



Neues Datenschutzrecht - ab dem 25.05.2018 -



EU-Datenschutzgrundverordnung (DSGVO)

Seite 2
15.02.2018

**DSGVO gilt ab dem 25.05.2018
unmittelbar**

**Ziel Harmonisierung des
Datenschutzes in der EU**

**Bundesregierung hat ergänzend neues
BDSG erlassen**



EU-Datenschutzgrundverordnung (DSGVO)

Seite 3
15.02.2018

Ziel Verbesserung des Datenschutzes

Stärkung der Betroffenenrechte

Recht auf Auskunft, Berichtigung, Löschung
(Vergessenwerden), Einschränkung der Verarbeitung,
Widerspruch und Recht zur Datenübertragung



Erwägungsgründe

„Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht.“



Neues Datenschutzrecht ist strenger!

Seite 5
15.02.2018

Bei Verstößen droht Geldbuße von bis zu 4 % des Umsatzes oder bis zu 20 Mio. €, Art. 83 DSGVO

Der Betroffene hat Anspruch auf Ersatz des materiellen und immateriellen Schadens, Art. 82 Abs. 2 DSGVO

Verbraucherschutzverbände haben eigenes Klagerecht

Nach Art. 24 Abs. 1 DSGVO gilt Beweislastumkehr



Bußgeldkriterien nach der DSGVO

- Art, Schwere und Dauer des Verstoßes?
- Vorsatz oder Fahrlässigkeit?
- Maßnahmen zur Minderung des Schadens?
- Bisherige technische / organisatorische Maßnahmen?
- Datenschutzkonzept?
- Etwaige frühere Verstöße?





Neues Datenschutzrecht





Prüfpflicht: Wann ist die Verarbeitung persönlicher Daten zulässig?

Verarbeitung zur
Vertragserfüllung

Verarbeitung aufgrund einer
Einwilligung des Betroffenen

Verarbeitung zur Wahrnehmung
berechtigter Interessen



Voraussetzungen der Einwilligung

- **Information über Umfang und Zweck der Verarbeitung**
- **Einfache und klare Sprache sowie Abgrenzung von anderen Sachverhalten**
- **Kopplungsverbot**
- **Hinweis auf kostenfreies Widerrufsrecht**



Dokumentationspflichten

Art. 24 Abs. 1:

Der Verantwortliche setzt geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.



Dokumentationspflichten

Das Unternehmen muss nachweisen können, dass die Datenverarbeitung rechtskonform erfolgt.



Dies macht neben der Vornahme technischer-organisatorischer Maßnahmen auch deren Dokumentation erforderlich!



Dokumentationspflichten - Überblick

Seite 12
15.02.2018

- **Verarbeitungsverzeichnis**
- **Datenschutzerklärung**
- **Auftragsverarbeitung**
- **Datenschutz-Folgeabschätzung**
- **Festlegung der Verantwortlichkeiten**
- **Bestellung des Datenschutzbeauftragten**

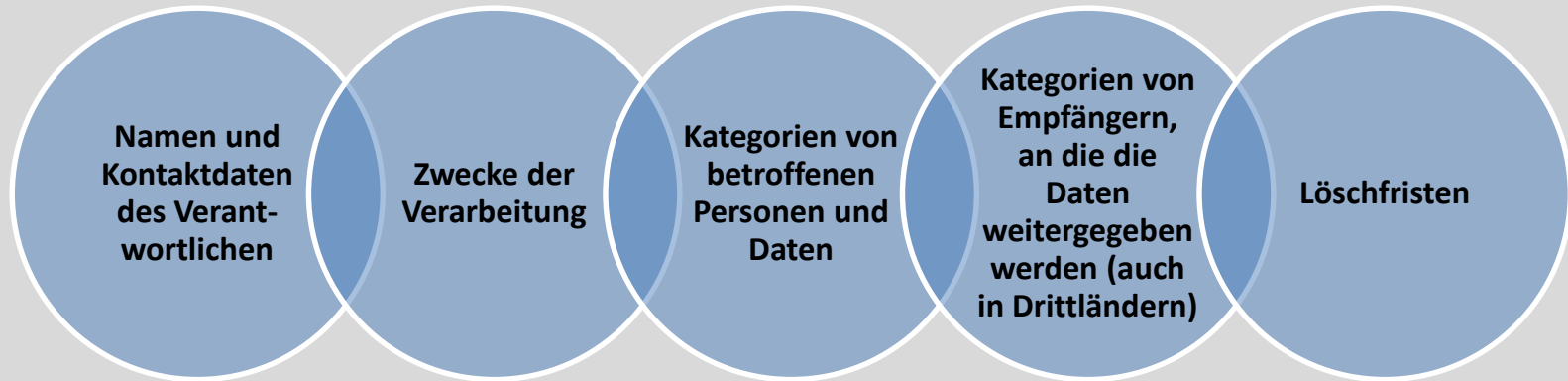


Verarbeitungsverzeichnis

„Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.“



Verzeichnis von Verarbeitungstätigkeiten





Informationspflichten

Fall:

**U hat eigene Webseite. Eine Datenschutzerklärung fehlt.
Verbraucherschutzverband V mahnt den U ab.**

Zu Recht?



Informationspflichten

Jeder Webseitenbetreiber benötigt eine vollständige Datenschutzerklärung.

