DEHOGA NORDRHEIN-WESTFALEN

MERKBLATT

STAND: FEBRUAR 2018

Datenschutz-Grundverordnung (EU-DSGVO) und Bundesdatenschutzgesetz (BDSG-neu) ab 25.05.2018 in Kraft

Ende Mai 2018 tritt neben einer neuen EU-weiten Datenschutz-Grundverordnung das neue Bundesdatenschutzgesetz in Kraft. Für das Gastgewerbe bedeuten diese Datenschutzvorschriften in einigen Bereichen eine Neuregelung des Umgangs mit personenbezogenen Daten. Aufgrund der Komplexität ist es ratsam, sich vor in Kraft treten der Verordnung zu informieren oder beraten zu lassen.

Unser Merkblatt soll Ihnen einen ersten Überblick über die wichtigsten Notwendigkeiten geben, mit besonderem Blick auf das Tagesgeschäft in Bezug auf Gäste- und Mitarbeiterdaten.

Für einen ausführlicheren Einstieg empfehlen wir die Erklärungen des DEHOGA Bundesverband, die im exklusiven Mitgliederbereich unter *Datenschutzrecht neu Merkblatt* zum Download bereit stehen. Der Leitfaden der IHA zum Thema ist im IHA-Shop unter www.iha-service.de erhältlich.

Aufbau:

Teil1: Allgemeine Regelungen und Grundsätze
Teil 2: Rechte der Betroffenen
Teil 3: Umgang mit Gästedaten
Teil 4. Umgang mit Mitarbeitern
Teil 5: Rechtsfolgen
Teil 6: Fazit

DEHOGA Nordrhein-Westfalen
DEHOGA-Center Neuss, Hammer Landstraße 45, 41460 Neuss, Fon 02131 7518 200
info@dehoga-nrw.de www.dehoga-nrw.de

Teil 1: Allgemeine Regelungen und Grundsätze

A. Personenbezogene Daten (Art. 4 DSGVO) –

sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen.

Relevant sind die Daten, wenn sie (teil-)automatisiert, also digital, erfasst bzw. verarbeitet (z.B. in einer Personalverwaltungssoftware), aber auch, wenn sie systematisch geordnet gesammelt werden (Kartei oder Visitenkartensammlung).

Besondere Kategorien personenbezogener Daten
Die Verarbeitung besonderer Kategorien (z.B. ethnische Herkunft, sexuelle Orientierung, Gesundheitsdaten oder genetische, biometrische Daten) ist – und das ist neu – grundsätzlich untersagt.

Ausnahmen gibt es gemäß Art. 9 Abs. 2 in bestimmten Fällen:

- Bei freiwilliger Einwilligung
- Wenn die Verarbeitung einem bestimmten definierten Zweck dient, zum Beispiel steuerrechtlichen Gründen / Lohnabrechnung wie Erfassung der Konfession zum Zwecke der Lohnberechnung, Krankmeldung und ähnliches – das trifft vor allen Dingen für Mitarbeiterdaten zu.

B. Grundsätze für die Verarbeitung personenbezogener Daten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  Verarbeitung der Daten nur, wenn durch Rechtsgrundlage gedeckt
- Zweckbindung
  Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke
- Datenminimierung
  Verarbeitung in angemessenem Rahmen und Zweckdienlichkeit
- Richtigkeit und Aktualität der Daten
- Speicherbegrenzung
  - Zeitliche Speicherung der Daten bis Zweckerfüllung
  - Dann Gewährleistung der Nicht-Identifizierbarkeit der Person
- Integrität und Vertraulichkeit
  - Angemessene, sichere Verarbeitung der Daten mit dem Ziel, vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, Zerstörung oder Schädigung zu schützen.

C. Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO)

- Nachweispflicht über Einhaltungen der verschiedenen Grundsätze (zusammen mit Compliance Anforderung – wie bisher)
- **Neu:** Konzept-Dokumentationspflicht
  Erstellung eines Konzepts zur Sicherstellung der Einhaltung der Grundsätze der DSGVO inklusive Kontrollfunktion

D. Dokumentationspflichten für Unternehmen

Jeder „Verantwortliche“ (der Daten verarbeitet) ist verpflichtet, ein **Verzeichnis von Verarbeitungstätigkeiten zu** führen (Art. 30/1), vor allen Dingen, wenn die Verarbeitung ein Risiko für Rechte und Freiheiten der betroffenen Person birgt, die Verarbeitung nicht nur gelegentlich oder eine Verarbeitung besonderer Datenkategorien erfolgt.

