Die Landesbeauftragte für den
Datenschutz Niedersachsen

Abschlussbericht November 2019

Querschnittsprüfung der LfD Niedersachsen von 50 Unternehmen zur Umsetzung der seit dem 25. Mai 2018 unmittelbar geltenden Datenschutz-Grundverordnung (EU) 2016/679 (DS-GVO)

Inhaltsverzeichnis

1. Teil: Zusammenfassung

50 große und mittelgroße Unternehmen mit Hauptsitz in Niedersachsen sollten in der sogenannten Querschnittsprüfung darlegen, ob und wie sie die Regelungen der Datenschutz-Grundverordnung (DS-GVO) in der betrieblichen Praxis mit Leben füllen. Hierfür sollten sie Fragen zu zehn Komplexen beantworten, welche die wesentlichen Bereiche der DS-GVO abdecken. In der Auswertung der Antworten wurde jedem Fragenkomplex eine Ampelfarbe zugeordnet, die zeigte, ob in diesem Bereich kein bzw. kaum (grün), normaler (gelb) oder erheblicher Handlungsbedarf (rot) herrschte. Ausgehend von den einzelnen Ergebnissen der zehn Komplexe erhielt jedes Unternehmen eine Gesamtbewertung, ebenfalls in Rot, Gelb oder Grün.

Die geringsten Schwierigkeiten bereiteten den Unternehmen die Bereiche Auftragsverarbeitung (AV), Datenschutzbeauftragte (DSB), Meldepflichten von Datenschutzverletzungen und Dokumentation. Hier wurden nur gelegentlich Defizite festgestellt. Etwas häufiger mussten die Antworten in den Komplexen Verzeichnis von Verarbeitungstätigkeiten, Einwilligungen und Betroffenenrechte bemängelt werden. Verbreitet erhebliche Defizite lagen bei den Themen technisch-organisatorischer Datenschutz und Datenschutz-Folgenabschätzung (DSFA) vor. Besonders gravierend: Zum Teil wurde bei der Risikoeinschätzung der Fokus auf die (finanziellen) Risiken für das Unternehmen gelegt statt – wie im Datenschutz nötig – auf die Risiken für die Betroffenen. Insgesamt standen nach zwei Prüfungsschritten 9 Unternehmen auf Grün, 32 auf Gelb und 9 auf Rot.

2. Teil: Vorbereitung und Durchführung

1. Ziel der Prüfung

In einer branchenübergreifenden Prüfung wurden Ende Juni 2018 50 Unternehmen unterschiedlicher Größe angeschrieben, denen Fragen zu zehn Bereichen des Datenschutzes gestellt wurden. Im Vordergrund der Querschnittsprüfung stand die Aufklärung und Sensibilisierung der Unternehmen. Das Hauptanliegen war es zu identifizieren, ob und wo es bei den verantwortlichen Stellen bei der Umsetzung der DS-GVO noch Nachholbedarf gibt. Zudem sollte mit der Prüfung das Bewusstsein für den Datenschutz im Allgemeinen und die Vorschriften der DS-GVO im Speziellen gestärkt werden. Im Vordergrund stand nicht der Kontrollaspekt. Ziel der Prüfung war es auch nicht, möglichst viele Fehler zu finden und Bußgelder zu verhängen. Sollten während der Prüfung gravierende Verstöße gegen die DS-GVO festgestellt werden, waren jedoch auch weitergehende Maßnahmen bis hin zur Verhängung eines Bußgeldes nicht ausgeschlossen.

2. Unternehmensauswahl

Den Fragebogen erhielten 20 große und 30 mittelgroße Unternehmen aus verschiedenen Branchen, die ihren Sitz in Niedersachsen haben. Eine umfassende Prüfung einzelner Branchen war nicht geplant. Bei den „großen Unternehmen“ orientierte sich die LfD Niedersachsen an einer Übersicht der Nord/LB zu den 100 größten niedersächsischen Unternehmen. Von dieser Liste wurden 20 ausgewählt.

Der Begriff „mittelgroße Unternehmen“ wurde gewählt, da der Fokus ausdrücklich nicht auf kleinen Unternehmen lag.

Bei der konkreten Auswahl der Unternehmen wurden folgende Aspekte berücksichtigt:

- Prüfung nicht allein von Firmen der Region Hannover, sondern von Unternehmen aus ganz Niedersachsen.
- Unternehmen sollten möglichst nicht nur die Daten ihrer Mitarbeiterinnen und Mitarbeiter verarbeiten, sondern auch die Daten ihrer Kundinnen und Kunden. Bei letzteren sollte es sich zudem möglichst nicht nur um Geschäftskunden, sondern verstärkt auch um solche aus dem Consumer-Bereich handeln.
- Abdeckung möglichst verschiedener Branchen: von Versicherungen über den Finanzbereich und den Handel bis hin zu Wirtschafts- und Steuerberatern. Von Versorgungsunternehmen und Personaldienstleistungen über Wach- und Schließgesellschaften bis hin zur Touristikbranche.
- Keine Teilnehmer von Schwerpunktprüfungen der LfD Niedersachsen in der jüngsten Vergangenheit zur Vermeidung einer übermäßigen Belastung einzelner Unternehmen.
- Möglichst eine Unternehmensgröße, die zur Bestellung eines Datenschutzbeauftragten verpflichtet. Der kleine Handwerksbetrieb oder Einzelhändler sollte nicht betroffen sein.

3. Fragebogen

Der für die Querschnittsprüfung erstellte Fragebogen (siehe Anlage 1) basierte auf der Checkliste für kleine und mittelständische Unternehmen, welche die LfD Niedersachsen im November 2017 veröffentlicht hatte. Mit dieser Liste hatte die LfD den Unternehmen sechs Monate vor dem 25. Mai 2018 eine Hilfestellung zur Vorbereitung auf die DS-GVO gegeben. Diese sollte die Unternehmen in die Lage versetzten, Bereiche zu identifizieren, in denen sie bereits gut aufgestellt waren und wo es noch Handlungs- bzw. Optimierungsbedarf gab. Bereits zu diesem Zeitpunkt wurde explizit darauf hingewiesen, dass die Inhalte dieser Checkliste zum Gegenstand zukünftiger Prüfungen gemacht würden.

Mit den zehn Fragenkomplexen der Querschnittsprüfung wurden die nach Ansicht der LfD Niedersachsen für Verantwortliche wesentlichen Bereiche der DS-GVO angesprochen. Die Fragen betrafen die Themen Verzeichnis von Verarbeitungstätigkeiten und Rechtsgrundlagen, die Betroffenenrechte, den technisch-organisatorischen Datenschutz, die DSFA, die Auftragsverarbeitung, die Bestellpflicht für Datenschutzbeauftragte, die Meldepflichten sowie die Rechenschaftspflicht. Zudem sollten die Unternehmen generell darstellen, wie sie sich auf die DS-GVO vorbereitet hatten, welche Unternehmensbereiche involviert waren und welche Maßnahmen initiiert wurden.

