Die Landesbeauftragte für den
Datenschutz Niedersachsen

# Kriterienkatalog zur Querschnittsprüfung in der Wirtschaft 2018/19

**Frage 1: Vorbereitung auf die DSGVO**

*Wie haben Sie sich als Unternehmen auf die DS-GVO vorbereitet? Schildern Sie (kurz) die Vorgehensweise, welche Bereiche involviert waren und welche Maßnahmen initiiert wurden. Sofern noch nicht alle Maßnahmen vollständig umgesetzt wurden, erläutern Sie bitte auch den Umsetzungsstatus.*

*Hinweis: Ziel dieser Frage war es, sowohl einen Überblick über die unterschiedlichen Herangehensweisen der Unternehmen zu bekommen als auch deren Selbsteinschätzung hinsichtlich ihrer Position auf dem Weg zur Umsetzung DS-GVO. Eine Bewertung der Methodik erfolgt explizit nicht.*

1. Wurden erkennbar alle wesentlichen Unternehmensbereiche eingebunden, die mit personenbezogenen Daten arbeiten (z.B. Personal, IT, Vertrieb/Kundenbetreuung, Marketing)?
2. Gibt es Hinweise darauf, dass Schulungen zur DS-GVO durchgeführt wurden?
3. Wurden erkennbar alle vom Unternehmen geplanten Maßnahmen umgesetzt?

**Frage 2: Verzeichnis von Verarbeitungstätigkeiten (VVT)**

*Wie haben Sie sichergestellt, dass alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen wurden? Wie stellen Sie dessen Aktualität sicher? Legen Sie bitte eine Übersicht Ihrer dokumentierten Verfahren sowie ein Beispielverfahren als Muster bei.*

Art. 30 DS-GVO

1. Wird deutlich, dass bestehende Verfahren an die neue Rechtslage angepasst bzw. neue Verfahren erfasst wurden?
2. Wird deutlich, dass das Verzeichnis von Verarbeitungstätigkeiten (VVT) regelmäßig überprüft und soweit erforderlich aktualisiert wird?
3. Ist aus der Verfahrensübersicht erkennbar, dass die Standardverfahren zur z.B. Bürokommunikation, Personalverwaltung, Lohnabrechnung, Bewerbermanagement, Homepage und Kundenverwaltung dokumentiert sind?
4. Entspricht das übersandte Musterverfahren den rechtlichen Vorgaben des. Art. 30 Abs. 1 DS-GVO?
    a. Sind Name und Kontaktdaten des Verantwortlichen angegeben?
    b. Sind – soweit einschlägig – Name und Kontaktdaten des ggf. gemeinsam mit ihm Verantwortlichen angegeben?
    c. Sind – soweit einschlägig – Name und Kontaktdaten des ggf. Vertreters des Verantwortlichen angegeben?
    d. Sind – soweit einschlägig – Name und Kontaktdaten des ggf. vorhandenen Datenschutzbeauftragten angegeben?

e. Werden die Zwecke der Verarbeitung genannt?
f. Werden die Kategorien betroffener Personen (z.B. Beschäftigte, Kunden, etc.) und die Kategorien personenbezogener Daten (z.B. Mitarbeiter-Stammdaten, Bewerberdaten, Kundenkontaktdaten, Bonitätsdaten, etc.) beschrieben?
g. Werden die Kategorien von Empfängern (z.B. Banken, Sozialversicherungsträger, unternehmensinterne Datenempfänger wie Betriebsrat oder -arzt) gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, angegeben?
h. Wird eine Aussage zur Übermittlung von personenbezogenen Daten an ein Drittland oder an eine intern. Organisation getroffen?
i. Werden die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien angegeben?
j. Erfolgt eine allg. Beschreibung der technischen u. organisatorischen Maßnahmen gem. Art. 32 Abs. 1 DS-GVO?

