4.4.2.1 Neue Regelungen zur Auftrags(daten)verarbeitung

Damit in der Union ein gleichmäßiges Datenschutzniveau im Rahmen einer Auftragsdatenverarbeitung (zukünftig „Auftragsverabeitung“) gewährleistet ist, wurden die diesbezüglich in den einzelnen Ländern vorhandenen Regelungen vereinheitlicht. Damit bestehen zukünftig unionsweit dieselben Pflichten und Zuständigkeiten für die Verantwortlichen und Auftragsverarbeiter, egal ob die Auftragsverarbeitung in oder außerhalb der Union stattfindet.
Die zukünftigen Regelungen zur Auftragsverarbeitung lehnen sich zwar stark an die Vorschriften des § 11 BDSG an, es gibt jedoch auch einige Neuerungen (z. B. bezüglich der Verantwortlichkeiten und Pflichten) zu beachten.
Auch wenn nach dem alten Recht abgeschlossene Verträge zur Auftragsverarbeitung gültig bleiben, sollten sie sukzessive an die neuen Regelungen angeglichen werden, um den zukünftigen Vorgaben gerecht werden zu können. Neue Verträge sollten gleich die neuen Regelungen berücksichtigen.

1. Neue Begriffe

Statt der bisherigen Begriffe Auftraggeber und Auftragnehmer werden nunmehr die Begriffe Verantwortlicher und Auftragsverarbeiter verwendet und die Auftragsdatenverarbeitung wird nunmehr – wie bereits erwähnt – als Auftragsverarbeitung bezeichnet.

a) Verarbeiter

Ein „Verarbeiter“ ist gemäß Art. 4 Nr. 7 DS-GVO 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche bzw. die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

b) Auftragsverarbeiter

Ein „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

2. Verantwortlichkeiten

Zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftrags-

4.4.2.2 Datenschutz-Folgenabschätzung

Damit die Datenschutz-Grundverordnung in Fällen, in denen die Verarbeitungsvorgänge wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, besser eingehalten wird, ist der Verantwortliche für die Durchführung einer Datenschutz-Folgenabschätzung, mit der insbesondere die Ursache, Art, Besonderheit und Schwere dieses Risikos evaluiert werden, verantwortlich. Die Ergebnisse der Abschätzung müssen berücksichtigt werden, wenn darüber entschieden wird, welche geeigneten Maßnahmen ergriffen werden müssen, um nachzuweisen, dass die Verarbeitung der personenbezogenen Daten mit der Datenschutz-Grundverordnung 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 muss die Aufsichtsbehörde vor der Verarbeitung konsultiert werden (Erwägungsgrund 84 zur DS-GVO) (1).
Die Datenschutz-Folgenabschätzung löst die bisher gemäß § 4d Abs. 5 BDSG durchzuführende **Vorabkontrolle** ab.

1. Begriff

„Eine Datenschutz-Folgenabschätzung ist ein Instrument, um das Risiko zu erkennen und zu bewerten, das für das Individuum in dessen unterschiedlichen Rollen (als Bürger, Kunde, Patient etc.) durch den Einsatz einer bestimmten Technologie oder eines Systems durch eine Organisation entsteht.“ (2)

2. Gesetzliche Pflicht zur Datenschutz-Folgenabschätzung

Hat eine Form der Verarbeitung, insbesondere bei **Verwendung neuer Technologien**, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge, so führt der Verantwortliche **vorab** eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden (Art. 35 Abs. 1 DS-GVO).
Auf der Grundlage einer Datenschutz-Folgenabschätzung müssen entsprechende technisch-organisatorische Datensicherheitsmaßnahmen geplant und verwirklicht werden.

5.1.4.1 Checkliste Zutrittskontrolle

Unbefugten soll gemäß Nr. 1 der Anlage zu § 9 Satz 1 BDSG der Zutritt zu Datenverarbeitungsanlagen (auch PC und mobile Rechner), mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt werden. Dies muss mithilfe geeigneter Sicherheitsmaßnahmen erreicht werden. Art und Umfang der notwendigen Sicherungsmaßnahmen richten sich nach der Sensibilität der gespeicherten Daten.
Mithilfe der folgenden Checkliste soll und kann überprüft werden, ob ausreichende und geeignete Maßnahmen zur Gewährleistung der Zutrittskontrolle ergriffen wurden oder noch weitergehende Maßnahmen zu ergreifen sind. Die Checkliste erhebt keinen Anspruch auf Vollständigkeit und kann jederzeit durch eigene Erkenntnisse ergänzt werden.