Der Fragebogen wurde mit Datum vom 29. Juni 2018 versandt. Die Unternehmen hatten sechs Wochen Zeit, um die Fragen schriftlich zu beantworten. Auf Antrag wurde die Frist verlängert, wovon acht Unternehmen Gebrauch machten. Beantwortet wurde der Fragebogen von allen angeschriebenen Unternehmen. Der Umfang der eingereichten Unterlagen lag zwischen 10 und mehr als 300 Seiten. Bei mehr als 40 Unternehmen waren die Unterlagen unvollständig, entsprechende Nachforderungsschreiben wurden im September 2018 versandt. Eine Nachforderung erfolgte nur bei fehlenden Antworten und Unterlagen wie z.B. Mustern. Bei inhaltlich unzureichenden Antworten stellte die LfD keine Nachforderung.

a. Abfrage der Unternehmensprozesse

Besonderer Wert wurde bei der Konzeption der Fragen auf die Darstellung der Prozesse in den betroffenen Unternehmen gelegt. Gerade diese geben in besonderer Weise Aufschluss darüber, wie gut ein Verantwortlicher in der Lage ist, die Anforderungen der DS-GVO zu erfüllen, da die Prozesse die grundsätzliche Vorgehensweise und Methodik wiederspiegeln. Die Fragen wurden zudem bewusst offen gehalten, um den Unternehmen die Möglichkeit zu eröffnen, ihre Antworten auf ihre konkrete Situation und Größe anzupassen. Gleichzeitig sollten durch die Fragen Hinweise darüber eingeholt werden, wie weit die einzelnen Anforderungen der DS-GVO bei den Unternehmen bereits erkannt und prozessual umgesetzt wurden. Dahinter stand der Ansatz, dass ohne die Verankerung der datenschutzrechtlichen Anforderungen in konkrete Unternehmensprozesse eine dauerhafte Erfüllung der Anforderungen nicht gewährleistet werden kann.

b. Eigenverantwortliche Darstellung statt Multiple-Choice

Neben dem Fokus auf der Darstellung von Prozessen wurde zudem bewusst auf eine kleinteilige Abfrage der Erfüllung rechtlicher Vorgaben verzichtet. Durch eine solche Abfrage wäre automatisch auch ein Teil des Lösungsweges vorgegeben worden. Das eigene (Mit-) Denken hätte nicht in dem Maße im Vordergrund gestanden, wie es bei offenen Fragen der Fall ist.

Bei einer Vielzahl an kleinteiligen Fragen ist es anhand der Antworten nicht mehr unbedingt erkennbar, ob der Befragte auch ohne die konkreten Fragen an diese Details gedacht hätte. Mit dem gewählten Ansatz ist der Lösungsweg dagegen nicht schon durch die Fragen selbst vorgezeichnet. Die Befragten mussten diesen vielmehr eigenverantwortlich darstellen und damit beweisen, dass sie sich mit der Thematik in ihrem Unternehmen auseinander gesetzt, die rechtlichen Anforderungen auf ihre Firma übertragen sowie die erforderlichen Prozesse entwickelt und implementiert hatten.

4. Kriterienkatalog

Um eine einheitliche Bewertung der Antworten zu gewährleisten, wurde zu den zehn Fragekomplexen ein detaillierter Katalog aus circa 200 Einzelkriterien erarbeitet (siehe Anlage 2). Mit dem Katalog war neben der Gewährleistung einer konsistenten Bewertung auch eine (weitere) Hilfestellung bezweckt. Anhand der Kriterien sollte verdeutlicht werden, was ein Verantwortlicher alles zu beachten hat, um datenschutzkonform aufgestellt zu sein. Daher wurde der Kriterienkatalog am Ende der Querschnittsprüfung veröffentlicht und so allen (niedersächsischen) Unternehmen zugänglich gemacht.

a. Gegenstand der Kriterien

Die Kriterien basieren auf den rechtlichen Anforderungen der DS-GVO. Im Hinblick auf das Ziel der Querschnittsprüfung, einen Überblick über den Umsetzungstand der DS-GVO in den Unternehmen zu erhalten, wurde bei den Kriterien der Fokus teilweise ausschließlich auf das methodische Vorgehen gelegt und keine inhaltliche Auswertung vorgenommen. Dies war insbesondere bei den DSFA der Fall. Das heißt, für diese wurde bewertet, ob die dazu eingereichten Unterlagen zumindest die Inhalte nach Art. 35 Abs. 7 DS-GVO enthalten. So wurde zum Beispiel geprüft, ob eine Einstufung der Schwere eines Risikos stattfand und diese begründet wurde. Es wurde dagegen nicht geprüft, ob die konkrete Einstufung von der LfD Niedersachsen für richtig gehalten wird. Eine detaillierte inhaltliche Prüfung hätte den für die Querschnittsprüfung kalkulierten zeitlichen Prüfungsrahmen bei knapp 200 vorgelegten DSFA weit überschritten.

b. Bewertungsmethodik

Im Zuge der Auswertung wurde die Erfüllung jedes Einzelkriteriums für alle der 50 befragten Unternehmen bewertet. Zu jedem Kriterium waren drei Bewertungen möglich: Kriterium erfüllt ja/nein/teilweise.

Alle Einzelkriterien, die es zu einer Frage gab, wurden anschließend zu einer Gesamtbewertung pro Fragenkomplex zusammengefasst und einer Ampelfarbe (rot/gelb/grün) zugeordnet.

- Mit „Grün“ wurden die Komplexe bewertet, die inhaltlich weitestgehend zufriedenstellend beantwortet worden waren, mit nur geringen Abweichungen bei der Bewertung der Einzelkriterien. Bei „Grün“ wurde kein konkreter Handlungsbedarf auf Seiten der Unternehmen gesehen.
- Mit „Gelb“ wurden die Fragenkomplexe bewertet, bei denen es noch Handlungsbedarf gab. „Gelb“ wurde vergeben, soweit die Einzelkriterien häufiger mit „teilweise“ oder zum Teil auch mit „nein“ bewertet wurden.
- Auf „Rot“ standen schließlich die Komplexe, bei denen die Antworten auf erheblichen Handlungsbedarf schließen ließen. Hier wurden die Einzelkriterien verbreitet mit „teilweise“ und „nein“ bewertet.

Der LfD Niedersachsen war dabei bewusst, dass die Nichterfüllung von Kriterien zum Teil auch daraus resultieren konnte, dass das eine oder andere Unternehmen den Erwartungshorizont der Aufsichtsbehörde hinsichtlich der Detailtiefe der Ausführungen nicht richtig eingeschätzt hatte. Hier war und ist jedes der geprüften Unternehmen im Nachgang gefordert, den jeweiligen individuellen Anpassungsbedarf auf Basis der mitgeteilten Prüfungsergebnisse zu erkennen und bei Bedarf die Unternehmensprozesse zu modifizieren.

Die eingereichten Unterlagen wurden zudem nur in dem für die Prüfung des Kriterienkataloges erforderlichen Rahmen gesichtet und ausgewertet. Darüber hinaus erfolgte keine Prüfung. Es kann somit am Ende der Querschnittsprüfung eine konkrete Aussage darüber getroffen werden, inwieweit die Unternehmen die bewerteten Kriterien erfüllt haben. Es kann jedoch keine Aussage darüber getroffen werden, inwieweit die von den Unternehmen eingereichten Unterlagen insgesamt inhaltlich datenschutzkonform gestaltet waren.

Unternehmen, die bei keinem der Fragenkomplexe mit Rot bewertet wurden, bekamen in der Gesamtbetrachtung ein Grün, Unternehmen, bei denen ein Fragenkomplex mit Rot bewertet wurde, bekamen in der Gesamtbetrachtung ein Gelb. Sowohl für die insgesamt mit Grün als auch für die insgesamt mit Gelb bewerteten Unternehmen wurde die Querschnittsprüfung mit Mitteilung des Prüfungsergebnisses beendet. Bei in der Gesamtbetrachtung gelben Unternehmen erfolgten mit der Mitteilung des Prüfungsergebnisses weitergehende Erläuterungen zum mit Rot bewerteten Fragenkomplex sowie der nachdrückliche Hinweis, dass die LfD davon ausgeht, dass der betreffende Komplex vom Unternehmen zeitnah aufgegriffen wird. Die Mitteilung des Prüfungsergebnisses beinhaltete jeweils auch die Übermittlung des detaillierten Kriterienkataloges inklusive der individuellen Bewertung jedes Einzelkriteriums.

