HAUFE.

UMSETZUNG DER DATENSCHUTZ-GRUNDVERORDNUNG

Checkliste

INHALT

DIE CHECKLISTE UMFASST FOLGENDE BEREICHE:

1. Datenschutzstrategien
2. Verfahrensmeldungen und -verzeichnisse
3. Rechtmäßigkeit
4. Datenschutzbeauftragter
5. Datenschutzfolgenabschätzung / Data Protection Impact Assessment (DPIA)
6. Datenschutzvorfälle
7. Dienstleister
8. Gemeinsame Verantwortlichkeit (Joint Controller)
9. Datenschutzrechte
10. Datenschutzaufsichtsbehörde
11. Technische und organisatorische Maßnahmen (TOM)
12. Freiwillige Maßnahmen

SO NUTZEN SIE DIE CHECKLISTE

Die Fragen der Checkliste können mit „ja“, „nein“ oder nicht anwendbar („N/A“) angekreuzt werden. Sofern eine Anforderung für das Unternehmen für nicht anwendbar gehalten wird, sollte unter „Begründung für N/A“ genauer ausgeführt werden, warum die Anforderung im konkreten Fall nicht einschlägig sein soll (z.B. Frage betrifft nur externe Datenschutzbeauftragte, es ist aber ein interner Datenschutzbeauftragter bestellt).

Die Checklisten sollen lediglich dazu beitragen einen Eindruck über den eigenen Umsetzungsstand zur DS-GVO und den datenschutzaufsichtsbehördlichen Umsetzungsleitlinien zu gewinnen, haben jedoch keinen Anspruch auf Vollständigkeit. Werden Fragen aber mit „nein“ beantwortet, lassen sich Verstöße gegen die DS-GVO zumindest nicht ausschließen.

Die Autoren: RA Dr. Thorsten B. Behling und RA Andreas Wigger, WTS Legal Rechtsanwaltsgesellschaft mbH; www.wts.de.

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
1		**Datenschutzstrategien**				
1	1	Bestehen allgemeine und besondere (z.B. zu Datenpannen, Videoüberwachung) Datenschutzrichtlinien, -guidelines und -anweisungen für Mitarbeiter?	☐	☐	☐	
1	2	Wurden die Richtlinien, Guidelines und Anweisungen bereits an die DS-GVO angepasst?	☐	☐	☐	
1	3	Enthalten die Richtlinien, Guidelines und Anweisungen Regelungen hinsichtlich der Verantwortlichkeiten und Zuständigkeiten in Bezug auf die Umsetzung des Datenschutzes?	☐	☐	☐	
1	4	Gibt es Regelungen für die Zusammenarbeit der unterschiedlichen Abteilungen des Unternehmens für datenschutzrechtliche Fragestellungen und Probleme?	☐	☐	☐	
1	5	Sofern es mehrere Standorte gibt: Sind diese in ein einheitliches Datenschutzkonzept eingebunden?	☐	☐	☐	
1	6	Wurden für alle personenbezogenen Daten Lösch- und Prüffristen identifiziert, implementiert und sind für sämtliche Verarbeitungsverfahren dokumentiert?	☐	☐	☐	
1	7	Wurden Mitarbeiter, die potentiell mit personenbezogenen Daten in Berührung kommen, auf das Datengeheimnis verpflichtet?	☐	☐	☐	
1	8	Gibt es Schulungskonzept, dass regelmäßige Schulungen der Mitarbeiter zum Datenschutz vorsieht?	☐	☐	☐	
1	9	Wurden Mitarbeiter bereits im Hinblick auf die DS-GVO geschult?	☐	☐	☐	
1	10	Sind finanzielle Ressourcen für die Umsetzung und Einhaltung datenschutzrechtlicher Vorschriften eingeplant?	☐	☐	☐	
2		**Verfahrensmeldungen und -verzeichnisse**				
2	1	Besteht ein Verarbeitungsverzeichnis, in dem Verarbeitungstätigkeiten dokumentiert sind, bei denen das Unternehmen als Verantwortlicher (Controller) handelt?	☐	☐	☐	
2	2	Besteht ein Verarbeitungsverzeichnis, in dem Verarbeitungstätigkeiten dokumentiert sind, bei denen das Unternehmen als Auftragsverarbeiter (Processor) für einen anderen Verantwortlichen (Controller) handelt?	☐	☐	☐	
2	3	Werden die Verarbeitungsverzeichnisse schriftlich (was auch in einem elektronischen Format erfolgen kann) geführt?	☐	☐	☐	
2	4	Wurden die Verarbeitungsverzeichnisse bereits an die inhaltlichen Anforderungen nach der DS-GVO angepasst?	☐	☐	☐	
2	5	Enthält das angepasste Verantwortlichen-Verarbeitungsverzeichnis insbesondere Angaben zu				

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
2	5.1	den Namen und die Kontaktdaten des Verantwortlichen?	☐	☐	☐	
2	5.2	den Namen und die Kontaktdaten des gemeinsam mit ihm Verantwortlichen (sofern eine Verarbeitung nach Art. 26 DS-GVO vorliegt)?	☐	☐	☐	
2	5.3	den Namen und die Kontaktdaten Vertreters des Verantwortlichen?	☐	☐	☐	
2	5.4	den Namen und die Kontaktdaten eines etwaigen Datenschutzbeauftragten?	☐	☐	☐	
2	5.5	die Zwecke der Verarbeitung?	☐	☐	☐	
2	5.6	eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten?	☐	☐	☐	
2	5.7	die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen?	☐	☐	☐	
2	5.8	gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation?	☐	☐	☐	
2	5.9	bei den in Art. 49 Ab. 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien?	☐	☐	☐	
2	5.10	eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO?	☐	☐	☐	
2	5.11	die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien?	☐	☐	☐	
2	6	Enthält das angepasste Verantwortlichen-Verarbeitungsverzeichnis auch folgende zweckmäßige Zusatzangaben zu				
2	6.1	falls Antwort auf 5.11 „nein“: die vorgesehenen Prüffristen und Prüfkriterien?	☐	☐	☐	
2	6.2	die Rechtsgrundlagen für die jeweilige Verarbeitungstätigkeit?	☐	☐	☐	
2	6.3	wenn die Verarbeitung auf Art. 6 Abs. 1 S. 1 Buchstabe f DS-GVO beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden?	☐	☐	☐	
2	7	Enthält das angepasste Auftragsverarbeiter-Verarbeitungsverzeichnis insbesondere Angaben zu				
2	7.1	den Namen und die Kontaktdaten des Auftragsverarbeiters?	☐	☐	☐	

