

## **Datenschutzerklärung**

navato GmbH  
Am Justizzentrum 5  
50939 Köln

### **1. Allgemeines**

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.
- (2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

### **2. Gegenstand des Auftrags**

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in Anlage 1 zu diesem Vertrag festgelegt.

### **3. Rechte und Pflichten des Auftraggebers**

- (1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.
- (2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.
- (3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen. Sofern Weisungen mündlich erteilt werden, müssen diese unverzüglich in Textform bestätigt werden.
- (4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.
- (5) Der Auftraggeber kann weisungsberechtigte Personen benennen.
- (6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

- (7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

#### **4. Allgemeine Pflichten des Auftragnehmers**

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.
- (2) Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.
- (3) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.
- (4) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.

#### **5. Datenschutzbeauftragter des Auftragnehmers**

Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Auftragnehmer wird dem Auftraggeber den Namen und die Kontaktdaten seines Datenschutzbeauftragten gesondert in Textform mitteilen.

#### **6. Meldepflichten des Auftragnehmers**

- (1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

- (2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.
- (3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber muss insbesondere folgende Informationen beinhalten:
  - eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
  - eine Beschreibung der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

## **7. Mitwirkungspflichten des Auftragnehmers**

- (1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.
- (2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
- (3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

## **8. Kontrollbefugnisse**

- (1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer im erforderlichen Umfang zu kontrollieren.
- (2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.
- (3) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Die Parteien gehen davon aus,

dass eine Kontrolle höchstens einmal jährlich erforderlich ist. Weitere Prüfungen sind vom Auftraggeber unter Angabe des Anlasses zu begründen. Im Falle von Vor-Ort-Kontrollen wird der Auftraggeber dem Auftragnehmer die entstehenden Aufwände inkl. der Personalkosten für die Betreuung und Begleitung der Kontrollpersonen vor Ort in angemessenem Umfang ersetzen. Die Grundlagen der Kostenberechnung werden dem Auftraggeber vom Auftragnehmer vor Durchführung der Kontrolle mitgeteilt.

- (4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß Anlage 3 zu diesem Vertrag zu überzeugen. Sollte der Auftraggeber begründete Zweifel an der Eignung des Prüfungsberichts i.S.d. Satzes 1 haben, kann eine Vor-Ort-Kontrolle durch den Auftraggeber erfolgen. Dem Auftraggeber ist bekannt, dass eine Vor-Ort-Kontrolle in Rechenzentren nicht oder nur in begründeten Ausnahmefällen möglich ist.
- (5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunftspflicht und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

## **9. Unterauftragsverhältnisse**

- (1) Der Auftragnehmer ist berechtigt, die in der Anlage 2 zu diesem Vertrag angegebenen Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den in Absatz 2 genannten Voraussetzungen zulässig.
- (2) Der Auftragnehmer hat den Unterauftragnehmer sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass dieser die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten kann. Der Auftragnehmer hat insbesondere vorab und regelmäßig während der Vertragsdauer zu kontrollieren, dass der Unterauftragnehmer die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat. Der Auftragnehmer wird den Auftraggeber im Falle eines geplanten Wechsels eines Unterauftragnehmers oder bei geplanter Beauftragung eines neuen Unterauftragnehmers rechtzeitig, spätestens aber 4 Wochen vor dem Wechsel bzw. der Neubeauftragung in Textform informieren („Information“). Der Auftraggeber hat das Recht, dem Wechsel oder der Neubeauftragung des Unterauftragnehmers unter Angabe einer Begründung in Textform binnen drei Wochen nach Zugang der „Information“ zu widersprechen. Der Widerspruch kann vom Auftraggeber jederzeit in Textform zurückgenommen werden. Im Falle eines Widerspruchs kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen. Wenn

kein Widerspruch des Auftraggebers binnen drei Wochen nach Zugang der „Information“ erfolgt gilt dies als Zustimmung des Auftraggebers zum Wechsel bzw. zur Neubeauftragung des betreffenden Unterauftragnehmers.