Unternehmen, die in mehr als einem Fragenkomplex mit Rot bewertet wurden, bekamen nach Mitteilung der Prüfungsergebnisse die Gelegenheit, zum Ergebnis Stellung zu nehmen und weitere Unterlagen einzureichen. An die neu eingereichten Unterlagen wurden dieselben Maßstäbe wie im ersten Prüfungsschritt angelegt und anschließend eine Neubewertung vorgenommen. Am Ende des zweiten Prüfungsschrittes wurde für alle Unternehmen die Querschnittsprüfung beendet. Unternehmen, die nun immer noch auf Rot standen, wurden allerdings darüber informiert, dass bei ihnen weiterhin gravierende Defizite zu erkennen sind. Weitergehende Kontrollen in separaten Prüfungen wurden angekündigt.

3. Teil: Prüfungsergebnisse

1. Überblick

Die meisten der geprüften Unternehmen hatten sich intensiv auf die DSG-VO vorbereitet, die größeren in der Regel im Rahmen eines 2017 gestarteten unternehmensweiten Projektes. Viele der in diesem Zuge identifizierten und initiierten Maßnahmen waren zum Prüfungszeitpunkt abgeschlossen, es gab aber auch noch zu erledigende Restarbeiten. 36 Unternehmen gaben an, Schulungen zur DS-GVO für ihre Beschäftigten durchgeführt oder kurzfristig geplant zu haben.

Nur 5 der geprüften 50 Unternehmen konnten am Ende des ersten Prüfungsschrittes eine grüne Bewertung aufweisen, d.h., nur bei diesen fünf wurde bei keinem Fragenkomplex ein erheblicher Handlungsbedarf festgestellt.

Bei 15 Unternehmen wurde bei einem der zehn Fragenkomplexe erheblicher Handlungsbedarf festgestellt, sie erhielten die Gesamtbewertung „Gelb“. Auffällig war hier, dass dieser eine mit Rot bewertete Komplex entweder den technisch-organisatorischen Datenschutz oder die DSFA betraf.

Bei 30 Unternehmen wurde bei mehr als einem Fragenkomplex erheblicher Handlungsbedarf festgestellt. Bei neun davon waren es sogar vier und mehr Fragenkomplexe, die mit Rot bewertet wurden. Alle der 30 Unternehmen, die bei mehr als einem Fragenkomplex auf Rot standen, hatten im technischen Datenschutz erheblichen Handlungsbedarf, 25 der 30 Unternehmen auch bei der DSFA. In diesen beiden Bereichen zeigten sich somit die mit Abstand größten Schwierigkeiten.

Alle der 30 im ersten Prüfungsschritt mit Rot bewerteten Unternehmen machten von der Möglichkeit Gebrauch, eine Stellungnahme einzureichen.

Im Zuge des zweiten Prüfungsschrittes konnten sich 4 der 30 Unternehmen von Rot auf Grün verbessern, hatten somit bei keinem der Fragenkomplexe mehr eine rote Bewertung. Dieser große Sprung in der Bewertung lässt sich auf zwei Faktoren zurückführen: Zum einen resultierten rote Bewertungen teilweise daraus, dass die Unternehmen den Erwartungshorizont der LfD Niedersachsen hinsichtlich der Antworttiefe nicht richtig eingeschätzt hatten. Zum anderen befanden sich einige Unternehmen zum Beginn der Querschnittsprüfung noch in der Umsetzungsphase zur DS-GVO. Zum Zeitpunkt ihrer zweiten Stellungnahme konnten sie aber eine aktualisierte Antwort geben, aus der hervorging, dass die Anforderungen zwischenzeitlich umgesetzt worden waren. Das wurde in der Bewertung berücksichtigt.

17 Unternehmen verbesserten sich insgesamt von Rot auf Gelb, standen somit noch bei einem Fragenkomplex auf Rot. Bei 10 dieser 17 Unternehmen war der einzige rote Bereich der technische Datenschutz, bei 6 die DSFA und bei einem der Komplex Einwilligung.

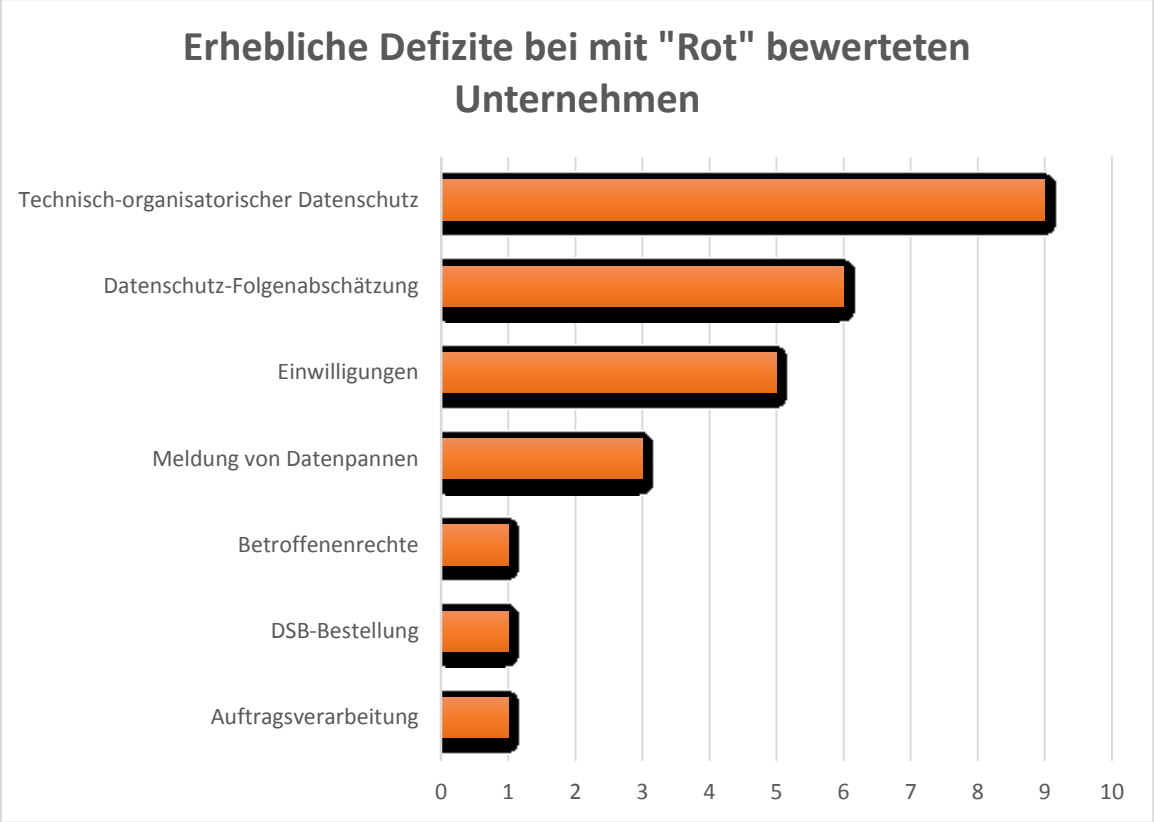

Abbildung 1

Bei den übrigen neun Unternehmen blieb es bei der Gesamtbewertung Rot. Sie hatten also trotz der ergänzenden Stellungnahme weiterhin mehr als einen „roten“ Fragenkomplex. Alle neun Unternehmen standen beim technisch-organisatorischen Datenschutz auf Rot, sechs auch bei der DSFA. Darüber hinaus gab es rote Bewertungen bei den Einwilligungserklärungen (5), beim Prozess zur Meldung von Datenpannen (3) sowie bei den Betroffenenrechten, der Bestellung von Datenschutzbeauftragten und der Auftragsverarbeitung (je 1) (siehe Abbildung 1). Insgesamt standen nach zwei Prüfungsschritten also 9 Unternehmen auf Grün, 32 auf Gelb und 9 auf Rot (siehe Abbildung 2).

