KISA

Datenschutz gemäß EU-DSGVO

Valentin Brinster
Radebeul, den 13. Februar 2019

kisa.it

KISA

Vorwort

*„Angesichts einer **Vielzahl technischer und medialer Innovationen** ist die informationelle Selbstbestimmung der Bürgerinnen und Bürger wichtig und problematisch zugleich. Im Berufs- und Privatleben, gegenüber Unternehmen, Verwaltungs- und Gesundheitsbehörden, im Umgang mit der vernetzten Öffentlichkeit des Internets oder als Person in öffentlichen Räumen: **Überall werden Daten unterschiedlichster Art erhoben, gespeichert, verknüpft, zusammengeführt und kombiniert**.*

***Für den Einzelnen ist nicht mehr überschaubar, wer wann welchem Personenkreis gegenüber welche personenbezogenen Daten preisgibt und für welche Zwecke sie verwendet werden**. Dadurch droht der Abbau oder Zerfall eines **Grundrechts unserer Gesellschaft**: die Möglichkeit und Fähigkeit, selbstbestimmt entscheiden zu können, wer Zugang zu Informationen über die eigene Person besitzt; mithin: **die eigene Privatsphäre vor unerwünschten Zugriffen zu schützen**.“*

KISA

Agenda

- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

KISA

Warum Datenschutz?

Interessenten an personenbezogenen Daten:

- Staat
  - Funktionieren der öffentlichen Verwaltung
  - Beeinflussung des Einzelnen im Sinne des jeweils Regierenden
- Unternehmen
  - Datensammler, Datenhändler
  - Beeinflussung des Einzelnen im Sinne des Einzelunternehmens
- Privatpersonen
  - Zugriff auf die riesige Menge der pbD im Netz
  - Einsatz zu persönlichen Zwecken

Schutz des Einzelnen durch den Schutz seiner Daten.

- Charta der Grundrechte der Europäischen Union
  - Kap. II Art. 7 (Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.)
  - Kap. II Art. 8 (Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten)
- Grundgesetz der Bundesrepublik Deutschland
  - allgemeines Persönlichkeitsrecht
  - Recht auf informationelle Selbstbestimmung
- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)

KISA

Agenda

- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

KISA

Wer oder was wird durch die DSGVO geschützt?

Die DSGVO enthält Vorschriften zum:

- Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
- Schutz der Grundrechte und Grundfreiheiten natürlicher Personen.
- Schutz deren Rechtes auf Schutz personenbezogener Daten.

… aber auch

- Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

KISA

Agenda

- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

KISA

Grundlagen des Datenschutzes nach der DSGVO

Grundsätze der DSGVO :

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glauben
- Transparenz

} auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden

- Zweckbindung } für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden
- Datenminimierung } dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein
- Richtigkeit } sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein
- Speicherbegrenzung } in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist
- Integrität
- Vertraulichkeit

} eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen

- Rechenschaftspflicht } Der Verantwortliche ist für die Einhaltung der Grundsätze verantwortlich und muss deren Einhaltung nachweisen können

KISA

Grundlagen des Datenschutzes nach der DSGVO

Rechte der betroffenen Person :

- Art. 12 DSGVO Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person
- Art. 13 DSGVO Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
- Art. 14 DSGVO Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
- Art. 15 DSGVO Auskunftsrecht der betroffenen Person
- Art. 16 DSGVO Recht auf Berichtigung
- Art. 17 DSGVO Recht auf Löschung ("Recht auf Vergessenwerden")
- Art. 18 DSGVO Recht auf Einschränkung der Verarbeitung
- Art. 19 DSGVO Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
- Art. 20 DSGVO Recht auf Datenübertragbarkeit
- Art. 21 DSGVO Widerspruchsrecht (gegen die Verarbeitung nach Art. 6 e, f)
- Art. 22 DSGVO Automatisierte Entscheidungen im Einzelfall einschließlich Profiling (nicht unterworfen werden)
- Art. 23 DSGVO Beschränkungen (der Rechte)

