Beratungsprotokoll Datenschutz und IT-Sicherheit nach DSGVO und BDSG neu

Zwischen

Kunde	Fachhändler

Die DS-GVO gilt für jede Person oder Organisation, die personenbezogene Daten elektronisch oder nicht automatisiert in einer strukturierten Ablage verarbeitet. Ausgenommen sind nur Verarbeitungen im Rahmen persönlicher oder familiärer Tätigkeiten und einige staatliche Aktivitäten. Betroffen von der DS-GVO sind folglich

- Unternehmen,
- Vereine,
- Verbände,
- Parteien,
- Stiftungen,
- Körperschaften des öffentlichen Rechts und
- Einrichtungen des Bundes, der Länder und Kommunen.

Die Vorschriften der DS-GVO sind von einem Ein-Personen-Unternehmen genauso einzuhalten wie von einem Konzern. Letzterer verfügt jedoch über mehr Ressourcen und zahlt im Zweifel geringere Bußgelder, da der maximale Bußgeldrahmen ab einem Umsatz von 500 Mio. Euro 4 Prozent des weltweiten Jahresumsatzes beträgt. Für Jahresumsätze unterhalb von 500 Mio. gilt der umsatzunabhängige Maximalbetrag von 20 Mio. Euro.

Der „Verantwortliche“ für den Datenschutz

Der nunmehr als der „Verantwortliche“ bezeichnet wird (Art. 4 Nr. 7), ist 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, wobei z.B. innerhalb eines Unternehmensverbunds auch mehrere als gemeinsam Verantwortliche kooperieren können (Art. 26). Also **Sie**, der Chef, die Geschäftsleitung des Unternehmens.

Bestellpflicht Datenschutzbeauftragter nach DSGVO

Die Pflicht zur Bestellung gilt nun durch die DSGVO europaweit. In Deutschland wird die Bestellpflicht durch Nutzung einer nationalen Öffnungsklausel beibehalten. Die zentrale Meldepflicht des Art. 37 Abs. 7 DSGVO macht die tatsächliche Bestellung aber viel leichter kontrollierbar, so dass eine Aufdeckung einer Unterlassung wahrscheinlich wird. Daher besteht Handlungsbedarf für Unternehmen, die der Verpflichtung bislang noch nicht nachgekommen sind. Nach der Art. 37 EU-DSGVO gilt eine Bestell-Pflicht eines Datenschutzbeauftragten nur noch für Unternehmen deren Kerngeschäft die Überwachung und der Umgang mit personenbezogenen Daten ist**.** Dies reduziert die Zahl der zur Bestellung eines DSB verpflichteten Unternehmen zunächst drastisch**. Allerdings gibt es eine Öffnungsklausel für nationale Ausnahmeregelungen** (s. zum BDSG NEU).

Bestellpflicht Datenschutzbeauftragter nach neuem BDSG NEU

Das allgemeine Bundesdatenschutzgesetz (BSDG NEU) – novelliert das BDSG nach der DSGVO und regelt die nationalen Öffnungsklauseln.
Die Bestellpflicht des DSB wird in §36 abweichend zur DSGVO erweitert und **behält die Regelungen des BDSG weitgehend bei**: demnach muss ein DSB bestellt werden, wenn **mindestens zehn Personen** ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind.

Die entsprechende Verordnung finden Sie hier:

Veröffentlichung der DS-GVO im Amtsblatt der Europäischen Union (deutsch):
http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

BDSG Neu (Bundesgesetzblatt Teil I (Nr. 44 vom 5.07.2017, Seite 2097)
https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1499259259176

- ❑ Der Kunde ist ausdrücklich informiert worden, dass Verstöße gegen die DSVGO und das BDSG neu, keine Kavaliersdelikte mehr sind.

- ❑ Der Kunde hat zur Kenntnis genommen, dass für die zukünftige weitere Zusammenarbeit mit dem Unternehmen und dem IT-Systempartner **ein Auftragsdatenverarbeitungs-Vertrag** zu schließen ist mit der **Übersicht der Verarbeitungstätigkeiten** des Dienstleisterns gem. Artikel 30 Abs.2 DSGVO und der entsprechenden Technischen und organisatorischen Maßnahmen (gem. Art 32 Abs. 2 lit. d DSGVO)

- ❑ Es wurde darauf hingewiesen, dass keine Rechtsberatung durch den Fachhändler erfolgt und das durchgeführte Beratungsgespräch keine solche ersetzt.

Es liegen schriftlich vor:
- ☐ Interne Verhaltensregeln
- ☐ Risikoanalyse
- ☐ Allgemeine Datensicherheitsbeschreibung
- ☐ Umfassendes Datensicherheitskonzept
- ☐ Wiederanlaufkonzept (Notfallkonzept)

_____	_____
Ort, Datum	Unterschrift Kunde
_____	_____
Ort, Datum	Unterschrift Fachhändler

.

Beratungsprotokoll
Aufbewahrungs-/Archivierungspflicht

Zwischen

Kunde	Fachhändler

Wer seine Geschäftsunterlagen vor Ablauf der gesetzlichen Aufbewahrungsfristen vernichtet oder diese erst gar nicht aufbewahrt, handelt fahrlässig.

- Jedes Unternehmen, das jetzt keine E-Mail-Archivierung nutzt, handelt fahrlässig!
- Eine verspätete Einführung erkennt das Finanzamt sofort! **Sie ist NICHT heilbar!**
  Jeder Mitarbeiter oder Geschäftspartner kann ggf. eine Anzeige erstatten!

Die entsprechende Verordnung finden Sie hier:
https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/Datenzugriff_GDPdU/2014-11-14-GoBD.pdf?__blob=publicationFile

☐ Der Kunde ist ausdrücklich informiert worden, dass Verstöße gegen die Aufbewahrungs-/Archivierungspflicht keine Kavaliersdelikte mehr sind. Rechnungen, Verträge, Angebote, Korrespondenz: Die Zahl an elektronischen Dokumenten, die täglich im Unternehmen entstehen und archiviert werden müssen, ist groß.

☐ Der Kunde hat zur Kenntnis genommen, dass für die Archivierung bereits seit dem 1. Januar 2017 die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD) uneingeschränkt, gelten.

☐ Es wurde darauf hingewiesen, dass keine Rechtsberatung durch den Fachhändler erfolgt und das durchgeführte Beratungsgespräch keine solche ersetzt.

_____	_____
Ort, Datum	Unterschrift Kunde

_____	_____
Ort, Datum	Unterschrift Fachhändler