

Vereinbarung Auftragsverarbeitung (AVV) oqio

Diese Vereinbarung Auftragsverarbeitung (AVV) (nachfolgend „**Vereinbarung**“) regelt die Datenverarbeitung im Auftrag des Auftraggebers als Verantwortlichem (nachfolgend „**Auftraggeber**“) durch die oqio GmbH als Auftragnehmer und Auftragsdatenverarbeiter (nachfolgend „**oqio**“; oqio und Auftraggeber nachfolgend gemeinsam „**Parteien**“ oder jeder einzeln „**Partei**“). Sie ist wesentlicher Bestandteil des Vertrages zwischen oqio und dem Auftraggeber (nachfolgend „**Hauptvertrag**“).

1. Vertragsgegenstand, Inhalt des Auftrags

- 1.1 oqio erbringt die Bereitstellung des SaaS-Systems oqio (nachfolgend „**Software**“) auf Grundlage des Hauptvertrags.
- 1.2 Zur Konkretisierung der datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die Vereinbarung. Gegenstand der Verarbeitung ist die Bereitstellung der cloudbasierten SaaS-Plattform von oqio zur zentralen Verwaltung, Abwicklung und Analyse von Versicherungsschäden in Immobilienbeständen. Die Software ermöglicht die digitale Erfassung und Nachverfolgung von Schäden über deren gesamten Lebenszyklus hinweg sowie die kollaborative Zusammenarbeit zwischen Beteiligten aus der Wohnungswirtschaft, dem Versicherungsvertrieb und handwerklichen Dienstleistern. Im Rahmen der Bereitstellung werden schadenrelevante Informationen, Dokumente und Fotos strukturiert gespeichert und verarbeitet, um den Bearbeitungsfortschritt transparent zu dokumentieren und die Kommunikation zwischen den Prozessbeteiligten zu steuern. Zudem umfasst die Leistung die Erstellung aggregierter Reports zur Analyse von Schadensverläufen und Versicherungsbeständen. Die Verarbeitung erfolgt zweckgebunden zur effizienten Schadensabwicklung und zum Management der Gebäudeversicherungen über einen browserbasierten Fernzugriff, wobei oqio den technischen Betrieb sowie die Wartung und Weiterentwicklung der Plattform übernimmt. Die Dauer der Leistungserbringung und Verarbeitung richtet sich nach der Laufzeit des Hauptvertrags und umfasst zusätzlich den Zeitraum bis zur vollständigen Löschung oder Rückgabe der Daten nach Vertragsbeendigung gemäß den vertraglichen Vereinbarungen. Die Regelungen der Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrags vor.

2. Umfang, Zweck und Durchführung der Datenverarbeitung; Art der Daten und Kreis der Betroffenen; Weisungsgebundenheit

- 2.1 Umfang und Zweck der Datenverarbeitung durch oqio ergeben sich aus dem Hauptvertrag und betreffen die Datenverarbeitung für die Bereitstellung der Onlineplattform oqio zur Verwaltung, Abwicklung und Analyse der Gebäudeversicherung für große Wohnungsbestände als SaaS (Software as a Service) für den Fernzugriff mittels eines Internetbrowsers.
- 2.2 oqio hat im Rahmen der Leistungserbringung potentiell Zugriff auf die in der Software gespeicherten Daten. Dabei handelt es sich um folgende Datenkategorien und potentiell Betroffene:
 - **Mitarbeitende des Auftraggebers:** Nutzeraccounts (inklusive Name, Benutzerkennung, E-Mail-Adresse, Passwort)
 - **Endkunden/Dritte:** Endkunden, Ansprechpartner bei Versicherern, Dienstleister, Geschädigte, Schadensverursacher (jeweils Kontaktdaten, Schadensdaten, Kommunikation).

Zudem fallen beim Betrieb der Software allgemeine Webserver-Logdaten an.