KISA

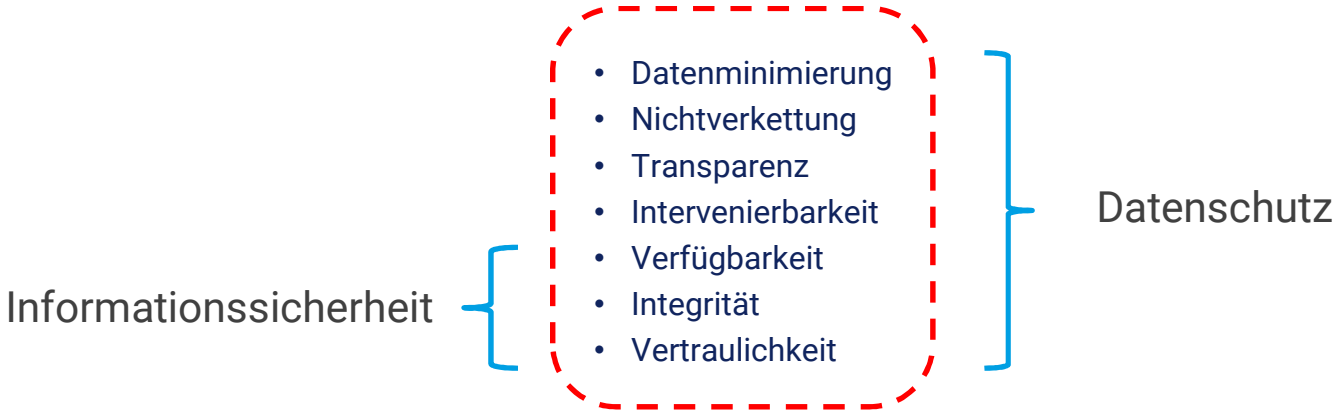
Agenda

- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

KISA

Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes

Gewährleistungsziele :



KISA

Agenda

- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

KISA

Unterscheidung von IT-Grundschutz und operativem Datenschutz

	IT-Sicherheit	Datenschutz
Schutzzweck	dient dem Interesse der datenverarbeitenden Stelle	dient dem Interesse des Betroffenen (und der Gesellschaftsstruktur)
Funktion	schützt vor dem Verlust der Vertraulichkeit, Integrität und Verfügbarkeit	schützt vor technischem Determinismus, Intransparenz und ungerechtfertigten Verkettung von Daten, Prozessen und Ereignissen mit Personenbezug
Maßnahmen	IT-Sicherheitsmaßnahmen realisieren auch Datenschutz	Datenschutzmaßnahmen realisieren auch IT-Sicherheitsmaßnahmen
Anwendungsbereich	bezieht sich auf automatisierte Datenverarbeitung	bezieht sich auf alle Verarbeitungsarten