**Frage 3: Zulässigkeit der Verarbeitung**

*Auf Basis welcher Rechtsgrundlagen verarbeiten Sie personenbezogene Daten? Sofern Sie auch auf Basis von Einwilligungen personenbezogene Daten verarbeiten, legen Sie bitte Ihre verwendeten Muster bei.*

Art. 6, 7 und 8 DS-GVO

1. Sind die genannten Rechtsgrundlagen auf Basis der vorgelegten Verfahrensübersicht plausibel?
2. Sind die Einwilligungserklärungen leicht verständlich, d.h. wird inhaltlich der betroffenen Person das „Ob“ und „Wie“ der Einwilligungserteilung in einer klaren und einfachen Sprache vor Augen geführt?
3. Wird auf die Identität des Verantwortlichen hingewiesen?
4. Wird der Zweck der Verarbeitung genannt?
5. Wird die Art der Daten, die erhoben und verwendet werden, genannt?
6. Wird auf das Widerrufsrecht hingewiesen?
7. Ist aus den Unterlagen erkennbar, dass der Widerruf so einfach ist wie die Erteilung der Einwilligung?
8. Gibt es Anhaltspunkte dafür, dass das Merkmal der Freiwilligkeit fehlen könnte?
9. Wird aus den Unterlagen deutlich, dass die Einwilligungen dokumentiert werden?

**Frage 4: Betroffenenrechte**

*Wie stellen Sie die Einhaltung der Betroffenenrechte (auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit) sicher? Skizzieren Sie Ihre diesbezüglichen Prozesse und gehen Sie insbesondere detailliert darauf ein, wie Sie Ihren Informationspflichten nachkommen. Vorhandene Musterinformationen fügen Sie bitte bei.*

Art. 12, 13, 14, 15, 16, 17, 18, 19, 20 DS-GVO

1. **Informationen nach Art. 13 und 14 (Muster):**
   a. Ist der Umgang mit der Informationspflicht nachvollziehbar und auf das Unternehmen bezogen beschrieben worden (z.B. in einem internen, konkret auf das Unternehmen bezogenen Handlungsleitfaden)?
   b. Werden die Informationen leicht zugänglich zur Verfügung gestellt (z.B. Aushang, Flyer, E-Mail, Brief …)?
   c. Sind die Informationen übersichtlich darstellt (z.B. durch Überschriften, Absätze, Gliederung)?
   d. Sind die Informationen verständlich und in einfacher Sprache formuliert?
   (keine Zweideutigkeit, Vermeidung von Fachvokabular, sofern Fachvokabular verwendet wird, Erläuterung der Fachbegriffe)
   e. Werden die Betroffenen über den für die Verarbeitung Verantwortlichen informiert (Name und Kontaktdaten)?
   f. Weist das Muster auf die Kontaktdaten der/des DSB hin?
   g. Informiert das Muster über die Zwecke der Verarbeitung und nennt die Rechtsgrundlagen?
   h. Wird das berechtigte Interesse beschrieben, sofern eine Verarbeitung nach Art. 6 Abs. 1 Buchstabe f. DS-GVO erfolgt?
   i. Werden die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten genannt?
   j. Informiert der Verantwortliche über die Übermittlung oder die Absicht einer Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation?
   k. Falls i. bejaht wird: Informiert der Verantwortliche über das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Fall von Übermittlungen gemäß Art. 46 oder 47 oder 49 Abs. 1 DS-GVO über die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist oder wo sie verfügbar sind?
   l. Wird bei Erhebung der Daten über die Speicherdauer informiert?
   m. Wird auf das Recht auf Auskunft hingewiesen?
   n. Wird auf das Recht auf Berichtigung hingewiesen?
   o. Wird auf das Recht Löschung hingewiesen?
   p. Wird auf das Recht zur Einschränkung der Verarbeitung hingewiesen?
   q. Wird auf das Widerspruchsrecht hingewiesen?
   r. Wird auf das Recht auf Datenübertragbarkeit hingewiesen?
   s. Wird auf das Recht auf Widerruf der Einwilligung hingewiesen?
   t. Wird auf das Beschwerderecht ggü. der Aufsichtsbehörde hingewiesen?
   u. Wird auf die gesetzliche oder vertragliche Pflicht zur Verarbeitung hingewiesen?

