DAS NEUE EUROPÄISCHE DATENSCHUTZRECHT – CHANCEN, RISIKEN UND NEBENWIRKUNGEN –

So bekommen Sie den Datenschutz im Unternehmen sicher in den Griff!

Gemeinsamen Veranstaltung der Wirtschaftsförderungsgesellschaft Untere Saar mbH (WFUS) und dem Verband Saarlouis für Handel, Handwerk, Industrie und Freie Berufe

TÜV NORD

WAS WERDEN SIE SEHEN

1. Motivation
2. Handlungsfelder
3. Empfehlungen

GRUNDSÄTZE DER DATENSCHUTZKONFORMEN VERARBEITUNG (ART. 5 DSGVO)

- Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Datenrichtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit im Sinne von IT-Sicherheit
- Verantwortlichkeit, Dokumentation

SELBSTERKENNTNIS UND TRANSPARENZ BEIM „SCHUTZ VON DATEN“

- Selbsterkenntnis hat viel mit Transparenz zu tun.
- Transparenz bedeutet u. a. „Durchsichtigkeit“.
- Denn erst wenn man (bei sich selber und seiner IT) „durchblickt“, ist man in der Lage zu gewährleisten, dass die Datenverarbeitung regelkonform ablaufen wird.
- Erst dann ist man auch in der Lage, andere (evtl. Betroffene, neutrale Entitäten etc.) über die relevanten Aspekte der Datenverarbeitung zu informieren.
- Transparenz ist deshalb eine der wesentlichen Säulen des „Schutzes von Daten“ und des „Datenschutzes“.

TRANSPARENZ IN DER DSGVO

- Konkret nach Art. 5 Abs. 1 lit. a) DSGVO

  „*Personenbezogene Daten müssen in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden*“ (Anforderung ohne Grundbedingung zu benennen)
- Die DSGVO beinhaltet damit in Art. 5 den Programmsatz, der sich wie ein roter Faden durch die DSGVO zieht …

TRANSPARENZANFORDERUNGEN IN DER DSGVO

- Transparenzanforderungen lassen sich mittel- und unmittelbar aus vielen Anforderungen der DSGVO ableiten.
- Ausreichende Transparenz ist z. B. notwendig, um:
  - die Betroffenenrechte der DSGVO zu erfüllen,
  - die von der DSGVO geforderten technisch-organisatorischen Maßnahmen („adäquate / erforderliche Sicherheit“) zu treffen oder
  - die Rechtmäßigkeit der Verarbeitung nachweisen zu können (inkl. Rechenschaftspflicht gem. Art. 5 Abs. 2).
  - Auch das von der DSGVO geforderte Verarbeitungsverzeichnis ist eine Ausformung des Transparenzgrundsatzes.

DAS „NEUE“ VERARBEITUNGSVERZEICHNIS

– WAS ÄNDERT SICH?

- Auch wenn das Konstrukt des Verfahrensverzeichnisses weiterhin gleich bleibt, kommen mit der DSGVO einige wesentliche Änderungen:
  - Grds. sind nun alle relevanten Verfahren / Tätigkeiten im Verzeichnis aufzuführen.
  - Das Verarbeitungsverzeichnis ist grundsätzlich für (den Verantwortlichen und) die Aufsichtsbehörde bestimmt (kein „Jedermannsverzeichnis“ mehr).
  - Ein Auftragsverarbeiter muss nun die Verarbeitungen für den Verantwortlichen aufführen.
  - Das Fehlen bzw. fehlerhafte Führen des Verarbeitungsverzeichnisses ist nun bußgeldbewährt!
  - Es ist nun auch klar geregelt, wer das Verarbeitungsverzeichnis führen muss.

DAS „NEUE“ VERARBEITUNGSVERZEICHNIS

– WAS GEHÖRT HINEIN (VERANTWORTLICHER)?

- Jeder Verantwortliche und ggf. sein Vertreter führt ein (schriftliches / digitales) Verzeichnis aller Verarbeitungstätigkeiten (seines Zuständigkeitsbereichs), das folgende Angaben enthalten muss:
  - den Namen und die Kontaktdaten des / der (gemeinsam) Verantwortlichen, ggf. des Vertreters sowie des Datenschutzbeauftragten (falls bestellt).
  - die Zwecke der (jeweiligen) Verarbeitung (Tätigkeit).
  - Kategorien betroffener Personen und Kategorien personenbezogener Daten.
  - Kategorien von Empfängern.
  - Empfänger in Drittländern oder internationalen Organisationen inkl. der Länderangabe und von „Garantien“.
  - ggf. vorgesehene Fristen für die Löschung.
  - ggf. allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO.

