Datenschutz-Checkliste

Version 1.0

# Datenschutzorganisation

## Bestellung eines Datenschutzbeauftragten

* + - Gesetzlich erforderlich?

Ja

Nein

* + - Ist ein Datenschutzbeauftragter bestellt?

Ja

Nein

* + - Ist die erforderliche Fachkunde des Datenschutzbeauftragten nachgewiesen?

Ja

Nein

* + - Ist die „Zuverlässigkeit“ des Datenschutzbeauftragter gewährleistet („keine Interessenskonflikte“)?

Ja

Nein

* + - Ist der Datenschutzbeauftragte direkt der Geschäftsleitung unterstellt und in die Informationsprozesse im Unternehmen, insbesondere bei der Planung und Anschaffung von Informationstechnologie eingebunden?

Ja

Nein

* + - Hat der Datenschutzbeauftragte die Möglichkeit, sich regelmäßig fortzubilden (Schulung, Literatur etc.)

Ja

Nein

## Verpflichtung auf das Datengeheimnis

* + - Sind alle Beschäftigten auf das Datengeheimnis i.S.d. § 5 BDSG verpflichtet worden?

Ja

Nein

* + - Werden auch externe Mitarbeiter (z.B. Reinigungskräfte, Werkstudenten u.ä.) auf das Datengeheimnis verpflichtet?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Verfahrensverzeichnis / Verarbeitungsübersicht

* + - Gibt es ein „Verfahrensverzeichnis für Jedermann“

Ja

Nein

* + - Gibt es eine interne Übersicht der Verfahren, mit denen personenbezogene Daten verarbeitet werden („internes Verfahrensverzeichnis“ / Verarbeitungsübersicht)

Ja

Nein

* + - Ist gewährleistet, dass bei der Anschaffung/Änderung neuer IT, bei der Gestaltung neuer IT-Abläufe oder der Änderung im IT-Bereich eine Anpassung der Verarbeitungsübersicht erfolgt?

Ja

Nein

## Meldepflicht

* + - „Gegenausnahmen“ vorhanden (geschäftsmäßige Übermittlung von Daten oder für Zwecke der Markt- und Meinungsforschung)?

Ja

Nein

* + - Falls ja, wurde Meldepflicht eingehalten?
      * Ja
      * Nein

## Vorabkontrolle

* + - Werden Vorabkontrollen (§ 4d Abs. 5, 6 BDSG) vor der Einführung von automatisierten Datenverarbeitungsvorgängen durchgeführt, wenn diese Vorgänge besondere Risiken für die Rechte der Betroffenen beinhalten?

Ja

Nein

# IT-Sicherheit

## Technische und organisatorische Maßnahmen gemäß § 9 BDSG und der Anlage zu § 9 Satz 1 BDSG

* + - Gibt es schriftliche Dokumentation der technischen und organisatorischen Maßnahmen i.S.d. § 9 BDSG

Ja

Nein

## Gibt es eine Leitlinie zur Informationssicherheit?

Ja

Nein

## Gibt es eine IT-Richtlinie (o.ä.) für Beschäftigte, aus der sich ergibt, ob und wie diese IT-Systeme im Unternehmen verwenden dürfen?

Ja

Nein

## Gibt es eine Risiko- und Schwachstellenanalyse im Hinblick auf Räume, IT-Systeme, IT-Applikationen und Netzwerkkomponenten?

Ja

Nein

## Gibt es einen Notfallplan?

Ja

Nein

# Compliance bei der Verarbeitung von Daten

## Direkterhebung

* + - Werden personenbezogene Daten grundsätzlich selbst beim Betroffenen erhoben?

Ja

Nein

## Rechtsgrundlage

* + - Wird Sorge dafür getragen, dass personenbezogene Daten grundsätzlich nur dann verarbeitet werden, wenn dies zur Erbringung vertraglicher Leistungen erforderlich, im Rahmen einer Interessenabwägung zulässig ist oder eine Einwilligung des Betroffenen vorliegt?

Ja

Nein

## Einwilligung

* + - Wird bei der Verwendung von Einwilligungen darauf geachtet, dass der Betroffene über Zweck, Art und Umfang der Verwendung der von ihm freiwillig angegebenen Daten informiert wird?

Ja

Nein

Anforderung nicht anwendbar/relevant

* + - Kann der Betroffene die Einwilligungserklärung auch ohne Fachkenntnisse verstehen und erkennen, dass die Einwilligung freiwillig ist und ggf. welche Konsequenzen eine Nichterteilung einer Einwilligung hat?

Ja

Nein

Anforderung nicht anwendbar/relevant

* + - Ist im Falle eines Widerrufs der Einwilligung gewährleistet, dass die betroffenen personenbezogene Daten nicht weiter verwendet werden?

Ja

Nein

Anforderung nicht anwendbar/relevant

# Auftragsdatenverarbeitung

## Gibt es eine Übersicht aller Dienstleister/Lieferanten, die entweder Daten im Auftrag des Unternehmens verarbeiten oder IT-Systeme warten und pflegen?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Wird Sorge dafür getragen, dass bei den Auftragnehmern/Dienstleistern ein Auftragsdatenverarbeitungsvertrag nach den Vorgaben des § 11 BDSG geschlossen wurde (und wird)?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Gibt es ein Muster für einen Auftragsdatenverarbeitungsvertrag im Unternehmen?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Wird Sorge dafür getragen, dass der Auftragnehmer bei einer Auftragsdatenverarbeitung vor Vertragsschluss im Hinblick auf die getroffenen IT-Sicherheitsmaßnahmen kontrolliert wird?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Ist gewährleistet, dass Auftragnehmer regelmäßig (grundsätzlich 1x jährlich) im Hinblick auf Änderungen im Bereich der IT-Sicherheit kontrolliert werden?

