmanagement-Portals der Staatskanzlei NRW werden personenbezogene Daten von Nutzenden zur Verwaltung der Buchung von kommunalen Sporteinrichtungen verarbeitet. Nut zende können natürliche Personen selbst sowie auch Ansprechpartner von juristischen Personen, wie z.B. einer Kommune, sein. Für die Nutzenden besteht die Möglichkeit, angebotene Sportstätten über das Serviceportal zu buchen und ihre Buchungen zu verwalten. Die Kommunen haben durch berechtigte Sachbearbeitende über das Portal die Möglichkeit, die Buchungen der Sportstätten zu verwalten. Hierzu gehört neben der Darstellung der angebotenen Sportstätten die Annahme oder Ablehnung der eingehenden Buchungsanträge. Der Service sieht vor, dass die Nutzenden sich jeweils registrieren müssen, um eine Buchung abschließen zu können. Die Sachbearbeitenden werden durch Administratoren, welche vom Betriebsteam berechtigt sind, freigeschaltet.

Die Staatskanzlei NRW ist als Betreiber des Onlinedienstes die datenschutzrechtliche verantwortliche Stelle für die Verarbeitung der personenbezogenen Daten im Sinne des Art. 4 Nr. 7 DSGVO.

Nach der aktuellen Rechtsauffassung hinsichtlich der Aufstellung der Verantwortlichkeit seitens der d-NRW AöR in Zusammenarbeit mit der Staatskanzlei NRW ergibt sich die Verantwortlichkeit der Staatskanzlei NRW aus § 8a Abs. 1, 4 OZG.

Die den länderübergreifenden Onlinedienst betreibende Behörde ist datenschutzrechtlicher Verantwortlicher, wenn Sie personenbezogene Daten auf Grundlage von § 8a Abs. 1 OZG verarbeitet. Die Verarbeitung der personenbezogenen Daten muss zu diesem Zweck zur Unterstützung bei der Inanspruchnahme einer elektronischen Verwaltungsleistung erfolgen.

Zum Zweck der Durchführung des Verwaltungsverfahrens werden Daten an die zuständigen Kommunen übermittelt und von diesen über den Onlinedienst abgerufen und verarbeitet. Die datenschutzrechtliche Verantwortung dieser Kommunen bleibt durch die Verantwortlichkeit der Staatskanzlei NRW gem. § 8a Abs. 4 OZG unberührt, sodass diese auch als eigenständig Verantwortliche i.S.v. Art. 4 Nr. 7 DSGVO fungieren. Die Verantwortlichkeit zur Durchführung des Verwaltungsverfahrens obliegt den jeweiligen Kommunen.

1. Dienstspezifische Datenkategorien, Zwecke und betroffene Personen

I. Zwecke der Verarbeitung

- Bereitstellung und Nutzung eines Online-Portals zur Buchung kommunaler Sportstätten.
- Registrierung und Verwaltung von Nutzerkonten sowie Verwaltung eingereichter Buchungen.
- Annahme, Ablehnung und Verwaltung von Buchungsanträgen durch berechtigte kommunale Sachbearbeitende.
- Freischaltung berechtigter Sachbearbeitender durch hierzu berechtigte Administratoren.
- Technische Bereitstellung des Dienstes einschließlich der hierbei anfallenden erforderlichen Nutzungs- und Protokolldaten.

II. Kategorien betroffener Personen

- Antragstellende / registrierte Nutzende (natürliche Personen und Ansprechpersonen juristischer Personen).
- Berechtigte Sachbearbeitende und sonstige Beschäftigte der nachnutzenden Kommunen.
- Administratoren des Online-Dienstes.
- Besuchende der Website bzw. des Online-Dienstes.

III. Datenarten und Datenkategorien

Im zwischen d-NRW AöR und Deloitte Consulting GmbH geschlossenen AVV sind die folgenden Kategorien ausdrücklich als verarbeitet gekennzeichnet:

- Personenstammdaten.
- Meta- und Kommunikationsdaten.
- Kontaktdaten.

