Prüfpunkte beim Audit	Antwort sowie Risikobeschreibung	Risiko	Handlungsbedarf nötig?	Maßnahmen zur Risikominderung / Empfehlung zur Risikominderung
Besprechung der identifizierten Risiken bei Bestandsaufnahme				
IT-Sicherheit				
PCs, Notebooks sind ohne Passwortschutz				
Passwörter werden nicht geändert				
Keine Vorgabe zur Passwortkomplexität				
Keine Rollen- Berechtigungskonzepte				
Benutzer haben Adminrechte				
WhatsApp wird zur geschäftlichen Kommunikation eingesetzt				
Soziale Medien				
Facebook ist aus Sicht der DSK nicht datenschutzkonform				
Im sozialen Netzwerk wird nicht auf die Datenschutzerklärung auf die Homepage verwiesen				
Das Impressum ist im sozialen Netzwerk eingepflegt				
Bewerbung				
Die Daten der Bewerber werden länger als 6 Monate ohne Einwilligung der Bewerber gespeichert				
Die Daten der Bewerber werden weniger als 6 Monate gespeichert. Hier besteht das Risiko, dass bei Einreichung einer Klage nach dem AGG der Verantwortliche keinen Nachweis über die Bewerberdaten vorlegen kann.				
Physikalische Sicherheit				
Die Büros werden bei Abwesenheit nicht verschlossen				
Der Serverraum ist nicht verschlossen				
Der Papierschredder entspricht nicht den datenschutzrechtlichen Vorgaben				
Dokumente werden ungeschreddert über die unverschlossene Papiertonne entsorgt				
Videoüberwachung				
Beim Betreten des Geländes wird nicht auf die Videoüberwachung hingewiesen				
Das Videomaterial wird länger als die empfohlenen 72 Stunden gespeichert				
Die Videoüberwachung zeichnet einen Großteil von privaten Grundstücken / öffentlichen Bereichen auf				
Personalangelegenheiten				
Beschäftigtenbilder werden ohne Einwilligung der Mitarbeiter veröffentlicht				
Der Schichtplan der Mitarbeiter ist für Dritte frei zugänglich und einsehbar				
Mitarbeiter können gegenseitig im Kalender die Krankheitstage einsehen				
Die Mitarbeiter/Praktikanten/Auszubildenden unterzeichnen keine Verschwiegenheitserklärung				
Personalakten sind nicht unter Verschluss				
Mitarbeiterumfragen werden nicht anonymisiert vorgenommen				
Lohnabrechnungen werden ohne Inhaltsverschlüsselung an Mitarbeiter versandt				
Webseite				
Die Kontaktdaten des DSB sind nicht in der DSE vorhanden				
Die Datenschutzerklärung ist in Bezug auf Plugings/Widgets nicht vollständig				
Die Datenschutzerklärung ist nicht mit einem Klick erreichbar				
Es wird kein Opt-in seitens des Nutzers bei Analysetools eingeholt				

Verfahrensverzeichnis

Welches Verfahren wurde insbesondere geprüft?
Welche neuen Verfahren wurden beim Audit neu identifiziert? Begründung, weshalb diese bei der Bestandsaufnahme nicht identifziert wurden.

Informationspflichten

Entsprechen die Informationspflichten noch dem aktuellen Stand?
Auf welchen Weg die Informationspflicht für die Kunden/Geschäftspartner/Dienstleister etc. zur Verfügung gestellt?
Wie werden die Kunden/Geschäftspartner/Dienstleister auf die Informationspflicht hingewiesen?
Kann das Vorhandensein der Informationspflicht an die Kunden/Geschäftspartner/Dienstleister etc. überprüft werden?
Wie werden die Informationspflichten den Mitarbeitern zugänglich gemacht?

Auftragsverarbeiter / AV-Verträge

Wurden alle Auftragsverarbeiter identifiziert? Wenn nein, warum?
Sind alle nötigen AV-Verträge vorliegend?
Wurden die Verträge auf die Vorgaben nach Art. 28 DSGVO geprüft?
Welche Verträge sind noch ausstehend / offen?

Begehung / Physikalische Sicherheit

Welche Räumlichkeiten wurden besichtigt?
Konnten sich Zutritt zu den Büroräumen verschafft werden?
Konnten sich Zutritt zum Serverraum verschafft werden?
Konnten offene Unterlagen von Kunden / Mitarbeitern eingesehen werden?
Wird das Clean-Desktop-Prinzip angewandt?
Konnte sich Zugriff auf den PC verschafft werden?
Werden sensible Telefonate im Empfangsbereich geführt?

Mitarbeitergespräch

Kennen die Mitarbeiter den zuständigen Ansprechpartner/DSB?
Wissen die Mitarbeiter, wie Sie den DSB erreichen könnnen?
Kennen die Mitarbeiter die Vorgaben zum Schutz personenebezogener Daten (z.B. IT-Sicherheitsrichtlinie)?
Wissen die Mitarbeiter, wie sie einen Datenschutzvorfall erkennen?
Kennen die Mitarbeiter den Ablauf für einen Datenschutzvorfall?
Wissen die Mitarbeiter, wie sie eine Betroffenenanfrage erkennen?
Kennen die Mitarbeiter, den Ablauf für die Beantwortung einer Betroffenenanfrage?

Datenschutzprozesse

Wurden die Datenschutzprozesse (Datenschutzvorfall und Betroffenenanfragen) besprochen?
Sind die Prozesse für die Mitarbeiter jederzeit zugänglich?

Wurde ein interner Ansprechpartner für die Bearbeitung der Datenschutzvorfälle und Betroffenenanfragen benannt?