DAS „NEUE“ VERARBEITUNGSVERZEICHNIS

– WAS GEHÖRT HINEIN (AUFTRAGSVERARBEITER)?

- Jeder Auftragsverarbeiter und ggf. sein Vertreter führt ein Verzeichnis zu allen Kategorien der für den Verantwortlichen durchgeführten (Verarbeitungs-) Tätigkeiten (Cross-Check mit Verantwortlichen möglich) und enthält folgende Angaben:
  - den Namen und die Kontaktdaten des Auftragsverarbeiters und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist (ggf. Vertreter) und eines etwaigen Datenschutzbeauftragten.
  - die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden (Fremdverarbeitung).
  - ggf. Übermittlungen von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation (inkl. Drittland inkl. Garantien).
  - ggf. allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

DAS „NEUE“ VERARBEITUNGSVERZEICHNIS

– WIE SOLLTE ICH VORGEHEN? (1)

- Man sollte „planvoll“ vorgehen.
- Alle relevanten Personen mit „ins Boot“ holen und von der Notwendigkeit überzeugen und Verantwortlichkeiten klären.
- Prüfen, ob ein „Verfahrens- / Verarbeitungverzeichnis“ oder sonstige Übersichten vorhanden sind, auf die man aufbauen kann.
- Da die Datenverarbeitung im Wesentlichen mittels IT erfolgt, sollte man praktisch alle der eingesetzten (internen / externen) IT-Komponenten (Soft- / Hardware) inkl. der technisch-organisatorischen Maßnahmen erfassen!

DAS „NEUE“ VERFAHRENSVERZEICHNIS

– WIE GEHE ICH VOR? (2)

- Nachdem die eingesetzte Hard- / Software inventarisiert wurde, gilt es alle „Tätigkeiten“ inkl. der Zwecke zu identifizieren, zu denen die Software eingesetzt wird inkl. der erfolgenden „Datenströme“.
- Bündelung der „Tätigkeiten“ entsprechend des Verarbeitungszwecks.
- Ferner gilt es dabei die Daten / Kategorien der Betroffenen und ggf. Empfänger der Daten zu ergründen.
- Überprüfung in regelmäßigen Abständen inkl. Aktualisierung.
- Somit ist das Verarbeitungsverzeichnis DAS Werkzeug zur Analyse, Dokumentation und Gewährleistung von Transparenz!

DAS „NEUE“ VERFAHRENSVERZEICHNIS

– FAZIT

- Das Verarbeitungsverzeichnis ist ein essenzielles / sinnvolles Instrument zur Schaffung und Gewährleistung von Transparenz und damit zur Schaffung von Selbsterkenntnis.
- Die Erstellung eines ordnungsgemäßen Verzeichnisses bedeutet einen nicht unerheblichen (Mehr-) Aufwand.
- Dieser (Mehr-)Aufwand ist jedoch die „bittere Pille“, die wir schlucken müssen, wenn wir bspw. immer mehr vernetzte, („smarte“) IT (halbwegs) rechtskonform einsetzen wollen!
- Nur durch eigene Selbsterkenntnis (Transparenz) sind wir in der Lage, die gesetzlichen Anforderungen zu erfüllen und damit dem Betroffenen (der jeder von uns sein kann), den notwendigen RESPEKT entgegenzubringen …

HANDLUNGSFELDER

HINSICHTLICH SICHERHEIT DER VERARBEITUNG

- Erwägungsgründe 78, 83 und 84

  Die Erwägungsgründe sind Ziele, die mit der Formulierung der Artikel der EU-Verordnung verfolgt wurden. Sie sind nicht die eigentlichen Rechtsnormen, aber sie sind hilfreich für die Interpretation der Rechtsnormen.

