ingra
Unternehmensberatung GmbH

DSGVO und ihre Auswirkungen

Zusammenfassung der Highlights

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

Ihr externer Datenschutzbeauftragter

Name: Jörg Iffländer

Baujahr: 1961

Kompetenzen: Dipl. Inform.

Fachkundezertifikat DS-GVO & BDSG
Certified Lead Auditor ISO/IEC 27001
Certified ITIL Expert
Certified ISO/IEC 20000 Manager and Consultant professional Level
Certified Prince2 Practitioner
Certified Prince2 agile Practitioner
Certified Business Process Professional
Certified Professional for Requirements Engineering

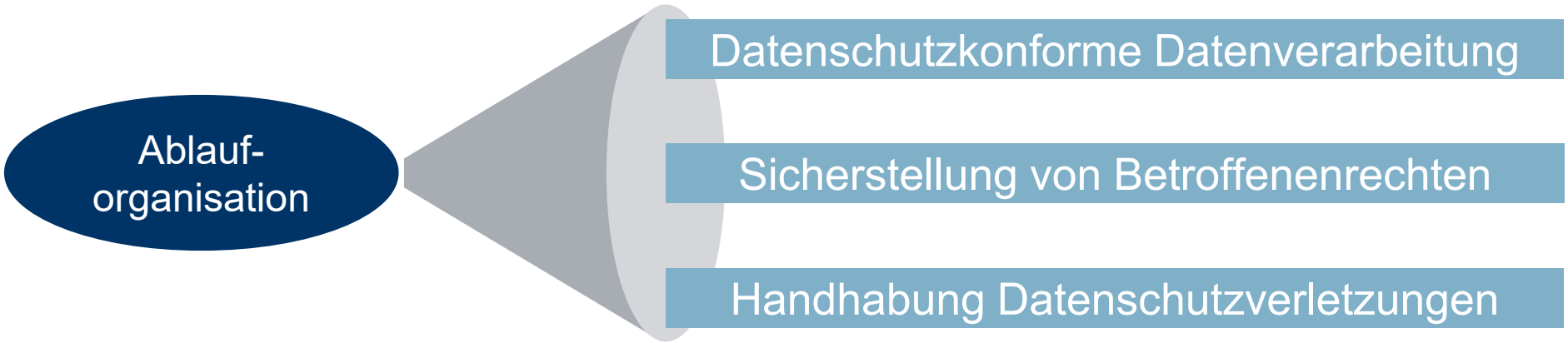
Schwerpunkte: Datenschutz
Informationssicherheit
IT Projektmanagement

