Zusammenfassung Maßnahmen

Teile der Regelungen in der DSGVO sind eine Fortführung der bereits bestehenden Datenschutzrichtlinien wie: Verarbeitung nach Treu und Glauben, Rechtmäßigkeit und Transparenz; Zweckbindung; Datensparsamkeit; Datenqualität; Sicherheit, Integrität und Vertraulichkeit.

Allerdings wird **die Rechenschaftspflicht für Verantwortliche verschärft, die Einhaltung der Grundsätze nachweisen zu können.** Darüber hinaus werden die derzeitigen Vorgaben in der DSGVO erweitert:
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz – Personenbezogene Daten müssen nun ausdrücklich so verarbeitetet werden, dass es für die betroffene Person nachvollziehbar ist.

Zweckbindung – Mit Einschränkungen ist die Weiterverarbeitung personenbezogener Daten für Archivzwecke, die im öffentlichen Interesse stehen, nicht unvereinbar mit dem ursprünglichen Zweck der Verarbeitung.

Speicherung – Personenbezogene Daten müssen so gespeichert werden, dass die Identifizierung der betroffenen Person nur so lange ermöglicht wird, wie es für die Zwecke der Verarbeitung notwendig ist.

Rechenschaftspflicht – Der Verantwortliche ist für die Einhaltung der Grundsätze und den Nachweis der Einhaltung verantwortlich.

Organisatorische Maßnahmen

Organisatorische Strukturanforderungen

Nach Vorgaben der DSGVO müssen Sie eine Reihe an Maßnahmen umsetzen, um die Risiken einer Datenschutzverletzung zu minimieren und nachzuweisen, dass Sie Daten-Management ernst nehmen. Zu den erforderlichen Maßnahmen im Rahmen der Rechenschaftspflicht zählen: **Datenschutz-Folgenabschätzung, Überprüfungen, Tätigkeitsberichte und (gegebenenfalls) Benennung eines Datenschutzbeauftragten.**

➡ Datenschutzbeauftragter	WEITERE INFORMATIONEN:
➡ One-Stop-Shop-Prinzip	WEITERE INFORMATIONEN:

Verarbeitungen, Verfahren und Maßnahmen

➡ Verletzung des Schutzes personenbezogener Daten	WEITERE INFORMATIONEN:
➡ Datenschutz durch Technikgestaltung	WEITERE INFORMATIONEN:
➡ Datenschutz-Folgenabschätzung	WEITERE INFORMATIONEN:
➡ Internationale Datenübermittlung (gruppenintern/an externe Entitäten)	WEITERE INFORMATIONEN:

Sensibilisierung für Datenschutz

➡ Intern – Mitarbeiter	WEITERE INFORMATIONEN:

Technische Maßnahmen

Rechenschaftspflicht – technische Maßnahmen

Die DSGVO nimmt Verantwortliche in die Pflicht, die Einhaltung der Datenschutzgrundsätze jederzeit nachweisen zu können. Sie müssen bei möglichen Anfragen einer nationalen Aufsichtsbehörde klare Richtlinien vorweisen, die den geforderten Standard einhalten. Dies betrifft die Überwachung, Prüfung und Bewertung Ihrer Datenverarbeitungsprozesse, die Umsetzung von Schutzmaßnahmen und umfassende Schulungen der Mitarbeiter zu ihren Pflichten.

Datenschutzverletzung – technische Maßnahmen

Beugen Sie unter Einsatz von **angemessenen Maßnahmen und getesteten Verfahren** Datenschutzverletzungen vor (definiert als *"eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden"*), um **schnell reagieren und einen Vorfall gemäß der Vorschriften umgehend melden zu können.**

Erfolgt die Schadensmeldung nicht im geforderten Zeitraum, sieht das Gesetz hohe Strafen und Bußgelder vor.

Gewährleistung der Rechte betroffener Personen

Die DSGVO stärkt die Rechte betroffener Personen , zum Beispiel mit dem Recht auf Auskunft zu ihren erhobenen Daten, dem Recht auf Zugang unter bestimmten Umständen sowie dem Recht auf Berichtigung der Informationen.

➡ Auskunftsrecht der betroffenen Personen	WEITERE INFORMATIONEN:
➡ Recht auf Löschung („Recht auf Vergessenwerden")	WEITERE INFORMATIONEN:
➡ Automatisierte Entscheidungen und Profiling	WEITERE INFORMATIONEN:
➡ Datenübertragbarkeit	WEITERE INFORMATIONEN:
➡ Widerspruchsrecht (einschließlich Widerspruch gegen Direktwerbung)	WEITERE INFORMATIONEN:

Vermittlung von Datenschutz-Informationen (Einwilligung, Aufklärung über Verarbeitung)

➡ Einwilligung	WEITERE INFORMATIONEN:
➡ Elterliche Einwilligung	WEITERE INFORMATIONEN:
➡ Informationspflicht	WEITERE INFORMATIONEN:

Datensicherheit (Integrität und Vertraulichkeit)

In der DSGVO wird ein Teil der Datenschutzregeln aus den bestehenden Vorgaben beibehalten, wie z.B.: Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz; Zweckbindung; Datenminimierung; Datenqualität; Sicherheit, Integrität und Vertraulichkeit.

Sie müssen sicherstellen, dass die **Verarbeitung personenbezogener Daten stets angemessen geschützt ist, insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigter Zerstörung, Schädigung oder unbeabsichtigtem Verlust:** *"der Verantwortliche und der Auftragsverarbeiter [treffen] geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten".*

In der Verordnung werden **eine Reihe an Maßnahmen genannt, mit denen die Datensicherheit gewährleistet werden soll**, einschließlich: Pseudonymisierung und Verschlüsselung; Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung, wie wirksam die technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit in der Informationsverarbeitung sind.

➡ Verschlüsselung

Die DSGVO nennt ausdrücklich Verschlüsselung als eine Methode zur Einhaltung einiger Regelungen.

Artikel 32 – **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 unter anderem Folgendes ein:
a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten (...)".

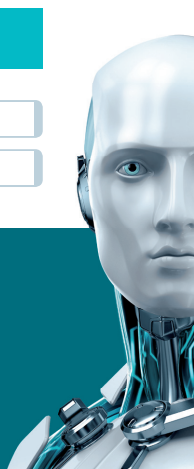
Artikel 34 – **Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person:**

"3. Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:
a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, **durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung** (...)".

Maßnahmen auf Datenebene

Datendokumentation, Rechtmäßigkeit und Überprüfungen

➡ Existenz und Klassifizierung von personenbezogenen Daten	WEITERE INFORMATIONEN:
➡ Rechtmäßigkeit der Verarbeitung personenbezogener Daten	WEITERE INFORMATIONEN:



ENJOY SAFER TECHNOLOGY™

ESET Deutschland GmbH
Spitzweidenweg 32 | 07743 Jena
Tel.: +49 3641 3114 220 | Fax: +49 3641 3114 229, www.eset.de