Checkliste für die Umstellung kleinerer Unternehmen auf die Datenschutzgrundverordnung

Die Datenschutz-Grundverordnung (DS-GVO) ist ab dem 25. Mai 2018 unmittelbar in den Mitgliedsstaaten der EU anwendbar.
Sie schreibt inhaltlich im Wesentlichen die bisherigen datenschutzrechtlichen Grundprinzipien fort und entwickelt sie weiter.
Die Grundsätze des „Verbots mit Erlaubnisvorbehalt“, der „Datenvermeidung und Datensparsamkeit“, der „Zweckbindung“ und der „Transparenz“ prägen auch die DS-GVO.
Zusätzlich werden neue Transparenzanforderungen eingeführt: Stärkung der Rechte auf Information, Zugang und Löschung („Recht auf Vergessenwerden“).
Auch für kleinere Unternehmen ergeben sich aus der DS-GVO erweiterte Dokumentations- und Nachweispflichten, um der Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO zu genügen.
Die Artikel der DS-GVO sind zusammen mit den Erwägungsgründen zu lesen. Diese erläutern die damit verfolgten Ziele und sind hilfreich für die Interpretation der Rechtsnormen.

Nutzen Sie zur Umstellung auf die DS-GVO die folgende Checkliste:

1. Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO

Dieses löst das bisherige Verfahrensverzeichnis ab, d.h. es bedarf im Regelfall nur einer Anpassung.
Verarbeitungstätigkeiten, die in einem kleinen Unternehmen (z.B. des Einzelhandels) anfallen können, sind beispielsweise eine Kundendatei (Kundenkarte, Newsletter), die Gehaltsabrechnung für die Beschäftigten (ggf. über ein externes Buchhaltungsbüro), die Abwicklung von EC-bzw. -Kreditkartenzahlungen (zumeist über einen Zahlungsdienstleister) sowie ggf. der Betrieb einer eigenen Internetseite (oft gehostet über einen externen Dienstleister).
Hinweise hierzu sowie ein Muster für die Erstellung finden Sie auf der Internetseite der LfD Niedersachsen: https://lfd.niedersachsen.de/startseite/datenschutzreform/ds_gvo/verzeichnis_von_verarbeitungstatigkeiten/verzeichnis-von-verarbeitungstatigkeiten-179665.html

2. Informationspflichten

Art. 12 DS-GVO festigt den Leitgedanken der DS-GVO nach transparenter Information. So müssen Unternehmen ihre Kunden und Beschäftigten umfassend gem. Art. 13 und 14 DS-GVO über die Erhebung personenbezogener Daten informieren.

Einwilligungen müssen den Anforderungen des Art. 7 DS-GVO genügen.

Die Informationen müssen den betroffenen Personen sehr zeitnah zur Verfügung gestellt werden und leicht verständlich sein.
Implementieren Sie Verfahren, um Ihren Pflichten frist- und formgerecht zu genügen.
Beachten Sie hierzu auch das Kurzpapier Nr. 10 „Informationspflichten“ auf der Internetseite der LfD Niedersachsen: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html.

3. Betroffenenrechte

Die Rechte der von einer Datenverarbeitung betroffenen Personen auf Auskunft, Berichtigung, Löschung und Widerspruch werden umfangreicher. Neu hinzugekommen ist das Recht auf Datenübertragbarkeit.
Entwickeln Sie auch hier Verfahren, um den Rechten der Betroffenen frist- und formgerecht nachkommen zu können. Eine gute Basis bildet das Verzeichnis von Verarbeitungstätigkeiten.
Weitere Informationen finden Sie im Kurzpapier Nr. 6 „Auskunftsrecht“ auf der Internetseite der LfD Niedersachsen: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html sowie auf dieser Seite beim Thema „Wirtschaft“.

Sie müssen als Unternehmen sicherstellen, dass die personenbezogenen Daten gelöscht werden, wenn die Notwendigkeit der Verarbeitung zur Zweckerreichung entfallen ist. Dies ist bei der Beendigung der Kundenbeziehung der Fall bzw. bei Auflösung des Arbeitsverhältnisses und entspricht der bisherigen Regelung im BDSG.
D.h. die Speicherung zur Erfüllung steuerlicher oder handelsrechtlicher Aufbewahrungspflichten ist selbstverständlich weiterhin zulässig.
Es sind die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen, damit z.B. die Daten ehemaliger Kunden bzw. Beschäftigter nicht mehr im aktuellen Dateibestand vorhanden sind. Beachten Sie auch das Kurzpapier Nr. 11 „Recht auf Löschung“, aufzurufen über: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html.