v. Wird bei Bestehen einer automatisierten Entscheidungsfindung (z.B. Profiling) über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person informiert?
w. Wird bei einer beabsichtigten Zweckänderung sichergestellt, dass die betroffene Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen (s. vorstehend lit. l bis v) erhält?
x. Gibt es eine Datenschutzerklärung auf der Website?
y. Ist die Datenschutzerklärung leicht zu finden (max. 2 Clicks ab der Startseite)?
z. Ist die Datenschutzerklärung verständlich und in einfacher Sprache formuliert? (Definition s. Buchst. d)

**2. Auskunftsrecht**

a. Ist der Umgang mit dem Auskunftsrecht plausibel und logisch nachvollziehbar und auf das Unternehmen bezogen beschrieben worden (z.B. in einem internen, konkret auf das Unternehmen bezogenen Handlungsleitfaden)?
b. Wird beschrieben, dass die Identität der natürlichen Person als betroffene Person überprüft wird?
c. Wird aus dem beschriebenen Prozess deutlich, dass die Auskunft unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags erteilt wird?
d. Kann der Prozessbeschreibung entnommen werden, dass durch den Verantwortlichen voraussichtlich vollständige Auskünfte erteilt werden (z.B. durch Beschreibung der eingebundenen Unternehmensbereiche, Hinweis auf Nutzung einer Softwareanwendung)?
   *<u>Hinweis:</u> Eine vollständige Auskunft muss folgende Inhalte abdecken:*
   - *alle Verarbeitungszwecke*
   - *alle Kategorien der verarbeiteten personenbezogenen Daten*
   - *alle Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden*
   - *alle Empfänger in Drittländern oder bei int. Organisationen*
   - *die geplante Speicherdauer oder soweit dazu Angaben nicht möglich sind, die Kriterien für die Festlegung der Speicherdauer*
   - *das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde*
e. Ist aus den Unterlagen erkennbar, dass der Verantwortliche auf Antrag eine Kopie der personenbezogenen Daten zur Verfügung stellt?

**3. Berichtigungsrecht**

a. Ist der Umgang mit dem Berichtigungsrecht nachvollziehbar und auf das Unternehmen bezogen beschrieben worden (z.B. in einem internen, konkret auf das Unternehmen bezogenen Handlungsleitfaden)?
b. Wird beschrieben, dass die Identität der natürlichen Person als betroffene Person überprüft wird?
c. Wird aus dem beschriebenen Prozess deutlich, dass die betroffene Person in Bezug auf die ergriffenen Maßnahmen (Berichtigung) unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags informiert wird?
d. Ist den Unterlagen zu entnehmen, dass der Verantwortliche, soweit er die Daten anderen Empfänger offengelegt hat, allen Empfängern jede Berichtigung mitteilt?

**4. Löschung**

a. Ist der Umgang mit dem Recht auf Löschung nachvollziehbar und auf das Unternehmen bezogen beschrieben worden (z.B. in einem internen, konkret auf das Unternehmen bezogenen Handlungsleitfaden)?

b. Wird beschrieben, dass die Identität der natürlichen Person als betroffene Person überprüft wird?

c. Wird aus dem beschriebenen Prozess deutlich, dass die betroffene Person in Bezug auf die ergriffenen Maßnahmen (Löschung) unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags informiert wird?