1. Inhalte des Verzeichnisses:

- Name und Kontaktdaten des Datenschutzbeauftragten
- Zweck der Verarbeitung
- Beschreibung der Kategorien betroffener Personen
- Beschreibung der Kategorien personenbezogener Daten
- Aufzählung des Empfangs personenbezogener Daten
- Fristen für die Löschung der personenbezogenen Daten
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen. Diese werden nicht vorgegeben, der Verantwortliche muss erarbeiten, welches Schutzniveau die verarbeiteten Daten benötigen und welche Maßnahmen zum Schutz geeignet und erforderlich sind.

2. Kritische Punkte:

- Vertraulichkeit von Daten
  Bsp: Zugriffskontrolle auf Daten oder getrennte Verarbeitung
- Integrität
  Bsp: Nachvollziehbarkeit des Zugriffs und Manipulationsschutz
- Verfügbarkeit
  Bsp: Schutz vor ungewolltem Verlust oder Möglichkeit der Widerherstellung
- Überprüfung von Daten
  Bsp: Überprüfung weisungsgemäßer Verarbeitung

Der Unternehmer sollte auf Vollständigkeit + Aktualität prüfen (inkl. Mechanismus „auf aktuellem Stand halten“). Das gilt insbesondere für

- Verwaltung der Personalakten
- Arbeitszeiterfassung
- Lohn- und Gehaltsabrechnung
- Bewerbungsmanagement
- Betriebliche Altersvorsorge

Hinweise:

- Mögliche Befreiung für Betriebe mit <250 Mitarbeitern, wenn Verarbeitung personenbezogener Daten nur gelegentlich. Achtung: Verzeichnis wird trotzdem grundsätzlich wegen Nachvollziehbarkeit empfohlen!
- Mögliche Unterschiede bei Verarbeitung von Gäste-/ Mitarbeiterdaten
- Auch ein Auftragsverarbeiter, extern beauftragter Dienstleister (z.B. externe Lohnbuchhaltung, IT-Service, nicht aber Steuerberater oder Rechtsanwalt) muss ein Verzeichnis führen und dokumentieren.

3. **Datenschutzkonzept für Rechenschaftspflicht**
   Neben dem Verzeichnis von Verarbeitungstätigkeiten ist ein Datenschutzkonzept (-policy) notwendig, um seiner Rechenschaftspflicht (Art. 5/2) nachzukommen.

   - Datenschutzorganisation (grundsätzlicher Aufbau)
   - Wer ist für welche Bereiche verantwortlich?
   - Schutzmaßnahmen bei der Datenverarbeitung
   - Umgang mit Betroffenenrechten inklusive der Lösung
   - Prozedere für Umgang mit Datenpannen
   - Mitarbeiterschulung, um Einhaltung des Konzepts sicherzustellen

4. **Risikoanalyse**
   Durchführung und Dokumentation einer Risikobewertung bezüglich Rechte und Freiheiten natürlicher Personen mit folgenden Inhalten:

   - Klassifizierung drohender Schäden
   - Prognose Eintrittswahrscheinlichkeit
   - Analyse, ob Verarbeitung Risiko darstellt

   Bei hohem Risiko durch die Verarbeitung (z.B. durch die Verwendung neuer Technologien, Art, Umfang, Zweck) muss eine **Datenschutz-Folgeabschätzung** (Art. 35) zu diesen Punkten durchgeführt und dokumentiert werden.

   - Systematische Beschreibung der Verarbeitungsvorgänge
   - Zweck der Verarbeitung, Bewertung der Notwendigkeit
   - Welche Interessen verfolgt die Verarbeitung
   - Bewertung Notwendigkeit und Verhältnismäßigkeit
   - Bewertung der Risiken für Rechte und Freiheiten der Betroffenen
   - Getroffene und geplante Abhilfemaßnahmen zur Sicherstellung des Schutzes der personenbezogenen Daten

E: Datenschutzbeauftragte

Betriebe mit mehr als 10 Mitarbeitern, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, müssen einen Datenschutzbeauftragten bestellen.
Wenn diese(-r) aus dem Mitarbeiterteam kommen soll, ist zu beachten, dass sich daraus kein Interessenskonflikt mit der neuen Aufgabe ergibt. IT Verantwortliche oder für Personalangelegenheiten Zuständige sind hierfür nicht einzusetzen.

Tipp: Der Datenschutzbeauftragte muss nicht unbedingt zertifiziert sein, es empfiehlt sich aber.