4. Verpflichtung der Beschäftigten

Nach Art. 29 DS-GVO dürfen Beschäftigte eines verantwortlichen Unternehmens personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor. Ergänzend dazu regelt Art. 32 Abs. 4 DS-GVO, dass der verantwortliche Unternehmer Schritte unternehmen muss, um sicherzustellen, dass ihm unterstellte Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf seine Anweisung verarbeiten. Die Umsetzung dieser Verpflichtung ist gesetzlich nicht festgelegt. Es ist aber zu empfehlen, dies in Form einer schriftlichen oder elektronischen Verpflichtungserklärung umzusetzen Dies betrifft z.B. die Mitarbeitenden in der Unternehmensverwaltung, die mit der Verarbeitung personenbezogener Daten von Beschäftigten bzw. Kunden betraut wurden.

Weitere Informationen sowie ein Muster für die Verpflichtung Ihrer Beschäftigten finden Sie im Kurzpapier Nr. 19 auf der Internetseite der LfD Niedersachsen: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html.

5. Auftragsverarbeitung

Wie bislang, so besteht auch unter der DS-GVO mit Art. 28 DS-GVO eine Sonderregelung für Verarbeitungen von personenbezogenen Daten durch Beauftragung eines anderen. Eine Auftragsverarbeitung liegt z.B. vor, wenn ein Unternehmen seine personenbezogenen Daten an eine Stelle außerhalb des eigenen Unternehmens abgibt (z.B. externe Buchhaltung), aber auch, wenn die Rechner durch einen externen Dienstleister (IT-Firma) gewartet werden und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Es muss ein den Anforderungen des Art. 28 DS-GVO genügender Vertrag geschlossen werden. Bestehende Verträge können fortgelten, sofern sie den Anforderungen der DS-GVO entsprechen, andernfalls sind sie anzupassen. In jedem Fall ist jedoch die Rechtsgrundlage (im Vertrag, sowie im Verarbeitungsverzeichnis) anzupassen, da die ursprüngliche seit dem 25.05.2018 entfallen ist. Neu sind die erweiterten Pflichten und die Verantwortlichkeit des Auftragsverarbeiters. So hat dieser z.B. zukünftig ebenfalls ein Verzeichnis der Verarbeitungstätigkeiten zu führen (Art. 30 DS-GVO) und gilt selbst als Verantwortlicher, wenn er die Daten des Auftraggebers verordnungswidrig für eigene Zwecke oder Zwecke Dritter verarbeitet, mit allen rechtlichen Folgen.
Zur rechtssicheren Gestaltung des Vertrags wird die Verwendung der Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO empfohlen: https://lfd.niedersachsen.de/startseite/themen/auftragsverarbeitung_nach_art_28_ds_gvo/auftragsverarbeitung-nach-art-28-ds-gvo-179673.html

6. Datenschutzbeauftragte

Wie bisher hat ein Unternehmen nach Art. 37 Abs. 4 DS-GVO i.V.m. § 38 Abs. 1 S.1 BDSG-neu einen Datenschutzbeauftragten zu benennen, wenn in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Maßgeblich ist die Zahl der Köpfe, nicht die Zahl der Stellen. Dies betrifft insbesondere die mit der Personal- und Kundenverwaltung beschäftigten Mitarbeitenden. Verkaufspersonal, welches die Kunden mit Namen anspricht, zählt nicht dazu. Darüber hinaus kann sich zudem eine Benennungspflicht aus Art. 37 Abs. 1 lit. b.) oder c.) DS-GVO, sowie aus § 38 Abs. 1 S. 2 BDSG-neu ergeben. Weitere Informationen zum Thema Datenschutzbeauftragte finden Sie im Kurzpapier Nr. 12 auf der Internetseite der LfD Niedersachsen: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html.
Sofern Sie jedoch benennungspflichtig sind, haben Sie nach Art. 37 Abs. 7 DS-GVO die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen (z.B. auf der Internetseite) und diese der LfD Niedersachsen als zuständiger Aufsichtsbehörde mitzuteilen.