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
2	7.2	den Namen und die Kontaktdaten jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist?	☐	☐	☐	
2	7.3	den Namen und die Kontaktdaten des Vertreters des Verantwortlichen oder des Auftragsverarbeiters?	☐	☐	☐	
2	7.4	den Namen und die Kontaktdaten eines etwaigen Datenschutzbeauftragten?	☐	☐	☐	
2	7.5	die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden?	☐	☐	☐	
2	7.6	gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation?	☐	☐	☐	
2	7.7	bei den in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien?	☐	☐	☐	
2	7.8	eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO?	☐	☐	☐	
3		**Rechtmäßigkeit**				
3	1	Wurden die einzelnen Verarbeitungstätigkeiten auf Rechtmäßigkeit nach der DS-GVO geprüft und die jeweiligen Rechtsgrundlagen dokumentiert?	☐	☐	☐	
3	2	Sofern und soweit eine Einwilligung als Rechtsgrundlage herangezogen wird: Ist die betroffene Person vor Abgabe mindestens informiert worden über				
3	2.1	die Identität und Kontaktdaten des Verantwortlichen und etwaiger gemeinsam Verantwortlicher?	☐	☐	☐	
3	2.2	Die Zwecke der Verarbeitung?	☐	☐	☐	
3	3	Sofern und soweit eine Einwilligung als Rechtsgrundlage herangezogen wird: Ist gewährleistet, dass die Einwilligung				
3	3.1	unmissverständlich erteilt wird?	☐	☐	☐	
3	3.2	in klarer und verständlicher Form abgefasst ist?	☐	☐	☐	
3	3.3	durch eine Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung erteilt wird (Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit nicht ausreichend)?	☐	☐	☐	
3	3.4	im Falle besonderer Kategorien personenbezogener Daten ausdrücklich erteilt wird?	☐	☐	☐	
3	3.5	für den konkreten Fall erteilt wird?	☐	☐	☐	
3	3.6	im Falle vorformulierter Einwilligungserklärungen den betroffenen Personen in verständlicher und leicht auffindbarer Form zu Verfügung gestellt wird?	☐	☐	☐	
3	3.7	keine missbräuchliche Klausel beinhaltet?	☐	☐	☐	

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
3	3.8	im Falle elektronischer Einwilligung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgt?	☐	☐	☐	
3	4	Sofern und soweit eine Einwilligung als Rechtsgrundlage herangezogen wird: Ist gewährleistet, dass die Einwilligung freiwillig erfolgt, insbesondere				
3	4.1	eine echte und freie Wahl für die betroffenen Personen besteht?	☐	☐	☐	
3	4.2	die betroffene Person in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden?	☐	☐	☐	
3	4.3	zwischen der betroffenen Person und dem Verantwortlichen kein klares Ungleichgewicht besteht?	☐	☐	☐	
3	4.4	zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten gesondert eine Einwilligung eingeholt wird (es sei denn dies ist im Einzelfall unangebracht)?	☐	☐	☐	
3	4.5	die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, nicht von der Einwilligung abhängig ist, sofern nicht diese Einwilligung für die Erfüllung erforderlich ist (Kopplungsverbot)?	☐	☐	☐	
3	5	Werden die betroffenen Personen über ihr Recht zum jederzeitigen Widerruf ihrer Einwilligung aufgeklärt?	☐	☐	☐	
3	6	Ist gewährleistet, dass der Widerruf der Einwilligung ebenso einfach ist, wie deren Erteilung (keine strengere Form, Äquivalenz, keine zusätzlichen Aufwände, kein Medienbruch)?	☐	☐	☐	
3	7	Werden geeignete Verfahren zur Einholung von Einwilligungen von Kindern in Bezug auf Dienste der Informationsgesellschaft nach den Anforderungen und Bedingungen nach Artikel 8 DS-GVO gewährleistet?	☐	☐	☐	
3	8	Wurden insgesamt bereits bestehende Einwilligungen auf ihre Vereinbarkeit mit der DS-GVO geprüft (insbes. hins. Kopplungsverbot[1])?	☐	☐	☐	
3	9	Ist durch dokumentierte Prozesse gewährleistet, dass (bestehende und künftige) Betriebsvereinbarungen, welche eine Verarbeitung personenbezogener Beschäftigtendaten als Rechtsgrundlage regeln, die Anforderungen nach Art. 88 Abs. 2 DS-GVO beachten?	☐	☐	☐	

[1] Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt wird, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist (Art. 7 Abs. 4 DS-GVO und Erwägungsgrund 43 DS-GVO). M.a.W.: Der Vertrag darf nicht von der Erteilung einer Einwilligung zu anderen Verarbeitungen (z.B. Werbezwecke, Tracking) abhängig gemacht werden.

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
3	10	Ist sichergestellt, dass etwaige Betriebsvereinbarungen, welche eine Verarbeitung personenbezogener Beschäftigtendaten als Rechtsgrundlage regeln, nicht unter das Schutzniveau der DS-GVO und des BDSG zurückfallen?	☐	☐	☐	
3	11	Ist durch geeignete Maßnahmen (z.B. Unterwerfungsklauseln in Datenschutzverträgen oder durch BCR) sichergestellt, dass Betriebsvereinbarungen, die auf die Arbeitgebergesellschaft anwendbar sind, durch die Übermittlung innerhalb einer Unternehmensgruppe (z.B. Matrixorganisation, Zentralisierung von Beschäftigungsverarbeitungen etc.) nicht unterminiert werden?	☐	☐	☐	
4		**Datenschutzbeauftragter**				
4	1	Sofern es nicht offensichtlich ist, dass ein Datenschutzbeauftragter (folgend: „DSB“) gesetzlich nicht erforderlich ist: Wurde die rechtliche Erforderlichkeit zur Bestellung eines DSB bewertet und ist die Bewertung einschließlich der zugrundeliegenden Fakten und ihrer relevanten Faktoren[2] dokumentiert?	☐	☐	☐	
4	2	Sofern ein DSB gesetzlich nicht erforderlich ist: Ist ein Ansprechpartner für die Aufsichtsbehörden und Betroffenenanfragen bestimmt?	☐	☐	☐	
4	3	Wurde geprüft und dokumentiert, welche internen Funktionen mit der Bestellung eines DSB unvereinbar sind (z.B. Interessenkonflikte, fehlende Unabhängigkeit)?[3]	☐	☐	☐	
4	4	Ist vorgesehen, dass das Unternehmen positiv erklärt, dass der DSB frei von einem Interessenkonflikt ist?	☐	☐	☐	
4	5	Bestehen interne Regeln und Absicherungen um einen Interessenkonflikt zu vermeiden, einschließlich allgemeiner Erläuterung zu Interessenkonflikten?	☐	☐	☐	
4	6	Ist sichergestellt, dass die Stellenausschreibung für die Position des DSB oder der Dienstvertrag ausreichend präzise und detailliert ist, um einen Interessenkonflikt zu vermeiden?	☐	☐	☐	
4	7	Bestehen Guidelines und Prozesse zur Auswahl eines DSB gemäß Qualifikationsanforderungen der DS-GVO?[4]	☐	☐	☐	

