Vertrag zur Auftragsverarbeitung

Zwischen

_____
_____
_____
_____

– Verantwortlicher –
im Folgenden „Auftraggeber“ genannt

und

neylux GmbH
Färbergraben 10
80331 München
Deutschland

– Auftragsverarbeiter –
im Folgenden „Auftragnehmer“ genannt

(im Folgenden zusammen: die Parteien)

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Beratungsleistungen im Bereich der Softwareimplementierung für die elektronische Reisekostenabrechnung. Hierzu haben die Parteien am _____ einen Vertrag geschlossen. Gegenstand des Auftrags ist in Anlage 1 genauer beschrieben. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer personenbezogenen Daten des Auftraggebers zur Kenntnis nimmt. Zur Wahrung der Anforderungen nach Art. 28 DSGVO schließen die Parteien die nachfolgende Vereinbarung. Diese Vereinbarung gilt ab dem Inkrafttreten der DSGVO am 25. Mai 2018. Für den Fall, dass bereits eine Auftragsdatenverarbeitung zwischen den Parteien gemäß § 11 BDSG besteht, sind sich die Parteien einig, dass diese durch die neue Vereinbarung mit Wirkung zum 25. Mai 2018 ersetzt wird.

1. Anwendungsbereich

Bei der Erbringung der Leistungen gemäß dem Hauptvertrag kann ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden, bezüglich derer der Auftraggeber als Verantwortlicher im datenschutzrechtlichen Sinn fungiert („Auftraggeber-Daten"). Dieser Vertrag spezifiziert die Datenschutzpflichten und -rechte der Parteien im Zusammenhang mit der Verarbeitung der Auftraggeber-Daten zur Erbringung der Leistungen nach dem Hauptvertrag.

2. Umfang der Beauftragung/Weisungsbefugnisse des Auftraggebers

2.1 Der Auftragnehmer wird die Auftraggeber-Daten ausschließlich im Auftrag und gemäß den dokumentierten Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht gesetzlich dazu verpflichtet ist. In letzterem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt ausschließlich in der Art, dem Umfang und zu dem Zweck wie in Anlage 1 spezifiziert; die Verarbeitung betrifft ausschließlich die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen.

2.3 Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

2.4 Der Auftraggeber behält sich das Recht zur Erteilung von Weisungen über Art, Umfang, Zwecke und Mittel der Verarbeitung von Auftraggeber-Daten vor.

3. Anforderungen an Personal

3.1 Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, bezüglich der Verarbeitung von Auftraggeber-Daten zur Vertraulichkeit zu verpflichten.

3.2 Der Auftragnehmer stellt sicher, dass ihm unterstellte natürliche Personen, die Zugang zu Auftraggeber-Daten haben, diese nur auf seine Anweisung verarbeiten, es sei denn, sie sind nach dem Recht der europäischen Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

4. Sicherheit der Verarbeitung

4.1 Der Auftragnehmer ergreift alle geeigneten technischen und organisatorischen Maßnahmen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

4.2 Der Auftragnehmer hat vor dem Beginn der Verarbeitung der Auftraggeber-Daten insbesondere die in Anlage 2 spezifizierten technischen und organisatorischen Maßnahmen zu ergreifen und während des Hauptvertrags aufrechtzuerhalten sowie sicherzustellen, dass die Verarbeitung von Auftraggeber-Daten im Einklang mit diesen Maßnahmen durchgeführt wird.

5. Inanspruchnahme weiterer Auftragsverarbeiter

5.1 Der Auftraggeber genehmigt hiermit in allgemeiner Weise die Inanspruchnahme weiterer Auftragsverarbeiter durch den Auftragnehmer. Die gegenwärtig vom Auftragnehmer eingesetzten weiteren Auftragsverarbeiter sind in Anlage 3 genannt.

5.2 Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter informieren. Der Auftraggeber ist berechtigt, gegen jede beabsichtigte Änderung Einspruch zu erheben. Erhebt der Auftraggeber Einspruch, ist dem Auftragnehmer die beabsichtigte Änderung untersagt. Im Falle zugelassener Änderungen wird der Auftragnehmer die Liste der Unterauftragnehmer in Anlage 3 entsprechend aktualisieren und dem Auftraggeber unverlangt zur Verfügung stellen.

