Art. 32 DSGVO Sicherheit der Verarbeitung

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:
	1. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
	2. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
	3. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
	4. 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](https://dsgvo-gesetz.de/art-40-dsgvo/) oder eines genehmigten Zertifizierungsverfahrens gemäß [Artikel 42](https://dsgvo-gesetz.de/art-42-dsgvo/) 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.

Art. 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen

1. Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
2. 1Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach [Artikel 58](https://dsgvo-gesetz.de/art-58-dsgvo/) Absatz 2 Buchstaben a bis h und j verhängt. 2Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:
	1. Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
	2. Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
	3. jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
	4. Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den [Artikeln 25](https://dsgvo-gesetz.de/art-25-dsgvo/) und [32](https://dsgvo-gesetz.de/art-32-dsgvo/) getroffenen technischen und organisatorischen Maßnahmen;
	5. etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
	6. Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
	7. Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
	8. Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
	9. Einhaltung der nach [Artikel 58](https://dsgvo-gesetz.de/art-58-dsgvo/) Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
	10. Einhaltung von genehmigten Verhaltensregeln nach [Artikel 40](https://dsgvo-gesetz.de/art-40-dsgvo/) oder genehmigten Zertifizierungsverfahren nach [Artikel 42](https://dsgvo-gesetz.de/art-42-dsgvo/) und
	11. jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.
3. Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.
4. Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:
	1. die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln [8](https://dsgvo-gesetz.de/art-8-dsgvo/), [11](https://dsgvo-gesetz.de/art-11-dsgvo/), [25](https://dsgvo-gesetz.de/art-25-dsgvo/) bis [39](https://dsgvo-gesetz.de/art-39-dsgvo/), [42](https://dsgvo-gesetz.de/art-42-dsgvo/) und [43](https://dsgvo-gesetz.de/art-43-dsgvo/);
	2. die Pflichten der Zertifizierungsstelle gemäß den [Artikeln 42](https://dsgvo-gesetz.de/art-42-dsgvo/) und [43](https://dsgvo-gesetz.de/art-43-dsgvo/);
	3. die Pflichten der Überwachungsstelle gemäß [Artikel 41](https://dsgvo-gesetz.de/art-41-dsgvo/) Absatz 4.

§ 42 BDSG Strafvorschriften

1. Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,
	1. einem Dritten übermittelt oder
	2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

1. Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,
	1. ohne hierzu berechtigt zu sein, verarbeitet oder
	2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.