d. Wird beschrieben, unter welchen Voraussetzungen Daten gelöscht werden?
*Hinweis: Es bedarf in folgenden Fällen einer Datenlöschung:*
- *wenn die Speicherung der Daten nicht mehr erforderlich ist*
- *bei Widerruf der Einwilligung, sofern keine anderweitige Rechtsgrundlage für die Verarbeitung einschlägig ist*
- *bei Widerspruch gegen die Verarbeitung gem. Art. 21 Abs. 1 DS-GVO und Nichtvorlage vorrangiger berechtigter Gründe oder bei Widerspruch gegen die Verarbeitung gem. Art. 21 Abs. 2 DS-GVO (Werbewiderspruch)*
- *bei unrechtmäßiger Verarbeitung (Verarbeitung der Daten ohne Rechtsgrundlage)*
- *soweit die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist*

e. Ist den Unterlagen zu entnehmen, dass der Verantwortliche, soweit er die Daten anderen Empfänger offengelegt hat, allen Empfängern jede Löschung mitteilt?

**5. Einschränkung der Verarbeitung**

a. Ist der Umgang mit dem Recht auf Einschränkung der Verarbeitung nachvollziehbar und auf das Unternehmen bezogen beschrieben worden (z.B. in einem internen, konkret auf das Unternehmen bezogenen Handlungsleitfaden)?
*Hinweis: In folgenden Fällen hat eine Einschränkung der Verarbeitung zu erfolgen:*
- *wenn die Richtigkeit der verarbeiteten Daten strittig ist, solange die Richtigkeit der Daten überprüft wird*
- *bei unrechtmäßiger Verarbeitung, soweit die betroffene Person eine Löschung ablehnt und eine Einschränkung der Verarbeitung verlangt*
- *soweit der Verantwortliche die Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt*
- *bei Widerspruch der betroffenen Person gem. Art. 21 Abs. 1 DS-GVO, bis feststeht, ob die berechtigten Gründe der betroffenen Person oder des Verantwortlichen überwiegen*

b. Wird beschrieben, dass die Identität der natürlichen Person als betroffene Person überprüft wird?

c. Wird aus dem beschriebenen Prozess deutlich, dass die betroffene Person in Bezug auf die ergriffenen Maßnahmen (Einschränkung der Verarbeitung) unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags informiert wird?

d. Ist beschrieben, dass die betroffene Person sowohl über die Einschränkung als auch vor deren Aufhebung über die Aufhebung unterrichtet wird?

e. Ist den Unterlagen zu entnehmen, dass der Verantwortliche, soweit er die Daten anderen Empfänger offengelegt hat, allen Empfängern jede Einschränkung mitteilt?

6. **Datenübertragbarkeit**
    a. Ist der Umgang mit dem Recht auf Datenübertragbarkeit nachvollziehbar und auf das Unternehmen bezogen beschrieben worden (z.B. in einem internen, konkret auf das Unternehmen bezogenen Handlungsleitfaden)?
    b. Wird beschrieben, dass die Identität der natürlichen Person als betroffene Person überprüft wird?
    c. Wird aus dem beschriebenen Prozess deutlich, dass der betroffenen Person die Daten unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung gestellt werden?
    d. Wird beschrieben, dass der Verantwortliche bezüglich des Rechts auf Datenübertragbarkeit sicherstellt, dass die Daten in einem gängigen, strukturierten und maschinenlesbaren Format zur Verfügung gestellt werden (d.h. von einer gebräuchlichen Softwareanwendung leicht zu identifizieren, zu extrahieren und zu öffnen)?

**Frage 5: technischer Datenschutz**

*a. Wie stellen Sie sicher, dass Ihre technischen und organisatorischen Maßnahmen bzw. die Ihrer Dienstleister ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten?*

Art. 32 DS-GVO

1. Ist ein risikobasierter Ansatz in der Antwort berücksichtigt?
2. Wurde gezeigt, dass verstanden wurde, dass auf Basis des ermittelten Risikos die dargelegten technisch- und organisatorischen Maßnahmen geeignet sind, das Risiko auf ein angemessenes Schutzniveau zu reduzieren?
3. Zeigt die Antwort, dass verstanden wurde, dass ein Abwägungsprozess erfolgen muss (Risiko, Implementierungskosten und Stand der Technik), um ein angemessenes Schutzniveau zu erreichen?
4. Zeigt die Antwort, dass das Unternehmen erkannt hat, dass die Verantwortung für die technisch- und organisatorischen Maßnahmen des Dienstleisters beim Verantwortlichen bleibt?

