Allgemeine Geschäftsbedingungen
für die Nutzung des Services RezeptDirekt durch Apotheken

Die DIGAPO - Digitale Dienstleistungen für Apotheken vor Ort GmbH, Karl-Heinrich-Ulrichs-Str. 9, 10787 Berlin („DIGAPO“) ist Anbieterin des Services „RezeptDirekt“, der es teilnehmenden Apothekerinnen und Apothekern („Apotheken“) ermöglicht, elektronische Vorbestellungen von Apothekenkunden („Nutzern“) entgegen zu nehmen und zu bearbeiteten.

Diese Nutzungsbedingungen regeln die näheren Bedingungen zur Nutzung dieses Services im Verhältnis zwischen DIGAPO und der jeweils teilnehmenden Apotheke.

1. Leistungsbeschreibung / Anbieterkennzeichnung

1.1 Die Apotheke erhält für die Dauer des Nutzungsvertrages das Recht zur Teilnahme am Service „RezeptDirekt“. Hierzu wird die Apotheke in die Liste der am Service teilnehmenden Apotheken aufgenommen und erhält Zugriff auf eine browserbasierte Verwaltungssoftware für Apotheken. Unverbindliche Vorbestellungen von Nutzern, die diese mittels einer mobilen Anwendung („App“) für Smartphones per Texteingabe oder Rezeptablichtung an die teilnehmende Apotheke senden, werden über diese Web-Anwendung angezeigt und können von der Apotheke bearbeitet werden. Die Apotheke kann mit dem Nutzer per Chat-Funktion kommunizieren und ihn darüber informieren, wann die vorbestellte Ware zur Abholung bereit steht.

1.2 Die weiteren Rechtsbeziehungen zwischen Apotheke, Nutzer und der Anbieterin richten sich nach den gesonderten „Nutzungsbedingungen zur App für Apothekenkunden“ gemäß Anlage 2.

2. Vertragsschluss

2.1 Der Antrag auf Teilnahme der Apotheke am Service „RezeptDirekt“ zu den Bedingungen dieses Vertrages nebst Anlagen kann durch ihren approbierten Inhaber sowohl schriftlich, in Textform, als auch auf elektronischem Weg gegenüber der in Anlage 1 aufgeführten berechtigten und von DIGAPO bevollmächtigten Stellen erklärt werden. Bei der Anmeldung geben Apotheken ihre IK-Nummer an und bestätigen, dass sie zum Zeitpunkt der Anmeldung über eine gültige Approbation verfügen.

2.2 Nach Prüfung des Antrags auf Vollständigkeit schaltet DIGAPO die Apotheke für den Service frei. Die berechtigte und von DIGAPO bevollmächtigte Stelle nach Anlage 1 übersendet der Apotheke die zur Nutzung der Verwaltungssoftware erforderlichen Zugangsdaten. Durch die Freischaltung erklärt DIGAPO zugleich die Annahme des Teilnahmeantrags. Damit ist der Nutzungsvertrag zustande gekommen.

3. Anbieterkennzeichnung der Apotheke innerhalb der App

Die Apotheke ist für die Vorhaltung einer gesetzeskonformen Anbieterkennzeichnung (Impressum) gemäß § 5 Abs. 1 TMG innerhalb der App selbst verantwortlich. Hierfür hat sie die Möglichkeit, mit der ihr zur Verfügung gestellten Verwaltungssoftware eine Verlinkung auf das Impressum ihres eigenen Internetauftritts zu hinterlegen. Der Hinweis auf das Impressum wird innerhalb der App in der Detailansicht der jeweiligen Apotheke als sprechende Verlinkung angezeigt.

4. Nutzungsentgelte / Preisanpassungen / Änderung der Nutzungsbedingungen

4.1 Die Nutzung des Services „RezeptDirekt“ durch die Apotheke ist kostenfrei.

4.2 Über Änderungen der Nutzungsbedingungen wird DIGAPO die Apotheke mindestens 4 Wochen im Voraus informieren. Die Änderung gilt als von der Apotheke akzeptiert, sofern diese nicht binnen 4 Wochen nach Bekanntgabe der Änderung widerspricht. Auf diese Rechtsfolge wird DIGAPO in ihrer Änderungsankündigung gesondert hinweisen. Macht die Apotheke von ihrem Widerspruchsrecht Gebrauch, so gilt der Vertrag in seiner zuvor geltenden Fassung fort.

5. Gewährleistung

DIGAPO gewährleistet, dass die der Apotheke überlassene Verwaltungssoftware sowie die hiermit verbundene App für Nutzer die Eignung für den vertragsgemäßen Gebrauch gemäß Leistungsbeschreibung aufweist. DIGAPO gewährleistet eine Erreichbarkeit seiner Server von 99% im Jahresmittel. Hiervon ausgenommen sind Zeiten, in denen die Server aufgrund technischer oder sonstiger Probleme, die nicht im Einflussbereich von DIGAPO liegen (z.B.

Verschulden Dritter, höhere Gewalt) über das Internet nicht zu erreichen sind.

