Abschnitt	Frage
Struktur und Verantwortlichkeit	Existiert das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist?
Struktur und Verantwortlichkeit	Existiert in Ihrem Unternehmen bereits ein betrieblicher oder externer Datenschutzbeauftragter?
Übersicht Verarbeitungen	Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 DS-GVO erstellt?
Übersicht Verarbeitungen	Wie haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen Berücksichtigung finden (Privacy by Design -Art. 25 DS-GVO)?
Externe Dienstleister	Haben Sie zur Erledigung Ihrer Arbeiten externe Auftragsverarbeiter eingebunden?
Informationspflichten, Betroffenenrechte	Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst?
Informationspflichten, Betroffenenrechte	Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DS-GVO zeitnah und vollständig erfüllen zu können (Art. 12 Abs. 1 DS-GVO)?
Informationspflichten, Betroffenenrechte	Haben Sie Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen zu können (Art. 20 DS-GVO)?
Umgang mit Risiken	Gibt es für jede Verarbeitungstätigkeit Angaben, mit der Sie die Rechtmäßigkeit Ihrer Verarbeitung nachweisen können, z.B. bezüglich Zwecken, Kategorien personenbezogener Daten, Empfängern und/oder Löschfristen (Art. 5 Abs. 2 DS-GVO)?
Umgang mit Risiken	Haben Sie Ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art. 32 DS-GVO angepasst?
Umgang mit Risiken	Haben Sie sich auf die evtl. Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung vorbereitet?
Umgang mit Risiken	Haben Sie Ihr individuelles Risiko in Bezug auf die Folgen von Datenrechtsverletzungen und der Cyber-Kriminalität ermittelt und haben Sie sich in punkto einer angepassten Lösung zur Absicherung von Restrisiken beraten lassen?
Datenschutzverletzungen	Ist die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde geregelt?
Mitarbeiter	Werden Mitarbeiter, die mit personenbezogenen Daten arbeiten, auf das Datengeheimnis verpflichtet?
Mitarbeiter	Werden Mitarbeiterdaten nur mit schriftlicher Zustimmung oder gar nicht veröffentlicht (z.B. im Internet, Mitarbeiter-/Unternehmenszeitung)?
Mitarbeiter	Welche Festlegungen bestehen zur privaten Nutzung dienstlicher Kommunikationsmittel (Telefon/Handy, Smartphone, PC/Laptop, Internet, E-Mails)?
Mitarbeiter	Ist die Verwendung privater Kommunikationsmittel für dienstliche Zwecke erlaubt (Smartphone, Laptop)?

DS Managementsystem	Haben Sie ein Datenschutzmanagementsystem installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gemäß der DS-GVO erfolgt (Art 24 Abs. 1 DS-GVO)?
DS Managementsystem	Verwenden Sie auf Ihrer Homepage ein gesetzeskonformes Impressum und eine gesetzeskonforme Datenschutzerklärung?