*b. Wie stellen Sie sicher, dass Ihre technischen und organisatorischen Maßnahmen an den jeweiligen Stand der Technik angepasst werden?*

Art. 32 Abs. 1 Buchstabe d) DS-GVO

*<u>Hinweis:</u> Der Stand der Technik bezieht sich auf die bestmöglichen marktfähigen Techniken, die aktuell einen hohen Sicherheitsstandard aufweisen, selbst wenn sich ihr Einsatz in der Praxis (noch) nicht durchgesetzt hat. Im Einzelfall ist die Forderung dadurch begrenzt, dass lediglich das jeweils technisch Machbare gefordert wird. Durch den technischen Wandel ist die Auswahlentscheidung bei Vorliegen neuer technischer Maßnahmen erneut zu treffen. Die Einordnung ist dadurch dynamisch zu verstehen. Nach unten grenzt sich der Stand der Technik von den „anerkannten Regeln der Technik“ (z.B. DIN-Normen), nach oben vom „Stand von Wissenschaft und Technik“ (neueste technische und wissenschaftliche Erkenntnisse) ab.*

1. Wurde der Begriff "Stand der Technik" richtig verstanden?

2. Zeigt die Antwort, dass verstanden wurde, dass das Unternehmen nachweisen muss, dass die gewählten technisch-organisatorischen Maßnahmen den Stand der Technik berücksichtigen?
3. Zeigt die Antwort, dass verstanden wurde, dass sich der "Stand der Technik" kontinuierlich weiterentwickelt?
4. Zeigt die Antwort, dass verstanden wurde, dass die technisch-organisatorischen Maßnahmen kontinuierlich den jeweiligen "Stand der Technik" berücksichtigen müssen?

*c. Wie stellen Sie sicher, dass Sie für die von Ihnen aktuell oder zukünftig eingesetzten IT-Anwendungen ein dokumentiertes datenschutzkonformes Rollen- und Berechtigungskonzept haben?*

Art. 32 Abs. 1 Buchstabe b) DS-GVO

1. Zeigt die Antwort, dass verstanden wurde, dass die Kenntnis und Berücksichtigung der Organisation für das Rechte- und Rollenkonzept relevant ist?
2. Zeigt die Antwort, dass verstanden wurde, dass eine Funktionstrennung, sowie die Trennung von Person und Rolle berücksichtigt werden muss?
3. Zeigt die Antwort, dass verstanden wurde, dass die Dokumentation der zugelassenen Benutzer und Rechteprofile im Rechte- und Rollenkonzept berücksichtigt werden muss?
4. Zeigt die Antwort, dass verstanden wurde, dass die Auswahl von Identitäts- und Berechtigungsmanagementsystemen im Rechte- und Rollenkonzept berücksichtigt werden muss?

*d. Wie stellen Sie sicher, dass bei der Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mit berücksichtigt werden (Privacy by Design und by Default)?*

Art. 25 DS-GVO

1. Zeigt die Antwort, dass verstanden wurde, dass Datenschutz als Standardeinstellung zu berücksichtigen ist?
2. Zeigt die Antwort, dass verstanden wurde, dass der Datenschutz während des gesamten Lebenszyklus beachtet werden muss?
3. Zeigt die Antwort, dass verstanden wurde, dass die Minimierung der Verarbeitung personenbezogener Daten anzustreben ist?
4. Zeigt die Antwort, dass verstanden wurde, dass Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt werden sollte?