6. Haftung

DIGAPO haftet nicht für leicht fahrlässige Pflichtverletzungen, sofern diese keine vertragswesentlichen Pflichten, Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit oder Garantien betreffen oder Ansprüche nach dem Produkthaftungsgesetz oder sonstige Ansprüche, bei denen gesetzlich zwingend gehaftet wird, berührt sind. Wesentliche Vertragspflichten sind solche Pflichten, die vertragswesentliche Rechtspositionen der Apotheke schützen, die ihr dieser Vertrag nach seinem Inhalt und Zweck gerade zu gewähren hat; wesentlich sind ferner solche Vertragspflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung die Apotheke regelmäßig vertraut hat und vertrauen darf. Im Falle der Haftung der DIGAPO nach den vorstehenden Sätzen haftet diese nur für den typischen und vorhersehbaren Schaden.

7. Vertragslaufzeit, Kündigung

Der Nutzungsvertrag wird auf unbestimmte Zeit geschlossen und kann von beiden Seiten in Textform in einer Frist von zwei Wochen zum jeweiligen Monatsende gekündigt werden.

8. Einwilligung des Nutzers, Auftragsdatenverarbeitung

8.1 Die zur Nutzung der App notwendige Erhebung und Verarbeitung personenbezogener Daten durch DIGAPO im Auftrag der Apotheke setzt die Einwilligung des Nutzers voraus. Diese Einwilligung des Nutzers wird vor dessen erster Nutzung der App eingeholt und protokolliert. Die „Datenschutzerklärung zur Nutzung der App RezeptDirekt durch den Kunden“ mit dem Text der Einwilligung ist als Anlage 3 beigefügt.

Die Apotheke verpflichtet sich, personenbezogene Daten von Nutzern nach Maßgabe der Datenschutzerklärung ausschließlich zum Zwecke der Abwicklung von Vorbestellungen zu verwenden.

8.2 DIGAPO verarbeitet über die App übermittelte Daten zu Vorbestellungen von Nutzern im Auftrag und nach Weisung der jeweils teilnehmenden Apotheke im Rahmen der als Anlage 3 beigefügten „Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO in Ergänzung der Nutzungsbedingungen RezeptDirekt“. Diese Vereinbarung ist Bestandteil dieser Nutzungsbedingungen.

9. Schlussbestimmung

Der Vertrag unterliegt dem materiellen Recht der Bundesrepublik Deutschland. Für Streitigkeiten, die aus diesem Nutzungsvertrag resultieren, gilt der Gerichtsstand von DIGAPO (Berlin) als vereinbart. Ist eine der vorstehenden Bestimmungen aufgrund gesetzlicher Bestimmungen, Vorschriften oder Gesetzesänderungen ganz oder teilweise unwirksam, bleiben alle anderen Bestimmungen hiervon unberührt und gelten weiterhin in vollem Umfang.

Anlage 1
Berechtigte und von DIGAPO bevollmächtigte Stellen zur Anmeldung des Dienstes RezeptDirekt

Die nachfolgen aufgeführten Institutionen sind gemäß Ziffer 2.1 und 2.2 der Allgemeine Geschäftsbedingungen für die Nutzung des Services RezeptDirekt durch Apotheken berechtigt und von DIGAPO bevollmächtigt das Anmeldeverfahren zu der Dienstleistung RezeptDirekt von Apotheken abschließend durchzuführen:

- Berliner Apotheker-Verein, Apotheker-Verband Berlin (BAV) e. V.
- Apothekerverband Brandenburg e. V.
- Bremer Apothekerverein e. V.
- Hamburger Apothekerverein e. V.
- Landesapothekerverband Niedersachsen e. V.
- Apothekerverband Nordrhein e. V.
- Apothekerverband Mecklenburg-Vorpommern e. V.
- Landesapothekerverband Sachsen-Anhalt e.v.
- Apothekerverband Schleswig-Holstein e. V.
- ARZ Service GmbH
- AVN Apotheken Verrechnungsstelle Dr. Carl Carstens GmbH & Co.KG
- Norddeutsches Apotheken-Rechenzentrum e.V. (NARZ)
- PRISMA Datensysteme GmbH (aposoft)
- Rechenzentrum Berliner Apotheken GmbH

Anlage 2
Nutzungsbedingungen zur App RezeptDirekt für Apothekenkunden

Diese Bedingungen regeln den Inhalt des Nutzungsverhältnisses bei der Verwendung der mobilen Anwendung RezeptDirekt (im Folgenden: „App“) zwischen der Anbieterin der Anwendung, der jeweils teilnehmenden Apotheke und dem Apothekenkunden („Nutzer“).

Anbieterin der App ist die DIGAPO – Digitale Dienstleistungen für Apotheken vor Ort GmbH, Karl-Heinrich-Ulrichs-Str. 9, 10787 Berlin.

1. Leistungsbeschreibung / Unverbindlichkeit von Vorbestellungen / kostenfreie Nutzung

1.1 Die App stellt eine technische Plattform zur Kommunikation zwischen Apotheke und Nutzer dar. Sie ermöglicht es Nutzern, Waren auf elektronischem Weg bei einer Apotheke vorzubestellen. Hierzu kann der Nutzer Rezepte oder Produktverpackungen über die Kamera seines Smartphones ablichten und an eine von ihm ausgewählte Apotheke in seiner Nähe senden. Alternativ kann er eine Vorbestellung auch per Texteingabe vornehmen. Der Nutzer wird von der Apotheke per Anzeige in der App oder optional per Push-Benachrichtigung darüber informiert, zu welchem Zeitpunkt die bestellte Ware zur Abholung bereit steht.