[2] Es empfiehlt sich hierbei möglichst die Faktoren und Erwägungen aus den Guidelines on Data Protection Officers, WP 243, 13 December 2016, ausdrücklich in der Dokumentation in Bezug zu nehmen.
[3] In der Regel werden Senior Management Positionen von der Datenschutzaufsicht als nicht konfliktfrei für die Funktion als DSB angesehen.
[4] Hierzu sollten die Kriterien der Guidelines on Data Protection Officers, WP 243, 13 December 2016, der Artikel 29 Datenschutzgruppe herangezogen werden.

CHECKLISTE					
Nr.	Thema/Frage	Ja	Nein	N/A	Begründung für N/A
4 8	Sofern freiwillig, d.h. ohne gesetzliche Pflicht, ein DSB bestellt worden ist: Ist sichergestellt, dass hinsichtlich des freiwillig bestellten DSB die gleichen Anforderungen im Hinblick auf die gesetzlichen Voraussetzungen zu Benennung, Position und Aufgaben eingehalten sind?	☐	☐	☐	
4 9	Sofern andere Positionen als ein gesetzlich vorgeschriebener oder freiwillig bestellter DSB mit Datenschutzaufgaben betraut sind: Ist sichergestellt, dass es im Hinblick auf Titel, Status, Position und Aufgaben nicht zu einer Verwechslung mit einem DSB kommen kann (insbes. im Rechtsverkehr, z.B. in Interaktion mit Betroffenen und/oder Aufsichtsbehörden)?	☐	☐	☐	
4 10	Sofern ein DSB für eine Unternehmensgruppe bestellt worden ist: Ist der DSB von jeder Niederlassung aus leicht zu erreichen (d.h. auch sprachlich)?[5]	☐	☐	☐	
4 11	Erhält die Funktion des DSB aktive Unterstützung durch das Senior Management (wie Vorstandsebene)?	☐	☐	☐	
4 12	Sofern der DSB nicht Vollzeit als DSB arbeitet: Ist eine angemessene Zeit in Prozent sowie ein Arbeitsplan zur prioritären Pflichtenerfüllung in dokumentierter Weise festgelegt, die sicherstellt, dass der DSB ausreichend Zeit zur Erfüllung seiner Pflichten hat?	☐	☐	☐	
4 13	Wurde geprüft und dokumentiert festgestellt, wie viel Unterstützung der DSB im Hinblick auf finanzielle Ressourcen, Infrastruktur (Räumlichkeiten, Einrichtung Ausstattung) und Personal benötigt, damit der DSB seine Aufgaben und Pflichten im Unternehmen angemessen wahrnehmen kann?	☐	☐	☐	
4 14	Wurde geprüft, inwiefern aufgrund von Größe und Struktur des Unternehmens die Notwendigkeit des Einsatzes eines DSB-Teams besteht?	☐	☐	☐	
4 15	Sofern ein DSB-Team eingerichtet wurde, wurde die interne Struktur des Teams, und die Aufgaben und Verantwortlichkeiten für jedes Team-Mitglied klar aufgezogen und ist dies dokumentiert?	☐	☐	☐	
4 16	Sofern die Funktion des DSB durch einen externen Anbieter wahrgenommen wird, in dem ein Team von Personen beschäftigt ist: Ist ein primärer Ansprechpartner für den Mandanten benannt?	☐	☐	☐	
4 17	Werden dem DSB Fortbildungen ermöglicht und der DSB ermutigt diese wahrzunehmen?	☐	☐	☐	

[5] D.h. der DSB muss in der Lage sein, effektiv mit betroffenen Personen zu kommunizieren und mit den betroffenen Datenschutzbehörden zu kooperieren. Dies bedeutet insbesondere, dass die Kommunikation in der Sprache oder den Sprachen der betroffenen Personen und Datenschutzaufsichtsbehörden erfolgen können muss. Dies dürfte regelmäßig erfüllt sein, wenn der DSB oder einer seiner Mitarbeiter die Landessprache beherrscht, in der die Dienstleistungen angeboten werden und zusätzlich Englisch.

CHECKLISTE					
Nr.	Thema/Frage	Ja	Nein	N/A	Begründung für N/A
4 18	Hat der DSB notwendigen Zugriff auf andere Dienste, wie HR, Legal, IT, Security, etc., um notwendige Unterstützung, Input und Informationen aus diesen Bereichen zu erhalten?	☐	☐	☐	
4 19	Sofern ein externer DSB bereits bestellt ist: Wurde dessen Geschäftsbesorgungsvertrag den Aufgaben nach der DSGVO angepasst?[6]	☐	☐	☐	
4 20	Sind die Kontaktdaten des DSB für die Betroffenen (Mitarbeitern, Kunden, Lieferanten) veröffentlicht worden (Intranet und Internet)?	☐	☐	☐	
4 21	Ist auch der Name des DSB für Betroffene (Mitarbeiter, Kunden, Lieferanten) veröffentlicht worden (Intranet, internes Telefonverzeichnis, Organisationscharts, Internet)?	☐	☐	☐	
4 22	Berichtet der Datenschutzbeauftragte unmittelbar an die höchste Managementebene?	☐	☐	☐	
4 23	Erfolgt die Berichterstattung an die höchste Managementebene durch einen jährlichen Datenschutzbericht?	☐	☐	☐	
4 24	Ist sichergestellt, dass der DSB in Ausübung seiner Aufgaben keinen Weisungen unterliegt?[7]	☐	☐	☐	
4 25	Wird der DSB regelmäßig zu Meetings des Senior und Middle Managements eingeladen?	☐	☐	☐	
4 26	Bestehen dokumentierte Prozesse, nach denen neue Verarbeitungsverfahren vor ihrer Einführung dem DSB gemeldet werden?	☐	☐	☐	
4 27	Wird der DSB hinsichtlich der Rechtmäßigkeit von Verarbeitungsvorgängen um eine Bewertung gebeten?	☐	☐	☐	
4 28	Wird dem DSB mitgeteilt, wenn neue Verarbeitungsverfahren tatsächlich in Betrieb genommen werden?	☐	☐	☐	
4 29	Werden dem DSB im Falle notwendiger Datenschutzverträge die Entwürfe der Datenschutzverträge mit der Bitte um Einschätzung zur Verfügung gestellt?	☐	☐	☐	
4 30	Werden dem DSB auch die tatsächlich unterschriebenen Datenschutzverträge zur Kenntnis gegeben?	☐	☐	☐	
4 31	Wird dem DSB das dokumentierte Ergebnis der Prüfung der technisch-organisatorischen Maßnahmen (auch in Bezug auf Dienstleister) durch die interne Informationssicherheit zur Verfügung gestellt?	☐	☐	☐	
4 32	Wird der DSB um eine Einschätzung gebeten, inwieweit eine Datenschutzfolgenabschätzung erforderlich ist?	☐	☐	☐	