Eine feldgenaue Aufstellung (z. B. Vor- und Nachname, E-Mail-Adresse, Nutzerkennung, Buchungsbezug, IP-Adresse, Zeitstempel) ist im bereitgestellten AVV nicht verbindlich spezifiziert. Diese Angaben dürfen daher erst nach Abgleich mit dem tatsächlich eingesetzten SBM-Datenmodell ergänzt werden. Ebenso sind etwaige in Buchungsfreitexten enthaltene personenbezogene Daten und ihre datenschutzrechtliche Behandlung zu prüfen.

IV. Arten der Verarbeitung

Erheben / Erfassen; Speichern; Bereitstellen / Übermitteln; Lesen; Schreiben / Verändern; Löschen.

V. Ort der Verarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen, schriftlichen Zustimmung des Auftraggebers erfolgen.

2. Technische und organisatorische Maßnahmen (TOM)

Für die dem Online-Dienst zugrunde liegenden Leistungen der Deloitte Consulting GmbH gelten die von Deloitte dokumentierten technischen und organisatorischen Maßnahmen gemäß folgendem Dokument:

„Deloitte TOMs – Technische und organisatorische Maßnahmen“, Mandantenversion 01.11.2025, Version 3.0, gültig bis 30.09.2027 (nachfolgend „Deloitte-TOM“). Das unveränderte, 16-seitige Dokument wird als Unteranlage 4a beigefügt. [Anwendbarkeit auf sämtliche für SBM eingesetzten Systeme und Freigabe der Weitergabe an Kommunen bestätigen.]

Die Deloitte-TOM enthalten insbesondere folgende Regelungsbereiche:

1. Pseudonymisierung und Verschlüsselung	**Pseudonymisierung; Verschlüsselung personenbezogener Daten bei Speicherung und Übertragung.**
2. Vertraulichkeit, Integrität und Belastbarkeit	Physische Zutrittskontrolle; Zugangskontrolle; rollenbasiertes Berechtigungsmanagement; Eingabe-, Trennungs- und Weitergabekontrolle; Belastbarkeit.
3. Verfügbarkeit und Wiederherstellung	Sicherung und Verfügbarkeit; Datenlöschung; Notfall- und Wiederherstellungsmaßnahmen.
4. Wirksamkeitskontrolle / PDCA	Auftragskontrolle; dokumentierte und regelmäßig überprüfte Sicherheits- und Datenschutzprozesse.
5. Datenschutzfreundliche Voreinstellungen	Privacy by Design und Privacy by Default.

Wesentliche Änderungen der TOM und der Nachweis eines dem Risiko angemessenen Schutzniveaus richten sich nach der Rahmen-AV und den für die Leistung verbindlichen Verträgen. Die Übernahme der Deloitte-TOM in diese Einzel-AV ersetzt keine Prüfung SBM-spezifischer Betriebs- oder Hosting-Maßnahmen.

3. Genehmigte Unterauftragnehmer

Für die vorgelagerte Verarbeitungskette benennt die bestehende AVV zwischen d-NRW AöR und Deloitte Consulting GmbH folgenden Unterauftragnehmer:

Unterauftragnehmer	**Deloitte Advisory Sp. z o.o. sp. k.**
Anschrift	al. Jana Pawła II 22, Warszawa, 00-133, Polska
Leistung	Bereitstellung von Ressourcen zur Vertragserfüllung.

Die Deloitte Consulting GmbH ist Vertragspartnerin von d-NRW AöR für die Entwicklung und den Betrieb von SBM. Ob und in welcher rechtlichen Rolle Deloitte Consulting GmbH und Deloitte Advisory Sp. z o.o. sp. k. im Einzelabruf Kommune–d-NRW als (weitere) Unterauftragnehmer aufzuführen sind, ist anhand der gesamten AV-Vertragskette und der Rahmen-AV zu bestätigen. Die obige Liste kann nicht ohne diese Prüfung als abschließend gelten.