- 2.3 oqio verarbeitet personenbezogene Daten ausschließlich weisungsgebunden. Diese Weisungen werden durch diese AVV und den Hauptvertrag festgelegt und können vom Auftraggeber durch einzelne Weisungen in Textform geändert, ergänzt und ersetzt werden. Während der Vertragslaufzeit erfolgende Einzelweisungen des Auftraggebers sind sowohl durch die Verantwortliche als auch durch oqio zu dokumentieren.
- 2.4 oqio hat Einzelweisungen des Auftraggebers über die Erhebung, Verarbeitung oder Nutzung von Daten zu beachten und umzusetzen. Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen in Textform berechtigt. Dies umfasst auch Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Ist oqio der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, wird oqio den Auftraggeber unverzüglich darauf hinweisen und ist berechtigt, die Ausführung der Einzelweisung bis zu einer Bestätigung oder Änderung der Weisung durch den Auftraggeber auszusetzen. Die angemessenen Kosten der Durchführung von Weisungen, die über die vertraglichen Leistungen des Hauptvertrags hinausgehen, werden vom Auftraggeber nach Maßgabe der jeweils geltenden Stundensätze von oqio erstattet, es sei denn, die Weisung war erforderlich, um einen Verstoß von oqio gegen datenschutzrechtliche Bestimmungen oder diesen Vertrag abzustellen.

2.5 oqio stellt sicher, dass die vertragsgegenständlichen personenbezogenen Daten des Auftraggebers nur auf dokumentierte Weisung des Auftraggebers – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet werden, sofern er nicht durch das Recht der Union oder der Bundesrepublik Deutschland hierzu verpflichtet ist; in einem solchen Fall teilt oqio dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Sofern eine Mitteilung aus diesem Grund zunächst unterbleibt, wird oqio den Auftraggeber unverzüglich informieren, sobald das rechtliche Verbot entfallen ist. Jede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Auftraggeber und oqio die maßgeblichen datenschutzrechtlichen Bestimmungen der Union oder der Bundesrepublik Deutschland einhalten und so auch in dem jeweiligen Drittland ein angemessenes Datenschutzniveau erhalten; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten aus dem betreffenden Drittland oder der betreffenden internationalen Organisation an ein anderes Drittland oder eine andere internationale Organisation.

3. Unterauftragsverhältnisse

3.1 oqio ist zur Einschaltung von weiteren Auftragsverarbeitern als Unterauftragsverarbeiter berechtigt. Derzeit setzt oqio die folgenden Unterauftragsverarbeiter ein:

Unterauftragsverarbeiter	Verarbeitungstätigkeit	Lokation
Netways GmbH (Deutschland)	Hosting der oqio-Plattform und Backup	EU
Twilio Ireland Limited (Irland)	Versand von Transaktions-E-Mails	EU (EU Data Residency)
Intercom R&D Unlimited Company (Irland)	Support/Ticketing	EU (EU Data Residency)

Vertragliche Vereinbarungen mit Unterauftragsverarbeitern werden durch oqio so gestaltet, dass sie den Bestimmungen der DSGVO entsprechen.

3.2 Die Auftragsverarbeiterin informiert die Verantwortliche vorab über jede beabsichtigte Änderung in Bezug auf die Unterauftragsverarbeiter, wodurch die Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen innerhalb von 14 Tagen nach Zugang der Benachrichtigung aus sachlichen Gründen Einspruch zu erheben. Für die Zustimmung ist der Unterauftragsverarbeiter, welchen die Auftragsverarbeiterin einsetzen möchte mit Namen, Anschrift, Ort der Verarbeitung und Tätigkeitsbereich (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter autorisiert sein sollen) zu nennen. Erhebt die Verantwortliche Einspruch, ist die Auftragsverarbeiterin berechtigt, den Hauptvertrag (und damit diesen AVV) mit einer Frist von drei Monaten zu kündigen, wenn sich die Verantwortliche nach Ansicht der Auftragsverarbeiterin ohne triftigen Grund weigert, den Unterauftragsverarbeiter zu genehmigen, oder wenn es der Auftragsverarbeiterin nicht möglich ist, ihre Dienstleistungen ohne den abgelehnten Unterauftragsverarbeiter zu erbringen und die Parteien keine einvernehmliche Lösung finden konnten.