**Frage 6: Datenschutz-Folgenabschätzung**

*a. Wie stellen Sie sicher, dass Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen erkannt und für diese eine Datenschutz-Folgenabschätzung durchgeführt wird?*

Art. 35 DS-GVO

1. Werden alle Normen, nach denen ein hohes Risiko zu bejahen ist, geprüft?
    b. Art. 35 Abs. 4?
    c. Art. 35 Abs. 3?
    d. Art. 35 Abs. 1?
2. Welche Methodik zur Risikobestimmung wird verwendet?
    a. WP 248?
    b. KP Nr. 18 – Risiko?
    c. Eigene Methode?
    d. Ist die beschriebene eigene Methode geeignet, hochriskante Verfahren zu identifizieren?
3. Ist beschrieben, wer für die Prüfung zuständig ist?
4. Wird beschrieben, wo die Schwellwertprüfung dokumentiert wird?

*b. Haben Sie in Ihrem Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen identifiziert? Welche? Fügen Sie bitte die jeweilige Dokumentation zur Datenschutz-Folgenabschätzung bei.*

Art. 35, 36 DS-GVO

1. Welche DSFA wurde beispielhaft ausgewertet?
2. Wurden Verfahren mit voraussichtlich hohen Risiken für die Rechte und Freiheiten natürlicher Personen durch den Verantwortlichen identifiziert?
3. Inhaltliche Prüffähigkeit
    a. Liegt eine systematische Beschreibung der Verarbeitungsvorgänge vor?
    b. Liegt eine systematische Beschreibung der Verarbeitungszwecke vor?
    c. Ergebnis
4. Musste für die vorliegende Form der Verarbeitung eine DSFA gemacht werden?
    a. Ja
    b. Nein, weil kein hohes Risiko
    c. Nein, weil bereits für einen ähnlichen Verarbeitungsvorgang eine DSFA durchgeführt wurde
    d. Nein, weil die Verarbeitung vor dem 25. Mai 2018 begonnen hat und die Datenschutzaufsichtsbehörde oder der Datenschutzbeauftragte das Verfahren im Rahmen einer Vorabkontrolle geprüft haben und sich die Risiken seitdem nicht geändert haben

5. Liegt eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck vor?
    a. Ist die Notwendigkeit der Verarbeitung behauptet?
    b. Ist die Notwendigkeit begründet?
    c. Ist die Verhältnismäßigkeit der Verarbeitungsvorgänge behauptet?
    d. Ist die Verhältnismäßigkeit der Verarbeitungsvorgänge begründet?
6. Liegt eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen vor?
    a. Wird die Methode zur Risikobewertung beschrieben?
    b. Wieviel der folgenden Gewährleistungsziele werden betrachtet: Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz, Intervenierbarkeit, Nichtverkettung
    c. Werden Risiken benannt?
    d. Wird die Schwere des Schadens angegeben?
    e. Sind die Einstufungen der Schwere des Schadens begründet?
    f. Wird die Eintrittswahrscheinlichkeit angegeben?
    g. Sind die Einstufungen der Eintrittswahrscheinlichkeiten begründet?
    h. Erfolgt die Begründung unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung?
    i. Werden Risikoquellen benannt? Z.B. Hacker, Hardwareausfall, eigene Mitarbeiter
7. Abhilfemaßnahmen
    a. Sind Abhilfemaßnahmen genannt?
    b. Sind die Abhilfemaßnahmen beschrieben?
    c. Berücksichtigen die Abhilfemaßnahmen die festgestellten Risiken?
    d. Berücksichtigen die Abhilfemaßnahmen die Implementierungskosten?
    e. Berücksichtigen die Abhilfemaßnahmen den Stand der Technik?
    f. Erfolgt eine Restrisikobetrachtung?
8. Ist geprüft worden, ob ein Verfahren der vorherigen Konsultation nach Art. 36 durchzuführen ist?
9. Ist der Rat des Datenschutzbeauftragten nach Art. 35 Abs. 2 eingeholt worden?
10. Ist der Standpunkt der betroffenen Personen nach Art. 35 Abs. 9 eingeholt worden?