Frage	Ja	Nein	Anmerkungen
Wurden die schutzbedürftigen Räume eines Gebäudes bestimmt? (1)	☐	☐	
Wurden die Verantwortlichkeiten für die Regelung und Überwachung der Zutrittskontrollmaßnahmen festgelegt? (2)	☐	☐	
Wurden Vertretungsregelungen geschaffen? (3)	☐	☐	
Wurden und werden die Regelungen zur Gewährleistung der Zutrittssicherheit ständig aktualisiert und den Mitarbeitern bekanntgegeben?	☐	☐	
Werden die Zutrittskontrollmaßnahmen regelmäßig auf ihre Wirksamkeit hin untersucht?	☐	☐	
Werden Kontrollgänge durchgeführt? (4)	☐	☐	

5.1.6.1 Muster eines Dienstleistungsvertrages für die Bestellung eines IT-Sicherheitsbeauftragten

Nachfolgend wurde ein Muster für einen Dienstleistungsvertrag für die Bestellung eines IT-Sicherheitsbeauftragten entworfen, der allerdings möglichst universell gehalten ist und insbesondere an den verschiedenen, besonders gekennzeichneten Stellen noch aufgabenspezifisch anzupassen ist. Der Mustervertrag erhebt keinen Anspruch auf Vollständigkeit.

Die *kursiv* gehaltenen Texte sind durch eigene Angaben zu ersetzen.

Vereinbarung

zwischen .....
(Name der Behörde/des Unternehmens)
und .....
(Name der bestellten Person)

§ 1 Gegenstand der Vereinbarung

Das Unternehmen/Die Behörde ..... setzt Informations- und Kommunikationstechnik zur Unterstützung nahezu aller Bereiche ein. Die Anforderungen an die Zuverlässigkeit und Sicherheit des IT-Betriebes sind entsprechend hoch.
Die *Geschäfts-/Behördenleitung* bestellt daher *Herrn/Frau* ..... zum IT-Sicherheitsbeauftragten. Der IT-Sicherheitsbeauftragte unterstützt und berät die *Geschäfts-/Behördenleitung* in Fragen der IT-Sicherheit und ist in dieser Funktion direkt der *Geschäfts-/Behördenleitung* unterstellt und verantwortlich.

§ 2 Geltungsbereich

(1) Dieser Dienstleistungsvertrag gilt für *das gesamte Unternehmen/die gesamte Behörde mit Zweigstellen*.
(2) Er gilt auch für zugehörige dezentral eingerichtete Arbeitsplätze (z. B. Telearbeitsplätze, mobile Arbeitsplätze usw.).
(3) Mit diesem Dienstleistungsvertrag werden die Aufgaben, Befugnisse und Verantwortlichkeiten des IT-Sicherheitsbeauftragten im Verhältnis zur *Geschäfts-/Dienststellenleitung* und der Anwenderebene geregelt.

8.1.3.2 Checkliste zur Browser-Nutzung

Während die früheren Browser lediglich über externe Zusatzprogramme abgesichert werden konnten, beinhalten die neuen Versionen der gängigen Browser selbst umfangreiche Sicherheitsfunktionen, die auch von den Mitarbeitern eines Unternehmens genutzt werden sollten.
Ob dies der Fall ist, kann mit der nachfolgenden Checkliste überprüft werden. Die Checkliste erhebt keinen Anspruch auf Vollständigkeit.

Frage	Ja	Nein	Anmerkungen
Wurden allgemeingültige Regelungen für die Nutzung der Browser erlassen?	☐	☐	
Besteht eine Vereinbarung mit der Arbeitnehmervertretung über die Nutzung der Browser? (1)	☐	☐	
Wurden die Browser-Nutzer auf die Einhaltung aller vorgegebenen Sicherheitsmaßnahmen schriftlich verpflichtet?	☐	☐	
Wird die Einhaltung der Anweisungen kontrolliert?	☐	☐	
Wird eine Änderung der vorgegebenen Sicherheitseinstellungen – soweit möglich – verhindert?	☐	☐	
Findet eine regelmäßige Überprüfung der angeordneten und aktivierten Schutzfunktionen hinsichtlich ihrer Nutzung und Erforderlichkeit statt? (2)	☐	☐	