[6] Insbes. hinsichtlich der neuen Überwachungsfunktionen und des hierdurch entstehenden Mehraufwandes.
[7] Es empfiehlt sich im Auftrag/Bestellung des DSB sowie in der Unternehmensrichtlinie zum Datenschutz ausdrücklich aufzunehmen, dass er in Ausübung seiner Aufgaben vollständig weisungsfrei ist.

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
4	33	Sofern einer Auffassung des DSB nicht gefolgt wird, bestehen Prozesse zur Dokumentation der Gründe, warum von der Auffassung des DSB abgewichen wird?	☐	☐	☐	
4	34	Werden Datenschutzanfragen und Beschwerden von Betroffenen frühzeitig an den DSB weitergeleitet?	☐	☐	☐	
4	35	Ist die Geheimhaltung und Vertraulichkeit von Beschwerden und Anfragen von Betroffenen und der Datenschutzaufsicht an den DSB sichergestellt?[8]	☐	☐	☐	
4	36	Gibt es Regelungen und/oder andere Prozesse, die die Mitarbeiter darüber aufklären, in welchen Fällen der DSB wann und wie einzubeziehen ist?	☐	☐	☐	
5		**Datenschutzfolgenabschätzung/Data Protection Impact Assessment (DPIA)**				
5	1	Gibt es eine Richtlinie und Prozesse zur Durchführung eines DPIA (einschließlich Definition von Verantwortlichkeiten)?	☐	☐	☐	
5	2	Entsprechen diese dem Prüfungsmaßstab und den inhaltlichen Anforderungen der DS-GVO (auch hinsichtlich Dokumentation)?	☐	☐	☐	
5	3	Ist durch dokumentierte Prozesse sichergestellt, dass bei der Ausführung des DPIA ein etwaig anwendbarer (datenschutzrechtlicher) Code of Conduct (Art. 40 DS-GVO „Verhaltensregeln“) berücksichtigt wird?	☐	☐	☐	
5	4	Ist durch dokumentierte Aufgabenbeschreibungen sichergestellt, dass die am DPIA Beteiligten im Hinblick auf das zu bewertende „Risiko“ das Risiko für die Rechte und Freiheiten der Betroffenen zugrunde legen und nicht, wie bei anderen Risk Management Prozessen, die Unternehmensrisiken?	☐	☐	☐	
5	5	Wird für das DPIA eine nach Annex 1 der Leitlinien zur Datenschutzfolgenabschätzung der Artikel 29 Datenschutzgruppe anerkannte Vorgehensweise („Methodologie“) verwendet, und ist diese standardmäßig festgelegt (z.B. das sog. Standard Datenschutzmodell (SMD) der deutschen Datenschutzaufsichtsbehörden)?	☐	☐	☐	
5	6	Falls nein, ist durch dokumentierte Prozesse sichergestellt, dass eine Methodologie für das DPIA angewendet wird, die den Kriterien des Annex 2 der Leitlinien zur Datenschutzfolgenabschätzung der Artikel 29 Datenschutzgruppe entspricht?	☐	☐	☐	
5	7	Werden etwaige Auftragsverarbeiter in den Prozess des DPIA einbezogen?	☐	☐	☐	

[8] Insbes. E-Mail-Postfach, auf das nur der DSB Zugriff hat; ungeöffnete Weiterleitungen von Briefen, die unmittelbar zu Händen des DSB adressiert sind.

CHECKLISTE					
Nr.	Thema/Frage	Ja	Nein	N/A	Begründung für N/A
5 8	Ist sichergestellt, dass die IT-Abteilung und/oder der CISO - sofern ein solcher bestellt ist - die Durchführung einer Datenschutzfolgenabschätzung vorschlagen kann?	☐	☐	☐	
5 9	Wird die IT-Abteilung und/oder der CISO hinsichtlich Fragestellung zu den bestehenden Sicherheitsrisiken einer Verarbeitung und angemessener technisch-organisatorischer Maßnahmen beteiligt?	☐	☐	☐	
5 10	Wird der DSB um Rat gebeten, inwieweit aus seiner Sicht ein DPIA durchzuführen ist?	☐	☐	☐	
5 11	Wird bei der Durchführung der DPIA auch der Rat des DSB eingeholt?	☐	☐	☐	
5 12	Wird der DSB auch um Rat gebeten, welche Methodologie für die Durchführung des DPIA angewendet werden sollte?	☐	☐	☐	
5 13	Wird der DSB um Rat gebeten, inwieweit das DPIA in-house durchgeführt oder durch Fremdvergabe erfolgen sollte?	☐	☐	☐	
5 14	Wird durch die Verantwortlichen des DPIA im Einzelfall geprüft, ob es angemessen ist, dass das DPIA besser durch unabhängige Dritte (z.B. Rechtsanwälte, Techniker, Sicherheitsexperten, Soziologen, Ethiker) vorgenommen wird?	☐	☐	☐	
5 15	Wird der DSB im Rahmen des DPIA um Rat gebeten, welche Schutzmaßnahmen, einschließlich technisch-organisatorische Maßnahmen, angewendet werden sollten, um etwaige Risiken für die Rechte und Interessen der Betroffenen zu mindern?	☐	☐	☐	
5 16	Wird der DSB nach Abschluss des DPIA um eine Einschätzung gebeten, inwieweit das DPIA richtig ausgeführt worden ist und ob die Schlussfolgerungen (namentlich ob das Verarbeitungsverfahren fortgesetzt werden sollte und welche Sicherheitsmaßnahmen angewendet werden sollen) mit der DS-GVO im Einklang stehen?	☐	☐	☐	
5 17	Wird der DSB auch um Rat gebeten, inwieweit er eine Konsultation der Datenschutzaufsichtsbehörde für geboten hält?	☐	☐	☐	
5 18	Werden der Rat und die Auffassung des DSB in die Dokumentation der Datenschutzfolgenabschätzung aufgenommen?	☐	☐	☐	
5 19	Sofern einer Auffassung des DSB zum Ergebnis des DPIA nicht gefolgt wird, wird spezifisch schriftlich begründet, warum von der Auffassung des DSB abgewichen wird?	☐	☐	☐	

