GATACA®
Datenschutz GmbH

NIS-2 Compliance Test

Gesetzesauszug § 30 Abs. 2 Nr. 1-10	**Indikatoren**	**Check**
„Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik“	Existiert in Ihrem Unternehmen ein Rechtskatastar, welches die Vorgaben an die IT erfasst?	☐
„Bewältigung von Sicherheitsvorfällen“	Gibt es ein Konzept zum Umgang mit Sicherheitsvorfällen? Anzeichen eines fehlenden Konzepts: • Sie wissen nicht, was ein Sicherheitsvorfall ist.	☐
„Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,“	Existiert für Ihren Arbeitsplatz ein Konzept, wie Sie notwendigste Arbeiten auch im Falle eines Cyberangriffs erledigen können? Wird dieses Konzept überprüft?	☐
„Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern“	Werden Dienstleister folgender Leistungen (Softwarelieferant, Wartung von Hard- & Software, Externer Datenschutzbeauftragter) im Unternehmen nach vorgegebenen Sicherheitskriterien ausgewählt und überprüft? Werden Dienstleistern Sicherheitsvorgaben gemacht? Anzeichen fehlender Kriterien/Prüfungen: • Fehlende Erreichbarkeit des Dienstleisters auch in wichtigen dringenden Fällen. • Die Wartung der Software oder Hardware ist unzureichend oder wurde gar nicht erstellt.	☐
„Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen“	Werden bei Ihnen im Unternehmen die Informationen klassifiziert/gekennzeichnet und wird diese Klassifizierung/Kennzeichnung auch externen Dienstleistern mitgeteilt? Anzeichen fehlender Kriterien/Prüfungen: • Dokumente und Informationen werden ohne Kennzeichnungen wie: ***Vertraulich***, ***Geheim*** oder ***Interner Gebrauch*** versendet und abgelegt. • Wenn Sie ein solches Schema haben, wird dies in der Kommunikation mit externen beachtet?	☐
„Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,“	Wenn Sicherheitsmaßnahmen, gleich welcher Art eingeführt wurden, finden hier Überprüfungen der Wirksamkeit statt und ggf. Anpassungen?	☐
„Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik“	Werden Ihre Mitarbeiter ausreichend und rechtzeitig hinsichtlich der Gefahren durch Cyberkriminelle geschult? Anzeichen unzureichender/nicht rechtzeitiger Schulung: • Schulungen behandeln das Thema der Gefahr nur am Rande z.B. Teil in einer allg. Datenhschutzschulung. • Neue Mitarbeiter erhalten bereits Zugriffe werden aber erst wesentlich später geschult. • Es finden gar keine Schulungen statt. • Teile der Belegschaft werden nicht geschult, da sie im Urlaub, krank oder im Homeoffice waren. • Der Schulungsinhalt hat mit der Lebenswirklichkeit des Unternehmens nichts zu tun oder ist unverständlich.	☐

GATACA© Datenschutz GmbH | Eine Tochter der GATACA© Holding GmbH | seit 2005

Am Riettor 4 | 78048 Villingen-Schwenningen
+49 (0) 7721 / 887979-0
info@gataca.de | www.gataca.de

Geschäftsführer: Moritz Gängel
Handelsregister: HRB 727757 Freiburg
USt-Id-Nr.: DE263703807

„Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung“	Gibt es Regelungen in Ihrem Unternehmen technischer oder organisatorischer Art zur Verschlüsselung. Beispiele: • Dateien werden mit Passwörtern versehen • (Nur) verschlüsselte Kommunikation • Generelle Regelung, wann welche Daten wie gesondert gesichert werden (z.B. durch Passwort) oder nur verschlüsselt verschickt werden dürfen	☐
„Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management und Anlagen“	Ist es sichergestellt, dass betriebsfremde Personen oder unbefugte Mitarbeiter Ihr Unternehmen oder einzelne Abteilungen nicht unbemerkt/ungewollt betreten? Anzeichen dass dem nicht so ist, können sein: • Keine Einzäunung • Keine Videoüberwachung • Offene Türen und Tore • Auch Nachts können Mitarbeiter der Produktion in die Verwaltung • Fehlende Schlüssel fallen nicht auf	☐
„Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.“	Nutzen Sie in Ihrem Unternehmen beim Zugriff auf Daten ein Verfahren, bei welchem Sie neben der Passworteingabe noch einen weiteren Nachweis Ihrer Identität erbringen? Beispiele: • Ihnen wird ein Code zugesendet • Fingerabdruckscan • Sie haben einen Token, welcher verwendet werden muss.	☐
Gesamtzahl der mit ***„Ja“*** beantworteten Fragen		____

Ergebnisbewertung

10 Punkte	**Glückwunsch! Sie sind bereits sehr gut aufgestellt.** Sie haben ein Niveau erreicht, auf das Sie stolz sein können. Beachten Sie, dass die aller letzten Feinheiten oft die schwierigsten sind. Gerne unterstützen wir Sie dabei, diese zu meistern.
5 - 9 Punkte	**Gut gemacht, Sie sind auf dem richtigen Weg!** Sie machen bereits vieles richtig. Nun stellt sich die Frage, ob Sie sich sicher fühlen, die zweite Hälfte der Strecke zu meistern. Wir können Ihnen helfen, Ihre Fähigkeiten weiter zu verbessern und vollständige Sicherheit in Ihrem Wissen zu erreichen.
1 - 4 Punkte	**Ein guter Anfang, es gibt jedoch Verbesserungspotenzial** Sie haben ein Niveau erreicht, auf das Sie stolz sein können. Beachten Sie, dass die aller letzten Feinheiten oft die schwierigsten sind. Gerne unterstützen wir Sie dabei, diese zu meistern.
0 Punkte	**Es ist wichtig, von Grund auf zu beginnen** Sie haben ein Niveau erreicht, auf das Sie stolz sein können. Beachten Sie, dass die aller letzten Feinheiten oft die schwierigsten sind. Gerne unterstützen wir Sie dabei, diese zu meistern.

Wichtig:

Bitte beachten Sie, dass dieser Test nur einen Bruchteil der Anforderungen des § 30 der NIS2-Regelung abdeckt. Das Gesetz, das bis zum 17. Oktober vollständig umgesetzt sein muss, ist deutlich umfangreicher. Daher sollten die Ergebnisse dieses Tests, unabhängig davon, ob Sie 0 oder 10 Punkte erreichen, im Kontext seiner begrenzten Reichweite betrachtet werden. Dieser Test dient als erster Anhaltspunkt und nicht als umfassende Bewertung Ihrer Compliance mit der gesamten NIS2-Regelung. Weitere Untersuchungen und Maßnahmen könnten erforderlich sein, um eine vollständige Übereinstimmung sicherzustellen.

GATACA© Datenschutz GmbH | Eine Tochter der GATACA© Holding GmbH | seit 2005

Am Riettor 4 | 78048 Villingen-Schwenningen
+49 (0) 7721 / 887979-0
info@gataca.de | www.gataca.de

Geschäftsführer: Moritz Gängel
Handelsregister: HRB 727757 Freiburg
USt-Id-Nr.: DE263703807