5.3 Der Auftragnehmer wird jedem weiteren Auftragsverarbeiter vertraglich dieselben Datenschutzpflichten auferlegen, die in diesem Vertrag in Bezug auf den Auftragnehmer festgelegt sind.

5.4 Der Auftragnehmer wird vor jeder Beauftragung sowie regelmäßig während der Beauftragung überprüfen, dass die weiteren Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergriffen haben und diese so durchgeführt werden, dass die Verarbeitung der Auftraggeber-Daten gemäß dieser Anlage erfolgt.

6. Rechte der betroffenen Personen

6.1 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren mit technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der ihnen zustehenden Rechte betroffener Personen nachzukommen.

6.2 Der Auftragnehmer wird insbesondere:

- den Auftraggeber unverzüglich informieren, falls sich eine betroffene Person mit einem Antrag auf Wahrnehmung ihrer Rechte in Bezug auf Auftraggeber-Daten unmittelbar an den Auftragnehmer wenden sollte;
- dem Auftraggeber auf Anfrage alle bei ihm vorhandenen Informationen über die Verarbeitung von Auftraggeber-Daten geben, die der Auftraggeber zur Beantwortung des Antrags einer betroffenen Person benötigt und über die der Auftraggeber nicht selbst verfügt.

7. Sonstige Unterstützungspflichten des Auftragnehmers

7.1 Der Auftragnehmer meldet dem Auftraggeber, unverzüglich nachdem ihm eine solche bekannt geworden ist, jede Verletzung des Schutzes von Auftraggeber-Daten, insbesondere Vorkommnisse, die zur Vernichtung, zum

Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Auftraggeber-Daten führen. Die Meldung enthält nach Möglichkeit eine Beschreibung:

- der Art der Verletzung des Schutzes der Auftraggeber-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;
- der wahrscheinlichen Folgen der Verletzung des Schutzes der Auftraggeber-Daten;
- der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes der Auftraggeber-Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7.2 Für den Fall, dass der Auftraggeber verpflichtet ist, die Aufsichtsbehörden und/oder Betroffenen nach Art. 33, 34 DSGVO zu informieren, wird der Auftragnehmer den Auftraggeber auf dessen Anfrage unterstützen, diese Pflichten einzuhalten.

7.3 Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren bei Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

7.4 Der Auftragnehmer wird den Auftraggeber unverzüglich informieren, sobald Weisungen des Auftraggebers gegen die DSGVO oder andere Europäische Datenschutzbestimmungen verstoßen.

8. Datenlöschung und -zurückgabe

Der Auftragnehmer wird auf die Weisung des Auftraggebers hin mit Beendigung des Hauptvertrages alle Auftraggeber-Daten entweder vollständig und unwiderruflich löschen oder an den Auftraggeber zurückgeben, sofern nicht gesetzlich eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

9. Nachweise und Überprüfungen

9.1 Der Auftragnehmer hat sicherzustellen und regelmäßig zu kontrollieren, dass die Verarbeitung der Auftraggeber-Daten mit diesem Vertrag, einschließlich des in Anlage 1 festgelegten Umfangs der Verarbeitung der Auftraggeber-Daten, sowie den Weisungen des Auftraggebers in Einklang steht.

9.2 Der Auftragnehmer wird die Umsetzung der Pflichten nach diesem Vertrag in geeigneter Weise dokumentieren und dem Auftraggeber entsprechende Nachweise auf dessen Anfrage vorlegen. Der Auftragnehmer wird insbesondere dokumentieren:

- alle Vertraulichkeitsverpflichtungen von Personen, die Auftraggeber-Daten verarbeiten;
- alle sich in seinem Einwirkungsbereich ereignenden Verletzungen des Schutzes von Auftraggeber-Daten einschließlich aller damit im Zusammenhang stehenden Fakten, deren Auswirkungen und von ihm ergriffene Abhilfemaßnahmen;
- alle Verträge über die Inanspruchnahme weiterer Auftragsverarbeiter und alle Prüfungen weiterer Auftragsverarbeiter im Sinne von Ziffer 5.;
- alle auf Weisung des Auftraggebers erfolgten Löschungen von Auftraggeber-Daten.