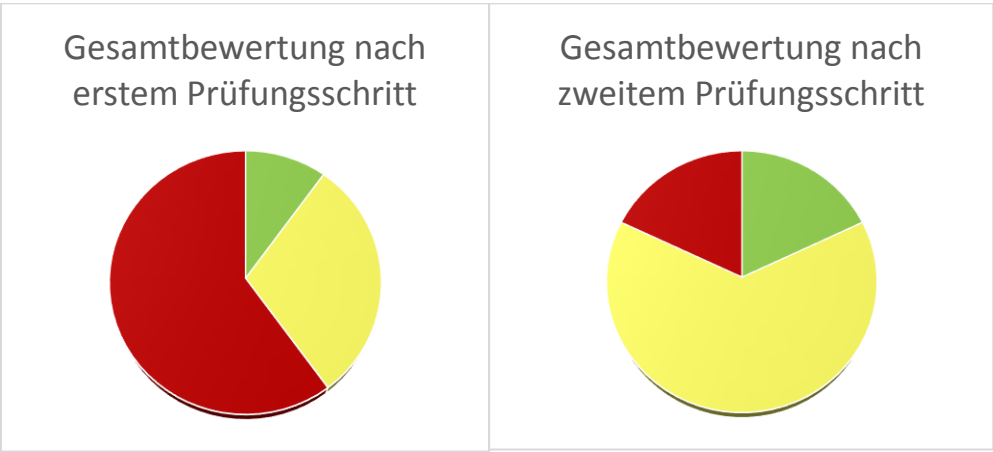

Abbildung 2

Zusammenfassend ließ sich feststellen, dass hinsichtlich der AV-Verträge, der DSB, der Meldepflichten und der Dokumentation nur gelegentlich Defizite festgestellt werden konnten. Bei den AV-Verträgen wurden z.B. teilweise Muster verwendet, die nicht vollumfänglich der Rechtsauffassung der Aufsichtsbehörden entsprachen. Bei den DSB wurde nicht immer die Fachkunde ausreichend nachgewiesen. In Bezug auf die Meldeprozesse war zum Teil die Darstellung nicht vollständig nachvollziehbar, es fehlte teilweise eine klare Regelung der Verantwortlichkeiten oder eine eindeutige Berücksichtigung der 72-Stunden-Frist.

Hinsichtlich der Verzeichnisse von Verarbeitungstätigkeiten (VVT), der Einwilligungen sowie der Betroffenenrechte lagen häufiger Defizite bei den Antworten vor. So war beim VVT teilweise der Aktualisierungsprozess unklar, Standardverfahren konnten nicht erkannt werden (z.B. für das Betreiben der Webseite oder für das Bewerbungsverfahren) und Kontaktangaben fehlten. Einwilligungserklärungen waren unklar, es fehlten differenzierte Auswahlmöglichkeiten und es fehlten Angaben, wo und wie ein Widerruf möglich ist. Hinsichtlich der Informationspflichten war ein Einsatz von Mustern erkennbar, ohne dass eine individuelle Anpassung an das jeweilige Unternehmen deutlich gemacht wurde.

Bei den Themen technisch-organisatorischer Datenschutz und DSFA lagen bei den Antworten verbreitet erhebliche Defizite vor. Im technisch-organisatorischen Datenschutz wurden Begrifflichkeiten ganz überwiegend nicht richtig verstanden. Den Verantwortlichen war z.B. die Definition des Begriffes „Stand der Technik“ ebenso regelmäßig nicht bekannt wie die in diesem Zusammenhang erforderliche Abgrenzung gegenüber den allgemein anerkannten Regeln der Technik auf der einen und dem Stand von Wissenschaft und Technik auf der anderen Seite. Des Weiteren schienen die Konzepte Privacy by Design bzw. by Default mehrheitlich noch wenig vertraut zu sein. In einigen Unternehmen wurde in der Risikoeinschätzung zudem der Fokus auf die (finanziellen) Risiken für das Unternehmen gelegt. Es wurde nicht erkannt, dass beim Datenschutz der Fokus auf die Risiken für die Betroffenen zu legen ist. Beim Thema DSFA wiederum war verbreitet bei der Schwellwertprüfung keine systematische Herangehensweise erkennbar.

2. Ergebnisse im Detail

a. Fragenkomplex 1 – Vorbereitung auf die DS-GVO

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.

Mit dieser weit gefassten, einleitenden Frage wollte die LfD Niedersachsen einen Überblick sowohl über die unterschiedlichen Herangehensweisen der Unternehmen erhalten als auch über deren Selbsteinschätzung hinsichtlich ihres Umsetzungsstandes. Eine Bewertung der Methodik erfolgte hier explizit nicht.

Bei der Auswertung achtete die LfD besonders darauf, ob jeweils alle Unternehmensbereiche, die personenbezogene Daten verarbeiten, in die Planungen und Maßnahmen zur Umsetzung der DS-GVO involviert waren. Dies war bei nahezu allen der Fall, nur sehr vereinzelt blieb hier etwas unklar. Die zur Umsetzung der DS-GVO geplanten Maßnahmen waren bei knapp der Hälfte der Unternehmen zum Prüfungszeitpunkt abgeschlossen, bei den übrigen waren einzelne Maßnahmen noch im Umsetzungsprozess. Erfreulich war auch, dass die Unternehmen überwiegend Schulungen für ihre Beschäftigten durchgeführt oder noch kurzfristig geplant hatten.

b. Fragenkomplex 2 – Verzeichnis von Verarbeitungstätigkeiten

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.

Das Verzeichnis von Verarbeitungstätigkeiten (VVT) ist das Herzstück jedes Datenschutzkonzeptes. Es dient als wesentliche Grundlage für eine strukturierte Dokumentation und als Nachweis der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO. Deshalb müssen Verantwortliche dafür Sorge tragen, dass das VVT vollständig ist, regelmäßig überprüft und falls nötig auch aktualisiert wird. Auch in diesem Bereich waren die Unternehmen überwiegend gut aufgestellt. Nur gelegentlich konnten die Prüferinnen und Prüfer der LfD den zur Verfügung gestellten Übersichten nicht entnehmen, dass alle Standardverfahren wie z. B. das Personal- und Bewerbermanagement oder das Betreiben der Webseite dokumentiert waren. Vereinzelt fehlten auch die Kontaktdaten des DSB. Insgesamt stellte die LfD hier aber bei keinem Unternehmen erheblichen Handlungsbedarf fest.

c. Fragenkomplex 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.

Die Verarbeitung personenbezogener Daten ist nur auf Basis einer gültigen Rechtsgrundlage zulässig. Maßgeblich ist hier besonders Art. 6 Abs. 1 DS-GVO. In diesem Fragenkomplex erwartete die LfD Niedersachsen eine vollständige und plausible Nennung aller für die verschiedenen Verfahren einschlägigen Rechtsgrundlagen. Mehrfach fiel in den Antworten die Aussage, dass keine Datenverarbeitung auf Basis von Einwilligungen erfolge. Zugleich musste aber auf der jeweiligen Webseite der Nutzung von Cookies zugestimmt werden. Oder es ergab sich aus den sonstigen Antworten, dass Newsletter auf Einwilligungsbasis verschickt wurden.

