Anlage 3

Vereinbarung zur Auftragsverarbeitung zum Einzelabruf und technisch-organisatorische Maßnahmen

betreffend die OZG-Verwaltungsleistung:

„Untersuchungsberechtigungsschein“

Zwischen dem Leistungsbezieher (Auftraggeber/Kommune) und dem Leistungserbringer (Auftragnehmer/Kommunalvertreter.NRW) wird mit Vertragsschluss des Einzelabrufs die folgende Einzel-Auftragsvereinbarung (nachstehend „Einzel-AV“) zum Einzelabruf betreffend die OZG-Verwaltungsleistung „Untersuchungsberechtigungsschein“ als Anlage 3 geschlossen.

Präambel

Diese Einzel-AV regelt auf Grundlage der zwischen den Vertragsparteien geschlossenen Rahmenvereinbarung die Einzelheiten der Datenverarbeitung im Zusammenhang mit dem Einzelabruf „Untersuchungsberechtigungsschein“. Verantwortliche Stelle i.S.d. DSGVO gem. Art. 4 Nr. 7 sind die jeweiligen Kommunen. Der Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke als die in diesem Auftragsverarbeitungsvereinbarungen festgelegten Zwecke.

1. OZG-Verwaltungsleistungs-spezifische Datenkategorien, Zwecke, Betroffene

Der Auftragnehmer verarbeitet im Rahmen der OZG-Verwaltungsleistung „Untersuchungsberechtigungsschein“ die folgenden personenbezogenen Daten:

I. Zwecke

Erhebung und weitere Verarbeitung personenbezogener Daten zur Beantragung eines Untersuchungsberechtigungsscheins und zur Abrechnung der daraus folgenden Untersuchungskosten.

II. Betroffene

- Antragstellende (Jugendliche unter 18 Jahren oder Personensorgeberechtigte)
- Amtsmitarbeitende
- Prozessverantwortliche des Landes (Einblick in Statistiken)

III. Datenkategorien

Die erhobenen Daten gehören zu den sensiblen Daten nach Art. 9 Abs. 1 DSGVO. Aus der Auswahl bestimmter Nachuntersuchungsarten können unter Umständen Rückschlüsse auf den Gesundheits- bzw. Entwicklungsstand der jugendlichen Person gezogen werden. Folgende Datenkategorien werden verarbeitet:

- Personenstammdaten (Name, Vorname, Geburtsdatum)

- Adressdaten
- Kontaktdaten (E-Mail der Verwaltungsadministratoren zur Authentifizierung am Dienst)
- Arbeitgeberdaten (nur falls Antragsteller wohnhaft im Ausland)
- Sensible Daten nach Art. 9 Abs. 1 DSGVO
    - Gesundheitsdaten (Art der Untersuchung)

IV. 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 Bereitstellung des Online-Dienstes Untersuchungsberechtigungsschein (UBS) wurde die NextgoviT durch den Auftragnehmer beauftragt.

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen. Für die Bestimmung geeigneter TOM ist zunächst der Schutzbedarf der zu verarbeitenden personenbezogenen Daten festzulegen und hier zu dokumentieren.

Schutzbedarf der Daten gemäß Systematik der DSK: hoch

Es müssen Regelungen zu folgenden Punkten getroffen werden:

Für die Vernichtung gem. DIN 66399 gilt Schutzklasse 2.

2.1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

a. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern - (räumlich) vorhanden

- Elektronische Zutrittscodekarten/ Zutrittstransponder
- Begleitung von Besucherzutritten durch eigene Mitarbeiter
- Auslagerung von Servern in Rechenzentren

b. Zugangskontrolle

Verhindern des Eindringens Unbefugter in die DV-Systeme oder deren unbefugter Nutzung

- Verschlüsselung von Netzwerken
- Verwendete von verschlüsselten Zugriffskanälen auf Kundenserver und Unternehmensdaten (VPN, SSH, https)
- Passwortsicherung von Bildschirmarbeitsplätzen
- Verwendung von individuellen Passwörtern
- Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern
- Passwort-Policy mit Mindestvorgaben zur Passwortkomplexität

- Rollenbasierte Rechtevergabe für Produktionssysteme
- Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
- Prozess zum Rechteentzug bei Austritt von Mitarbeitern
- Verpflichtung zur Vertraulichkeit

c. Zugriffskontrolle

Verhinderung von unerlaubten Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen

- Regelung zur Wiederherstellung von Daten aus Backups (wer, wann, auf wessen Anforderung)
- Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Daten und Datenbanken

d. Trennungskontrolle

Getrennte Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten

- Trennung von Kunden (Mandantenfähigkeit oder Separierung des verwendeten Systems)
- Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern)
- Trennung von Entwicklungs-, Test- und Produktivsystem

2.2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

a. Weitergabekontrolle

Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln

- Weitergabe personenbezogene Daten nur auf expliziter vertraglicher oder rechtlicher Grundlage
- Datenaustausch über gesicherte Verbindung
- Verschlüsselung vertraulicher Datenträger

b. Eingabekontrolle

Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege

- Festlegung von Benutzerberechtigungen (Profile)
- Differenzierte Benutzerberechtigungen
- Lesen, Ändern, Löschen
- Teilzugriff auf Daten bzw. Funktionen
- Verpflichtung auf das Datengeheimnis

2.3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

a. Verfügbarkeitskontrolle

Schutz gegen zufällige Zerstörung oder Verlust

- Datensicherungs- und Backupkonzepte
- Durchführung der Datensicherungs- und Backupkonzepte
- Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft Katastrophen-
- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben)
- Generelle Maßnahmen Belastbarkeit
- Härtung von Systemen
- Durchführung von automatisierten Schwachstellenscans

- Regemäßige Patchzyklen
- Bedarfsorientierte Durchführung von Penetrationstests

b. Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

Fähigkeit des Umgangs mit risikobedingten Veränderungen, Toleranz und Ausgleichsfähigkeit gegenüber Störungen

- Abgrenzung kritischer Komponenten
- Systemhärtung (Deaktivierung nicht erforderlicher Komponenten)
- Auslagerung von Datensicherungen

Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmwareupdates:

- Progressive Bereitstellung von Updates / Patches, um Probleme frühzeitig zu erkennen, ohne mehrere Geräte zu beeinträchtigen.
- Festlegung einer Testperiode, um die korrekte Implementierung des Updates zu überprüfen und sicherzustellen, dass die Operationen mit den neuen Updates weiterhin reibungslos ablaufen.

Sicherheit wird während der Entwurfsphase der Systeme als Hauptbetrachtung mit umfasst:

- Definition von Sicherheitsmaßnahmen zum Schutz und zur Validierung der Kommunikation zwischen Systemkomponenten
- Begrenzung von Berechtigungen auf Bedarfsnotwendigkeit.
- Externe Auftragsverarbeiter und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist.

2.4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

a. Kontrollverfahren

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherheitsmaßnahmen

- Interne Verfahrensverzeichnisse werden mind. jährlich aktualisiert
- Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- Es werden datenschutzfreundliche Voreinstellungen gewählt
- Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen

Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt.

b. Auftragskontrolle

Sicherstellung der weisungsgemäßen Datenverarbeitung durch Dienstleister

- Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO)
- Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)
- Regelmäßige Kontrollen beim Auftragsverarbeiter nach Vertragsbeginn (während Vertragsdauer)
- Überprüfung des Datensicherheitskonzepts beim Auftragsverarbeiter
- Sichtung vorhandener IT-Sicherheitszertifikate der Auftragsverarbeiter

3. Liste der genehmigten Subunternehmer

	Name des Subunternehmers	Anschrift	Leistung
1	nextgov iT GmbH	Lombardenstraße 24 52070 Aachen	Pflege, Wartung, Support, Weiterentwicklung

Die d-NRW informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung weiterer oder Ersetzung bestehender Subunternehmer für die Auftragsverarbeitung. d-NRW teilt dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mit. Es ist keine Zustimmung seitens Auftraggeber erforderlich, die Liste der Subunternehmer der jeweiligen Einzel-AV wird von d-NRW entsprechend aktualisiert und dem Auftraggeber zur Verfügung gestellt.

Verträge mit Subunternehmern sind in schriftlicher oder elektronischer Form zu vereinbaren und müssen dem Subunternehmer mindestens mit diesem Vertrag vergleichbare Datenschutzpflichten auferlegen, insbesondere die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen umfassen. Der Auftragnehmer wird sicherstellen, dass der Auftraggeber auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer erhalten kann.

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:

Name + Emailadresse

Weisungsempfänger beim Auftragnehmer sind:

Kommunalvertreter.NRW

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.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift (Auftraggeber)	Unterschrift (Auftragnehmer)
_____	_____
Name, Vorname, Funktion des/der Vertretungsberechtigten	Name, Vorname, Funktion des/der Vertretungsberechtigten