Begriffsbestimmungen

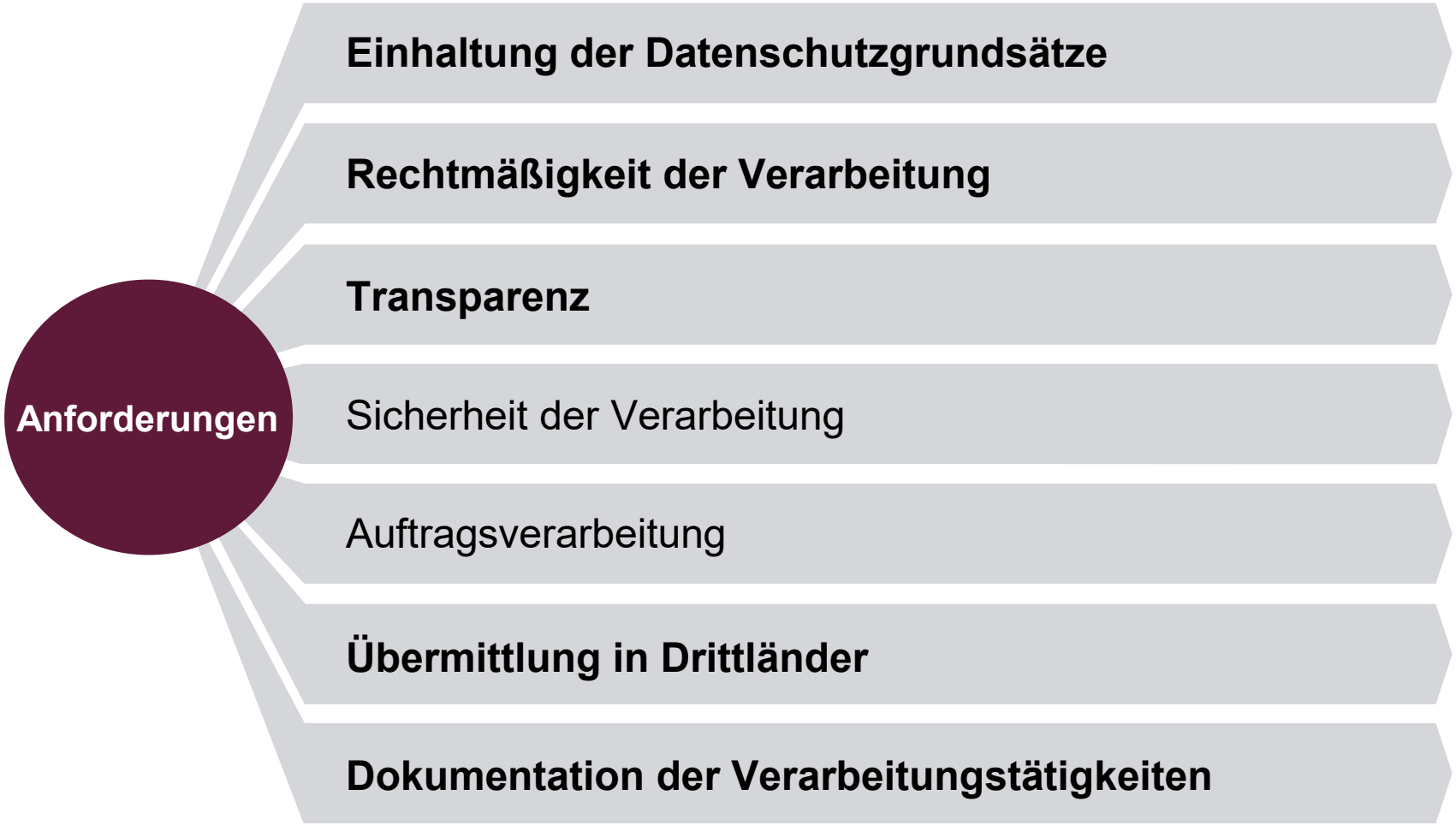
Wesentliche Änderungen

- Rechenschaftspflicht
- Rechtmäßigkeit der Verarbeitung
- Einwilligungen
- Anwendungsbereich
- Sanktionen

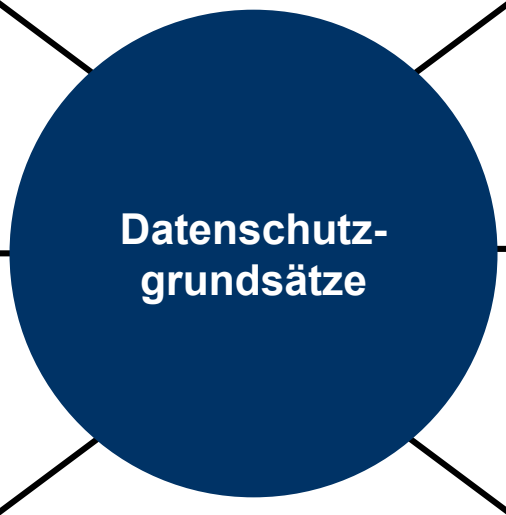
Datenschutz-Kernprozesse



KP: Datenschutzkonforme Datenverarbeitung



KP: Datenschutzkonforme Datenverarbeitung
Einhaltung der Datenschutzgrundsätze



Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

- Rechtsgrundlage der Verarbeitung?
- Risiken für Betroffene ausreichend bedacht?
- Verarbeitung für Betroffenen transparent?

Richtigkeit

- Sind die Daten richtig?
- Können unrichtige Daten unverzüglich gelöscht oder berichtigt werden?

Zweckbindung

- Zwecke festgelegt und dokumentiert?
- Erfolgt Verarbeitung nur für die eindeutig festgelegten und mitgeteilten Zwecke erfolgt?

Speicherbegrenzung

- Speicherung nur so lange, wie dies für die Zwecke erforderlich ist?
- Festlegung Lösch- und Speicherfristen. Rechtsgrundlage?
- Keine „Vorratsdatenspeicherung“

Datenminimierung

- Werden nur Daten verarbeitet, die für den festgelegten Zweck angemessen und auch wirklich erforderlich sind?
- Ist die Verarbeitung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt?

Integrität und Vertraulichkeit

- Wird eine angemessene Sicherheit der Daten gewährleistet?