Teil 2: Rechte der Betroffenen (Art. 12-23)

1. **Grundsätzliche Informationspflicht des Unternehmers zu:**

   - Name und Adresse des Verantwortlichen
   - Adresse des Datenschutzbeauftragten
   - Zwecke der Datenverarbeitung
   - Berechtigte Interessen (ggfs.)
   - Empfänger der Daten
   - Ggfs. Absicht zur Übermittlung an Drittland
   - Dauer der Speicherung (Datenaufbewahrungspflichten)
   - Hinweis auf Betroffenenrechte (besonders Beschwerderecht)
   - Widerrufsrecht (wenn auf Einwilligung basieren)

2. **„Recht auf Vergessenwerden“ – Recht auf Löschung** (Art. 17) - bei:

   - Zweckentfall
   - Widerruf der Einwilligung
   - Widerspruch gegen Verarbeitung und fehlende Gründe für Weiterverarbeitung
   - Unrechtmäßiger Verarbeitung der Daten

   Hinweis: Neu ist nur die Rechenschaftspflicht für die Einhaltung der Regeln.

3. **Recht auf Datenübertragbarkeit** (Art. 20)

   Neu: Betroffene Personen haben jetzt das Recht, verarbeitete personenbezogene Daten strukturiert in gängigem, maschinenlesbarem Format (z.B. Excel, Word, open Office) zu erhalten oder an einen Dritten übermitteln zu lassen.
   Vor der Übertragbarkeit: Einwilligung des Betroffenen sowie die Verarbeitung in einem automatisierten Verfahren.

4. **Widerspruchsrecht** (Art. 21)

   Betroffene Personen haben das Recht, jederzeit gegen die Verarbeitung ihrer personenbezogenen Daten Widerspruch einzulegen. Diesem Recht können nur zwingende Gründe der Verarbeitung, die dem überwiegen, entgegenwirken (z.B. Ausübung von Rechtsansprüchen).

5. **Fristen bei Datenpannen** (Art. 33)

   Neu: 72 Stunden Frist für Meldung an die Aufsichtsbehörde bei „Verletzung des Schutzes personenbezogener Daten“ (Datenpanne)

   Achtung: Gilt auch, wenn eigentlicher Verstoß nicht vom Unternehmen selbst, sondern von einem eingesetzten Dritten (Auftragsarbeiten, z. B. Lohnbuchhalter) begangen wird! Verzögerungen müssen begründet werden!

6. **Regelungen für Auftrags(daten)verarbeitung** (Art. 28)

Neu: Vereinbarungen dazu können auch in elektronischer Form erfolgen (Anklicken einer Box, elektronische Signatur etc.). Früher war dazu Schriftform nötig.
Eine Prüfung der technischen und organisatorischen Maßnahmen des Auftragsverarbeiters durch den Verantwortlichen ist nicht mehr nötig,
Der Auftragsarbeiter muss aber nachweisen, dass geeignete technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten getroffen wurden.

Tipp: Bestehende Verträge prüfen!

Teil 3: Mitarbeiterdaten

Mitarbeiterdaten sind mit besonderer Sorgfalt zu verarbeiten, da sie im besonderen Maße personenbezogene Daten enthalten, die zudem noch in sensible Kategorien fallen können, die einen entsprechenden Umgang damit benötigen.

Einwilligung in Datenverarbeitung durch Arbeitnehmer, (Art. 7)

Mitarbeiter müssen Verarbeitung personenbezogenen Daten zustimmen.

- Der Einwilligung muss die Kenntnis des vollen Umfangs der geplanten Verarbeitung vorangehen und sie muss freiwillig sein.
- Der nötige Hinweis auf das Widerrufsrecht kann mündlich oder elektronisch erfolgen.
- Der Nachweis der Einwilligung muss erbracht werden können.
  Wenn nicht anders (digital) möglich, muss die Einwilligung in schriftlicher Form erfolgen. Wenn im Arbeitsvertrag enthalten, ist auf eine klare und „einfache“ Sprache zu achten.
- Die Einwilligung ab dem 16. Lebensjahr ohne Einwilligung des Erziehungsberechtigten ist möglich.

Tipp: Bereits jetzt umstellen und auf Konformität prüfen, damit diese auch nach dem 25.5.2018 gelten.

Besonderheit der Einwilligung über den Arbeitsvertrag
Die freiwillige Einwilligung ist dann in Ordnung, wenn

- für Arbeitnehmer ein rechtlich oder wirtschaftlicher Vorteil entsteht oder
- gleichgelagerte Interessen bestehen.