Ja

Nein

Anforderung nicht anwendbar/relevant

# Informationspflicht bei „Datenpannen“

## Werden Verfahren, mit denen besondere Arten personenbezogener Daten (§ 3 Absatz 9), personenbezogene Daten, die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder personenbezogene Daten zu Bank- oder Kreditkartenkonten gesondert intern gekennzeichnet bzw. überwacht?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Wird Sorge dafür getragen, dass im Falle einer unbefugten Kenntnisnahme durch Dritte von Daten, die nach § 42a BDSG geschützt sind, sofort der Datenschutzbeauftragte informiert wird?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Gibt es einen Ablaufplan für den Fall einer Datenpanne?

Ja

Nein

Anforderung nicht anwendbar/relevant

# Betroffenenrechte

## Gibt es ein „Betroffenenmanagement“ dahingehend, dass Betroffene, die ihre Betroffenenrechte i.S.d. BDSG geltend machen, direkten Kontakt zum Datenschutzbeauftragten erhalten?

Ja

Nein

## Werden Auskunftsersuchen von Betroffenen kurzfristig und vollständig beantwortet?

Ja

Nein

## Gibt es ein Löschkonzept im Unternehmen, das Regelfristen für die Löschung von Daten vorsieht?

Ja

Nein

# Internet / E-Mail

## Internetseite

* + - Gibt es für die Internetseite des Unternehmens gesonderte Datenschutzhinweise, die von jeder Seite der Internetseite aus erreichbar sind (nicht nur im „Impressum“)

Ja

Nein

* + - Wird über Webanalyse-Software informiert?

Ja

Nein

Anforderung nicht anwendbar/relevant

* + - Wird über die Verwendung und das „Blocken“ von Cookies informiert?

Ja

Nein

Anforderung nicht anwendbar/relevant

* + - Wird über Tracking-Pixel oder sonstige verwendete Methoden für Zwecke der Werbung oder des Marketings informiert und werden Möglichkeiten für ein „Opt-Out“ angezeigt?

Ja

Nein

Anforderung nicht anwendbar/relevant

# E-Mail-Marketing

## Wird ein E-Mail-Newsletter angeboten?

Ja

Nein

## Werden Newsletter-Abonnenten hinreichend über Zweck, Art und Umfang der Datenverarbeitung beim E-Mail-Newsletter informiert (insbes. Tracking von „Open Rates“, „Click Rates“ u.Ä.)?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Gibt es ausreichende vertragliche Regelungen zur Verwendung der Daten durch einen externen Newsletter-Dienstleister (z.B. Auftragsdatenverarbeitungsvertrag, Einwilligung etc.)

Ja

Nein

Anforderung nicht anwendbar/relevant

# Private Internet-/E-Mail-Nutzung im Unternehmen

## Gibt es eine unternehmensinterne Regelung zur privaten Nutzung des Internets im Unternehmen

Ja

Nein

## Gibt es eine unternehmensinterne Regelung zur privaten Nutzung von E-Mail im Unternehmen

Ja

Nein

# Betriebsrat

## Gibt es einen Betriebsrat im Unternehmen

Ja

Nein

## Gibt eine Übersicht der Betriebsvereinbarungen, die Regelungen zum Umgang mit personenbezogenen Daten enthalten?

Ja

Nein

Anforderung nicht anwendbar/relevant

# Datenflüsse im Konzern

## Gehören mehrere Unternehmen zur Unternehmensgruppe („Konzern“)?

Ja

Nein

## Falls ja, gibt es Regelungen zur gemeinsamen Nutzung von Daten oder IT-Infrastrukturen im Unternehmen?

Ja

Nein

Anforderung nicht anwendbar/relevant

# Grenzüberschreitender Datenverkehr

## Werden Daten des Unternehmens im Ausland verarbeitet bzw. in das Ausland übermittelt?

Ja

Nein

## Europäische Union / EWR

* + - Ist im Falle einer Verarbeitung von Daten in anderen EU-Mitgliedsstaaten oder EWR-Staaten gewährleistet, dass eine Rechtsgrundlage für die Verwendung im Ausland besteht (z.B. § 28 BDSG und ggf. Auftragsdatenverarbeitung)?

Ja

Nein

Anforderung nicht anwendbar/relevant

## „Drittstaaten“

* + - Werden Daten in „Drittstaaten“ verwendet bzw. dorthin übermittelt?

Ja

Nein

## Ist vom Unternehmen geprüft worden, ob es für die Übermittlung in den Drittstaat bzw. die Verarbeitung dort eine Rechtsgrundlage im BDSG gibt („erste Stufe“)?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Handelt es sich bei dem Drittstaat um einen Staat mit „angemessenen Datenschutzniveau“?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Gibt es eine Einwilligung des Betroffenen zur Übermittlung von personenbezogene Daten an das Unternehmen in dem Drittstaat?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Ist mit dem Unternehmen in dem Drittstaat ein Vertrag auf Basis der EU-Standardvertragsklauseln geschlossen worden?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Befindet sich das Unternehmen, zu dem Daten übermittelt werden, in den USA und befindet sich dieses in der „Safe Harbor“-Liste?

Ja

Nein

Anforderung nicht anwendbar/relevant

## Wurde die Einhaltung der Safe-Harbor-Prinzipien durch das Unternehmen in dem Drittstaat von Ihrem Unternehmen geprüft?

Ja

Nein

Anforderung nicht anwendbar/relevant

Stand: 08.07.2015