KP: Datenschutzkonforme Datenverarbeitung
Rechtmäßigkeit der Verarbeitung

Verbot mit Erlaubnis-vorbehalt

- Einwilligung der betroffenen Person
- Notwendig zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen
- Vorliegen einer rechtlichen Verpflichtung zur Verarbeitung
- Schutz lebenswichtiger Interessen
- Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt
- Berechtigte Interessen, sofern nicht die Interessen oder Grundfreiheiten der betroffenen Person überwiegen

KP: Datenschutzkonforme Datenverarbeitung Transparenz

Informations-pflicht I

- Name und Kontaktdaten der/des Verantwortlichen
- Kontaktdaten der/des Datenschutzbeauftragten
- Zwecke der Verarbeitung und Rechtsgrundlage
- Empfänger bzw. Kategorien von Empfängern
- (Absicht der) Übermittlung in ein Drittland
- Speicherdauer
- Hinweis auf Rechte betroffener Personen

KP: Datenschutzkonforme Datenverarbeitung Transparenz

Informations-pflicht II

- Recht auf Widerruf einer Einwilligung
- Recht auf Beschwerde bei einer Aufsichtsbehörde
- Rechtsgrundlage. Möglichen Folgen einer Nichtbereitstellung
- Hinweis auf das Bestehen einer automatisierten Entscheidungsfindung
- Bei der Erhebung der personenbezogenen Daten von einem Dritten Angabe der Quelle der Daten

Beabsichtigt der Verantwortliche die personenbezogenen Daten später für einen anderen Zweck als den ursprünglich festgelegten zu verarbeiten, so erfordert dies vorab eine erneute Information des Betroffenen (und bedarfsweise eine neue Einwilligung).

KP: Datenschutzkonforme Datenverarbeitung Übermittlung in Drittländer

Räumlicher Anwendungsbereich

Niederlassungsprinzip

- Verarbeitungen im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder Auftragsverarbeiters in der EU

Marktortprinzip

Verarbeitungen personenbezogener Daten betroffener Personen, die sich in der EU befinden in

- Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen
- Beobachten von Verhalten […]