1.2 Zudem kann sich der Nutzer mit der App über geöffnete Notdienstapotheken in seiner Nähe informieren.

1.3 Die App steht für die Betriebssysteme iOS (ab Version 9) und Android (ab Version 5.0) zur Verfügung.

1.4 Die Vorbestellung von Waren ist für Nutzer und Apotheke unverbindlich. Die Apotheke ist zur Ausführung von Vorbestellungen nicht verpflichtet und haftet insbesondere nicht für die Nichtausführung. Dem Nutzer wird empfohlen, im Zweifel eine Eingangsbestätigung zu seiner Vorbestellung einzuholen. Ein verbindlicher Kaufvertrag über die vorbestellte Ware kommt erst dann zustande, wenn der Nutzer die Ware in der Apotheke abholt. Die Anbieterin ist in das Vertragsverhältnis zwischen Nutzer und Apotheke nicht involviert.

1.5 Die Nutzung der App ist für den Nutzer kostenlos. Der Nutzer trägt jedoch die bei der Datenübertragung gegenüber seinem Provider anfallenden Nutzungsentgelte.

2. Zustandekommen, Inhalt, Dauer und Beendigung des Nutzungsvertrages

2.1 Ein Nutzungsvertrag zwischen dem Nutzer und der Anbieterin kommt dadurch zustande, dass der Nutzer die App über den Appstore von Apple oder Google-Play auf seinem Smartphone installiert und diesen Nutzungsbedingungen und den Datenschutzbestimmungen zustimmt.

2.2 Der Nutzer erhält für die Dauer des Nutzungsvertrages ein einfaches Recht zur Nutzung der App zu dem in Ziffer 1 beschriebenen Zweck. Im Falle der Einstellung des Services endet der Nutzungsvertrag automatisch. Eine Kündigung des Nutzungsvertrages ist für beide Seiten jederzeit und ohne Angabe von Gründen möglich.

3. Pflichten des Nutzers im Rahmen der Rezeptablichtung und -einsendung

3.1 Der Nutzer ist verpflichtet, nur seine eigenen Rezepte abzulichten und einzusenden. Die Einsendung von Rezepten eines Dritten (etwa eines Familienangehörigen) bedarf der Zustimmung des Dritten. Die Ablichtung und Einsendung anderer Motive als Rezepte oder Verpackungen von Medikamenten ist untersagt.

3.2 In Arztpraxen ausgestellte Rezepte enthalten neben den Patientendaten auch Daten des die Verordnung ausstellenden Arztes. Diese Daten dürfen zum Zwecke der Vorbestellung aus Gründen des Datenschutzes grundsätzlich nur mit vorheriger Einwilligung des Arztes abgelichtet und übertragen werden. Die App sieht hierzu eine technische Lösung in Form einer Fotoschablone vor, welche die Bereiche mit Arztdaten (dies sind die Betriebsstätten-Nr., die Arzt-Nr. und der Arztstempel mit Unterschrift) ausspart. Sollte die Verwendung der Schablone im Einzelfall nicht zu einer vollständigen Schwärzung der Arztdaten führen, etwa weil der Arztstempel sich ausnahmsweise nicht auf der rechten Seite des Rezeptvordrucks befindet, ist von einer Übersendung der Rezeptablichtung abzusehen. Der Nutzer ist verpflichtet, seine Vorbestellung in diesem Fall per Texteingabe vorzunehmen.

4. Änderung der Nutzungsbedingungen

Über Änderungen der Nutzungsbedingungen wird die Anbieterin den Nutzer mindestens 4 Wochen im Voraus informieren. Die Änderung gilt als akzeptiert, sofern der Nutzer nicht binnen 4 Wochen nach Bekanntgabe der Änderung widerspricht. Auf diese Rechtsfolge wird die Anbieterin in ihrer Änderungsankündigung gesondert hinweisen. Macht der Nutzer von seinem Widerspruchsrecht Gebrauch, so gilt der Nutzungsvertrag in seiner zuvor geltenden Fassung fort.

5. Gewährleistung, Haftung

5.1 Die Anbieterin gewährleistet die Eignung der App für den in Ziffer 1.1 dieser Nutzungsbedingungen genannten Einsatzzweck. Voraussetzung hierfür ist die Verwendung der App in ihrer jeweils aktuellen Version und des Smartphone-Betriebssystems in seiner für das jeweilige Smartphone jeweils verfügbaren Version.

5.2 Die Anbieterin haftet nicht für leicht fahrlässige Pflichtverletzungen, sofern diese keine vertragswesentlichen Pflichten, Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit oder Garantien betreffen oder Ansprüche nach dem Produkthaftungsgesetz oder sonstige Ansprüche, bei denen gesetzlich zwingend gehaftet wird, berührt sind. Wesentliche Vertragspflichten sind solche Verpflichtungen, die vertragswesentliche Rechtspositionen des Nutzers schützen, die ihm der Nutzungsvertrag nach seinem Inhalt und Zweck gerade zu gewähren hat; wesentlich sind ferner solche Vertragspflichten, deren Erfüllung die ordnungsgemäße Durchführung des Nutzungsvertrags überhaupt erst ermöglicht und auf deren Einhaltung der Nutzer regelmäßig vertraut hat und vertrauen darf.