7. Beschäftigtendatenschutz

Aufgrund einer sog. Öffnungsklausel in Art. 88 Abs. 1 DS-GVO bildet § 26 Abs. 1 S. 1 BDSG-neu die maßgebliche Rechtsgrundlage für den Beschäftigtendatenschutz in Deutschland. Dies entspricht weitgehend der bisherigen Regelung, d.h. personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, soweit dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Bitte beachten Sie hierzu auch das Kurzpapier Nr. 14 „Beschäftigtendatenschutz“, zu finden unter: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html.

8. Sicherheit der Verarbeitung

Jedes verantwortliche Unternehmen hat gem. Art. 32 Abs. 1 DS-GVO geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko der konkreten Datenverarbeitung jeweils angemessenes Schutzniveau zu gewährleisten. Sie sollten stets auf aktuelle Betriebssysteme und Anwendungen zurückgreifen, die automatisch aktualisiert werden sowie regelmäßige Backups durchführen und aktuelle Virenscanner einsetzen. Ein effektiver Passwortschutz muss selbstverständlich sein. Beachten Sie hierzu auch das Kurzpapier Nr. 18 „Risiko für die Rechte und Freiheiten natürlicher Personen“ auf der Internetseite der LfD Niedersachsen: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html.

9. Datenschutzfolgeabschätzung

Ob eine Datenschutzfolgeabschätzung (DSFA) nach Art. 35 DS-GVO durchzuführen ist, zeigt sich bei Abschätzung der Risiken der Verarbeitungsvorgänge. Nur wenn sich hier ein voraussichtlich hohes Risiko ergibt, ist eine DSFA durchzuführen. Verarbeitungsvorgänge, für die aufgrund eines voraussichtlich hohen Risikos für die Rechte und Freiheiten natürlicher Personen stets eine DSFA durchzuführen ist, finden sich auf einer sog. „Blacklist“ wieder, abzurufen auf der Internetseite der LfD Niedersachsen.
Die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA sollte jedoch stets schriftlich dokumentiert werden.
Sofern Sie eine DSFA durchführen, beachten Sie das entsprechende Kurzpapier Nr. 5, zu finden unter: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html und ergänzend das bei Ziff. 8 erwähnte Kurzpapier Nr. 18 zum Thema Risiko.

10. Videoüberwachung

Sofern Sie Kameras installiert haben, ist für die Prüfung der Rechtmäßigkeit zunächst auf Art. 6 Abs. 1 S. 1 lit. f DS-GVO abzustellen. Danach ist die Verarbeitung rechtmäßig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Die formellen und materiellen Anforderungen für den Einsatz einer Videoüberwachung werden mit Inkrafttreten der DS-GVO nicht abgesenkt. Weitere Informationen zum Thema finden Sie auch im Kurzpapier Nr. 15 „Videoüberwachung“ auf der Internetseite der LfD Niedersachsen: https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html.

11. Datenpannen (Verletzung des Schutzes personenbezogener Daten)

Hier greifen nunmehr die Regelungen in Art. 33 und 34 DS-GVO.
In der Praxis kommt es auf vielfältigste Weise zu sog. Datenpannen, z.B. durch einen Hacker-Angriff, aber auch aufgrund eines Diebstahls des Laptops im Rahmen eines Einbruchs in die Geschäftsräume.
Liegt eine Verletzung des Schutzes personenbezogener Daten vor, müssen Sie diese innerhalb von 72 Stunden mit den in Art. 33 Abs. 3 DS-GVO genannten Mindestinformationen der zuständigen Datenschutzaufsichtsbehörde (LfD Niedersachsen) melden. Eine Ausnahme besteht, wenn die Verletzung voraussichtlich nicht oder nur zu einem geringen Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt. (vgl. Art. 33 Abs. 1 DS-GVO, z. B. weil durch eine geeignete Verschlüsselung der Daten eine unbefugte Kenntnis ausgeschlossen werden kann.
Hierfür gibt es ein Online-Meldeportal auf der Internetseite www.lfd.niedersachsen.de.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstr. 5, 30159 Hannover
Tel.: 0511 - 120 4500 / Fax: 0511 - 120 4599
eMail: poststelle@lfd.niedersachsen.de