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
5	20	Ist vorgesehen, dass – soweit im Einzelfall angemessen – der Standpunkt der betroffenen Personen (z.B. Kunden- oder Mitarbeiterumfrage) oder deren Interessenvertreter (z.B. Verbraucherverbände, Kundenbeirat oder bei Beschäftigten z.B. Betriebsrat) eingeholt wird und dass dieser Input im Rahmen des DPIA berücksichtigt wird?	☐	☐	☐	
5	21	Ist prozessual vorgesehen, dass zu Beginn eines DPIA geprüft und dokumentiert wird, inwieweit eine solche Beteiligung der Betroffenen oder Interessenvertreter im Einzelfall angemessen ist bzw. mit welcher Begründung auf eine Beteiligung verzichtet wird?	☐	☐	☐	
5	22	Wird im Rahmen des DPIA dokumentiert, wenn und aus welchen Gründen von der Auffassung der betroffenen Personen oder ihrer Interessenvertreter abgewichen wird?	☐	☐	☐	
5	23	Ist geplant, auch für bereits bestehende Risikoverfahren (z.B. Bonitätsscoring, Online Behavioural Advertising, Fraud Detection, Warndateien, Blacklisting, Videoüberwachung großer öffentlich zugänglicher Flächen, biometrische Zugangskontrollen, Verfahren mit riskantem Drittstaatenbezug) ein DPIA durchzuführen?	☐	☐	☐	
5	24	Werden Risikoverfahren alle drei Jahre auf wesentliche Veränderungen und die Notwendigkeit der Durchführung eines erneuten DPIA überprüft und besteht hierzu ein dokumentierter Prozess?	☐	☐	☐	
5	25	Ist durch dokumentierte Prozesse vorgesehen, dass das DPIA oder angemessene Teile davon (z.B. Management Summary) veröffentlicht werden, sofern das Verarbeitungsverfahren Teile der Öffentlichkeit betrifft?	☐	☐	☐	
6		**Datenschutzvorfälle**				
6	1	Sind Verantwortlichkeiten, Berichtslinien und Prozesse zur Meldung, Ermittlung und Aufklärung von Datenschutzvorfällen definiert („Reaktionsplan“)?	☐	☐	☐	
6	2	Enthält dieser Reaktionsplan auch	☐	☐	☐	
6	2.1	Kriterien zur Identifikation eines Datenschutzvorfalles?	☐	☐	☐	
6	2.2	Kriterien zur Bewertung des Risikos einer Datenschutzverletzung?	☐	☐	☐	
6	2.3	Regelungen, wie die Verletzungen beseitigt und mögliche nachteilige Folgen für Betroffene abgemildert werden können?	☐	☐	☐	
6	2.4	Kriterien für die Entscheidung über die Meldung der Datenschutzverletzung an Behörden und betroffene Personen?	☐	☐	☐	

CHECKLISTE					
Nr.	Thema/Frage	Ja	Nein	N/A	Begründung für N/A
6 3	Sind insoweit bestehende Konzepte an die Anforderung der DS-GVO angepasst worden, insbesondere hins. des Umstandes, dass nicht nur eine Verletzung der Vertraulichkeit sondern auch der Verfügbarkeit oder Integrität einen Datenschutzvorfall darstellen kann?	☐	☐	☐	
6 4	Orientieren sich die Prozesse und Bewertungskriterien eines Datenschutzvorfalles und der Bewertung einer Meldepflicht an den Beispielen im Annex der Leitlinien in Bezug auf Datenschutzvorfälle der Artikel 29 Datenschutzgruppe (WP250)?	☐	☐	☐	
6 5	Ist über definierte Prozesse sichergestellt, dass der DSB und die Geschäftsleitung unverzüglich über den Verdacht eines Datenschutzvorfalles informiert und durch das Ermittlungsteam ständig auf dem Laufenden gehalten werden?	☐	☐	☐	
6 6	Erfolgt eine Dokumentation des Datenschutzvorfalles und der Ermittlungen, die geeignet ist, der Datenschutzaufsicht vorgelegt zu werden, und die den inhaltlichen Anforderungen der DS-GVO genügt (einschließlich aller im Zusammenhang mit dem Vorfall stehenden Fakten, Anzahl der Betroffenen, Identifikation der Risiken, der Bewertung des Vorfalles, risikomindernde Maßnahmen)?	☐	☐	☐	
6 7	Ist durch die Prozesse sichergestellt, dass ein Datenschutzvorfall innerhalb von 72 Stunden der Datenschutzaufsicht und überdies unverzüglich den Betroffenen gemeldet werden kann?	☐	☐	☐	
6 8	Ist in den vorgesehenen Prozessen berücksichtigt, dass die Frist bereits zu laufen beginnt, wenn ein Auftragsverarbeiter bereits Grund zu der Annahme eines Datenschutzvorfalles hat und nicht erst mit der Meldung des Auftragsverarbeiters an den Verantwortlichen?	☐	☐	☐	
6 9	Ist entsprechend datenschutzvertraglich und im Reaktionsplan sichergestellt, dass auch bei einer Datenschutzverletzung im Kontext einer Auftragsverarbeitung oder gemeinsamen Verantwortlichkeit eine eigene Untersuchung, Risikobewertung und Meldung innerhalb der Meldepflicht erfolgen kann?	☐	☐	☐	
6 10	Kann festgestellt werden, welche technischen und organisatorischen Sicherheitsvorkehrungen zum Schutz von Verletzungen zum Zeitpunkt der Verletzung bestanden?	☐	☐	☐	
6 11	Werden Übungen hinsichtlich der Abläufe bei einem Datenschutzvorfall durchgeführt (vergleichbar einer Feuerwehrübung)?	☐	☐	☐	
6 12	Gibt es Prozesse, um bei/nach einem Ernstfall Ursachen, Folgen und Abhilfemaßnahmen zu analysieren und auszuwerten, um Mängel festzustellen und diese zu beheben?	☐	☐	☐	