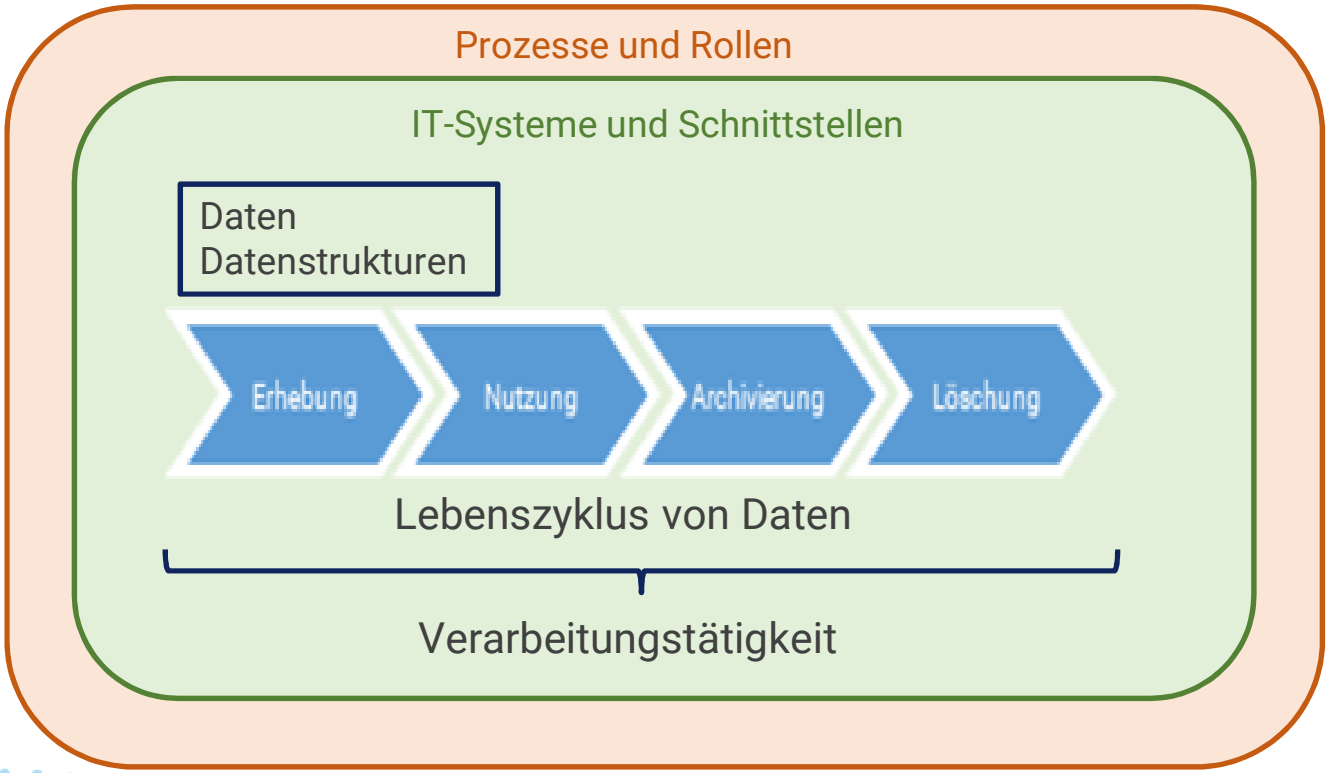
KISA

Agenda

- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

KISA

Verfahrenskomponenten: Daten, Systeme, Prozesse



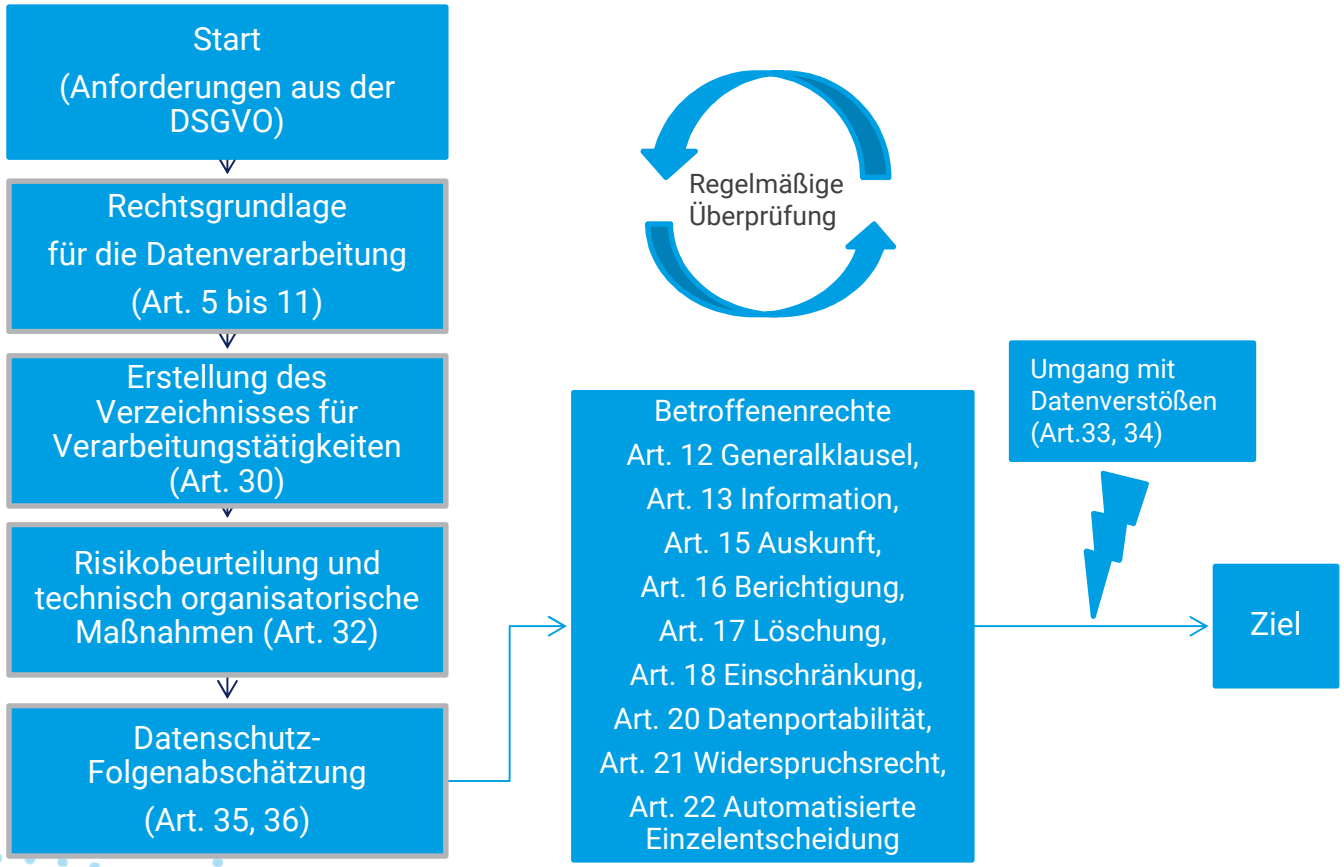
KISA

Agenda

- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

KISA

Prozessablauf DSGVO

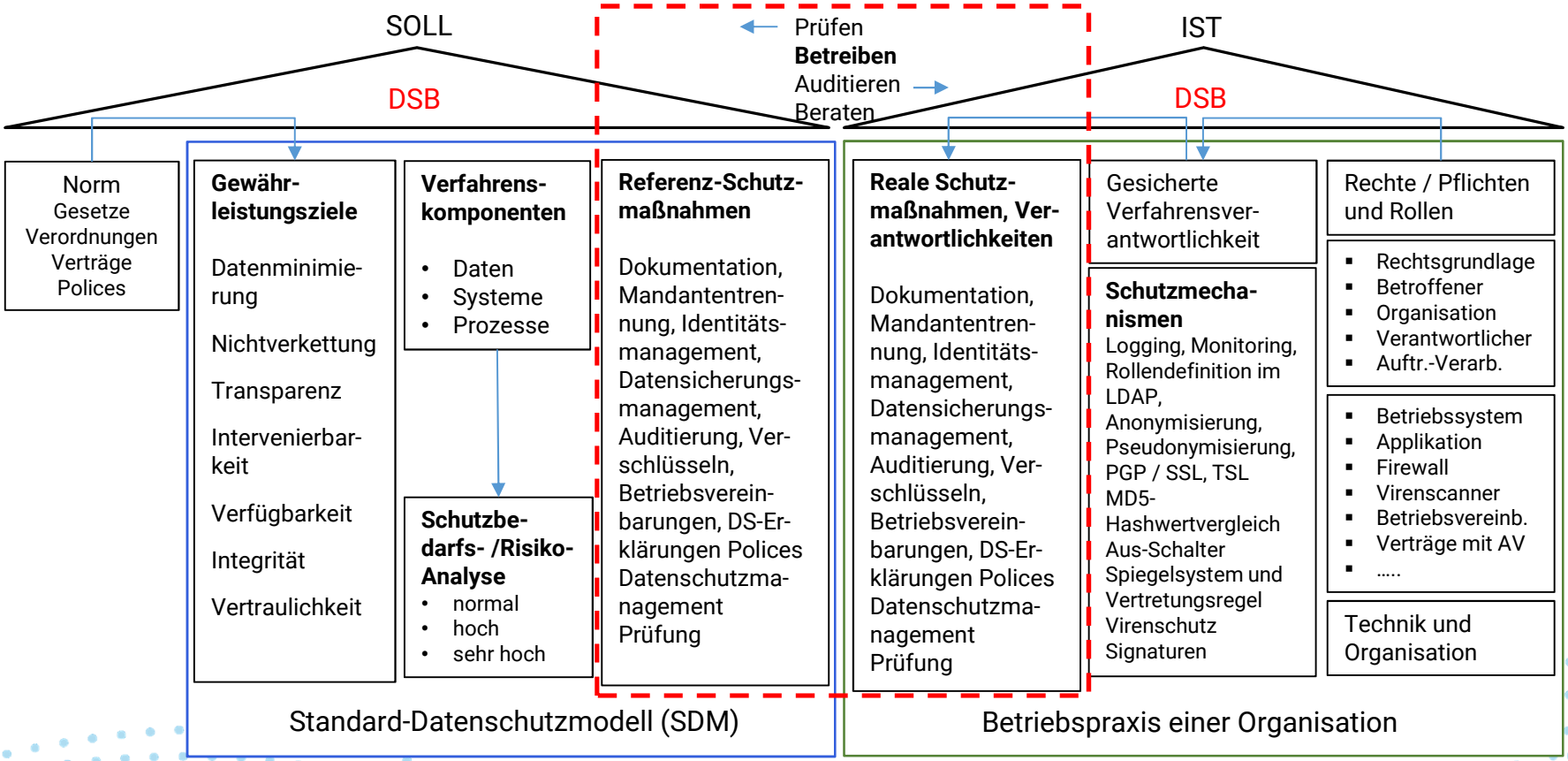


KISA

Agenda

- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

Anwendung des Standard-Datenschutzmodells „SDM“



KISA

Agenda

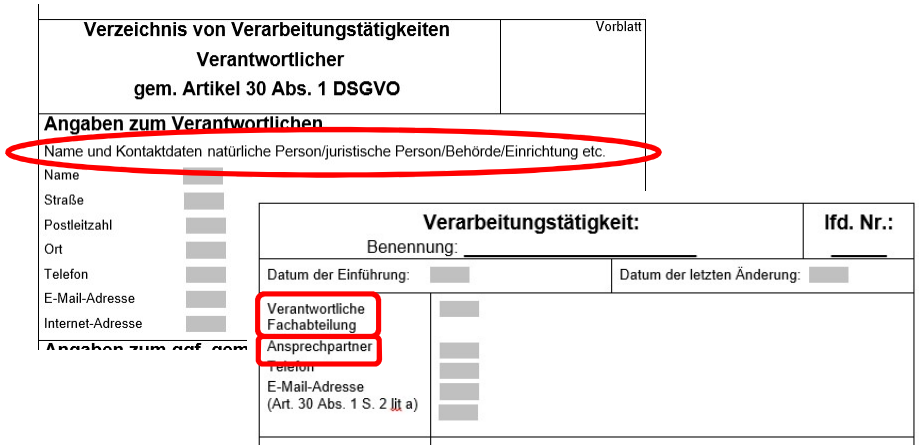
- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

KISA

Verantwortung des für die Verarbeitung Verantwortlichen