5.3 Die Daten zu den Öffnungszeiten von lokalen Notdienstapotheken (siehe Ziffer 1.2) werden von dritter Seite zur Verfügung gestellt und können von der Anbieterin nicht im Vorhinein auf Aktualität und Vollständigkeit hin überprüft werden. So kann es etwa aufgrund kurzfristigen Ausfalls eines Apothekers zu unvorhergesehenen Änderungen im Notdienst kommen. Eine Haftung für die Aktualität und Vollständigkeit dieser Daten kann deshalb nicht übernommen werden. In besonders eiligen Fällen wird dem Nutzer empfohlen, sich die Öffnung der jeweiligen Apotheke telefonisch bestätigen zu lassen.

6. Datenschutz

Hinweise zum Datenschutz sowie der Text der Einwilligung in die für die Nutzung der App notwendige Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind in der gesonderten „Datenschutzerklärung zur Nutzung der App RezeptDirekt durch den Apothekenkunden“ enthalten.

7. Schlussbestimmung

Der Nutzungsvertrag unterliegt dem materiellen Recht der Bundesrepublik Deutschland. Für Streitigkeiten, die aus diesem Nutzungsvertrag resultieren, gilt der Gerichtsstand der Anbieterin (Berlin) als vereinbart. Sofern der Nutzer Kaufmann ist. Ist eine der vorstehenden Bestimmungen aufgrund gesetzlicher Bestimmungen, Vorschriften oder Gesetzesänderungen ganz oder teilweise unwirksam, bleiben alle anderen Bestimmungen hiervon unberührt und gelten weiterhin in vollem Umfang.

Anlage 3
Datenschutzerklärung zur Nutzung der App RezeptDirekt durch den Apothekenkunden

Nachfolgend informieren wir Sie gemäß Art. 13 DSGVO und § 13 Abs. 1 TMG über Art, Umfang und Zwecke der Erhebung, Verwendung und Nutzung Ihrer personenbezogenen Daten im Rahmen der Nutzung der App „RezeptDirekt".

1. Verantwortliche Stellen, Inanspruchnahme eines Rechenzentrums als Auftragsverarbeiter, Datenschutzbeauftragter

Die für die Erhebung und Verwendung Ihrer personenbezogenen Daten verantwortliche Stelle ist die am Service teilnehmende jeweilige Apotheke, an die Sie als Nutzer Vorbestellungen übersenden. Die namentliche Bezeichnung der jeweiligen Apotheke mit Adresse und Kontaktinformationen ist in der App bei der Apothekenauswahl hinterlegt.

Die am Service teilnehmende Apotheke bedient sich zum Zwecke der Abwicklung des Nutzungsverhältnisses mit dem Nutzer der DIGAPO – Digitale Dienstleistungen für Apotheken vor Ort GmbH, Karl-Heinrich-Ulrichs-Str. 9, 10787 Berlin (im Folgenden: Servicedienstleister) im Wege eines Auftragsverarbeitungsverhältnisses. Der Servicedienstleister hat mit dem Betrieb der Server, auf denen die vom Nutzer an die Apotheke übermittelten Daten gespeichert werden, das Rechenzentrum DARZ GmbH mit Sitz in Darmstadt beauftragt. Mit diesem Rechenzentrum hat der Servicedienstleister einen Vertrag zur Auftragsdatenverarbeitung abgeschlossen.

Der Servicedienstleister ist überdies selbst verantwortliche Stelle im Hinblick auf die Verarbeitung und Nutzung übermittelter Standortdaten, die für die Zusatzfunktion der Apotheken-Notdienstsuche erforderlich sind.

Beim Servicedienstleister ist ein Datenschutzbeauftragter bestellt. Die Kontaktdaten können auf der Webseite des Servicedienstleisters unter https://www.rezeptdirekt.de/impressum.html abgerufen werden.

2. Beschreibung der erhobenen und verarbeiteten Daten, Zweckbestimmung, Rechtsgrundlage

Folgende Daten werden von der Apotheke bzw. dem von ihr eingesetzten Servicedienstleister im Rahmen der Erbringung des Services „RezeptDirekt" erhoben, verarbeitet und genutzt:

- Ihre jeweilige Geräte-ID (zur Identifikation bei der Installation der App auf Ihrem Smartphone);
- Ihre an die Apotheke zum Zwecke einer Vorbestellung übermittelten Rezepte sowie Textnachrichten;
- Ihre Standortdaten, sofern von Ihnen freigegeben (für die Suche der nächstgelegen Apotheke im Rahmen des Vorbestellungs-Services sowie für die Suche nach Notdienstapotheken).

Bei der Installation der App auf Ihrem Smartphone erfolgt eine Identifizierung am Server des Servicedienstleisters ausschließlich auf Basis einer zufällig generierten Installations-ID in Verbindung mit der jeweiligen Geräte-ID. Eine hierüber hinausgehende Nutzung dieser Daten zu anderen Zwecken erfolgt nicht.

Die Erhebung und Verarbeitung der Bestelldaten erfolgt ausschließlich zum Zwecke der Entgegennahme und Ausführung von Vorbestellungen des Nutzers im Rahmen des Services RezeptDirekt. Hierbei werden nur solche Daten erhoben, verarbeitet und genutzt, die für den Betrieb der App zwingend erforderlich sind. Der Inhalt Ihrer Vorbestellungen ist nur für die jeweils von Ihnen kontaktierte Apotheke einsehbar. Nach Ablauf von vier Wochen nach Absendung ihrer Bestellung wird diese von den Servern gelöscht und ist dann auch für die Apotheke nicht mehr einsehbar.