Die LfD Niedersachsen weist beim Thema Einwilligungen immer wieder darauf hin, dass sie in der Regel nicht eingeholt werden sollten, wenn die Verarbeitung auf eine andere Rechtsgrundlage gestützt werden kann. Zudem muss die betroffene Person vor Abgabe der Einwilligung von ihrem Recht auf jederzeitigen Widerruf in Kenntnis gesetzt werden. Da der Widerruf so einfach wie die Erteilung der Einwilligung sein muss, ist u.a. unbedingt anzugeben, an welche Stelle der Widerruf zu richten ist. Dies war bei den Antworten der Unternehmen häufiger nicht klar zu erkennen. Insgesamt wurde in diesem Fragenkomplex bei fünf Unternehmen erheblicher Handlungsbedarf festgestellt.

d. Fragenkomplex 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.

Zu beachten waren hier besonders die Informationspflichten aus Art. 13 und 14 DS-GVO, das Auskunftsrecht (Art. 15 DS-GVO), die Rechte auf Berichtigung und Löschung (Art. 16 und 17 DS-GVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) sowie das Recht auf Datenübertragbarkeit aus Art. 20 DS-GVO. Die ganz grundsätzlichen Erwartungen der LfD ergaben sich aus Art. 12 DS-GVO, wonach alle Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zu übermitteln sind.

Bei den auf Antrag gemäß den Art. 15 bis 22 DS-GVO ergriffenen Maßnahmen sind den betroffenen Personen die Informationen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung zu stellen. Informationen gemäß den Art. 13 und 14 DS-GVO sowie alle Mitteilungen und Maßnahmen gemäß den Art. 15 bis 22 und Art. 34 DS-GVO sind vorbehaltlich der Ausnahmen gem. Art. 12 Abs. 5 DS-GVO unentgeltlich zur Verfügung zu stellen. Die Unternehmen

sollten für alle Rechte entsprechende Verfahren implementiert haben, um den Anforderungen der DS-GVO form- und fristgerecht zu genügen.

Bei den Informationspflichten war bei der Hälfte der geprüften Unternehmen die Darstellung des Prozesses nicht oder nur teilweise nachvollziehbar beschrieben worden. Ebenfalls bei der Hälfte war das berechtigte Interesse gar nicht beschrieben worden, sofern eine Verarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO erfolgte. Bei einem weiteren Viertel war die Beschreibung des berechtigten Interesses nicht vollständig ausgeführt oder es fehlte die Abwägung mit den Betroffeneninteressen. Ganz überwiegend konnte den Antworten nicht entnommen werden, dass bei einer beabsichtigten Zweckänderung sichergestellt ist, dass die betroffene Person vor dieser Weiterverarbeitung Informationen über den anderen Zweck und alle anderen maßgeblichen Informationen erhält.

Bezogen auf das Auskunftsrecht war die Darstellung des entsprechenden Prozesses bei fast allen Unternehmen nachvollziehbar. Es fehlte jedoch bei knapp der Hälfte an einer Darstellung, dass die Identität des um Auskunft Ersuchenden überprüft wird. Darüber hinaus wurde bei der überwiegenden Anzahl der Unternehmen nicht der Umgang mit Art. 15 Abs. 3 DS-GVO (Kopie der verarbeiteten Daten) dargestellt. Es konnte den Antworten überwiegend nicht entnommen werden, dass den Betroffenen auf Antrag eine Kopie der verarbeiteten Daten zur Verfügung gestellt wird.

Die übrigen Betroffenenrechte wurden von den meisten Unternehmen allerdings trotz expliziter Erwähnung in der Fragestellung nicht näher beschrieben.

Insgesamt sah die LfD in diesem Bereich bei zwei Unternehmen erheblichen Handlungsbedarf.

e. Fragenkomplex 5 – technisch-organisatorischer Datenschutz

Die Fragen zum technisch-organisatorischen Datenschutz waren ausschließlich als Verständnisfragen formuliert und zielten nicht auf die konkrete Umsetzung technisch-organisatorischer Maßnahmen (TOM) in einzelnen Verfahren der Verantwortlichen ab.

Das überdurchschnittlich schlechte Abschneiden der geprüften Unternehmen zu diesem Themenkomplex lässt sich nur in Teilen mit der mangelnden Vertrautheit mit der durch die DS-GVO entstandenen neuen Rechtslage begründen, da z. B. der Stand der Technik oder das Rechte-/Rollenkonzept (in Form der Zugangs- und Zugriffskontrolle) schon in der Anlage zu § 9 Satz 1 des alten Bundesdatenschutzgesetzes (BDSG) zu beachten war.

Nach dem ersten Prüfungsschritt wurde bei 41 Unternehmen erheblicher Handlungsbedarf gesehen, im Verlauf des zweiten Prüfungsschrittes konnte sich ein Drittel der Unternehmen verbessern.

i. Frage 5a

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

Im Rahmen dieser Frage war nicht nur der Stand der Technik (s. Frage 5b) zu beachten, sondern auch Risiken, Implementierungskosten, risikominimierende Voreinstellungen (vergl. Frage 5d) sowie Art, Umfang, Umstände und Zwecke der Verarbeitung. Im Falle einer AV war durch die Unternehmen zu berücksichtigen, dass neben der eigenen planerischen und gestalterischen Verantwortung auch die für die Handlungen des Auftragsverarbeiters zu tragen ist.

Wesentlich für die Beantwortung waren vor allem die Ermittlung des Risikos für die im Verfahren relevanten Gewährleistungsziele (Vertraulichkeit, Verfügbarkeit, Integrität, Nichtverkettung, Transparenz und Intervenierbarkeit) sowie die Bestimmung geeigneter Maßnahmen zur Erzielung eines angemessenen Schutzniveaus unter Berücksichtigung des Standes der Technik.

Von manchen Verantwortlichen wurde der risikobasierte Ansatz genannt, ohne aber aufzuzeigen, wie dieser konzeptionell, d. h. nach standardisiertem systematisch-strukturiertem Vorgehen, umgesetzt wird. Hinzu kam, dass bereits aufgrund von mangelnder Kenntnis über den Stand der Technik (vergl. Frage 5b) eine Ermittlung angemessener Maßnahmen scheiterte.

Unternehmen, die sich der AV bedienten, erwähnten nur zur Hälfte, dass sie auch für die Verarbeitung und die Schutzmaßnahmen ihrer Auftragsverarbeiter verantwortlich sind. Auffällig war hier, dass Verantwortliche, die wesentliche Teile ihrer Verarbeitung durch Auftragsverarbeiter erledigen ließen, oder als konzernangehörige Unternehmen oder Mitgliedsunternehmen anderer Unternehmensverbünde den dortigen Vorgaben in der Auswahl ihrer Verfahren unterlagen, im Bereich des technisch-organisatorischen Datenschutzes häufig signifikant schlechter abschnitten, als Unternehmen, die ihre Verfahren eigenständig planen und realisieren konnten.

ii. Frage 5b

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

Im Hinblick auf Frage 5b war das korrekte Verständnis des Begriffes „Stand der Technik“ wesentlich. Er 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. Was „Stand der Technik“ ist, ist dynamisch zu betrachten. Nach unten grenzt er sich von den

„anerkannten Regeln der Technik“ (z.B. DIN-Normen) ab, nach oben vom „Stand von Wissenschaft und Technik“ (neueste technische und wissenschaftliche Erkenntnisse).[1]

Die TOM müssen den aktuellen Stand der Technik berücksichtigen. Darüber hinaus sind Vorkehrungen zu treffen, um die Maßnahmen anhand des fortschreitenden Standes der Technik weiter zu entwickeln. Dies setzt eine Beobachtung der Fortentwicklung sowohl der eingesetzten Maßnahmen als auch die der Entwicklung von Alternativen voraus.