➡ **Verantwortlicher:** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Wie sieht es die Aufsichtsbehörde:



Verzeichnis von Verarbeitungstätigkeiten
Verantwortlicher
gem. Artikel 30 Abs. 1 DSGVO

Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name
Straße
Postleitzahl
Ort
Telefon
E-Mail-Adresse
Internet-Adresse

Verarbeitungstätigkeit: Benennung: _____ **lfd. Nr.:** ____

Datum der Einführung:
Datum der letzten Änderung:

Verantwortliche Fachabteilung
Ansprechpartner
Telefon
E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)

KISA

Verantwortung des für die Verarbeitung Verantwortlichen

Erhöhte Anforderungen durch EU-DSGVO! (Art. 5)

(NEU: Die Einhaltung der DSGVO-Grundsätze ist nachzuweisen, Rechenschaftspflicht)

• Rechenschaftspflicht bedeutet dokumentiertes Vorgehen und Change Management

- Verzeichnis von Verarbeitungstätigkeiten ist anzulegen (Art. 30 DSGVO)
- Erfassung und Risikobeurteilung der technisch organisatorischen Maßnahmen (Art. 32 DSGVO)
- Datenschutzfolgeabschätzung (Art. 35, 36 DSGVO)
- Dokumentation der Auftragsverarbeitung (Art. 28 DSGVO)
- Konzept zum Umgang mit Datenschutzverletzungen (Art. 33 DSGVO)
- Konzept für die Auskunftserteilung (Art. 12 DSGVO)
- Löschkonzept (17 DSGVO)
- technisch:
  - IT-Sicherheitskonzept
  - Konzept technisch-organisatorische Maßnahmen
  - Prozessübersichten
  - Netzwerkpläne etc.