Beispiele (laut BDSG) bei

- Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung
- Erlaubnis zur Privatnutzung betrieblicher IT-Systeme
- Aufnahme von Namen und Geburtstag in Geburtstagsliste
- Nutzung eines Fotos für das Intranet

Teil 4: Gästedaten

Für die Verarbeitung von Gästedaten, die im Zusammenhang mit einer Reservierung oder während des Aufenthaltes bis hin zum Check Out entstehen, braucht es für die weitere Verwendung die ausdrückliche Zustimmung des Gastes. Ansonsten gilt es, notwendige Daten zu sichern, spätestens wenn der Gast ausgecheckt hat.
Das gilt auch für die Fälle, in denen Sie personenbezogene Daten für Ihre **Marketing Aktivitäten** nutzen wollen. Beispiele:

- Newsletter
- Email-Mailings
  Einwilligung über Double-Opt-In-Verfahren (Einwilligung durch Anklicken eines Links in einer Bestätigungsmail) einholen und dokumentieren
- Gewinnspiele, Rabattaktion: Achtung Falle „Kopplungsverbot“!
  Auch wenn die Einwilligung für das Zusenden eines Newsletters vorliegt, wird sie durch eine Kopplung (x% Rabatt auf die nächste Buchung bei Anmeldung zum NL) unwirksam.
- Meldeschein
  Daten aus dem Meldeschein sind zweckgebunden und für Marketingzwecke nur nach unbedingter Einwilligung nutzbar.
- Gästebefragungen
  Achten Sie hier auch darauf, dass der Fragebogen keinem anderen zum Lesen zugänglich ist. Wenn Sie Ihre Gäste ermuntern, einen Fragebogen auszufüllen, der auf dem Zimmer ausgelegt ist, sollten Sie sicherstellen, dass Ihre Mitarbeiter den Bogen einsammeln, bevor der nächste Gast das Zimmer bezieht.

Prüfen Sie Ihre AGB:

- Die Einwilligung z.B. über die Zusendung von Werbung oder den digitalen Newsletter darf nicht in den AGB „versteckt“ werden. Sie muss deutlich erkennbar möglichst zu Beginn der AGB mit einem Hinweis auf die datenschutzrechtliche Einwilligung hervorgehoben sein.
- Die Einwilligung muss aktiv sein, z.B. durch Anklicken. Ein Anklicken, wenn man nicht einverstanden ist, gilt nicht als Einwilligung.

Prüfen Sie die Datenschutzbestimmungen auf Ihrer Website:

- Kontaktdaten des Verantwortlichen (Unternehmensdaten)
- Kontaktdaten des Datenschutzbeauftragten
- Zwecke der personenbezogenen Datenverarbeitung, Rechtsgrundlage, berechtigte Interessen
- Speicherdauer
- Hinweis auf Auskunftsrecht und Widerrufsrecht der Betroffenen
- Auflistung der Empfänger bei Übermittlung von Daten an Dritte innerhalb und außerhalb der EU
- Bei Verwendung bestimmter Applikationen z.B.:
  - SSL-Verschlüsselung der Webseite
  - Verschlüsselte Formulare zur Eingabe personenbez. Daten
  - Verwendung von Daten z.B. für Newsletter
  - Verwendung von Google-Services, Social-Media-Plugins etc.

  - Umgang mit Webformularen
  - Verwendung von Cookies (Zweck, Empfänger etc.)
  - Verwendung von Analyse-Tools (z.B. Google Analytics)
- Verarbeitung der IP Adresse (weil personenbezogene Daten)

Tipp: Prüfen Sie Verträge mit Ihren Partnern:
- Was machen z.B. Suchmaschinen mit Daten Ihrer Gäste?

Teil 5: Rechtsfolgen

Wer die Entwicklung der Rechtsfolgen bei Verstößen betrachtet, stellt fest, dass es dem Gesetzgeber ernst ist, dem Schutz personenbezogener Daten eine besonders wichtige Stelle künftig einzuräumen.

Bußgelder (Art. 83)
Achtung: Die Obergrenze liegt bei 10 bzw. 20 Millionen Euro oder bis zu 4% des Jahresumsatzes, je nach dem, was höher ist. Bisher lag sie bei lediglich 50 – 300.000 Euro)!

Mit der deutlichen Erhöhung soll eine „abschreckende Wirkung“ erzielt werden. Darüber hinaus ist in jedem Fall mit vermehrten Prüfungen zu rechnen.

Teil 6: Fazit

Das Thema Datenschutz erfährt eine immer größer werdende Bedeutung, was sich an Rechten, Pflichten und Konsequenzen bei Verstößen erkennen lässt. Sensibilisieren Sie deshalb Ihre Verantwortlichen für die Wichtigkeit des Schutzes personenbezogener Daten und schaffen Sie Ressourcen für Dokumentation und beginnen Sie schnellstmöglich.

- Verzeichnis der Verarbeitungstätigkeiten zusammenstellen
- Risikobewertung vornehmen
- Formulare prüfen und aktualisieren (Einwilligungserklärungen, Vereinbarungen etc.)
- Datenschutzkonzept aktualisieren
- Schulung und Sensibilisierung der relevanten Beschäftigten