Den Verantwortlichen war die Definition des Begriffes „Stand der Technik“ ebenso regelmäßig nicht bekannt wie die in diesem Zusammenhang erforderliche Abgrenzung gegenüber den allgemein anerkannten Regeln der Technik auf der einen und dem Stand von Wissenschaft und Technik auf der anderen Seite.

Auf Seiten der LfD Niedersachsen gab es die Erwartung, dass der Verantwortliche seine Verfahren ständig wiederkehrend mit den besten marktverfügbaren Lösungen vergleicht und erforderlichenfalls seine Maßnahmen so weit anpasst, bis das Restrisiko auf ein tragbares Maß gesenkt wird. Darüber hinaus war erwartet worden, dass der Verantwortliche den Stand von Wissenschaft und Technik verfolgt, um mögliche Bedrohungen (z. B. bei neuen Erkenntnissen zu Verschlüsselungsverfahren) zu erkennen, noch bevor neue Produkte, die diesen Bedrohungen begegnen, verfügbar werden, um zu einer jederzeit angemessenen Risikobeurteilung zu gelangen.

Die Frage nach dem Stand der Technik wurde jedoch - oftmals bereits abschließend - lediglich mit einem Hinweis auf automatisierte Aktualisierungen der Betriebssysteme und Büroanwendungen, sowie regelmäßig angepasste Virensignaturdateien beantwortet. Der Stand der Technik wurde zudem vielfach fälschlich mit den allgemein anerkannten Regeln der Technik gleichgesetzt, häufiger aber sogar als „neueste Programmversion marktbeherrschender Produkte“ missverstanden.

iii. Frage 5c

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

Hinsichtlich der Frage nach einem datenschutzkonformen Rechte-/Rollenkonzept hatte die LfD Niedersachsen die Kenntnis der eigenen Organisation, die Beachtung einer ggf. nötigen Funktionstrennung, eine ordnungsgemäße Dokumentation sowie die Auswahl eines geeigneten Identitäts- und Berechtigungsmanagementsystems erwartet. Ohne genaue Kenntnis der Organisation und der Zuständigkeiten ist eine Zuweisung der erforderlichen Berechtigungen an die Mitarbeiterinnen und Mitarbeiter nicht möglich. Kontrollaufgaben können nur wirksam umgesetzt werden, wenn eine ausreichende Funktionstrennung vorliegt.

[1] Der Stand der Technik wird in Artikel 25 Abs. 1 DS-GVO erwähnt. Zwar gibt es zu diesem Begriff keine Legaldefinition. Er ist aber – vor allem im datenschutzrechtlichen Kontext – insbesondere unter Heranziehung des Kalkar I-Beschlusses des Bundesverfassungsgerichts (BVerfG, Beschluss vom 8.8.1978 – 2 BvL 8-77, BVerfGE 49, 89 - Kalkar I) sowie der Drei-Stufen-Theorie auszulegen.

Eine Dokumentation der implementierten Rollen- und Berechtigungskonzepte macht die getroffenen Entscheidungen nachvollziehbar und dient der Prüfung der Notwendigkeit erteilter Zugriffsrechte. Die Auswahl eines geeigneten Berechtigungsverwaltungssystems für die Umsetzung einer datenschutzkonformen Berechtigungsvergabe ist wesentlich.

In der Praxis werden diese Systeme jedoch bereits durch die im Verfahren genutzten kommerziellen Anwendungen, sowie die von diesen vorausgesetzten Betriebssysteme, Datenbanken etc. vorgegeben. So ist eine eigene, an das Unternehmen angepasste Gestaltung der Berechtigungsvergabe praktisch kaum möglich und wurde vor diesem Hintergrund von den Verantwortlichen in ihren Antworten auch nicht dargestellt.

Schon bei der Auswahl von Anwendungssoftware bzw. von Betriebssystemen, Datenbanken etc. wäre das in diesen implementierte Rollen- und Berechtigungskonzept in die Auswahlentscheidung mit einzubeziehen, da es aus Datenschutzsicht eine ganz wesentliche Funktion betrifft. Zumindest sollten jedoch die bereits aus dem Bereich der Informationssicherheit bekannten Konzepte, vor allem zum Identitäts- und Berechtigungsmanagement, berücksichtigt werden. Daraus können sich auch konzeptionelle Anforderungen an ergänzende Hard- und Softwarelösungen oder Funktionen ergeben, die der Verantwortliche implementieren bzw. in Auftrag geben muss. Eine derartige Vorgehensweise war verbreitet jedoch nicht erkennbar.

iv. Frage 5d

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)?

Die Frage nach den Grundsätzen des Datenschutzes durch Technik (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default) wurde von allen Fragen zu TOM mit Abstand am häufigsten mangelhaft bzw. lückenhaft beantwortet. Die Anforderungen ergeben sich aus Art. 25 Abs. 1 und 2 DS-GVO sowie Erwägungsgrund 78. Ziel ist es, die Datenverarbeitung hinsichtlich Umfang, Dauer und Personenbezug zu minimieren, die Vorgänge für die Betroffenen transparent zu machen und ihnen Wahlmöglichkeiten mit datenschutzfreundlichen Voreinstellungen zu bieten. Es wurde hier erwartet, dass Unternehmen, die personenbezogene Daten über internetbasierte Anwendungen verarbeiten, zumindest der aus der Zeit vor der DS-GVO existierende Grundsatz der datenschutzfreundlichen Voreinstellungen in Form der aktiven Einwilligung (Opt-In) aus dem § 13 Abs. 2 Telemediengesetz bekannt ist.

Da die Verarbeitung personenbezogener Daten oft in vorkonfektionierten Standardanwendungen erfolgt, haben die Verantwortlichen vielfach nur eingeschränkte Möglichkeiten, ihre Verfahren entsprechend anzupassen. Mit diesem Mangel der Umsetzungsmöglichkeit korreliert auch der Mangel an Kenntnissen über diese Vorgabe. Wie schon zu Frage 5c dargestellt, sind auch diese Aspekte – Privacy by Design und by Default – bereits bei der Auswahl von (Standard-) Anwendungen zu berücksichtigen. Eine solche Vorgehensweise war jedoch auch hier verbreitet nicht erkennbar.

f. Fragenkomplex 6 – Datenschutz-Folgenabschätzung

i. Frage 6a

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?

Bei den Antworten zu Frage 6a hatte die LfD Niedersachsen zum einen erwartet, dass durch die Unternehmen die Tatbestände geprüft werden, die sich aus der Norm des Art. 35 DS-GVO ergeben. Die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung kann sich aus Art. 35 Abs. 4, der Muss-Liste bzw. Black-List ergeben, aus den Tatbeständen des Art. 35 Abs. 3 DS-GVO, welcher nicht abschließende Beispiele nennt und aus Art. 35 Abs. 1 DS-GVO. Allein die Nennung der einzelnen Tatbestände wäre hier bereits positiv bewertet worden.

