Hinweise zur Umsetzung der erweiterten Beratung nach der Präsentation:

PHASE 1 (6 WOCHEN NACH DER PRÄSENTATION):
An diesem Tag werden die Umsetzungen bzw. vorhandenen Dokumente zu folgenden Fragen geprüft oder gemeinsam erstellt:

1. Wie wird sichergestellt, dass die Verarbeitung personenbezogener Daten rechtmäßig erfolgt?

- Prüfung der Prozesse zu den Verarbeitungen mit personenbezogenen Daten. Es sollte eine dokumentierte Analyse aller Verarbeitungen vorliegen. Die Ergebnisse werden nun gruppiert und in die entsprechenden Verarbeitungen übernommen.
- Prüfung der Organisation der Kontrollmaßnahmen (Compliance) und Umsetzung eines Datenschutzmanagementsystems.

2. Erteilung der Einwilligung, Art.7 DSGVO.

- Prüfung der Erhebung der Daten
- Dokumentation der Einwilligung
- Prüfung der Applikationen der Verarbeitung.

3. Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person, Art. 12 DSGVO.

Der Verantwortliche muss danach geeignete Maßnahmen treffen, um dem Betroffenen alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu vermitteln.

4. Einhaltung der Informationspflichten, Art. 13 DSGVO.

Danach müssen die entsprechenden Informationen:

- für den Betroffenen leicht erreichbar,
- in leicht verständlicher Weise und Sprache,
- in schriftlicher oder elektronischer Form verfasst sein.

5. Datenschutz durch Technik, Art.25 DSGVO.

- Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen sind diverse Aspekte wie
  - Stand der Technik,
  - Kosten,
  - Umstände und Zweck der Datenverarbeitung,
  - Eintrittswahrscheinlichkeit und Schwere der Risiken zu berücksichtigen.
- Nach dem Grundsatz „data protection by default“ soll der Datenschutz schon durch entsprechende „Voreinstellungen“ bzw. die Möglichkeit, etwaige Einstellungen in der verwendeten Soft- und Hardware vornehmen zu können, gewährleistet werden. Mittels dieser Maßnahmen soll ferner sichergestellt werden, dass nur die notwendigen Daten auch verarbeitet werden (Datenminimierung) und die Daten nicht von beliebig vielen Personen zur Kenntnis genommen werden können.

PHASE 2: (BERATUNG NACH 10 WOCHEN)

6. Auskunftsrecht der betroffenen Person, Art.15 DSGVO

Mitteilung der Informationen über

- die Verarbeitungszwecke,
- die Kategorien personenbezogener Daten,
- (sämtliche) Empfänger/Kategorien von Empfängern (insbesondere ob Übermittlung in Drittland erfolgt),
- über die bestehenden „Garantien“, falls Daten in ein Drittland übermittelt werden sollen,
- die Speicherdauer inkl. der Kriterien für die Festlegung der Dauer,
- das Recht auf Berichtigung, Löschung, Sperrung, Widerspruch,
- das Beschwerderecht bei der Aufsichtsbehörde,
- die Herkunft der Daten (bei fehlender Direkterhebung),
- ob eine automatisierte Entscheidungsfindung einschließ-

pb-055_10/18

lich Profiling stattfindet.

7. Recht auf Berichtigung und Löschung.
Prüfung der Prozesse bzw. Dokumentation wie ein Betroffener dies beantragen und umsetzen lassen kann!

8. Umsetzung der Speicherbegrenzung, Art. 5 DSGVO.
Beschreiben Sie bitte den Prozess der sicherstellt, dass die Datenspeicherung dem Zweck angemessen und auf das notwendige Maß beschränkt ist.

9. Umsetzung der Sicherheit der Verarbeitung, Art. 32 DSGVO.
Prüfung der Dokumentation ob die technischen und organisatorischen Maßnahmen ausreichen und dokumentiert werden.

10. Auflistung aller Auftragsdatenverarbeiter.
Prüfung der Dokumentation der ADV-Verhältnisse.

11. Umgang mit Datenschutzverletzungen.
Prüfung des Prozesses und die geplante Durchführung im Falle eines Data-Breach-Verfahren.

12. Darstellung der Meldepflicht an Aufsichtsbehörden.
Prüfung der Durchführung der Meldepflicht an die Aufsichtsbehörde

13. Risikobewertung / Datenschutzfolgenabschätzung.
Prüfung, ob die Risikobewertung den Anforderungen der DSGVO entspricht und durchgeführt wurde. Vergleiche die Liste der Verarbeitungen in der Veröffentlichung der entsprechenden Aufsichtsbehörde.

14. Dokumentation von Audits.
Prüfung der Anforderungen an Prüfmaßnahmen Datenschutz- und –sicherheit sowie deren Dokumentation

15. Dokumentation von Awareness-Maßnahmen.
Prüfung ob die Umsetzung der DSGVO nachhaltig in das Bewusstsein der Mitarbeiter verankert und in ein aktives Bewusstsein gefördert wird.

pb-055_10/18

TÜV Rheinland Akademie
Am Grauen Stein
51105 Köln
akademie.tuv.com

TÜVRheinland®
Genau. Richtig.