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
7		**Dienstleister**				
7	1	Bestehen Guidelines und Prozesse zur Auswahl datenschutzrechtlich zuverlässiger Dienstleister?	☐	☐	☐	
7	2	Ist durch dokumentierte Prozesse gewährleistet, dass nur Auftragsverarbeiter ausgewählt und eingesetzt werden, die hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen bestehen, die die Konformität mit der DS-GVO und den Schutz der rechte der betroffenen Personen sicherstellen?	☐	☐	☐	
7	3	Sind die Auftragsverarbeitungsvertragsmuster den Anforderungen an Artikel 28 DS-GVO angepasst worden, sodass diese insbesondere spezifische Regelungen enthalten?	☐	☐	☐	
7	3.1	zum Gegenstand der Verarbeitung?	☐	☐	☐	
7	3.2	zur Dauer der Verarbeitung?	☐	☐	☐	
7	3.3	zur Art der Verarbeitung?	☐	☐	☐	
7	3.4	zum Zweck der Verarbeitung?	☐	☐	☐	
7	3.5	zur Art der personenbezogenen Daten?	☐	☐	☐	
7	3.6	zu den Kategorien der betroffenen Personen?	☐	☐	☐	
7	3.7	zu den Pflichten und Rechten des Verantwortlichen?	☐	☐	☐	
7	3.8	dazu, dass der Auftragsverarbeiter die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet?	☐	☐	☐	
7	3.9	dazu, dass der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen?	☐	☐	☐	
7	3.10	dazu, dass der Auftragsverarbeiter alle gemäß Artikel 32 DS-GVO erforderlichen Maßnahmen ergreift?	☐	☐	☐	
7	3.11	dazu, dass der Auftragsverarbeiter die in Artikel 28 Absätze 2 und 4 DS-GVO genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält?	☐	☐	☐	

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
7	3.12	dazu, dass der Auftragsverarbeiter angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Person nachzukommen?	☐	☐	☐	
7	3.13	dazu, dass der Auftragsverarbeiter unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten unterstützt?	☐	☐	☐	
7	3.14	dazu, dass der Auftragsverarbeiter nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht?	☐	☐	☐	
7	3.15	dazu, dass der Auftragsverarbeiter dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Artikel 28 DS-GVO niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt?	☐	☐	☐	
7	4	Unter Berücksichtigung des aufsichtsbehördlichen Verständnisses, dass eine sog. Funktionsübertragung unter der DS-GVO nicht mehr besteht[9]: Wurden bisherige Funktionsübertragungssituationen neu bewertet und daraufhin überprüft, ob bestehende Funktionsübertragungsverträge aufgehoben bzw. durch einen Auftragsverarbeitungs- oder Joint-Controller-Vertrag ersetzt werden müssen?	☐	☐	☐	
7	5	Im Hinblick auf 7.4: Wurden Funktionsübertragungsverträge bereits aufgehoben bzw. durch Auftragsverarbeitungs- oder Joint-Controller-Vertrag ersetzt?	☐	☐	☐	
7	6	Wurden Vertragspartner kontaktiert und bestehende Datenschutzverträge so nachverhandelt, dass sie den neuen Anforderungen der DS-GVO genügen?	☐	☐	☐	
8		**Gemeinsame Verantwortlichkeit (Joint Controller)**				
8	1	Bestehen Verarbeitungen bei denen eine gemeinsame Verantwortlichkeit mit einem anderen Unternehmen besteht (Joint Controller)?[10]	☐	☐	☐	
8	2	Falls ja, wurden Joint-Controller-Verträge geschlossen?	☐	☐	☐	

[9] Kurzpapier Nr. 13 der der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 16.01.2018.
[10] Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche, Art. 26 Abs. 1 Satz 1 DS-GVO.

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
8	2.1	Enthalten die Joint-Controller-Verträge insbesondere Regelungen zwischen den gemeinsam Verantwortlichen dazu,	☐	☐	☐	
8	2.2	wer von ihnen welche Verpflichtung gemäß der DS-GVO erfüllt?	☐	☐	☐	
8	2.3	insbesondere wer die Wahrnehmung der Rechte der betroffenen Person erfüllt?	☐	☐	☐	
8	2.4	wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt?	☐	☐	☐	
8	2.5	Ist in der Vereinbarung eine Anlaufstelle für die betroffenen Personen angegeben?	☐	☐	☐	
8	2.6	spiegelt die Vereinbarung die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend wider (und gibt es dokumentierte Prozesse anhand dessen dies vorab geprüft wird)?	☐	☐	☐	
8	2.7	dass das wesentliche der Vereinbarung den betroffenen Personen zur Verfügung gestellt wird?	☐	☐	☐	
8	3	Werden in dem Joint-Controller-Vertrag auch die Verantwortlichkeiten, Beteiligungen und Prozesse im Hinblick auf die Durchführung einer Datenschutzfolgenabschätzung und im Falle von Datenschutzvorfällen geregelt?	☐	☐	☐	
9		**Datenschutzrechte**				
9	1	Wurden die Informationspflichten gegenüber Betroffenen den Mindestanforderungen der Art. 12 DS-GVO, Art. 13 DS-GVO und Art. 14 DS-GVO[11] angepasst (insbes. Datenschutzinformationsblätter sowie Datenschutzerklärung im Internet und Intranet)?	☐	☐	☐	
9	2	Ist durch dokumentierte Prozesse gewährleistet, dass der Adressatenkreis (und ihr Verständnishorizont) der Datenschutzinformation im Hinblick auf die jeweilige Verarbeitung identifiziert wird (z.B. Verbraucher oder Kinder)?	☐	☐	☐	
9	3	Sind die Datenschutzinformationen	☐	☐	☐	
9	3.1	in präziser Form gefasst (insbesondere konkret und bestimmt)?	☐	☐	☐	

[11] Dies umfasst:
Name und Kontaktdaten des Verantwortlichen, Kontaktdaten des DSB, Zwecke der Datenverarbeitung, Rechtsgrundlage für die Verarbeitung, die berechtigten Interessen für die Verarbeitung, Empfänger personenbezogener Daten, Drittstaatenübermittlungen und die Garantien für ein angemessenes Datenschutzniveau im Drittland, wie eine Kopie der Garantien angefordert werden kann, Quellen woher die personenbezogenen Daten stammen, Dauer der Datenspeicherung oder Kriterien zur Festlegung der Dauer, Datenschutzrechte (inklusive Datenportabilität), Widerrufsmöglichkeit von Einwilligungen ohne Wirkung für die Vergangenheit, Beschwerderecht bei Datenschutzaufsicht, bestehende der nicht bestehende Bereitstellungspflicht von personenbezogenen Daten durch den Betroffenen und mögliche Folgen bei Nichtbereitstellung, Bestehen einer automatisierten Entscheidungsfindung, einschließlich Profiling, und aussagekräftige Informationen über die involvierte Logik sowie Tragweite und angestrebte Auswirkungen für den Betroffenen.