Von den 50 geprüften Unternehmen ließen in der Antwort auf die Frage nach den geprüften Normen 26 nicht erkennen lassen, dass ihnen die von den Aufsichtsbehörden veröffentlichte Muss-Liste bekannt ist. Die anderen Unternehmen kannten diese Liste dementsprechend. Doch obwohl die Aufsichtsbehörden immer wieder darauf hinweisen, dass diese nicht abschließend ist, haben mehrere Unternehmen geantwortet, sie hätten die Liste geprüft, ihre Verfahren seien dort nicht enthalten und man hätte daher keine DSFA durchgeführt. Was die anderen Tatbestände des Art. 35 DS-GVO angeht, war bei 31 Unternehmen nicht ersichtlich, dass sie die Beispiele des Art. 35 Abs. 3 DS-GVO prüfen. Bei 17 war nicht erkennbar, dass ihnen die rechtliche Grundlage des Art. 35 Abs. 1 DS-GVO bekannt ist.

Darüber hinaus bestand die Erwartung, dass eine methodische Herangehensweise an die Prüfung von Art. 35 Abs. 1 DS-GVO erkennbar ist. Bei vielen Unternehmen ist dieser Punkt leider noch nicht ausgereift. Das Working Paper 248 bietet hier eine gute Hilfestellung. Mit den in diesem Working-Paper genannten Kriterien werden die Verantwortlichen in die Lage versetzt, die Entscheidung für oder gegen die Durchführung einer DSFA in angemessener Zeit nachvollziehbar zu dokumentieren. Eine Vielzahl der Unternehmen hat diese Hilfestellung jedoch nicht verwendet oder hat eigene Ansätze entwickelt, die dann häufig für die betroffenen Personen kein vergleichbares Schutzniveau herstellen konnten.

Weiterhin war erwartet worden, dass die Unternehmen die DSFA-Prüfung organisatorisch mit einer klaren Zuständigkeit versehen und dokumentieren. Wichtig war, dass es insbesondere in größeren Unternehmen eine klare Aufgabenzuweisung gibt, damit die Prüfung nicht schon deshalb entfällt, weil sich niemand zuständig fühlt. Die Dokumentation ist zum einen erforderlich, damit das Unternehmen seine Nachweispflichten erfüllen kann. Zum anderen kann es bei einer Veränderung der Risikolage auf die entsprechende Dokumentation zurückgreifen, um sich nachvollziehbar für oder gegen die Durchführung einer DSFA zu entscheiden. Zunächst war auffällig, dass eine erhebliche Anzahl von Unternehmen hier antwortete, dass die Prüfung durch den betrieblichen Datenschutzbeauftragten durchgeführt wird. Das ist grundsätzlich problematisch, da der DSB eine beratende und kontrollierende Funktion hat, die er nur sinnvoll wahrnehmen kann, wenn er sich

nicht selbst berät und kontrolliert. Im Übrigen waren die Ergebnisse durchmischt. Die überwiegende Zahl der Unternehmen hatte Zuständigkeiten festgelegt und ungefähr die Hälfte dokumentierte die Prüfung auch. Dem entsprechend gab es aber auch zahlreiche Unternehmen, die diese Anforderungen noch nicht erfüllt hatten.

Als Fazit lässt sich festhalten, dass – von einigen hervorragenden Ergebnissen abgesehen – im Bereich der DSFA erhebliche Lücken in der Umsetzung der DSG-VO festgestellt wurden. Bei 29 Unternehmen bestand am Ende des ersten Prüfungsschrittes erheblicher Handlungsbedarf. Im Rahmen des zweiten Prüfungsschrittes konnte sich knapp die Hälfte der Unternehmen verbessern.

ii. Frage 6b

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.

Von den 50 geprüften Unternehmen hatten 21 bereits Datenschutz-Folgenabschätzungen durchgeführt. Der LfD Niedersachsen wurden insgesamt 172 DSFA vorgelegt. Die thematischen Schwerpunkte lagen im Bereich der Videoüberwachung (nicht branchenspezifisch), Personalmanagementsysteme (nicht branchenspezifisch) und Verarbeitung von Gesundheitsdaten (Pflegeheim, Fitnessstudio). Aufgrund dieser großen Menge wurde entschieden, jeweils eine DSFA als Stichprobe zu prüfen. Die LfD beschränkte sich darauf zu prüfen, ob die in Art. 35 Abs. 7 DS-GVO vorgeschriebenen Inhalte vorhanden waren. Es wurde nicht geprüft, ob die Maßnahmen angemessen waren, sondern nur, ob die Unternehmen die von der DS-GVO geforderten Inhalte überhaupt dokumentiert hatten.

Im ersten Schritt wurde geprüft, ob eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung vorlag. Dieser Teil der DSFA ist besonders wichtig, weil diese systematische Beschreibung die Grundlage für alle darauffolgenden Prüfschritte ist, ohne die keine belastbaren Ergebnisse erlangt werden können. An diesem Punkt scheiterte bereits knapp die Hälfte der geprüften DSFA. Eine halbe Seite Sachverhaltsbeschreibung oder sogar nur wenige Stichpunkte können insbesondere bei komplexen Verarbeitungsvorgängen nicht die Grundlage für eine vertiefte Risikoanalyse und die Festlegung darauf basierender Maßnahmen sein. In diesen Fällen blieb auch unklar, welchem Ablauf die Verarbeitung folgt, welche personenbezogenen Daten verarbeitet werden und welche Hard- und Software dabei verwendet wird. Hatte eine DSFA hier bereits Defizite, folgte auch keine angemessene Risikoanalyse.

Weiterhin wurde geprüft, ob bei der Risikoanalyse die Eintrittswahrscheinlichkeit und die Schwere des Risikos bestimmt wurden. Das Erfordernis ergibt sich aus den Art. 24, 25, 32 DS-GVO und aus Erwägungsgrund 75. Wie man als Verantwortlicher an diese Aufgabe heranzugehen hat, ist nicht festgeschrieben. Es muss jedoch sichergestellt sein, dass die Methodik zu nachvollziehbaren Ergebnissen kommt, um den Zweck der DSFA zu erfüllen: die Planung von Maßnahmen, durch welche

die Einhaltung der DS-GVO nachgewiesen wird. Bei vielen der vorgelegten DSFAs war das methodische Vorgehen nicht nachvollziehbar. Dies war z.B. der Fall, wenn von einer „Schadensklasse 2“ die Rede war, ohne dass dieser Begriff näher erläutert wurde. Ähnlich war es, wenn ein Risiko als „gering“ eingestuft wurde, aber nicht deutlich wurde, warum.

Bei den geplanten Abhilfemaßnahmen war oft nicht klar, welchen Risiken damit konkret begegnet werden soll. Art. 35 Abs. 7 DS-GVO hat aber eine logische Abfolge. Die Risikoanalyse ist die Grundlage für die anschließend zu bestimmenden Maßnahmen. Es muss deutlich erkennbar sein, dass den Risiken bestimmte Maßnahmen zugeordnet werden und diese damit auf ein vertretbares Niveau herabgesenkt werden.

Darüber hinaus waren oft überhaupt keine konkreten Maßnahmen genannt. Wenn ein Verantwortlicher als Maßnahme lediglich „Verschlüsselung“ angab, blieb unklar, ob er damit meint, dass personenbezogene Daten verschlüsselt übertragen oder ob sie verschlüsselt gespeichert werden und welcher Verschlüsselungsalgorithmus jeweils zum Einsatz kommt. Auffällig war auch, dass Unternehmen auf bestehende Maßnahmen verwiesen, ohne dass diese konkretisiert wurden.

g. Fragenkomplex 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.