KISA

Agenda

- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

KISA

Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?

Aufgaben für die Kommunen im Zusammenhang mit der Umsetzung der Vorgaben aus der Datenschutz-Grundverordnung.

1) Benennung eines Datenschutzbeauftragten entsprechend des Art. 37 Abs. 1 lit. a DSGVO
2) Umsetzung aller Vorgaben der Datenschutz-Grundverordnung (Initialprojekt)

Vorschlag KISA:

zu 1)

- Wir übernehmen für Sie die Aufgaben des Datenschutzbeauftragten auf der Grundlage des Art. 37 Abs. 6 DSGVO

zu 2)

- Wir unterstützen Sie bei der Umsetzung des Initialprojektes:
  1. im Rahmen eines Projektes mit unserer Begleitung über die Projektdauer
  2. mit Beratungsleistungen auf Abruf bei der selbstständigen Durchführung des Initialisierungsprojektes

KISA

Agenda

- Warum Datenschutz?
- Wer oder was wird durch die DSGVO geschützt?
- Grundlagen des Datenschutzes nach der DSGVO
- Nachweis von Maßnahmen für die Gewährleistung des Datenschutzes
- Unterscheidung von IT-Grundschutz und operativem Datenschutz
- Verfahrenskomponenten: Daten, Systeme, Prozesse
- Prozessablauf DSGVO
- Anwendung des Standard-Datenschutzmodells „SDM“
- Verantwortung des für die Verarbeitung Verantwortlichen
- Wie können wir Sie bei der Umsetzung der DSGVO unterstützen?
- mögliche Kombinationen der angebotenen Leistungen

KISA

Mögliche Kombinationen der angebotenen Leistungen

- Beratungsleistungen ohne Stellung eines ext-DSB
- Kombination 1
  - Anlage 1 Beratung/Unterstützung/konzeptionelle Vorplanung
  - Anlage 2 ext-DSB incl. für die Projektlaufzeit
- Kombination 2
  - Anlage 1a Beratung
  - Anlage 2a ext-DSB Vertrag
- Kombination 3 (nach Art. 37 Abs. 3)
  - Anlage 1 Beratung/Unterstützung/konzeptionelle Vorplanung (geteilt zw. beteiligten Kommunen)
  - Anlage 2a ext-DSB Vertrag (separat pro Kommune)
- Kombination 4 (nach Art. 37 Abs. 3)
  - Anlage 1a Beratung (geteilt zw. beteiligten Kommunen)
  - Anlage 2a ext-DSB Vertrag (separat pro Kommune)

KISA

Mögliche Kombinationen für Verbandsmitglieder

		Umsetzung Systemimplementierung			
		Anlage 1 Beratung/ Unterstützung/ konzeptionelle Vorplanung	Anlage 1a	Anlage 1 (nach Art. 37 Abs. 3)	Anlage 1a (nach Art. 37 Abs. 3)1234
Benennung eines DSB	ext-DSB incl. (Anlage 2)	30.000,00 €	-	-	-
	ext-DSB (Anlage 2a) Bsp. für 10.000 EW	-	3.500,00 € + Aufwand	30.000,00 € / n zzgl. 2.500,00 € * n	(1.000,00 € + Aufwand) / n zzgl. 2.500,00 € * n
	int-DSB	30.000,00 €	1.000,00 € + Aufwand	30.000,00 € / n	(1.000,00 € + Aufwand) / n

n = Anzahl der Gemeinden im Sharing-Modell

KISA

Ihr Ansprechpartner

Valentin Brinster
Datenschutzbeauftragter
Tel.: +49 351 86652-442
Mobil: +49 151 55038301
E-Mail: valentin.brinster@kisa.it

Ich freue mich auf gute Gespräche mit Ihnen.