3.3 Nimmt oqio die Dienste eines Unterauftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Unterauftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in der Vereinbarung festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der oqio gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Unterauftragsverarbeiters.

4. Datengeheimnis und Vertraulichkeit

oqio stellt sicher, dass die zur Verarbeitung der personenbezogenen Daten eingesetzten Mitarbeiter zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung des Arbeitsverhältnisses zwischen dem Mitarbeiter und oqio bestehen bleiben.

5. Schutzmaßnahmen und Kontrolle

- 5.1 oqio trifft die gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (TOMs), insbesondere wie in **Anlage 1** näher beschrieben. oqio kann die technischen und organisatorischen Maßnahmen ändern und anpassen, insbesondere an Fortentwicklungen des Standes der Technik, sofern dadurch das anfängliche Sicherheitsniveau nicht unterschritten wird. oqio informiert den Auftraggeber über wesentliche Änderungen der TOMs, die das Sicherheitsniveau beeinträchtigen könnten.
- 5.2 oqio stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten gemäß Art. 28 DSGVO zur Verfügung, z.B. durch Vorlage geeigneter Dokumentation. oqio ermöglicht zudem die Überprüfung durch den Auftraggeber oder einen anderen von diesem beauftragten Prüfer. Zu diesem Zweck gestattet oqio dem Prüfer, sich zu Prüfzwecken in den Betriebsräumen von oqio zu den üblichen Geschäftszeiten ohne erhebliche Störung des Betriebsablaufes von der Einhaltung der für die Auftragsverarbeitung einschlägigen Pflichten zu überzeugen. Vor-Ort-Prüfungen sind grundsätzlich mit angemessener Vorlaufzeit anzukündigen, es sei denn, besondere Umstände (z. B. dringender Verdacht auf Datenschutzverstöße) erfordern eine unverzügliche Prüfung. Die angemessenen Kosten der Mitwirkung bei einer solchen Prüfung auf Seiten von oqio werden vom Auftraggeber nach Maßgabe der Stundensätze von oqio erstattet, sofern nicht ein Verschulden von oqio die Notwendigkeit der Prüfung ausgelöst hat.

6. Informations- und Unterstützungspflichten

- 6.1 Wenn oqio eine Verletzung des Schutzes personenbezogener Daten des Auftraggebers bekannt geworden ist, meldet oqio diese unverzüglich, spätestens innerhalb von 24 Stunden, dem Auftraggeber. oqio wird im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene ergreifen. oqio unterstützt den Auftraggeber bei der Erfüllung der Melde- und Benachrichtigungspflichten an Betroffene und die Behörden gemäß Art. 33 und 34 DSGVO.
- 6.2 oqio unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erstellung von Datenschutzfolgenabschätzungen gemäß Art. 35, 36 DSGVO. Die angemessenen Kosten der Unterstützung durch oqio werden vom Auftraggeber nach Maßgabe der Stundensätze von oqio erstattet.
- 6.3 Sollten die Daten bei oqio durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat oqio den Auftraggeber unverzüglich darüber zu informieren. oqio wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DSGVO liegen.
- 6.4 oqio wird dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung stellen und Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglichen und dazu beitragen.

7. Löschung von Daten

Nach Abschluss der Erbringung der Verarbeitungsleistungen hat die Auftragsverarbeiterin alle personenbezogenen Daten nach Wahl der Verantwortlichen entweder zu löschen oder zurückzugeben und die vorhandenen Kopien zu löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Die Auftragsverarbeiterin fordert die Verantwortliche rechtzeitig vor Abschluss der Erbringung der Verarbeitungsleistungen auf, ihr Wahlrecht auszuüben. Die Verantwortliche hat ihre Wahl innerhalb von 14 Tagen nach Zugang der Benachrichtigung auszuüben. Teilt die Verantwortliche zum Ablauf dieser Frist ihr Wahlrecht nicht mit, ist die Auftragsverarbeiterin berechtigt, die personenbezogenen Daten zu löschen.