- Art. 5, Art. 25 und Art. 32 DSGVO

DSGVO – ERWÄGUNGSGRUND 78

- Geeignete technische und organisatorische Maßnahmen*

  Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. (…)

* Dieser Titel ist eine inoffizielle Beschreibung des Erwägungsgrundes meinerseits.

DSGVO – ERWÄGUNGSGRUND 83

- Sicherheit der Verarbeitung*

  Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu ihrer Eindämmung, wie etwa eine Verschlüsselung, treffen. Diese Maßnahmen sollten unter Berücksichtigung des Stands der Technik und der Implementierungskosten ein Schutzniveau – auch hinsichtlich der Vertraulichkeit – gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Bei der Bewertung der Datensicherheitsrisiken sollten die mit der Verarbeitung personenbezogener Daten verbundenen Risiken berücksichtigt werden, wie etwa – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, insbesondere wenn dies zu einem physischen, materiellen oder immateriellen Schaden führen könnte.

* Dieser Titel ist eine inoffizielle Beschreibung des Erwägungsgrundes meinerseits.

DSGVO – ERWÄGUNGSGRUND 84

- Risikoevaluierung und Folgenabschätzung*

  Damit diese Verordnung in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, besser eingehalten wird, sollte der Verantwortliche für die Durchführung einer Datenschutz-Folgenabschätzung, mit der insbesondere die Ursache, Art, Besonderheit und Schwere dieses Risikos evaluiert werden, verantwortlich sein. Die Ergebnisse der Abschätzung sollten berücksichtigt werden, wenn darüber entschieden wird, welche geeigneten Maßnahmen ergriffen werden müssen, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit dieser Verordnung in Einklang steht. Geht aus einer Datenschutz-Folgenabschätzung hervor, dass Verarbeitungsvorgänge ein hohes Risiko bergen, das der Verantwortliche nicht durch geeignete Maßnahmen in Bezug auf verfügbare Technik und Implementierungskosten eindämmen kann, so sollte die Aufsichtsbehörde vor der Verarbeitung konsultiert werden.

* Dieser Titel ist eine inoffizielle Beschreibung des Erwägungsgrundes meinerseits.