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
9	3.2	in leicht zugänglicher Form gefasst (ohne Medienbruch)?	☐	☐	☐	
9	3.3	kostenfrei zugänglich?	☐	☐	☐	
9	3.4	für den Adressatenkreis (z.B. je nach Situation Verbraucher oder Kinder) verständlich?	☐	☐	☐	
9	3.5	in transparenter Form (d.h. auch unter Darlegung der Risiken und Konsequenzen der Verarbeitung)?	☐	☐	☐	
9	3.6	in klarer und einfacher Sprache abgefast (einfach und nicht komplex, jedoch konkret und bestimmt und nicht bloß abstrakt)?	☐	☐	☐	
9	3.7	werden ambivalente Begriffe wie „könnte“, „unter Umständen“, „mag sein, dass“, „oft“, „kann vorkommen, dass“ oder „möglicherweise“ vermieden?	☐	☐	☐	
9	3.8	soweit zur Verständlichkeit notwendig und angemessen, in unterschiedlichen Schichten der Informationsdichte gefasst (sog. layered approach)?	☐	☐	☐	
9	3.9	unterscheidbar (möglichst getrennt) von sonstigen Klauseln und Informationen?	☐	☐	☐	
9	4	Bestehen Prozesse zur Umsetzung von Auskunfts-, Berichtigungs-, Sperrungs- und Löschanfragen sowie zu Widersprüchen und Widerrufen?	☐	☐	☐	
9	5	Stellen die Richtlinien und Prozesse sicher, dass Auskunftsanfragen von Betroffenen innerhalb eines Monats beantwortet werden können?	☐	☐	☐	
9	6	Sind angemessene Authentifizierungsmechanismen implementiert, die sicherstellen, dass es sich tatsächlich um den Betroffenen handelt (insbes. Auskunft nicht an Unbefugte erteilt wird)?	☐	☐	☐	
9	7	Werden die entsprechenden Datenschutzprozesse dokumentiert?	☐	☐	☐	
9	8	Für Unternehmen mit direktem Online-Kundenkontakt zu natürlichen Personen (z.B. Online-Shops, Soziale-Netzwerke): Besteht die Möglichkeit der Betroffenen, per Fernzugriff auf ihre personenbezogenen Daten zuzugreifen?[12]	☐	☐	☐	
9	9	Werden die Betroffenen über ihr Recht auf Datenportabilität informiert?	☐	☐	☐	
9	10	Ist dabei sichergestellt, dass Betroffene das Recht auf Datenportabilität von anderen Rechten (z.B. auf Auskunft oder Kopie) unterscheiden können?	☐	☐	☐	
9	11	Werden Betroffene zusätzlich zu den gesetzlichen Informationspflichten über die regelmäßig zu erwartende Dauer der Bearbeitung von Datenportabilitätsanfragen informiert?	☐	☐	☐	

[12] z. B. Auskunftsportal, das über den Verantwortlichen zugänglich ist.

CHECKLISTE					
Nr.	Thema/Frage	Ja	Nein	N/A	Begründung für N/A
9 12	Werden Betroffene zusätzlich zu den gesetzlichen Informationspflichten über das Recht auf Datenportabilität noch einmal gesondert informiert, bevor ihr Konto geschlossen wird, damit sie dieses vor der Schließung noch umsetzen können?	☐	☐	☐	
9 13	Werden Betroffene innerhalb eines Monats nach Erhalt der Anfrage durch den Verantwortlichen darüber benachrichtigt, falls und warum eine Datenportabilitätsanfrage abgelehnt wird, sowie über das Beschwerderecht bei der Datenschutzaufsichtsbehörde?	☐	☐	☐	
9 14	Sofern sich Betroffene ohnehin authentifizieren müssen (z.B. Username und Passwort auf einer Webseite), ist sichergestellt, dass die Datenportabilität durch zusätzliche Authentifizierungsmerkmale abgesichert ist (z.B. zusätzliche Sicherheitsfrage, One-time-Passwort)?	☐	☐	☐	
9 15	Ist im Falle der Portierung von Ihnen zu einem anderen Verantwortlichen (z.B. falls der Betroffene eine Portierung zu einem Wettbewerber wünscht) eine sichere Authentifizierungsmethode des Empfängers (authentification-by-mandate) vorgesehen (z.B. Token-basierte Authentifizierung)?	☐	☐	☐	
9 16	Können die Daten in einem strukturierten, gängigen und maschinenlesbaren Format dem Betroffenen oder auf dessen Wunsch einem Dritten zur Verfügung gestellt werden?	☐	☐	☐	
9 17	Besteht bereits ein industrieller Standard für Ihre Branche und verwenden Sie diesen?	☐	☐	☐	
9 18	Falls kein industrieller Standard für Ihre Branche besteht, verwenden Sie ein allgemein übliches und offenes Format (wie XML, JSON, CSV), das keine zusätzlichen Lizenzen erfordert, damit die Daten ohne Hindernisse weiterverarbeitet werden können (zu beachten: PDF wäre ungeeignet)?	☐	☐	☐	
9 19	Ist durch dokumentierte Prozesse oder Tools sichergestellt, dass die Daten, welche der Datenportabilität unterliegen (z.B. gesammelte Bestellhistorie, Zugriffslogs, Webseitnutzungsprofil oder vom Betroffenen gemachte Angaben in Eingabemasken), von den Daten, die nicht der Datenportabilität unterliegen (z.B. von Ihnen aus den Rohdaten berechnete Bonitäts-Scorewerte, generiertes Kundensegment etc.), unterschieden werden können?	☐	☐	☐	
9 20	Sind – unter anderem – Mittel eingerichtet, um das Recht auf Datenportabilität durch Download-Tools und APIs umsetzen zu können?	☐	☐	☐	
9 21	Können die Betroffenen durch ein Tool im Einzelnen selbst auswählen und einstellen, welche Daten für die Portierung relevant sind bzw. welche Daten davon ausgeschlossen werden sollen?	☐	☐	☐	