Abschnitt	Frage
Verantwortung und Ressourcen	Hat sich die Geschäftsleitung schriftlich dazu verpflichtet die Gesamtverantwortung für die IT-Sicherheit zu übernehmen?
Verantwortung und Ressourcen	Sind die Verantwortlichen für die Informationssicherheit klar definiert und schriftlich fixiert?
Funktionstrennung	Ist das Prinzip der Funktionstrennung umgesetzt worden?
Richtlinien und Regelungen	Gibt es im Unternehmen IT-Sicherheits Leit- und Richtlinien?
Richtlinien und Regelungen	Ist die private Nutzung der Unternehmens IT geregelt?
Richtlinien und Regelungen	Haben Sie mit Ihren Dienstleistern verbindliche Regelungen zum Umgang mit den Daten und der IT des Unternehmens getroffen?
Richtlinien und Regelungen	Haben alle Mitarbeiter eine Vertraulichkeitserklärung unterschrieben?
Zutritt	Ist der Zutritt zu den zentralen IT-Systemen geregelt?
Zugang	Ist der Zugang zur IT-Infrastruktur konsequent geregelt?
Zugang	Gibt es eine spezielle Regelung für administrative Zugänge?
Zugriff	Ist der Zugriff auf Unternehmensdaten eindeutig geregelt?
Mobile Endgeräte	Haben Sie eine Richtlinie zur Nutzung von mobilen Endgeräten erstellt?
Mobile Endgeräte	Sind Daten auf mobilen Endgeräten vor unberechtigtem Zugriff geschützt?
Mobile Endgeräte	Nutzen Sie ein Mobile Device Managementsystem (MDM)?
Mobile Datenträger	Existiert eine Richtlinie zum Umgang mit mobilen Datenträgern?
Netzwerk	Ist der Zugriff auf das Internet durch geeignete Schutzmaßnahmen abgesichert?
Netzwerk	Erfolgt der Zugriff auf die IT-Infrastruktur verschlüsselt?
IT-System	Haben Sie eine genaue Aufstellung aller IT-Komponenten?
IT-System	Haben Sie ein validiertes Schutzkonzept Ihrer IT-Infrastruktur?
Prävention	Haben Sie geregelt was in einem IT-Sicherheitsvorfall zu tun ist?
Prävention	Sind alle wichtigen IT-Systeme vor physischem Zugriff geschützt?
Prävention	Sind alle wichtigen IT-Systeme vor Brandschäden geschützt?
Prävention	Sind alle wichtigen IT-Systeme mit einer unterbrechungsfreien Stromversorgung geschützt?
Prävention	Werden alle wichtigen Unternehmensdaten regelmäßig durch Datensicherungen geschützt?
Prävention	Werden regelmäßig Tests durchgeführt, die die Integrität der Datensicherungen sicherstellen?
Prävention	Werden Datensicherungen örtlich getrennt von den Produktivsystemen aufbewahrt?
Prävention	Haben Sie Wiederanlaufpläne für die wichtigsten Systeme in Ihrer IT-Infrastruktur?
Prävention	Nutzen Sie auf allen Systemen (auf denen das möglich ist) eine Antivirenschutzsoftware?
Management	Nutzen Sie IT-Systeme in der Cloud bzw. SaaS Dienste?
Management	Haben Sie ein IT-Managementsystem implementiert?
Management	Haben Sie Ihr individuelles Risiko in Bezug auf die Folgen von Datenrechtsverletzungen und der Cyber-Kriminalität ermittelt und haben Sie sich

	in punkto einer angepassten Lösung zur Absicherung von Restrisiken beraten lassen?

Abschnitt	Frage
Struktur und Verantwortlichkeit	Existiert das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist?
Struktur und Verantwortlichkeit	Haben Sie ein Datenschutzmanagementsystem (DSM) installiert, um sicherzustellen und den Nachweis erbringen zu können, dass Ihre Verarbeitung gemäß der DS-GVO erfolgt (Art 24 Abs. 1 DS-GVO)?
Struktur und Verantwortlichkeit	Existiert in Ihrem Unternehmen bereits ein betrieblicher oder externer Datenschutzbeauftragter (DSB)?
Struktur und Verantwortlichkeit	Haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen Berücksichtigung finden (Privacy by Design -Art. 25 DS-GVO)?
Übersicht Verarbeitungen	Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 DS-GVO erstellt?
Externe Dienstleister und Datenaustausch	Haben Sie zur Erledigung Ihrer Arbeiten externe Auftragsverarbeiter eingebunden?
Externe Dienstleister und Datenaustausch	Wurden die Zielländer der Datenübermittlung/en auf Datenschutzkonformität geprüft?
Informationspflichten, Betroffenenrechte	Wurden die Vorgaben und Regeln für die Durchführung der Informationspflicht geprüft?
Informationspflichten, Betroffenenrechte	Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Auskunft zu den eigenen Daten nach Art. 15 DS-GVO zeitnah und vollständig erfüllen zu können (Art. 12 Abs. 1 DS-GVO)?
Informationspflichten, Betroffenenrechte	Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Berichtigung zu den eigenen Daten nach Art. 16 DS-GVO zeitnah und vollständig erfüllen zu können (Art. 16 Abs. 1 DS-GVO)?
Informationspflichten, Betroffenenrechte	Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen auf Löschung der eigenen Daten nach Art. 17 DS-GVO zeitnah und vollständig erfüllen zu können (Art. 17 Abs. 1 DS-GVO)?
Informationspflichten, Betroffenenrechte	Haben Sie ein Verfahren eingerichtet, um Anträge von betroffenen Personen zur Einschränkung der Datenverarbeitung nach Art. 18 DS-GVO zeitnah und vollständig erfüllen zu können (Art. 18 Abs. 1 DS-GVO)?
Informationspflichten, Betroffenenrechte	Werden die Anforderungen hinsichtlich des Widerspruchsrechts datenschutzkonform umgesetzt?
Informationspflichten, Betroffenenrechte	Haben Sie Verfahren eingerichtet, um Anträge auf Datenübertragbarkeit betroffener Personen erfüllen zu können (Art. 20 DS-GVO)?
Rechtmäßigkeit der Datenverarbeitung	Gibt es für jede Verarbeitungstätigkeit Angaben, mit der Sie die Rechtmäßigkeit Ihrer Verarbeitung nachweisen können, z.B. bezüglich Zwecken, Kategorien personenbezogener Daten, Empfängern und/oder Löschfristen (Art. 5 Abs. 2 DS-GVO)?
Rechtmäßigkeit der Datenverarbeitung	Erhalten Sie die Einwilligungserklärungen zur „Speicherung und Weitergabe der personenbezogenen Daten“ von Kunden und Mitarbeitern zeitnah und datenschutzkonform?
Rechtmäßigkeit der Datenverarbeitung	Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst?