9.3 Der Auftraggeber ist berechtigt, den Auftragnehmer vor dem Beginn der Verarbeitung von Auftraggeber-Daten und regelmäßig während der Laufzeit des Hauptvertrags bezüglich der Einhaltung der Regelungen dieses Vertrages, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen gemäß Anlage 2, selbst oder durch einen von ihm beauftragten Prüfer zu überprüfen; einschließlich durch Inspektionen. Der Auftragnehmer ermöglicht solche Überprüfungen und trägt durch alle zweckmäßigen und zumutbaren Maßnahmen zu solchen Überprüfungen bei, unter anderem durch:

- die Gewährung der notwendigen Zugangs- und Zugriffsrechte und
- der Bereitstellung aller notwendigen Informationen.

10. Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus dieser Vereinbarung nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine

Weisung des Auftraggebers nicht ausführen kann oder will. Bei einfachen fahrlässigen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist, innerhalb welcher der Auftragnehmer den Verstoß abstellen kann.

11. Beendigung des Hauptvertrags

11.1 Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder — auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht — löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

11.2 Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren.

11.3 Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

12. Schlussbestimmungen

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

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertrags-abreden bleibt hiervon unberührt.

Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

Diese Vereinbarung unterliegt deutschem Recht unter Ausschluss von Kollisionsrecht. Ausschließlicher Gerichtsstand ist München.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift neylux GmbH	Unterschrift Auftraggeber
_____	_____
Name (bitte in Druckbuchstaben)	Name (bitte in Druckbuchstaben)
_____	_____
Funktion	Funktion

Anlagen

Anlage 1 — Spezifikation der Verarbeitung

Anlage 2 — Technisch-organisatorische Maßnahmen

Anlage 3 — Liste der Subunternehmer

Anlage 1

Spezifikation der Verarbeitung

A. Allgmeine Angaben

Datenschutzbeauftragter	Stefan Bachmann, INES AG Stefan.bachmann@ines-it.de +49 8634 988423

B. Angaben zur Verarbeitung der Daten

Kategorien von Betroffenen	Mitarbeiter des Auftraggebers
Datenkategorien	• Vorname, Nachname • E-Mail (beruflich) • Mitarbeiter-ID • Reisedaten (Beginndatum, Endedatum, Uhrzeiten, Ziel-Adressen, Reisegrund)

Verarbeitungsvorgänge	• Datenfluss:
	  ○ Periodische Datenübertragung von der SAP Concur Instanz des Kunden
	  ○ In die neylux Cloud Platform zur Datenprozessierung
	  ○ Ggf. Übertragung in weitere Daten-Prozessierende Systeme (bspw. ERP-System des Kunden, Lieferantensysteme etc.)
	• Datenübertragung mittels
	  ○ SAP Concur Client WebServices
	  ○ Spezifische Übertragungswege des Kunden oder Lieferanten (WebServices, SFTP etc.)
	• Datenspeicherung
	  ○ In der neylux Cloud Platform zum Zwecke der Versionierung / Änderungserkennung
	  ○ Über einen vom Kunden definierten Zeitraum

Ort der Verarbeitungsvorgänge	• Standort der neylux Server bei Microsoft Azure (Frankfurt am Main) • Bürostandorte der neylux GmbH in Deutschland (München, Frankfurt am Main) • Bei Homeoffice alle Wohnorte der neylux Mitarbeiter in Deutschland
Zwecke	Datenverarbeitung für erweiterte Prozesse im Concur Kontext des Auftraggebers
Dauer	Zeitraum der Datentransfers und Datenverarbeitung in neylux Cloud Platform
Aufbewahrungsfristen	Aufbewahrungsfrist definiert Auftraggeber
Übermittlung außerhalb des EWR	Nicht anwendbar