ART. 5 DSGVO-GRUNDSATZ

ANGEMESSENE SICHERHEIT

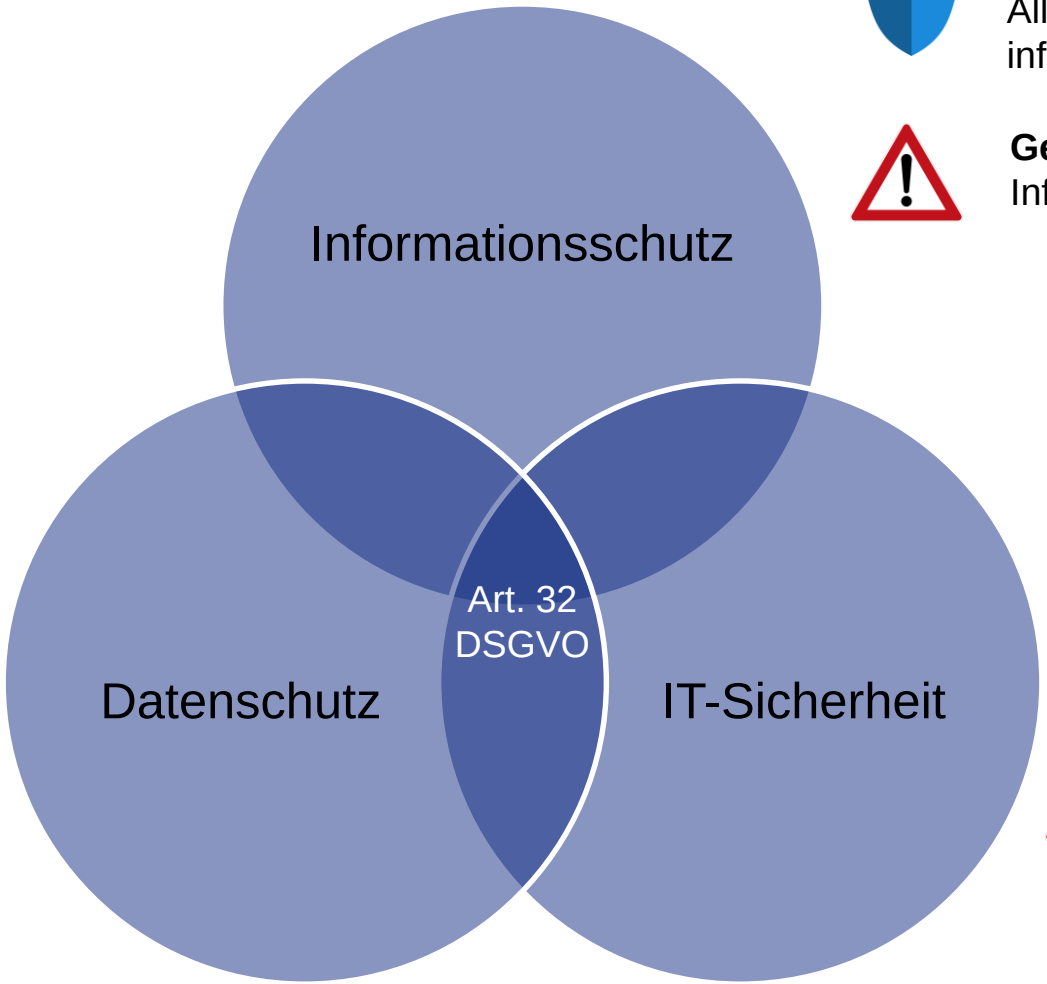
Personenbezogene Daten müssen

(…)

– in einer Weise verarbeitet werden, die 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 („Integrität und Vertraulichkeit“);

- Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

DATENSCHUTZ UND DATENSICHERHEIT (ART. 32 DSGVO)



Schutzobjekt:
Alle Unternehmens-informationen

Gefahr:
Informationsabfluss

Schutzobjekt:
Daten zu einer natürlicher Personen

Gefahr:
Verletzung der Grundrechte und -freiheiten

Schutzobjekt:
System
Prozess
Daten

Gefahr:
Verlust
Missbrauch
Zerstörung

ART. 25 DSGVO – DATENSCHUTZ DURCH

TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

- 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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.
- (…)

Risikoadäquanz

ART. 32 DSGVO – SICHERHEIT DER VERARBEITUNG

- 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:

  (…)

Risikoadäquanz

Angemessene TOMs

ART. 32 DSGVO – SICHERHEIT DER VERARBEITUNG

(…)

a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Sicherheitsmanagement

IT-Sicherheitsziele / Gewährleistungsziele

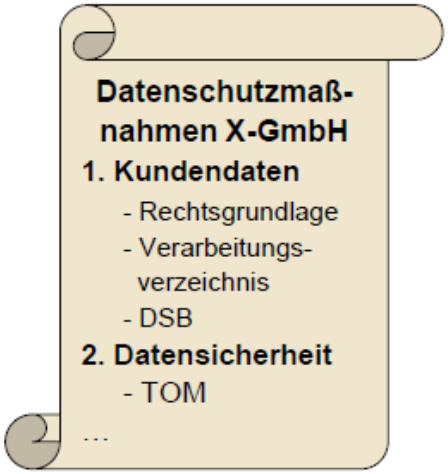
DATENSCHUTZ UND DATENSICHERHEIT (ART. 32 DSGVO)

Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter treffen 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 persönlichen Rechte und Freiheiten geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; **diese Maßnahmen schließen gegebenenfalls Folgendes** ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“

WAS ÄNDERT SICH UND WAS MUSS ICH TUN?

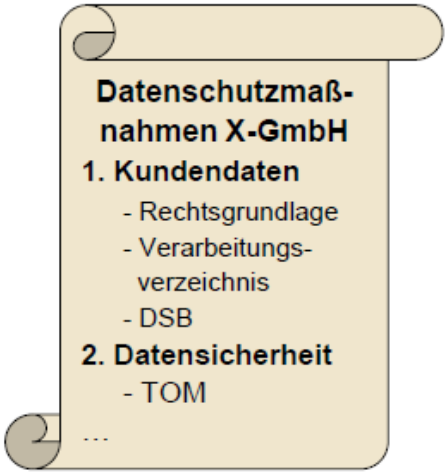
MEHR ORGA = WENIGER ÄRGER!