4. Weisungen des Auftraggebers

I. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers verarbeiten. Der Verantwortliche entscheidet allein über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten. Eine Verarbeitung für andere Zwecke, insbesondere für eigene Zwecke des Auftragnehmers ist nicht zulässig. Weisungen werden nur vom Auftraggeber und von keinem Dritten erteilt, auch wenn die Datenverarbeitung im Interesse oder Auftrag dieses Dritten erfolgt.

II. Mündliche Weisungen des Auftraggebers bestätigt der Auftragnehmer unverzüglich textlich (mind. per Mail). Der Auftragnehmer dokumentiert die Weisungen.

III. Der Auftragnehmer hat den Auftraggeber unverzüglich unter Angaben von Gründen zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

Weisungsberechtigte Personen des Auftraggebers sind:

Kommune
Name
Email
Rufnummer

Weisungsempfänger beim Auftragnehmer sind:

d-NRW AöR
Team Kommunalvertreter
kommunalvertreter@digitales.nrw.de
0231 222 438-100

5. Kontakt zur Aufsichtsbehörde

I. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

II. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

III. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

IV. Der Auftragnehmer unterstützt den Auftraggeber vollumfänglich durch geeignete Maßnahmen bei der Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der Betroffenen. Soweit eine betroffene Person sich in Ausübung ihrer Rechte unmittelbar an den Auftrag-nehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

6. Kontrollrechte des Auftraggebers

I. Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung, der Vorschriften der DSGVO und weiterer evtl. einschlägiger datenschutzrechtlicher Vorschriften durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Der Auftragnehmer unterstützt den Auftraggeber bei diesen Prüfungen. Ggf. sorgt der Auftragnehmer auch dafür, dass der Auftraggeber Prüfungen auch bei Unterauftragnehmern durchführen können und auch diese den Auftraggeber unterstützen.

II. Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftrag-nehmers nach Art. 28 EU-DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

III. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 EU-DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 EU-DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7. Mitwirkung des Auftragnehmers bei der Erfüllung der Pflichten nach Art. 32 ff. DSGVO

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen. Hierzu gehören u.a.:

- die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
- die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
- die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

8. Berichtigung, Einschränkung, Löschung und Rückgabe von Daten

I. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

II. Soweit vom Leistungsumfang erfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

III. Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

IV. Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und 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.

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

9. Außerordentliche Kündigung

Unabhängig von den getroffenen Regelungen über die Laufzeiten bzw. die Dauer der Vereinbarung, steht dem Auftraggeber ein Recht auf fristlose Kündigung bei schwerwiegenden Vertragsverletzungen des Auftragnehmers zu. Dies kommt insbesondere in Betracht bei Verstoß gegen datenschutzrechtliche Vorschriften, Datenschutz- und Datensicherheitsvereinbarungen oder falls der Auftragnehmer eine Kontrolle des Auftraggebers oder des nordrhein-westfälischen Datenschutzbeauftragten vertragswidrig verweigert.

10. Haftung

I. Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder seine Unterauftragnehmer bei der Erbringung der vertraglichen Leistung schuldhaft verursachen.

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

III. Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

11. Sonstiges

I. Sollten Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren.

II. Diese Vereinbarung enthält alle vertraglichen Regelungen zwischen den Parteien. Nebenabreden können getroffen werden. Sie bedürfen der Schriftform. Dies gilt auch für den Verzicht auf das Schriftformerfordernis.

III. Es besteht Einigkeit bei den Vertragsparteien darüber, dass die Allgemeinen Geschäftsbedingungen des Auftragnehmers auf diese Vereinbarung keine Anwendung finden.

IV. Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 BGB wird hinsichtlich des Anspruchs auf Rückgabe der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

V. Gerichtsstand ist, wenn in einer evtl. Leistungsvereinbarung nichts anderes vereinbart ist, Dortmund.

12. Geltung und Vertragsunterlagen

Diese Einzel-AV gilt für den Zeitraum des jeweiligen Einzelabrufs, soweit die Rahmenvereinbarung keine abweichende Regelung vorsieht.

Unteranlagen

- Unteranlage 4a: „2026-03-19_Deloitte_TOMs.pdf“ (Deloitte-TOM, 16 Seiten; unverändert beizufügen).