Standortdaten werden ausschließlich zum Zweck des Abgleichs mit der jeweils nächstgelegenen Apotheke übermittelt und genutzt. Hierzu wird eine temporäre Serveranfrage mit Ihrem Standort durchgeführt. Die Ergebnisse und Standortdaten werden nicht auf dem Gerät oder in der Datenbank gespeichert. Eine Nutzung der App ist zudem auch ohne Übermittlung von Standortdaten möglich, indem Sie im Rahmen der Apothekenauswahl anstelle der Suche nach der nächstgelegenen Apotheke eine Suche nach Orten/Postleitzahlen vornehmen. Sie können die Tracking-Funktion über die Einstellungen der App zudem jederzeit deaktivieren.

Rechtsgrundlage für die Verarbeitung Ihrer personenbezogenen Daten ist Art. 6 Abs. 1 lit. a DSGVO (Einwilligung) und Art. 6 Abs. 1 lit. b DSGVO (Erfüllung des mit Ihnen geschlossenen Nutzungsvertrages).

3. Beschreibung der Gerätefunktionen, auf die ein Zugriff erfolgt

Die App benötigt Zugriff auf folgende technische Gerätefunktionen und Sensoren Ihres Smartphones:

- Kamera (zur Ablichtung von Rezepten)
- Geolocation (zur Feststellung Ihrer Position, damit eine Apotheke in der Nähe angezeigt werden kann)
- Deviceinfos (zur eindeutigen Identifizierung des Geräts und zur Zuordnung von Anfragen)
- Push (für die Benachrichtigung über Rückmeldung der Apotheken)

4. Hinweis auf den besonderen Schutz von Gesundheitsdaten Sie werden darauf hingewiesen, dass es sich bei den von Ihnen an die Apotheke übermittelten Vorbestellungen in Form von Rezeptablichtungen und ggfs. auch solcher in Form von Chat-Eingaben um Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO handelt, die einem erhöhten Schutzbedarf unterliegen. Zu Ihrem Schutz erfolgt der Transport dieser Daten daher verschlüsselt (SSL). Zudem wird jeder Bestellvorgang einzeln abgespeichert. Im Falle einer Löschung der App von Ihrem Smartphone werden zudem automatisch auch sämtliche Vorbestellungen gelöscht. Ihnen wird empfohlen, den Zugriff auf die App und die darüber abrufbaren Gesundheitsdaten durch Einrichtung einer geeigneten Zugangssperre am Smartphone (z.B. PIN-Abfrage) zu beschränken.

5. Push-Benachrichtigungen

Sofern Sie dies bei der Installation erlaubt haben, können Sie über die App sog. Push-Nachrichten empfangen. Diese werden genutzt, um Sie über den aktuellen Stand der von Ihnen getätigten Vorbestellungen zu informieren. Für den Versand von Push-Nachrichten wird der Service OneSignal des Anbieters Lilomi Inc., Mountain View, USA genutzt. Die jeweils aktuelle Datenschutzrichtlinie des Anbieters können Sie unter der URL https://onesignal.com/privacy_policy abrufen und einsehen. Dieser Anbieter speichert Daten zu dem von Ihnen genutzten Gerät (u.a. Geräte-ID, IP-Adresse und verwendetes Betriebssystem) sowie zu Ihrem Standort. Einen Zugriff auf Ihre individuelle Kommunikation mit den Apotheken erhält der Anbieter nicht. Den Empfang von Push-Nachrichten können Sie jederzeit in den Einstellungen Ihres Betriebssystems deaktivieren.

6. Dauer der Speicherung

Die mit der jeweiligen Vorbestellung von Ihnen übermittelten Daten dienen allein der Abwicklung der Transaktion und werden im Anschluss hieran wieder gelöscht.

7. Ihre Rechte, Kontaktmöglichkeiten, Beschwerderecht

Sie haben gegenüber der verantwortlichen Stelle das Recht auf Auskunft über die zu Ihrer Person gespeicherten personenbezogenen Daten, auf Berichtigung unrichtiger Daten, auf Löschung sowie auf Einschränkung der Verarbeitung. Einem Verlangen nach Löschung oder Einschränkung der Verarbeitung können jedoch ggfs. gesetzliche Aufbewahrungspflichten entgegenstehen.

Bitte wenden Sie sich bei Fragen zur Erhebung, Verarbeitung oder Nutzung Ihrer personenbezogenen Daten an die jeweilige Apotheke, an Sie Ihre Vorbestellungen gesendet haben. Die Kontaktdaten Ihrer Apotheke finden Sie innerhalb der App bei der Apothekenauswahl.

Hierneben haben Sie auch die Möglichkeit, sich mit Ihrem Anliegen an die für die jeweilige Apotheke jeweils zuständige Datenschutzaufsichtsbehörde zu wenden. Die für den Servicedienstleister zuständige Behörde ist die Berliner Beauftragte für Datenschutz und Informationsfreiheit (Friedrichstr. 219, 10969 Berlin).