Anlage 2

Technisch-organisatorische Maßnahmen

1. Zutrittskontrolle	Alle Zugänge sind mit dem manuellen Schließsystem ausgestattet; Schlüsselregelung; Sorgfalt bei der Auswahl der Reinigungsdienste; Gäste und Besucher werden im Büro nicht unbeaufsichtigt gelassen, sondern immer von Auftragnehmer-Personal begleitet
2. Zugangskontrolle	Alle Mitarbeiter greifen mit einer eindeutigen Kennung (User-ID & Passwort) auf die IT-Systeme vom Auftragnehmer zu. Benutzerberechtigungen werden durch die minimale Anzahl der Admin-User verwaltet. Wenn ein Mitarbeiter das Unternehmen verlässt, werden dessen Zugriffsrechte aufgehoben. Es wird die Richtlinie „Sicheres Passwort“ & Passwort-Management-Tool bei der Kennwortvergabe, sowie die Richtlinie „Clean desk“ beim Verlassen des Arbeitsplatzes angewendet. Der Auftragnehmer arbeitet mit dem Anbieter LastPass zur Verwaltung von Kundenpasswörtern. Zugriff wird durch den Consulting Manager/Geschäftsführer vergeben. Jeder Computer verfügt über einen kennwortgeschützten Bildschirmschoner. Das Unternehmensnetzwerk ist durch Firewalls vor dem öffentlichen Netzwerk geschützt. Entsprechende Sicherheits-Updates werden regelmäßig durchgeführt.
3. Zugriffskontrolle	Für die Zugriffskontrolle auf die Auftraggeber-Daten ist der Auftraggeber / Softwareanbieter verantwortlich. Die Mitarbeiter des Auftragnehmers greifen nur auf die von SAP und SAP Concur bereitgestellten Services über HTTPS zu. Eine lokale Speicherung findet nicht statt - außer im Rahmen der Daten Prozessierung in der neylux Cloud Platform. Einhaltung und Überwachung des Berechtigungskonzeptes erfolgt über neylux sowie SAP Concur.
4. Weitergabekontrolle/ Übermittlungskontrolle	Der Auftragnehmer bearbeitet und gibt keine personenbezogenen Auftraggeber-Daten weiter. Bei Fehlerfällen Kommunikation ausschließlich über SAP Concur Ticket System (HTTPS). Referenz i.d.R. ist die Doc ID (20 stelliger Alphanumerischer-Schlüssel, der den Abrechnungsfall eindeutig spezifiziert).
5. Eingabekontrolle/ Plausibilitätskontrolle/ Transaktionskontrolle	Eingabekontrolle/ Plausibilitätskontrolle/ Transaktionskontrolle unterliegen dem Verantwortungsbereich des Auftraggebers / Softwareanbieters (SAP Concur), da vom Auftragnehmer keine zutreffenden Verarbeitungstätigkeiten erfolgen können.
6. Auftragskontrolle/ Vertragskonformitätskontrolle	Die Auftragskontrolle liegt beim Auftraggeber/ Softwareanbieter. Alle Mitarbeiter des Auftragnehmers sind der Verpflichtung auf die Wahrung der datenschutzrechtlichen Vorschriften unterzogen und werden darüber in regelmäßigen Abständen geschult.
7. Verfügbarkeitskontrolle	Personenbezogene Daten werden vor versehentlicher oder nicht autorisierter Vernichtung oder Verlust geschützt. neylux verfügt über regelmäßige Backup-Prozesse zur Wiederherstellung der Verfügbarkeit geschäftskritischer Systeme bei Bedarf. Notfallprozesse und -systeme werden regelmäßig getestet.
8. Datentrennungskontrolle/ Mandantentrennungskontrolle	Personenbezogene Daten, die für unterschiedliche Zwecke erfasst werden, können getrennt verarbeitet werden. neylux nutzt angemessene technischen Kontrollen, um jederzeit die Trennung von Auftraggeber- Daten zu erreichen.
9. Datenlöschkontrolle	Der Auftraggeber definiert einen Zeitraum zur Löschung der Daten vom Server / DBs des Auftragnehmers. Der Auftragnehmer garantiert die Löschung der Daten zu diesem Zeitpunkt.

Anlage 3

Liste der Subunternehmer

- Microsoft Azure
- Der Einsatz von weiteren Subunternehmern ist nicht beabsichtigt