- (3) Der Auftragnehmer ist verpflichtet, sich vom Unterauftragnehmer bestätigen zu lassen, dass dieser einen betrieblichen Datenschutzbeauftragten gemäß Art. 37 DSGVO benannt hat, sofern der Unterauftragnehmer zur Benennung eines Datenschutzbeauftragten gesetzlich verpflichtet ist.
- (4) Der Auftragnehmer hat sicherzustellen, dass die in diesem Vertrag vereinbarten Regelungen und ggf. ergänzende Weisungen des Auftraggebers auch gegenüber dem Unterauftragnehmer gelten.
- (5) Der Auftragnehmer hat mit dem Unterauftragnehmer einen Auftragsverarbeitungsvertrag zu schließen, der den Voraussetzungen des Art. 28 DSGVO entspricht. Darüber hinaus hat der Auftragnehmer dem Unterauftragnehmer dieselben Pflichten zum Schutz personenbezogener Daten aufzuerlegen, die zwischen Auftraggeber und Auftragnehmer festgelegt sind. Dem Auftraggeber ist der Auftragsdatenverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.
- (6) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse (Ziff. 8 dieses Vertrages) des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten und entsprechende Kontrollrechte von Auftraggeber und Aufsichtsbehörden vereinbart werden. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.
- (7) Nicht als Unterauftragsverhältnisse i.S.d. Absätze 1 bis 6 sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben. Dazu gehören beispielsweise Reinigungsleistungen, reine Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste. Der Auftragnehmer ist gleichwohl verpflichtet, auch bei Nebenleistungen, die von Dritten erbracht werden, Sorge dafür zu tragen, dass angemessene Vorkehrungen und technische und organisatorische Maßnahmen getroffen wurden, um den Schutz personenbezogener Daten zu gewährleisten. Die Wartung und Pflege von IT-Systemen oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i.S.d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des Auftraggebers verarbeitet werden.

## **10. Vertraulichkeitsverpflichtung**

- (1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer ist sich darüber bewusst, dass er im gleichen Maße wie der Auftraggeber zur Vertraulichkeit verpflichtet ist und sich bei Verstößen strafbar machen kann.
- (2) Der Auftragnehmer hat seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut gemacht und zur Vertraulichkeit verpflichtet.

- (3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

### **11. Wahrung von Betroffenenrechten**

- (1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.
- (2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.
- (3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

### **12. Geheimhaltungspflichten**

- (1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.
- (2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

### **13. Vergütung**

Die Vergütung des Auftragnehmers wird ggf. gesondert vereinbart.

### **14. Technische und organisatorische Maßnahmen zur Datensicherheit**

- (1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.
- (2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als Anlage 3 zu diesem Vertrag beigefügt. Die Parteien sind sich darüber

einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

### **15. Dauer des Auftrags**

- (1) Der Vertrag beginnt mit Unterzeichnung und läuft für die Dauer des zwischen den Parteien bestehenden Hauptvertrages über die Nutzung der Dienstleistungen des Auftragnehmers durch den Auftraggeber.
- (2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

### **16. Beendigung**

Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

### **17. Zurückbehaltungsrecht**

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

### **18. Schlussbestimmungen**

- (1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

....., den

Köln, den

- Auftraggeber -

- Auftragnehmer -

## **Anlage 1 - Gegenstand des Auftrags**

### **1. Art(en) der personenbezogenen Daten**

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Webhosting der Software PraxWin und der darin eingegebenen Daten.
- Fernwartungszugriff auf die Software PraxWin in der Praxis des Auftraggebers.
- Möglicher Zugriff auf die in der Software hinterlegten Daten von Patienten und Mitarbeitern.

### **2. Kategorien betroffener Person**

Kreis der von der Datenverarbeitung betroffenen Personen:

- Mitarbeiter des Auftraggebers  
Hierbei handelt es sich um Personenbezogene Daten: Kontaktdaten, die Anschrift und die Arbeits,- Urlaubs und Abwesenheitszeiten gespeichert werden. Letzte Login des Mitarbeiters, sowie Protokollierung von Datenänderungen.
- Patienten des Auftraggebers  
In PraxWin werden zu einem Patienten umfassende Daten abgespeichert.  
Die Art der Daten hängt von den gebuchten Modulen ab. Es handelt sich hierbei um personenbezogene Daten, sensitive Daten (Art. 9 DSGVO Verarbeitung besonderer Kategorien personenbezogener Daten), Personenstammdaten, Kontaktdaten (z.B. Telefon, Fax, E-Mail), Vertragsstammdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Rezeptabrechnungsdaten (gesetzlich und privat), Daten zur Versicherung des Patienten.