CHECKLISTE					
Nr.	Thema/Frage	Ja	Nein	N/A	Begründung für N/A
9 22	Ist im Rahmen der Zugriffsmöglichkeiten für die Betroffenen sichergestellt, dass sie die Definition, Schema und Struktur der Daten vollständig verstehen können?	☐	☐	☐	
9 23	Werden zu diesem Zweck Dashboards verwendet, die eine zusammenfassende Übersicht und sodann die Möglichkeit vorsehen, dass der Betroffene einzelne Unter-Sets an Daten auswählen und portieren kann?	☐	☐	☐	
9 24	Ist die Option vorgesehen, dass Betroffene bei nachfolgenden Datenportabilitätsanfragen auswählen können, nur den Teil an personenbezogenen Daten zu portieren, der sich seit der letzten Datenportierung geändert oder hinzugetreten ist?	☐	☐	☐	
9 25	Ist in dokumentierter Weise sichergestellt, dass die Datenübermittlung angemessen gesichert ist (insbesondere Ende-zu-Ende-Verschlüsselung)?	☐	☐	☐	
9 26	Sofern der Betroffene die Daten auf seine eigenen Systeme portieren will, wird dieser darauf hingewiesen und hierbei unterstützt, wie er die Datensicherheit angemessen sicherstellen kann (z.B. Anleitungen für Ver- und Entschlüsselungsmöglichkeiten der Daten, Bereitstellung der Möglichkeit die Daten selbst vor dem Download zu verschlüsseln)?	☐	☐	☐	
9 27	Ist sichergestellt, dass die Datenportabilität auf Wunsch des Betroffenen auch über einen vertrauenswürdigen Dritten vermittelt werden kann (sog. Personal Information Management Services, PIMS)?	☐	☐	☐	
9 28	Ist durch dokumentierte Prozesse sichergestellt, dass die Datenportierung nur durchgeführt wird, wenn und soweit dies nicht die Rechte und Freiheiten anderer Personen beeinträchtigt?	☐	☐	☐	
9 29	Ist durch dokumentierte Prozesse sichergestellt, dass Daten zu Drittpersonen, die in einem Datenset zum Betroffenen	☐	☐	☐	
9 30	Ist ein Mechanismus implementiert, der es ermöglicht, die Einwilligung von Drittbetroffenen zu der Portierung auch ihrer Daten einzuholen?	☐	☐	☐	
9 31	Sofern nach dem Recht auf Datenportabilität personenbezogene Daten von einem anderen Verantwortlichen für Sie zur Verfügung gestellt werden: Ist durch dokumentierte Prozesse sichergestellt, dass die Zwecke für die weitere Verarbeitung festgelegt sind, bevor der Betroffene sein Recht auf Datenportabilität bei dem anderen Verantwortlichen geltend macht?	☐	☐	☐	
9 32	Sofern nach dem Recht auf Datenportabilität personenbezogene Daten von einem anderen Verantwortlichen an Sie zur Verfügung gestellt werden: Ist durch dokumentierte Prozesse sichergestellt, dass nur solche personenbezogenen Daten portiert werden, die für diese Zwecke tatsächlich erforderlich und nicht exzessiv sind?	☐	☐	☐	

CHECKLISTE						
Nr.		Thema/Frage	Ja	Nein	N/A	Begründung für N/A
9	33	Wird durch dokumentierte Prozesse oder Mechanismen sichergestellt, dass keine Daten portiert werden, deren Datenportierung ein Geschäftsgeheimnis, geistiges Eigentum oder Urheberrecht verletzen würde?	☐	☐	☐	
9	34	Sofern Daten zu einer natürlichen Person öffentlich gemacht worden sind (z.B. auf der Webseite): Bestehen unter Berücksichtigung der verfügbaren Technologie und Kosten Maßnahmen, nach denen die Empfänger darüber informiert werden, dass die betroffene Person die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat?	☐	☐	☐	
9	35	Bei der Feststellung von Defiziten: Gibt es Verfahren zur Verbesserung des Umgangs mit Betroffenenrechten?	☐	☐	☐	
10		**Datenschutzaufsichtsbehörde**				
10	1	Sofern die Organisation international tätig ist: Wurde geprüft und festgestellt, welche Datenschutzaufsichtsbehörde unter der DS-GVO für Sie zuständig ist?	☐	☐	☐	
10	2	Wurden der Datenschutzaufsichtsbehörde die Kontaktdaten des DSB zur Verfügung gestellt?	☐	☐	☐	
10	3	Wurde der Datenschutzaufsichtsbehörde auch der Name des DSB bei Bestellung zur Verfügung gestellt?	☐	☐	☐	
10	4	Gibt es einen dokumentierten Prozess, der die zügige Bearbeitung von Anfragen von Aufsichtsbehörden regelt?	☐	☐	☐	
11		**Technische und organisatorische Maßnahmen (TOM)**				
11	1	Wurden und werden die TOM für Verarbeitungsverfahren nach Schutzbedarf und Risiko sowie dem Stand der Technik implementiert?	☐	☐	☐	
11	2	Schließen die TOM die Pseudonymisierung und Verschlüsselung personenbezogener Daten ein?	☐	☐	☐	
11	3	Umfassen die TOM die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen?	☐	☐	☐	
11	4	Schließen die TOM die Fähigkeit ein, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen?	☐	☐	☐	
11	5	Bestehen Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen?	☐	☐	☐	

CHECKLISTE					
Nr.	Thema/Frage	Ja	Nein	N/A	Begründung für N/A
11 6	Ist die Implementierung der TOM und ihre regelmäßige Überprüfung dokumentiert und kann dies Vertragspartnern, Aufsichtsbehörden und Gerichten über entsprechende Nachweise belegt werden?	☐	☐	☐	
11 7	Wurden Systeme und Anwendungen hinsichtlich ihrer technischen Ausgestaltung auf ihre Vereinbarkeit mit der DS-GVO geprüft und notwendigenfalls angepasst?	☐	☐	☐	
11 8	Werden bei der Entwicklung, Implementierung und Konfiguration von Systemen und Anwendungen die Grundsätze von Privacy-by-Design und Privacy-by-default sichergestellt?	☐	☐	☐	
12	**Freiwillige Maßnahmen**				
12 1	Werden Verhaltensregeln (Code of Conduct) gem. Art. 40 DS-GVO verwendet und ihre Umsetzung überprüft?	☐	☐	☐	
12 2	Wurden bestimmte Verarbeitungsvorgänge zertifiziert und deren Einhaltung auch überwacht?	☐	☐	☐	
12 3	Wurden verbindliche interne Datenschutzvorschriften (BCR) genehmigt und deren Einhaltung überwacht?	☐	☐	☐	