8. Einwilligung des Nutzers

Ihre Einwilligung in die Erhebung, Verarbeitung und Nutzung der vorstehend benannten personenbezogenen Daten wird bei der erstmaligen Verwendung der App elektronisch abgefragt und beim Servicedienstleister protokolliert. Den Wortlaut der von Ihnen erteilten Einwilligung können Sie über die App abrufen und ausdrucken. Ohne Ihre Einwilligung ist die Nutzung der App nicht möglich. Sie können Ihre Einwilligung gegenüber dem Servicedienstleister oder der jeweiligen Apotheke, an Sie Ihre Vorbestellungen gerichtet haben, jederzeit widerrufen.
Die bei der Installation eingeholte Einwilligungserklärung hat den folgenden Wortlaut:
Ich bin damit einverstanden, dass meine personenbezogenen Daten zum Zwecke der Nutzung der mobilen Anwendung „RezeptDirekt" nach Maßgabe der beigefügten Datenschutzerklärung von der jeweiligen Apotheke bzw. dem von ihr hierzu eingesetzten Servicedienstleister erhoben, verarbeitet und genutzt werden. Mir ist bekannt, dass meine Einwilligung sich auch auf die Verarbeitung und Nutzung von mir übermittelter Gesundheitsdaten (Vorbestellungen von Medikamenten) bezieht, die einem erhöhten Schutzbedarf unterliegen.
Meine Einwilligung kann ich gegenüber dem Servicedienstleister oder der jeweiligen Apotheke, an die ich eine Vorbestellung gerichtet habe, jederzeit widerrufen. Die zu meiner Person gespeicherten Daten werden dann gelöscht, soweit gesetzliche Aufbewahrungspflichten dem nicht entgegenstehen. Eine weitere Nutzung der App ist mir hiernach nicht mehr möglich. Mir ist bekannt, dass ich gegenüber den vorgenannten Stellen ein Recht auf unentgeltliche Auskunft über die zu meiner Person gespeicherten Daten habe.
Mir ist bekannt, dass ich ohne Einwilligung keine Rezepte Dritter ablichten und einsenden darf (siehe Ziffer 3.1 Nutzungsbedingungen). Mir ist außerdem bekannt, dass die auf Rezeptvordrucken enthaltenen Daten des behandelnden Arztes bei der Ablichtung mit der in die App integrierten Schablone unkenntlich zu machen sind, es sei denn, der Arzt ist mit der Ablichtung und Versendung seiner Daten zum Zwecke der Vorbestellung von Medikamenten einverstanden (siehe Ziffer 3.2 der Nutzungsbedingungen).

Anlage 4
Vereinbarung zur Auftragsverarbeitung zwischen Apotheke (Auftraggeber) und der DIGAPO – Digitale Dienstleistungen für Apotheken vor Ort GmbH (Auftragnehmer) nach Art. 28 DSGVO zum Pro-

§ 1
Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Kunden des Auftraggebers im Rahmen der Nutzung der mobilen Smartphone-Anwendung RezeptDirekt.

Der Vertrag beginnt mit seiner Unterzeichnung und wird auf unbestimmte Zeit geschlossen. Er endet automatisch mit Beendigung des Nutzungsvertrages RezeptDirekt zwischen dem Auftragnehmer und dem Auftraggeber.

§ 2
Art der personenbezogenen Daten, Kreis der betroffenen Personen, Art des Zugriffs auf Daten

(1) Art der personenbezogenen Daten sind insbesondere:
- Patienten- /Kundendaten (Angaben zur getätigten Vorbestellung, ggfs. Rezeptdaten, sofern diese vom Kunden übermittelt werden)
- ggfs. Arztdaten (z.B. Name, Anschrift, LANR, BSNR)
- technische Gerätedaten des Nutzers (Geräte-ID, Standortdaten, sofern vom Nutzer freigegeben)
- Personenstamm- und Kommunikationsdaten des Auftraggebers

(2) Bei den Betroffenen dieser Daten handelt es sich insbesondere um:
- Patienten / Kunden des Auftragnehmers
- Auftraggeber / Mitarbeiter des Auftraggebers
- ggfs. Ärzte

(3) Bestelldaten werden durch elektronische Vorbestellung des Kunden auf Server übertragen, die der Auftragnehmer im Rahmen eines Unterauftragsdatenverarbeitungsvertrages betreiben lässt. Zugriff auf den Inhalt von Bestellungen erhält nur die Apotheke, an die die jeweilige Bestellung gerichtet wurde. Standortdaten werden ausschließlich zum Zweck des Abgleichs mit der jeweils nächstgelegenen Apotheke übermittelt und genutzt. Die Ergebnisse und Standortdaten werden nicht auf dem Gerät oder in der Datenbank gespeichert. Die Ergebnisse und Standortdaten werden nicht auf dem Gerät oder in der Datenbank gespeichert.

§ 3
Verantwortlichkeit

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich (Art. 4 Nr. 7 DS-GVO).