**Frage 7: Auftragsverarbeitung**

*Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern an die neuen Regelungen der DS-GVO angepasst? Sofern Sie Musterverträge verwenden, fügen Sie diese bitte bei, darüber hinaus fügen Sie bitte einen aktuellen Beispielvertrag mit einem Ihrer Auftragsverarbeiter bei.*

Art. 28 DS-GVO

1. Ist den Unterlagen zu entnehmen, dass die bestehenden Verträge an die neue Rechtslage angepasst wurden?
2. Entspricht das übersandte Muster den rechtlichen Anforderungen?
    a. Wird der Gegenstand der Verarbeitung im Vertrag festgelegt?
    b. Wird die Dauer der Vereinbarung fixiert?
    c. Enthält der Vertrag Angaben zu Art (Modalitäten wie z.B. Erheben, die Organisation, die Anpassung, Verbreitung oder auch Vernichtung der Daten) und Zweck der Verarbeitung?

   d. Wurden die Art der personenbezogenen Daten und die Kategorien betroffener Personen festgelegt?
   e. Gibt es eine Dokumentation der Weisungsbefugnisse des Verantwortlichen?
   f. Gibt es eine Regelung in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation?
   g. Ist mittels des Mustervertrags gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben? (z.B. mittels Zusicherung, dass eine Verpflichtung gem. Art. 29 vorliegt?)
   h. Gibt es eine Regelung, wonach der Auftragsverarbeiter alle gem. Art. 32 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen ergreift?
   i. Wurde im Mustervertrag festgelegt, dass die Inanspruchnahme eines weiteren Auftragsverarbeiters der vorherigen Genehmigung des Verantwortlichen bedarf bzw. ein Unterauftragsverbot vereinbart?
   j. Wurde für den Fall einer Unterbeauftragung geregelt, dass den Unterauftragsverarbeiter die gleichen Pflichten aufzuerlegen sind, wie dem Auftragsverarbeiter?
   k. Enthält der Mustervertrag eine Regelung, wonach der Auftragsverarbeiter den Verantwortlichen bei dessen Umsetzung der Betroffenenrechte unterstützt?
   l. Beinhaltet der Mustervertrag eine Regelung, wonach der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 genannten Pflichten unterstützt?
   m. Wurden die Verpflichtungen des Auftragsverarbeiters nach Auftragsbeendigung fixiert (nach Wahl des Verantwortlichen Löschung oder Rückgabe aller personenbezogenen Daten)?
   n. Sind die Kontrollrechte des Verantwortlichen festgelegt worden?

3. Entspricht der übersandte Beispielvertrag den rechtlichen Anforderungen?
   a. Wurde der Gegenstand der Verarbeitung im Vertrag festgelegt?
   b. Wurde die Dauer der Vereinbarung fixiert?
   c. Enthält der Vertrag Angaben zu Art und Zweck der Verarbeitung?
   d. Wurden die Art der personenbezogenen Daten und die Kategorien betroffener Personen festgelegt?
   e. Gibt es eine Dokumentation der Weisungsbefugnisse des Verantwortlichen?
   f. Gibt es eine Regelung in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation?
   g. Ist mittels des Beispielvertrags gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben? (z.B. mittels Zusicherung, dass eine Verpflichtung gem. Art. 29 vorliegt?)
   h. Gibt es eine Regelung, wonach der Auftragsverarbeiter alle gem. Art. 32 DS-GVO erforderlichen technischen und organisatorischen Maßnahmen ergreift?
   i. Wurde im Beispielvertrag festgelegt, dass die Inanspruchnahme eines weiteren Auftragsverarbeiters der vorherigen Genehmigung des Verantwortlichen bedarf bzw. ein Unterauftragsverbot vereinbart?
   j. Wurde für den Fall einer Unterbeauftragung geregelt, dass den Unterauftragsverarbeiter die gleichen Pflichten aufzuerlegen sind, wie dem Auftragsverarbeiter?
   k. Enthält der Beispielvertrag eine Regelung, wonach der Auftragsverarbeiter den Verantwortlichen bei dessen Umsetzung der Betroffenenrechte unterstützt?
   l. Beinhaltet der Beispielvertrag eine Regelung, wonach der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 genannten Pflichten unterstützt?