Technische und Organisatorische Maßnahmen (TOMs)	Haben Sie Ihre bestehenden Prozesse zur Überprüfung der Sicherheit der Verarbeitung auf die neuen Anforderungen des Art. 32 DS-GVO angepasst?
Technische und Organisatorische Maßnahmen (TOMs)	Welche Festlegungen bestehen zur privaten Nutzung dienstlicher Kommunikationsmittel (Telefon/Handy, Smartphone, PC/Laptop, Internet, E-Mails)?
Technische und Organisatorische Maßnahmen (TOMs)	Ist die Verwendung privater Kommunikationsmittel für dienstliche Zwecke erlaubt (Smartphone, Laptop)?
Technische und Organisatorische Maßnahmen (TOMs)	Werden mobile Datenträger verschlüsselt?
Technische und Organisatorische Maßnahmen (TOMs)	Werden E-Mails mit personenbezogenen Daten nur verschlüsselt versendet?
Technische und Organisatorische Maßnahmen (TOMs)	Können Sie die Verfügbarkeit der datenverarbeitenden Systeme (regelmäßige Datensicherung/ Desaster Recovery Konzept sicherstellen?
Home-Office	Nutzen Sie für Ihre MitarbeiterInnen Home-Office und werden die Datenschutzbestimmungen eingehalten?
Homepage	Verwenden Sie auf Ihrer Homepage ein gesetzeskonformes Impressum und eine gesetzeskonforme Datenschutzerklärung?
Homepage	Werden Mitarbeiterdaten nur mit schriftlicher Zustimmung oder gar nicht veröffentlicht (z.B. im Internet, Mitarbeiter-/Unternehmenszeitung)?
Mitarbeiter	Werden die Mitarbeiter im Bereich Datenschutz geschult bzw. anderweitig unterrichtet und wird dies festgehalten?
Mitarbeiter	Werden Mitarbeiter, die mit personenbezogenen Daten arbeiten, auf das Datengeheimnis verpflichtet?
Datenschutz-Audit	Führen Sie jährlich ein Datenschutz-Audit in Ihrem Unternehmen durch und dokumentieren Sie dieses?
Aufbewahrung + Löschung	Ist die Aufbewahrung, Sperrung bzw. Löschung nicht mehr erforderlicher Daten in Ihrem Unternehmen datenschutzkonform festgelegt?
Aufbewahrung + Löschung	Werden Altgeräte bzw. Altdatenträger vor der Abgabe an Dritte sicher gelöscht?
Aufbewahrung + Löschung	Wird Altpapier datenschutzgerecht entsorgt?
Datenschutzverletzungen	Ist die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde geregelt?
Umgang mit Risiken	Haben Sie Ihr individuelles Risiko in Bezug auf die Folgen von Datenrechtsverletzungen und der Cyber-Kriminalität ermittelt und haben Sie sich in punkto einer angepassten Lösung zur Absicherung von Restrisiken beraten lassen?
Umgang mit Risiken	Haben Sie sich auf die evtl. Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung (DSFA) vorbereitet?
Umgang mit Risiken	Findet Videoüberwachung innerhalb oder außerhalb der Firma datenschutzkonform statt?