(2) Die Vertragspartner werden zur Durchführung des Vertrages nur solche Mitarbeiter oder sonstige Erfüllungsgehilfen einsetzen, die zuvor auf die Vertraulichkeit sowie die Verschwiegenheit gemäß § 203 StGB verpflichtet und mit den einschlägigen Datenschutzbestimmungen vertraut gemacht worden sind. Dabei ist auch darauf hinzuweisen, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

§ 4
Weisungsbefugnis des Auftraggebers

(1) Die Datenverarbeitung durch den Auftragnehmer erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers unter Beachtung der datenschutzrechtlichen Bestimmungen. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. In diesem Fall wird der Auftragnehmer den Auftraggeber – sofern möglich – vor Beginn der Verarbeitung über die rechtlichen Anforderungen informieren.
(2) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorgaben verstößt, informiert er gemäß Art. 28 Abs. 3 S.3 DS-GVO den Auftraggeber. Bis zur Klärung der Sach- und Rechtslage ist der Auftragnehmer in diesem Fall dazu berechtigt, die Ausführung der Weisung zu verweigern.

(3) Führt eine Weisung zu einer wesentlichen Änderung des Vertragsgegenstands oder einer wesentlichen Verfahrensänderung, so steht dem Auftragnehmer ein Widerspruchsrecht zu. Besteht der Auftraggeber trotz des Widerspruchs des Auftragnehmers auf die Änderung, steht dem Auftragnehmer ein außerordentliches Kündigungsrecht bezüglich des AV-Vertrages sowie des von der Weisung betroffenen Bestandteils des Hauptvertrages zu.

(4) Mündliche Weisungen wird der Auftraggeber unverzüglich mindestens in Textform dokumentieren. Ansprechpartner (weisungsberechtigte Person) auf Seiten des Auftraggebers ist in Ermangelung einer abweichenden schriftlichen Regelung der Apothekeninhaber.

§ 5
Leistungsort

Die Erbringung der vertraglich vereinbarten Datenverarbeitung durch den Auftragnehmer 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 Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

§ 6
Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Eine Dokumentation der derzeit getroffenen technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 DSGVO ist dieser Vereinbarung als Anlage beigefügt. Die jeweils aktuelle Fassung kann vom Auftraggeber beim Auftragnehmer angefordert werden.

§ 7
Sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer ist nach Art. 37 DS-GVO verpflichtet, einen Datenschutzbeauftragten zu benennen, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Die Person des Datenschutzbeauftragten nebst Kontaktdaten ist auf der Internetseite des Auftragnehmers (www.rezeptdirekt.de/impressum.html) benannt.

(2) Der Auftragnehmer führt ein Verzeichnis von Verarbeitungstätigkeiten im Sinne von Art. 30 Abs. 2 DS-GVO und stellt dieses der Aufsichtsbehörde auf Anfrage zur Verfügung.

(3) Der Auftragnehmer unterstützt den Auftraggeber mit allen ihm zur Verfügung stehenden Informationen bei der Erfüllung der Informationspflichten gegenüber der zuständigen Aufsichtsbehörde (Art. 33 DS-GVO) und ggfs. gegenüber den von der Verletzung des Schutzes personenbezogener Daten Betroffenen (Art. 34 DS-GVO). Er unterstützt den Auftraggeber bei der Datenschutzfolgeabschätzung (Art. 35 DS-GVO) sowie bei einer ggfs. erforderlichen Konsultation der Aufsichtsbehörde (Art. 36 DS-GVO). Der Auftragnehmer unterstützt den Auftraggeber ferner bei der Bereitstellung von Informationen, die für die Erteilung von Auskünften zur Erhebung, Verarbeitung oder Nutzung gegenüber betroffenen Personen erforderlich sind. Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung verlangen.

(4) Dem Auftragnehmer bekannt gewordene Verletzungen des Schutzes personenbezogener Daten wird dieser unverzüglich dem Auftraggeber melden. In einem solchen Fall trifft der Auftragnehmer nach Absprache mit dem Auftraggeber unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen.

(5) Die Vertragspartner arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragnehmer wird den Auftraggeber über auf diesen Auftrag bezogene Kontrollhandlungen und Maßnahmen der Aufsichtsbehörden unverzüglich informieren.

(6) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technisch-organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet ist.

§ 8
Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienst-leistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DS-GVO in Anspruch zu nehmen. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter vorab informieren. Der Auftraggeber kann gegen derartige Änderungen Einspruch einlegen, wenn aus seiner Sicht begründete Anhaltspunkte dafür bestehen, dass die beabsichtigte Auslagerung gegen datenschutzrechtliche Bestimmungen verstößt. Im Fall des Einspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung dem Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftragnehmer innerhalb von 4 Wochen nach Zugang des Einspruchs kündigen.

(3) Zum Zeitpunkt des Vertragsschlusses besteht ein Unterauftragsverhältnis mit der DARZ GmbH mit Sitz in Darmstadt. Der Dienstleister übernimmt Hosting-Dienstleistungen für den Auftragnehmer. Ort der Leistungserbringung ist die Bundesrepublik Deutschland. Ein weiteres Unterauftragsverhältnis besteht mit der Softlines & Consulting GmbH mit Sitz in Düsseldorf. Der Dienstleister übernimmt den Betrieb und den Support der Software.

(4) Im Falle einer weiteren Auslagerung durch den Subunternehmer sind dem weiteren Dienstleister dieselben Datenschutzpflichten aufzuerlegen, die auch in diesem Vertrag festgelegt sind.