### **3. Weisungsberechtigte Personen des Auftraggebers**

*Hier können Sie die weisungsberechtigten Personen benennen:*

-----

### **4. Weisungsempfangsberechtigte Personen des Auftragnehmers**

*Damian Moschny*

## **Anlage 2 - Unterauftragnehmer**

Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende Unternehmen:

- Hetzner – Webhosting  
Hetzner Online GmbH  
Industriestr. 25  
91710 Gunzenhausen

Internetseite: [www.hetzner.de](http://www.hetzner.de)

Tel.: +4998315050

Email [support@hetzner.com](mailto:support@hetzner.com)

Stand: 08.05.2018

- Hosteurope – Webhosting  
Host Europe GmbH  
Hansestrasse 111  
51149 Köln

Tel. +49 2203 9934 1040

Fax.: +492203 9934 1042

E-Mail: [Info@hosteurope.de](mailto:Info@hosteurope.de)

Stand 14.09.2018

In den Rechenzentren der beiden Unternehmen wird die PraxWin Datenbank, Datensicherungen und Updates gespeichert/gehostet.

## **Anlage 3 - Technische und organisatorische Maßnahmen des Auftragnehmers**

### **Anlage 3.1 In den Büroräumen der navato GmbH (Am Justizzentrum 5, 50939 Köln)**

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

#### **1. Vertraulichkeit**

##### **(1) Zutrittskontrolle**

*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.*

Hier sind Angaben vom Auftragnehmer zu folgenden Aspekten zu machen:

Aus den Büroräumen der navato GmbH wird über Remotezugriff auf die Server in den Rechenzentren zugegriffen. Der Zugang zu den Büroräumen ist durch eine Haustür und eine Bürotür abgeschlossen. Den Zugang haben nur Mitarbeiter der Firma navato.

## **(2) Zugangskontrolle**

*Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*

Die Berechtigungen zum Zugang zu den Daten und Systemen werden von Damian Moschny verteilt und verwaltet.

Für die Komplexität der Passwörter gibt es eine Richtlinie, die technisch erzwungen wird.

Mobile Endgeräte sind verschlüsselt.

Die IT-Systeme werden über Firewalls und Virens Scanner vor Viren und Schadsoftware geschützt.

Mit den Rechenzentren ist ein AV-Vertrag abgeschlossen.

## **(2) Zugriffskontrolle**

*Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*

Für die Systeme werden Berechtigungen differenziert über Benutzerrollen verwaltet.

Für jeden Server im Rechenzentrum hat jeder Mitarbeiter, der darauf Zugriff hat, ein eigenes Administratorkonto mit eigenem Passwort.

Beim Ausscheiden eines Mitarbeiters aus dem Unternehmen wird sein Konto deaktiviert. Den Zugriff auf die Server haben nur die Mitarbeiter soweit es notwendig ist.

Alle erfolgreichen und auch die fehlgeschlagenen Logins auf die Server werden elektronisch dokumentiert. Jeder Login wird in einer Logdatei protokolliert und per Email an navato gemeldet.

Entsorgung von ungenutzten Datenträgern: Die Datenträger in den Büroräumen von navato werden mechanisch zerstört. Papierunterlagen werden mit einem Papier Schredder klein geschnitten.

## **(3) Trennung**

*Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

*Hier sind Angaben vom Auftragnehmer zu folgenden Aspekten zu machen*

*- Wie wird sichergestellt, dass Daten, die zu verschiedenen Zwecken verarbeitet werden, getrennt voneinander verarbeitet werden?*

Für jeden Kunden wird auf dem Server eine eigene Datenbank (Sql Server: Catalog) eingerichtet. Mit dem Catalog wird eine Guid verknüpft. Zugriff auf die Daten kann nur über einen WCF Dienst (gehostet in ISS) erfolgen. Um den Zugriff zu bekommen, muss man sich in PraxWin mit einem Praxisnamen,

Benutzernamen und Passwort ausweisen. Alle Abfragen enthalten die Guid. Ohne Guid ist eine Abfrage nicht möglich.

Eine Praxis kann in PraxWin prüfen von welchen Endgeräten eine Anmeldung erfolgte und die Geräte für den Zugriff sperren.