m. Wurden die Verpflichtungen des Auftragsverarbeiters nach Auftragsbeendigung fixiert (nach Wahl des Verantwortlichen Löschung oder Rückgabe aller personenbezogenen Daten)?
n. Sind die Kontrollrechte des Verantwortlichen festgelegt worden?

**Frage 8: Datenschutzbeauftragter**

*Wie ist Ihr Datenschutzbeauftragter in Ihre Organisation eingebunden? Welche Fachkundenachweise hat er?*

Art. 37, 38 DS-GVO

1. Organisatorische Einbindung bei einem internen DSB:
   a. Berichtet der betriebliche Datenschutzbeauftragte (bDSB) in seiner Funktion direkt an die Geschäftsleitung?
   b. Hat der bDSB noch eine Linienaufgabe im Unternehmen?
   c. Falls ja: Welche Position wird im Unternehmen noch bekleidet?
   d. Besteht hierdurch die Gefahr einer Befangenheit und damit ein Interessenkonflikt? (z.B. DSB ist Inhaber selbst, Vorstand, Geschäftsführung oder Leitung HR oder IT)
2. Organisatorische Einbindung bei einem externen DSB:
   Besteht die Gefahr einer Befangenheit und damit ein Interessenkonflikt?
   (z.B. weil der benannte DSB daneben für das Unternehmen noch als Dienstleister für IT Dienstleistungen tätig ist)
3. Lässt sich aus den Unterlagen die aktuelle und ausreichende Fachkunde der/des DSB entnehmen?
   In die Bewertung der Fachkunde fließen z.B. ein: Aus- und Fortbildungen im Datenschutz, Umfang der Erfahrung (Dauer) im Datenschutz, berufliche Ausbildung (z.B. Jurist, Informatiker), Beteiligung in etablierten Datenschutznetzwerken (z.B. Erfa-Kreis, GDD, BvD)
4. Veröffentlichung der Kontaktdaten des DSB:
   a. Erfolgte die Veröffentlichung auf der Internetseite des Unternehmens?
   b. Sind die Kontaktdaten des DSB dort leicht auffindbar? (max. 2 Clicks ab der Startseite)
5. Erfolgte eine Meldung des DSB bei der Aufsichtsbehörde?

**Frage 9: Meldepflichten**

*Wie stellen Sie sicher, dass Ihr Unternehmen Datenschutzverstöße fristgemäß an die Aufsichtsbehörde meldet? Skizzieren Sie Ihre diesbezüglichen Prozesse.*

Art. 33, 34 DS-GVO

1. Wurde der Prozess zur Meldung der Datenschutzverstöße nachvollziehbar dargestellt?
2. Sind im Meldeprozess die Verantwortlichkeiten (wer macht was) klar geregelt?
3. Wird die 72-Std.-Frist erkennbar berücksichtigt?
4. Wird deutlich, dass die Mitarbeiter hinsichtlich dieses Prozesses sensibilisiert wurden?
5. Ist aus den Unterlagen erkennbar, dass die Datenschutzverstöße dokumentiert werden?

**Frage 10: Dokumentation**

*Wie können Sie die Einhaltung aller vorstehend in Ziff. 2 – 9 genannten Pflichten nachweisen?*

Art. 5 Abs. 2 DS-GVO

Ergibt sich aus der Antwort oder den sonstigen Unterlagen, dass eine Dokumentation zu jeder der abgefragten Pflichten vorhanden ist?