§ 9
Löschung und Rückgabe von personenbezogenen Daten

(1) 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, sofern dem keine den Auftragnehmer betreffenden gesetzlichen Aufbewahrungspflichten entgegenstehen. Ein Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, dürfen durch den Auftragnehmer über das Vertragsende hinaus aufbewahrt werden. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(3) Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

§ 10
Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen 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.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO
- 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).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

§ 11
Haftung

(1) Die Haftung der Vertragsparteien für Verstöße gegen Bestimmungen des Datenschutzrechts gegenüber den hiervon Betroffenen sowie das Verfahren für den Ausgleich solcher Schäden im Innenverhältnis richten sich nach Art. 82 DS-GVO.
(2) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 12
Schlussbestimmungen

(1) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam erweisen, so wird die Wirksamkeit der übrigen Vereinbarung hiervon nicht berührt. Für den Fall der Unwirksamkeit einzelner oder mehrere Regelungen werden die Vertragsparteien die unwirksame Regelung unverzüglich durch eine solche Regelung ersetzen, die der unwirksamen Regelung wirtschaftlich und datenschutzrechtlich am ehesten entspricht. Die Parteien verpflichten sich, die unwirksame Regelung unverzüglich, die der unwirksamen Regelung nach ihrem Sinn und Zweck am ehesten entspricht. Unter mehreren geeigneten Regelungen ist im Zweifel diejenige zu wählen, welche den wirksamen Schutz von Patientendaten am besten gewährleistet.

(2) Im Falle eines Widerspruchs zwischen den Nutzungsbedingungen und dieser Vereinbarung geht diese Vereinbarung vor, soweit der Widerspruch die Verarbeitung personenbezogener Daten betrifft.

(3) Es gilt deutsches Recht.

(4) Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist der Sitz des Auftragnehmers.

Anlage zur Vereinbarung zur Auftragsverarbeitung
Übersicht der technischen und organisatorischen Maßnahmen des Auftragnehmers

Im Folgenden werden die technischen und organisatorischen Maßnahmen beschrieben, welche zum Schutz der Daten der Auftraggeber getroffen sind.

A. Vertraulichkeit

I. Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

- Alarmanlage
- Automatisches Zugangskontrollsystem
- Schließsystem mit Codesperre
- Lichtschranken / Bewegungsmelder
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Sorgfältige Auswahl von Wachpersonal
- Absicherung von Gebäudeschächten
- Chipkarten-/Transponder-Schließsystem
- Manuelles Schließsystem
- Videoüberwachung der Zugänge
- Sicherheitsschlösser
- Personenkontrolle beim Pförtner / Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- Tragepflicht von Berechtigungsausweisen

II. Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

Es existieren folgende Maßnahmen zur Zugangskontrolle:

- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Sperren von externen Schnittstellen (USB etc.)
- Schlüsselregelung (Schlüsselausgabe etc.)
- Protokollierung der Besucher
- Sorgfältige Auswahl von Wachpersonal
- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von Smartphone-Inhalten
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Sicherheitsschlösser
- Personenkontrolle beim Pförtner / Empfang
- Sorgfältige Auswahl von Reinigungspersonal
- Tragepflicht von Berechtigungsausweisen
- Verschlüsselung von mobilen Datenträgern
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Einsatz einer Software-Firewall

III. Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Es existieren folgende Maßnahmen zur Zugriffskontrolle:

- Erstellen eines Berechtigungskonzepts
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Protokollierung von Zugriffen auf Anwendungen, ins-besondere bei der Eingabe, Änderung und Löschung von Daten
- physische Löschung von Datenträgern vor Wiederverwendung
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Verschlüsselung von Datenträgern
- Verwaltung der Rechte durch Systemadministrator
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Sichere Aufbewahrung von Datenträgern
- ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- Protokollierung der Vernichtung

IV. Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

Es existieren folgende Maßnahmen zur Trennungskontrolle:

- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- Trennung von Entwicklungs-/Test- und Produktivsystemen

V. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen

Es existieren folgende Maßnahmen zur Pseudonymisierung:

Im Rahmen eines Angebotes wird im ausgewiesenen CRM System eine eindeutige ID erzeugt.
Diese ID wird von den mit den folgenden Verarbeitungsschritten betrauten Rollen als eindeutige Identifikation verwendet. Aus einer oder mehreren ID’s lassen sich keine Rückschlüsse auf Betroffene ziehen.

B. Integrität

I. Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- Beim physischen Transport: sichere Transportbehälter/-verpackungen

II. Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingege-ben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

Es existieren folgende Maßnahmen zur Eingabekontrolle:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

C. Verfügbarkeit und Belastbarkeit

I. Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/off-line; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Melde-wege und Notfallpläne

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

- Unterbrechungsfreie Stromversorgung (USV)
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Alarmmeldung bei unberechtigten Zutritten zu Server-räumen
- Testen von Datenwiederherstellung
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Klimaanlage in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Erstellen eines Notfallplans
- Serverräume nicht unter sanitären Anlagen

II. Verfügbarkeitskontrolle

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

- Tägliche automatische Snapshoterstellung
- Auf Dateiebene: Sicherungskonzepte für Wiederherstellung einzelner Dateien auf Generationenprinzipbasis
- Bei Changes: gesonderte, manuelle Snapshoterstellung

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

- Datenschutz-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen
- Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Aus-wahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichts-punkten (insbesondere hinsichtlich Datensicherheit)
- schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag
- Auftragnehmer hat Datenschutzbeauftragten bestellt
- Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart
- Vertragsstrafen bei Verstößen
- vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

Stand: Februar 2019