KP: Datenschutzkonforme Datenverarbeitung Übermittlung in Drittländer

Risiko: das Drittland hat kein gleichwertiges Datenschutzniveau

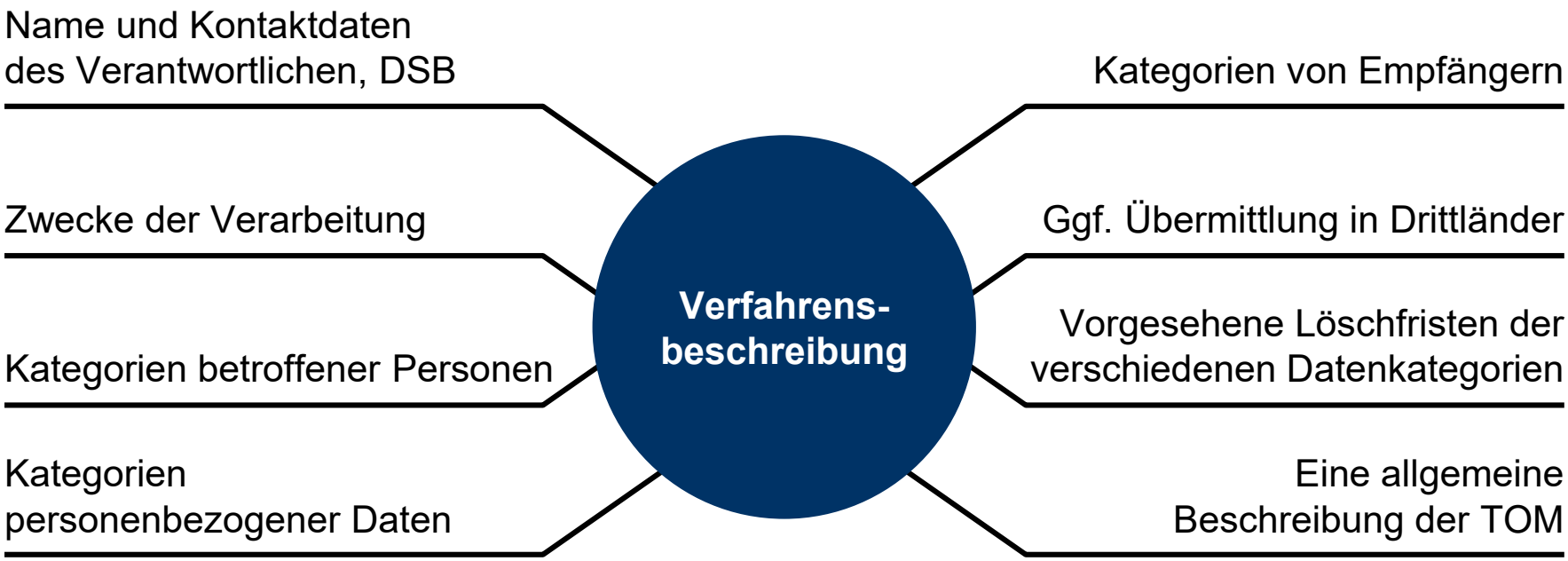
Nur zulässig durch

- Angemessenheits-beschluss der EU-Kommission
  - Länderliste
  - Privacy shield

- Geeignete Garantien
  - Standardvertragsklauseln
  - Binding Corporate Rules
  - Genehmigte Verhaltensregeln

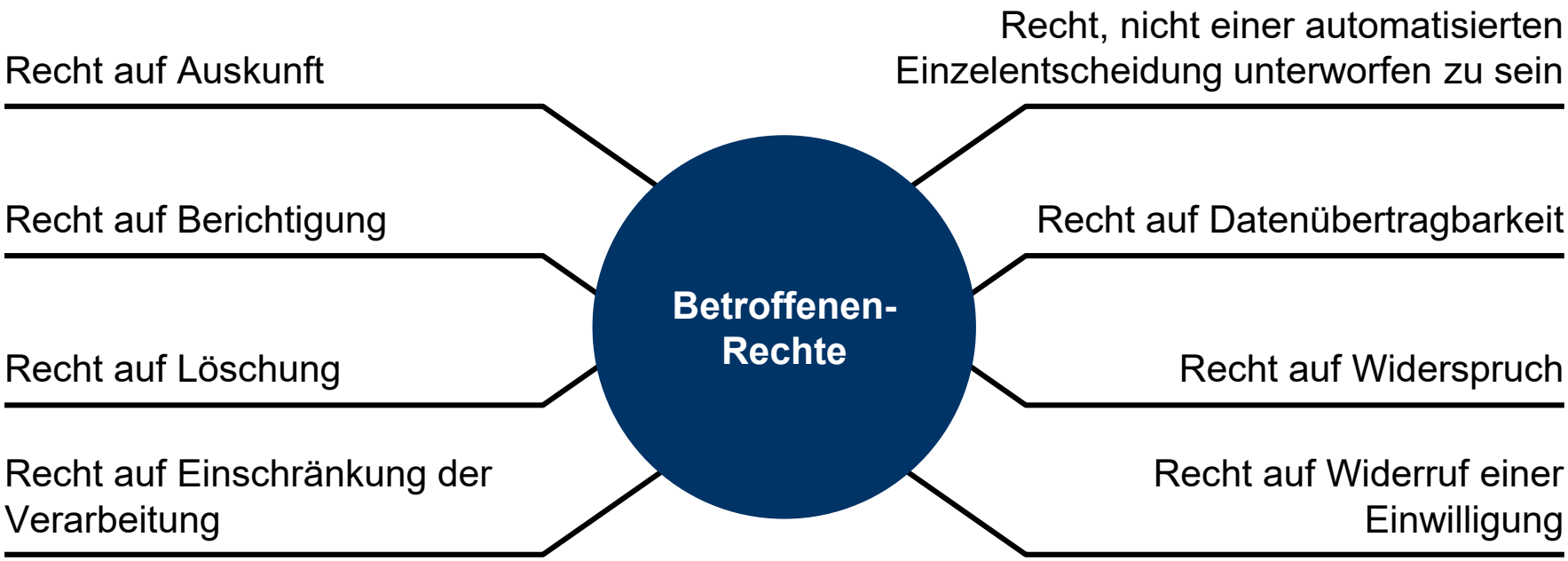
- Ausnahmen
  - „Ausdrückliche" Einwilligung
  - Vertragserfüllung
  - Im Betroffeneninteresse
  - Wichtige Gründe öffentlichen Rechts
  - […]

KP: Datenschutzkonforme Datenverarbeitung
Dokumentation der Verarbeitungstätigkeiten