Die aus dem Bundesdatenschutzgesetz bekannte Auftragsverarbeitung (AV) findet sich in Art. 28 DS-GVO wieder. An dieser Stelle wollte die LfD Niedersachsen zunächst wissen, inwieweit bestehende AV-Verträge an die neuen Regelungen angepasst worden waren. Bei knapp der Hälfte der Unternehmen war dieser Anpassungsprozess noch nicht vollständig abgeschlossen.

Zudem prüfte die LfD die übersandten Muster und Beispielverträge dahingehend, ob sie den rechtlichen Anforderungen entsprechen, was überwiegend der Fall war.

Vereinzelt tauchten Regelungen auf, die nicht der Rechtsauffassung der DSK entsprachen, insbesondere im Hinblick auf die fehlende Einordnung von Wartungsarbeiten an IT-Systemen als AV. Bezüglich der Nennung von Vertragsgegenstand, Dauer und Zweck kam es häufiger vor, dass auf den Hauptvertrag verwiesen wurde, ohne dass dieser zur Verfügung gestellt wurde. Dies führte dazu, dass diese Kriterien nur mit „teilweise“ bewertet wurden. Insgesamt musste hier nur bei einem Unternehmen dringender Handlungsbedarf festgestellt werden.

h. Fragenkomplex 8 – Datenschutzbeauftragte

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

Die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten (DSB) ergibt sich aus Art. 37 DS-GVO sowie aus § 38 BDSG. Die Bestellung erfolgt auf Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens im Bereich des Datenschutzrechts und der Datenschutzpraxis sowie auf Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DS-GVO genannten Aufgaben. Diese Fachkunde ist im Rahmen der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO umfassend nachzuweisen. Auch zu diesem Fragenkomplex waren die Ergebnisse erfreulich. Ein Interessenskonflikt stand nur bei einem Unternehmen im Raum, bzgl. der erforderlichen Fachkunde wurde ebenfalls nur in einem Fall dringender Handlungsbedarf festgestellt.

i. Fragenkomplex 9 – Meldepflichten

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

Rechtsgrundlage bilden hier die Art. 33 und 34 DS-GVO. Zur Umsetzung sollten Unternehmen einen Prozess zur Meldung von Datenschutzverstößen implementieren. In einer nachvollziehbaren Darstellung sollten insbesondere die Verantwortlichkeiten und Abläufe klar geregelt sein und allen Beschäftigten bekannt gemacht werden.

Im ersten Prüfungsschritt wurde bei circa einem Drittel der Unternehmen der Meldeprozess nicht oder nur teilweise nachvollziehbar dargestellt. Zudem fehlte es bei einem Drittel der Unternehmen an einer klaren Regelung der Verantwortlichkeit und an einer erkennbaren Berücksichtigung der 72-Stunden-Meldefrist. Nach dem zweiten Prüfungsschritt stellte die LfD nur noch bei drei Unternehmen erheblichen Handlungsbedarf beim Meldeprozess fest.

j. Fragenkomplex 10 - Dokumentation

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

Jeder Verantwortliche muss nachweisen können, dass er den Pflichten, die ihm die DS-GVO auferlegt, nachkommt (Art. 5 Abs. 2 DS-GVO). Daher prüfte die LfD Niedersachsen abschließend, inwiefern sich aus der Antwort zu diesem Komplex sowie aus der Summe der übrigen Antworten ergab, dass eine

Dokumentation zu jeder der abgefragten Pflichten vorhanden ist. Ganz überwiegend war hier festzustellen, dass die Unternehmen eine entsprechende Dokumentation vorhalten. Bei sieben Unternehmen wurde hier nur geringer Anpassungsbedarf gesehen, erheblicher Bedarf bei keinem.

3. Schlussfolgerungen

Aus der branchenübergreifenden Querschnittsprüfung haben sich für die LfD Niedersachsen Erkenntnisse ergeben, die sowohl ihre Vollzugsaufgaben berühren als auch ihre Pflicht zu Aufklärung und Sensibilisierung der Verantwortlichen. Was den Vollzug betrifft, so war die Prüfung zwar auch für die Unternehmen beendet, die nach der zweiten Stellungnahme immer noch mit Rot bewertet worden waren. Allerdings wurden fünf von Ihnen mit der Mitteilung des Ergebnisses gleichzeitig darüber informiert, dass bei ihnen aufgrund der gravierenden Defizite noch in diesem Jahr weitergehende Kontrollen in separaten Prüfungen folgen werden. Nicht auszuschließen ist, dass es auch zur Verhängung von Bußgeldern kommen kann. Dabei wird die LfD Niedersachsen u.a. berücksichtigen, wie schwerwiegend ein möglicherweise vorliegender Verstoß ist und wie das Unternehmen damit umgegangen ist. Zudem wird die LfD verstärkt weitere themen- und branchenbezogene anlasslose Kontrollen durchführen, um ihrer Aufgabe als Aufsichtsbehörde angemessen nachzukommen.

Zugleich wird die Behörde den eingeschlagenen Weg fortsetzen, das Beratungs- und Informationsangebot auf ihrer Webseite an die identifizierten Bedarfe anzupassen. Die Querschnittsprüfung hat sehr deutlich gezeigt, dass die größten Schwierigkeiten in der Umsetzung der DS-GVO in den Bereichen technisch-organisatorischer Datenschutz und Datenschutz-Folgenabschätzung liegen. Deshalb hat die LfD Niedersachsen beschlossen, Handlungsempfehlungen zu den Themen „Stand der Technik“, „Rollen- und Berechtigungskonzepte“, „Privacy by Design und by Default“ sowie zur Schwellwertprüfung bei der DSFA zu veröffentlichen. Darüber hinaus wird es auch eine Handlungsempfehlung für Einwilligungserklärungen geben.

Im Rahmen der Querschnittsprüfung ist teilweise der Eindruck entstanden – siehe z.B. die Ausführungen zur DSFA – dass selbst die sich aus den jeweiligen Normen klar ergebenen Tatbestandsvoraussetzungen nicht hinreichend berücksichtigt wurden. Bei zukünftigen Prüfungen müssen die Unternehmen sich mit den gesetzlichen Anforderungen vertieft auseinandersetzen, diese auf ihre individuelle Unternehmenssituation übertragen und umsetzen. Die daraus resultierenden Unternehmensprozesse sollten eine (nachvollziehbare) Methodik aufweisen, die sicherstellt, dass die gesetzlichen Anforderungen im Einzelfall erfüllt werden.

4. Anlagen

Anlage 1: Fragenkatalog zur Querschnittsprüfung 2018/19

1. Vorbereitung auf die DS-GVO
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.

2. Verzeichnis von Verarbeitungstätigkeiten
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.

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.

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.

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

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

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

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)?

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?

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.

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.

8. Datenschutzbeauftragter

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

9. Meldepflichten

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

10. Dokumentation

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

Anlage 2: Kriterienkatalog zur Querschnittsprüfung 2018/19

1. Vorbereitung auf die DSGVO

Wie haben Sie sich als Unternehmen auf die DS-GVO vorbereitet? Schildern Sie (kurz) die Vorgehens-weise, 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?

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?

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?

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 Klicks 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)?

<u>Hinweis:</u> 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)?

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

Hinweis: 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?

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?
    a. Art. 35 Abs. 4?
    b. Art. 35 Abs. 3?
    c. Art. 35 Abs. 1?

2. Welche Methodik zur Risikobestimmung wird verwendet?
    a. WP 248?
    b. KP Nr. 18 – Risiko?
    c. Eigene Methode?
    d. 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?

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 unter-stützt?
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?

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 Klicks ab der Startseite)
5. Erfolgte eine Meldung des DSB bei der Aufsichtsbehörde?

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?

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?

----ENDE----