# VERPFLICHTUNGSERKLÄRUNG

zur Wahrung der Verschwiegenheit und des Datengeheimnisses gemäß Artikel 32 Datenschutzgrundverordnung

_____

Vorname, Nachname)

Ich bin heute auf die Wahrung des Datengeheimnisses nach Artikel 32 und auf die Wahrung der Verschwiegenheit verpflichtet worden. Die Vorschriften der Datenschutzgrundverordnung (DSGVO) insbesondere über das Datengeheimnis, sind mir bekannt.

Danach ist es mir untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Das Erheben, Verarbeiten und Nutzen personenbezogener Daten ist nach dem BDSG nur zulässig, soweit dies zum jeweiligen Zweck der rechtmäßigen Aufgabenerfüllung erfolgt und notwendig ist.

Zum Schutz der Daten habe ich im Rahmen der mir zugewiesenen Aufgabe die notwendige Sorgfalt anzuwenden. Insbesondere habe ich die jeweiligen Datensicherungsvorschriften zu beachten. Ich werde von mir festgestellte Mängel im Sicherungssystem mitteilen.

Ich bin darüber belehrt worden, dass sich die Verschwiegenheitsverpflichtung auf alles erstreckt, was mir in Ausübung meiner Tätigkeit oder im Zusammenhang hiermit anvertraut oder bekannt geworden ist oder anvertraut oder bekannt wird.

Es ist mir bekannt, dass jeder Verstoß gegen diese Verpflichtungserklärung sowie jeder Verstoß gegen Datenschutzvorschriften zu Schadenersatzforderungen führen und mit Bußgeld bzw. Geld- oder Freiheitsstrafen geahndet werden können (Art. 83 DSGVO).

_____

(Ort, Datum)

_____

(Unterschrift)

*** Artikel 32 Datenschutzgrundverordnung (DSGVO)**

1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

   a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

   b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

   c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

   d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.