Die Sicherungen der einzelnen Praxisbetriebe werden jeweils in eigenen Dateien gespeichert.

Testumgebung: Jeder Mitarbeiter hat eine oder mehrere Testdatenbanken mit seinen Testdaten. Diese Daten enthalten keine echten Praxis- oder Patientendaten.

Eine Kopie der Praxisdaten wird nur mit Zustimmung der Praxis für eine vorgegebene Aufgabe (Fehler-suche) erstellt und danach gelöscht.

#### **(4) Pseudonymisierung & Verschlüsselung**

In PraxWin können im Rahmen des Dokumentationsmoduls eingescannte Dokumente gespeichert werden. Für diese Dokumente kann in der Praxis ein Passwort hinterlegt werden, mit dem die Dokumente in der Datenbank verschlüsselt gespeichert werden.

## **2. Integrität**

### **a) Eingabekontrolle**

*Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*

Innerhalb von PraxWin können auf Mitarbeiterebene Berechtigungen für Funktionen vergeben werden. Die Verwaltung der Berechtigungen erfolgt in PraxWin mit dem Administratorkonto oder einem anderen Konto mit ausreichenden Berechtigungen. Die Konten, Passwörter und Berechtigungen werden nur in der Praxis innerhalb von PraxWin verwaltet. Die Praxis ist für die Berechtigungsvergabe verantwortlich.

PraxWin protokolliert den letzten Zugriff von einem Endgerät für ein Benutzerkonto. Diese Informationen können innerhalb von PraxWin abgerufen werden.

### **b) Weitergabekontrolle**

*Maßnahmen, die gewährleisten, 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 vorgehen ist.*

Hier sind Angaben vom Auftragnehmer zu folgenden Aspekten zu machen:

Die Kommunikation zwischen den Clients der Praxis und den Server in den Rechenzentren erfolgt über das Protokoll HTTPS und ist somit SSL verschlüsselt.

Die Sicherungen werden verschlüsselt gespeichert.

Kündigt eine Praxis den Hostinvertrag, dann erhält die Praxis eine Kopie der Daten als Link zum Download und die Datenbanken (SQL Server: Catalog) inkl. Sicherungen werden auf den Server gelöscht.

### **3. Verfügbarkeit und Belastbarkeit**

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.*

S. Maßnahmen in Rechenzentren Hetzern und Hosteurope.

Die Navato GmbH erstellt täglich Full-Backups und überträgt diese verschlüsselt auf einen zweiten Server. Diese Full-Backups werden anschließend am gleichen Tag auf einem Ersatzserver eingespielt.

Im Verlauf des Tages, werden permanent Differenzial-Backups erstellt und verschlüsselt auf den Backserver übertragen. Bei Ausfall können die Differenzialbackups auf dem Ersatzserver kopiert und eingespielt werden. Das Kopieren und Einspielen der Differenzialbackups ist automatisiert und wird regelmäßig getestet. Der Vorgang muss manuell angestoßen werden.

### **4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

Damian Moschny ist als Geschäftsführer für Datenschutz und Informationssicherheit verantwortlich. Die Mitarbeiter werden mit einer Geheimschutzvereinbarung zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet.

Ein externer Datenschutzbeauftragter ist beauftragt und wird auf Wunsch genannt. Die Mitarbeiter werden vom Datenschutzbeauftragten geschult.

Anfragen von Betroffenen werden von Damian Moschny bearbeitet. In seiner Abwesenheit wird die Aufgabe an einen Mitarbeiter delegiert.

Für die Umsetzung der Vorgaben der DSGVO im Unternehmen lässt sich die navato GmbH von einem Rechtsanwalt und einem externen Datenschutzbeauftragten beraten.

#### **Anlage 3.2 Im Rechenzentrum Hetzner**

Siehe: „Anlage 2 Hetzner Online“ zum Auftrag gemäß Art. 28 DS-GVO: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO und Anlage (Seite 8-11).

Bei Hetzner setzen wir Dedicated Server ein.

#### **Anlage 3.3 Im Rechenzentrum Hosteurope**

Siehe: „Dokumentation der technischen und organisatorischen Maßnahmen gem. Anlage zu 32 DSGVO V 1.1“ (Seite 2-13)

Bei Hosteurope setzen wir Root Server ein. Im Vertrag als „unmanaged system“ bezeichnet.