8. Rechte der betroffenen Personen

- 8.1 Soweit ein Betroffener sich unmittelbar an oqio zwecks Wahrnehmung von Betroffenenrechten (z.B. bezüglich der Berichtigung, Sperrung bzw. Einschränkung der Verarbeitung oder Löschung von Daten) wenden sollte, wird oqio dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- 8.2 oqio unterstützt den Auftraggeber auf Anforderung bei der Wahrung dieser Rechte, z.B. im Hinblick auf die Informationspflichten (Benachrichtigung, Auskunftserteilung), Berichtigung, Sperrung bzw. Einschränkung der Verarbeitung und Löschung personenbezogener Daten. Die angemessenen Kosten der Unterstützung durch oqio werden vom Auftraggeber nach Maßgabe der Stundensätze der oqio erstattet.

9. Laufzeit und Schlussbestimmungen

- 9.1 Die vorliegende Vereinbarung endet mit der Beendigung des Hauptvertrags. Sie bleibt auch über die Beendigung des Hauptvertrags hinaus solange in Kraft, wie oqio über personenbezogene Daten des Auftraggebers verfügt.
- 9.2 Die zwischen den Parteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Haftung zwischen den Parteien im Zusammenhang mit dieser Vereinbarung.
- 9.3 Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- 9.4 Es gilt ausschließlich deutsches Recht unter Ausschluss solcher Rechtsnormen, die auf andere Rechtsordnungen verweisen. Das einheitliche UN-Kaufrecht (UNCITRAL) findet keine Anwendung.

Anlage 1 zur Vereinbarung Auftragsverarbeitung

Technische und organisatorische Maßnahmen (TOMs)

Vorbemerkung

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die oqio für die Software mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen. Diese Maßnahmen werden ergänzt durch technische und organisatorische Maßnahmen des von oqio eingesetzten Unterauftragsverarbeiters für Server- und Rechenzentrums-Dienstleistungen.

Die TOMs werden wie folgt gruppiert:

- System (Server, Datenbanken usw.)
- Anwendungssoftware
- Lokale IT-Infrastruktur von oqio (Desktop, Laptop usw.)

Die unterschiedlichen technischen und organisatorischen Maßnahmen pro Zugriffsart sind separat aufgelistet oder allgemein definiert.

Die Backend-Systeme (Server, Datenbanken usw.) werden von einem Unterauftragsverarbeiter betrieben. Der Unterauftragsverarbeiter setzt insoweit angemessene Sicherheitsmaßnahmen um und ist nach ISO27001 zertifiziert.

1. Verfahren und Anforderungen zur Gewährleistung der Verfügbarkeit der personen-bezogenen Daten

Gewährleisten, dass Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Um dies zu gewährleisten müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

Software:

- Backup-Verfahren / -konzept
- Funktionstrennung (Produktion- / Testsysteme)

Arbeitsplatz:

- Benutzer - Backup-Verfahren / -konzept
- Virenschutz
- Brandschutzmaßnahmen (Feuerlöscher, Brandmelder usw.)

2. Verfahren und Anforderungen zur Gewährleistung der Vertraulichkeit der personen-bezogenen Daten

Verhindern, dass Unbefugte Zutritt zu den Verarbeitungsanlagen haben. Um dies zu gewährleisten, müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

Arbeitsplatz:

- Schlüssel / Protokollierung der Schlüsselvergabe
- Mechanische Türsicherung
- Begleitung durch einen internen Mitarbeiter

Verhindern, dass Unbefugte Verarbeitungsanlagen nutzen können. Um dies zu gewährleisten, müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

Software:

- Verschlüsselte Verbindung (HTTPS)
- Kennwortverfahren (u.a. Mindestlänge, Zahl, Groß- und Kleinschreibung, usw.)
- Verschlüsselte Speicherung von Passwörtern (z.B. PBKBF2)
- Aktualität der verwendeten Software (Sicherheitspatches)

Arbeitsplatz:

- Virenschutz
- Kennwortverfahren (u.a. Mindestlänge, Zahl, Groß- und Kleinschreibung, usw.)
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro User
- Aktualität der verwendeten Software (max. 1 Jahr alt, regelmäßiges Einspielen von Sicherheitspatches)
- Verschlüsselung von Arbeitsplatzfestplatten
- Sichtschutz (Fensterplätze, unterwegs)

3. Verfahren und Anforderungen zur Gewährleistung der Integrität der personenbezogenen Daten

Gewährleisten, dass nur Berechtigte auf Daten zugreifen können und diese nicht unbefugt gelesen, verändert, kopiert oder entfernt werden können. Um dies zu gewährleisten, müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

Software:

- Datenschutzkonforme Löschung der Daten nach Vertragsbeendigung oder auf Verlangen des Auftraggebers
- Berechtigungskonzept mit differenzierten Berechtigungen (User, Profile und Rollen)
- Aktualität der verwendeten Software (Sicherheitspatches)

Arbeitsplatz:

- Berechtigungskonzept mit differenzierten Berechtigungen (User, Profile und Rollen)
- Verschlüsselung von Arbeitsplatzfestplatten

Gewährleisten, dass Daten bei der elektronischen Übertragung/Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Um dies zu gewährleisten, müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

- Die Mitarbeiter von oqio sind zur Wahrung des Datengeheimnisses gemäß DSGVO und zur Wahrung von Geschäftsgeheimnissen vertraglich verpflichtet

Sicherung bei der elektronischen Übertragung:

- Verschlüsselung (bspw. Mittels VPN)
- Authentisierung der Gegenstelle (Zertifikat)

Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (Speicherung, Veränderung, Löschung, Übermittlung). Um dies zu gewährleisten, müssen mindestens folgende Maßnahmen zur Trennungskontrolle durch oqio ergriffen werden:

Software:

- Dedizierte (virtuelle) Server
- Funktionstrennung (Produktion- / Testsysteme)

4. Gewährleistung der Belastbarkeit bei Verfahren zur Verarbeitung der personenbezogenen Daten

Gewährleisten, dass es nicht zur Überlastung des Verfahrens zur Verarbeitung von personenbezogenen Daten kommt. Um dies zu gewährleisten, müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

- Verwendung von ausreichend dimensionierter Hardware & Software

5. Verfahren und Anforderungen zur Gewährleistung Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall, rasch wiederherzustellen

Gewährleisten, dass Daten bei einem physischen oder technischen Zwischenfall, rasch wiederhergestellt werden können. Um dies zu gewährleisten, müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

Software:

- Backup- und Wiederherstellungsverfahren

Arbeitsplatz:

- Benutzer - Backup-Verfahren / -konzept
- Reserve Hardware

6. Verfahren und Anforderungen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Gewährleisten, dass oqio den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit führt und dokumentiert. Um dies zu gewährleisten, müssen mindestens folgende Maßnahmen durch oqio ergriffen werden:

- Audit- oder Kontrollverfahren zur Bewertung und Evaluierung der Wirksamkeit der TOMs
- Ggf. entsprechende Zertifizierung oder Verhaltensregeln
- Führung eines Verzeichnisses der Verarbeitungstätigkeiten
- Bestellung eines Datenschutzbeauftragten und Mitteilung der Kontaktdaten.

7. Sonstige Verfahren und Anforderungen

Gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Anweisungen des Auftraggebers verarbeitet werden können. Um dies zu gewährleisten, müssen mindestens folgende Maßnahmen zur Auftragskontrolle durch oqio ergriffen werden:

- Eindeutige Vertragsgestaltung durch AV-Vertrag (Weisungsbefugnisse, Kontrollrechte usw.)
- Verpflichtung der Mitarbeiter von oqio zur Wahrung des Datengeheimnisses gemäß DSGVO und zur Wahrung von Geschäftsgeheimnissen
- Angemessene Schulungs- und Sensibilisierungsmaßnahmen
- Führung eines Verzeichnisses der Verarbeitungstätigkeiten
- Bestellung eines Datenschutzbeauftragten und Mitteilung der Kontaktdaten