Ein Muster findet sich bei den Materialien

KP: Sicherstellen der Betroffenenrechte



KP: Handhabung von Datenschutzverletzungen

Datenschutzverletzung ist eine Verletzung der Sicherheit, die…

- **ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust oder zur Veränderung (Verlust der Verfügbarkeit bzw. Integrität) oder**
- **zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten (Verlust der Vertraulichkeit) führt**

Meldung an Aufsichtsbehörde

- Faktisch jede Datenschutzverletzung
- Unverzüglich, spätestens nach 72 Stunden
- Vorgeschriebener Inhalt

Information von Betroffenen

Bei voraussichtlich hohem Risiko für die Betroffenen (mit festgelegten Ausnahmen)

- unverzüglich
- Vorgeschriebener Inhalt

Prozess inkl. Dokumentation entwickeln und etablieren

Risikomanagement

Anforderungen an Verantwortlichen

- Risikobeurteilung anhand objektiver Bewertung
- Systematische Identifikation von Risiken, die mit einer Verarbeitung verbunden sind
- Analyse der Risiken hinsichtlich Eintrittswahrscheinlichkeit und Schwere der Folgen
- Qualitative Risikoklassifizierung (Feststellung, ob Risiko oder hohes Risiko)
- Risikobehandlung durch geeignete (und wirksame) Maßnahmen

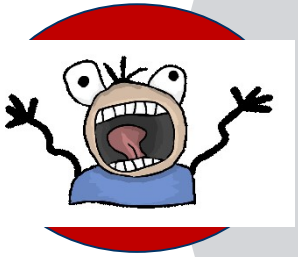
Risikomanagement
Datenschutzfolgenabschätzung bei hohem Risiko

- Schwellwertanalyse, d.h. Ermittlung der Notwendigkeit einer DSFA
- Vorbereitung der DSFA
- Durchführung der DSFA
- Nachverfolgung der DSFA

Datenschutzbeauftragte*r

- Interne*r oder externe*r DSB
- Konzern-DSB möglich, „one-stop-shop" Prinzip
- Weisungsfrei, → Kündigungsschutz
- Unterrichtung und Beratung, Überwachung
  AP für Aufsichtsbehörde und Betroffene
- Qualifikation

Ihr Weg zur DSGVO
Vorweg die Panik-Aktionen



DSB benennen und melden (ab 25.05.)

Datenschutzerklärung auf Webseite

Formulare auf Webseite
- https://
- opt-in
- Datenschutzhinweis

Tracker auf Webseite prüfen

Ihr Weg zur DSGVO
und nun geordnet zur Datenschutz-Compliance

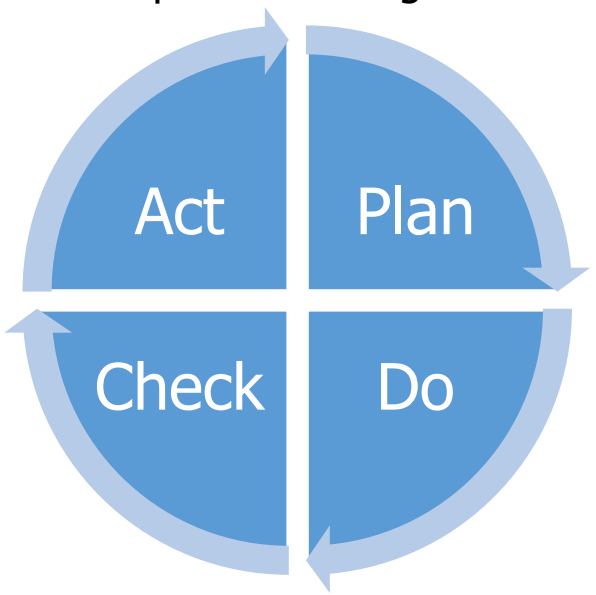
Materialien zum Download

www.ingra.gmbh/materialien

Backup

Aufbau Datenschutzmanagementsystem

Die DS-GVO fordert eine kontinuierliche Überarbeitung und Kontrolle der Verfahren und Prozesse zum Schutz personenbezogener Daten (Datenschutz Compliance Management System).



- Einrichten eines Dokumentationssystems
- Festlegen von Prüfzyklen
- Festlegen von Prüfungsmaßnahmen
- Festlegen von Prüfungsverantwortlichen
- Klassischer P-D-C-A Zyklus wie bei anderen Systemen

- Datenschutzorganisation zur Sicherstellung der Anforderungen wie Meldepflicht und Auskunftsersuchen