- **Beweislastumkehr zu Ungunsten datenverarbeitender Unternehmen**
  - Nachweispflicht für Einhaltung DSGVO beim Unternehmen
    - Wie?
      - **Dokumentation** von Datenschutzmaßnahmen
      - datenschutzrelevante Vorgänge im Unternehmen und Datenschutzrisiken identifizieren
      - risikoangemessene Sicherheitsmaßnahmen / Handlungsanleitungen
      - Kontrolle der datenschutzrechtlichen Maßnahmen

WAS ÄNDERT SICH UND WAS MUSS ICH TUN?

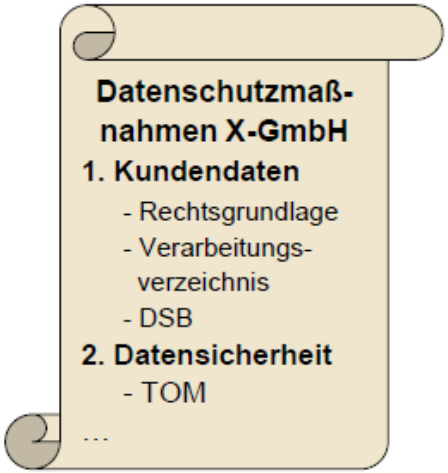
MEHR ORGA = WENIGER ÄRGER!



- **Beweislastumkehr zu Ungunsten datenverarbeitender Unternehmen**
  - Nachweispflicht für Einhaltung DSGVO beim Unternehmen
    - **Datenschutzmanagementsystem**
      - Datenschutzrelevante Prozesse dokumentieren
      - Interne Datenschutz-/ Sicherheitsrichtlinien für wesentliche Datenverarbeitungsvorgänge im Unternehmen
      - Risiko-und Datenschutz-Folgenabschätzungen (bei sensiblen personenbezogenen Daten)
      - umfassende Datenschutzdokumentation
      - Datenschutzschulungen
      - Prozesse für Kontrolle, Optimierung und Anpassung aller Datenschutzmaßnahmen

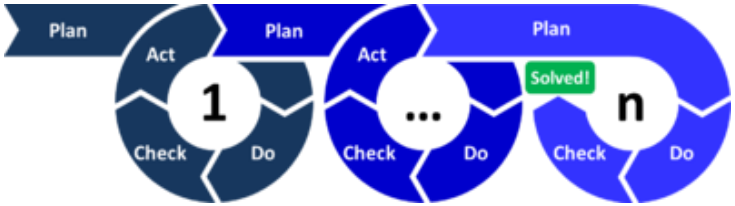
WAS ÄNDERT SICH UND WAS MUSS ICH TUN?

MEHR ORGA = WENIGER ÄRGER!



- **Beweislastumkehr zu Ungunsten datenverarbeitender Unternehmen**
  - Nachweispflicht für Einhaltung DSGVO beim Unternehmen
    - Was?
      - Prozesse mit personenbezogenen Daten
      - Verarbeitungsverzeichnis von Verarbeitungstätigkeiten für jeden Prozess
        - Name / Kontaktdaten des Verantwortlichen sowie des bDSB
        - Zwecke der Verarbeitung
        - Beschreibung der Kategorien betroffener Personen und Kategorien personenbezogener Daten
        - Kategorien von Empfängern
        - ggf. Übermittlungen von personenbezogenen Daten an Drittland
        - Fristen für die Löschung der verschiedenen Datenkategorien
        - allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

ORIENTIERUNG AN MANAGEMENTSYSTEMEN



Plan	Do	Check	Act
Planung und Konzeption	Umsetzung	Erfolgskontrolle und Überwachung	Optimierung und Verbesserung
Risikoorientiert, insbesondere hinsichtlich: 1) Art, Umfang, Umstand und Zweck der Verarbeitung 2) Eintrittswahrscheinlichkeit 3) Risiken für die persönlichen Rechte und Freiheiten	1) Geeignete technische und organisatorische Maßnahmen 2. Datenschutzvorkehrungen 3. Nachweis der Verarbeitung in Übereinstimmung mit der DSGVO	1) Überprüfung der Maßnahmen	1) Aktualisierung der Maßnahmen

Rechenschaftspflicht (Accountability)

Verantwortung und Nachweisführung für die Einhaltung der Prinzipien der DSGVO