Webseitenbetreiber die keine oder nur eine unvollständige Datenschutzerklärung haben, verstoßen gegen das Wettbewerbsrecht (vgl. LG Hamburg v. Urt. 07.01.2016).

Seit Oktober 2016 gilt zudem das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von Verbraucherschützenden Vorschriften des Datenschutzrechts.



Inhalt der Datenschutzerklärung

Verarbeitung persönlicher Daten

Cookies, Newsletter und Social Media

Speicherdauer

Betroffenenrechte

Kontakt Daten des Datenschutzbeauftragten

Beschwerderecht bei der Behörde

Kontakt Daten des Verantwortlichen



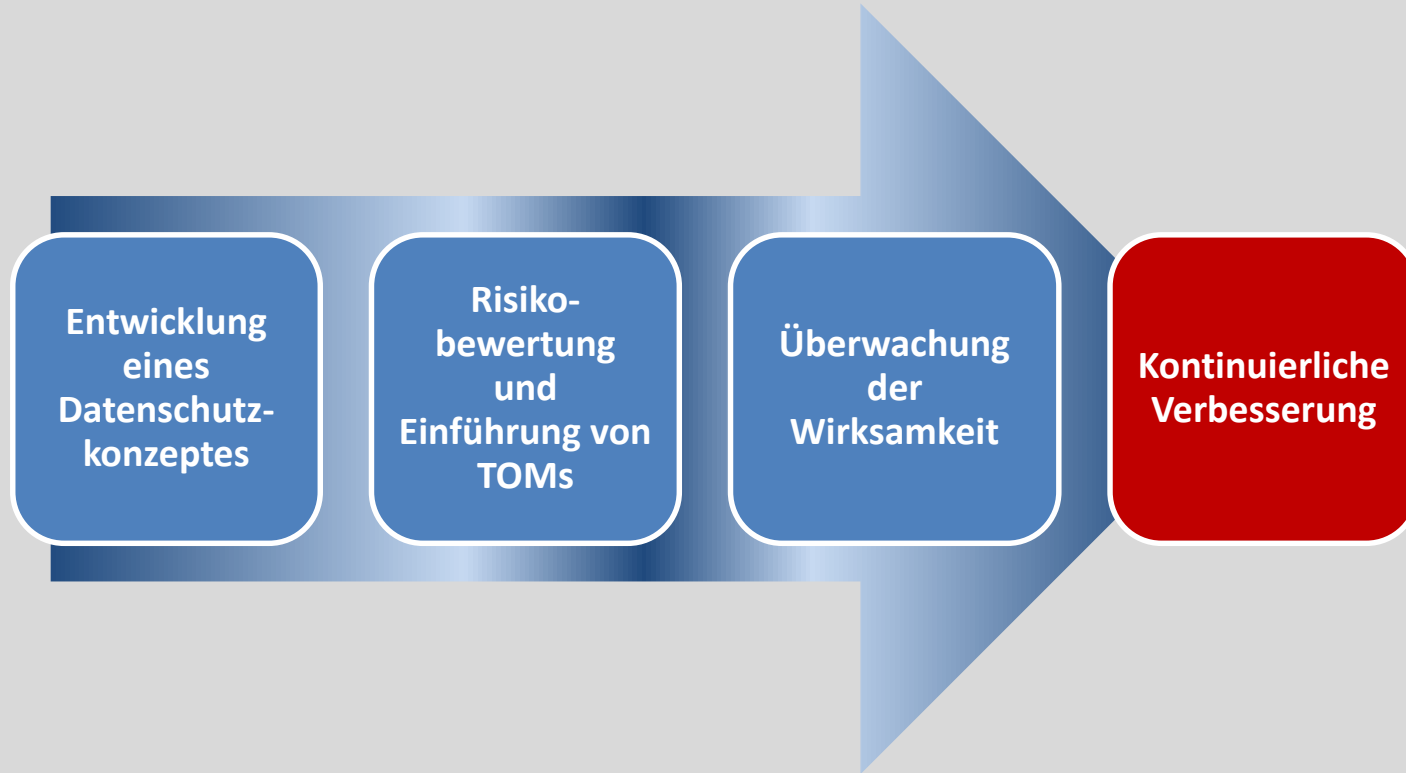
Schutzpflichten: IT- Sicherheit

- **Art. 32 DSGVO verlangt die Einhaltung eines angemessenen Schutzniveaus.**
- **Dabei sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind.**
- **Gefordert wird Schutz gegen Vernichtung, Verlust, Veränderung sowie unbefugte Offenlegung.**



Einrichtung des Datenschutzkonzepts

Seite 19
15.02.2018





Meldepflichten - Beispiele

Hacking

Verlust

Diebstahl

Fehlversand

Softwarefehler

Fehlentsorgung

Datenausspähung



Meldepflichten

Art. 33 DSGVO:

„Im Falle einer Verletzung des Schutzes persönlichen Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Std., nachdem ihm die Verletzung bekannt wurde, diese der gem. Art. 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes persönlicher Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Std., so ist ihr eine Begründung für die Verzögerung beizufügen.“



Inhalt der Meldung

**Beschreibung der Art der Verletzung/
Anzahl der Betroffenen**

Beschreibung der wahrscheinlichen Folgen

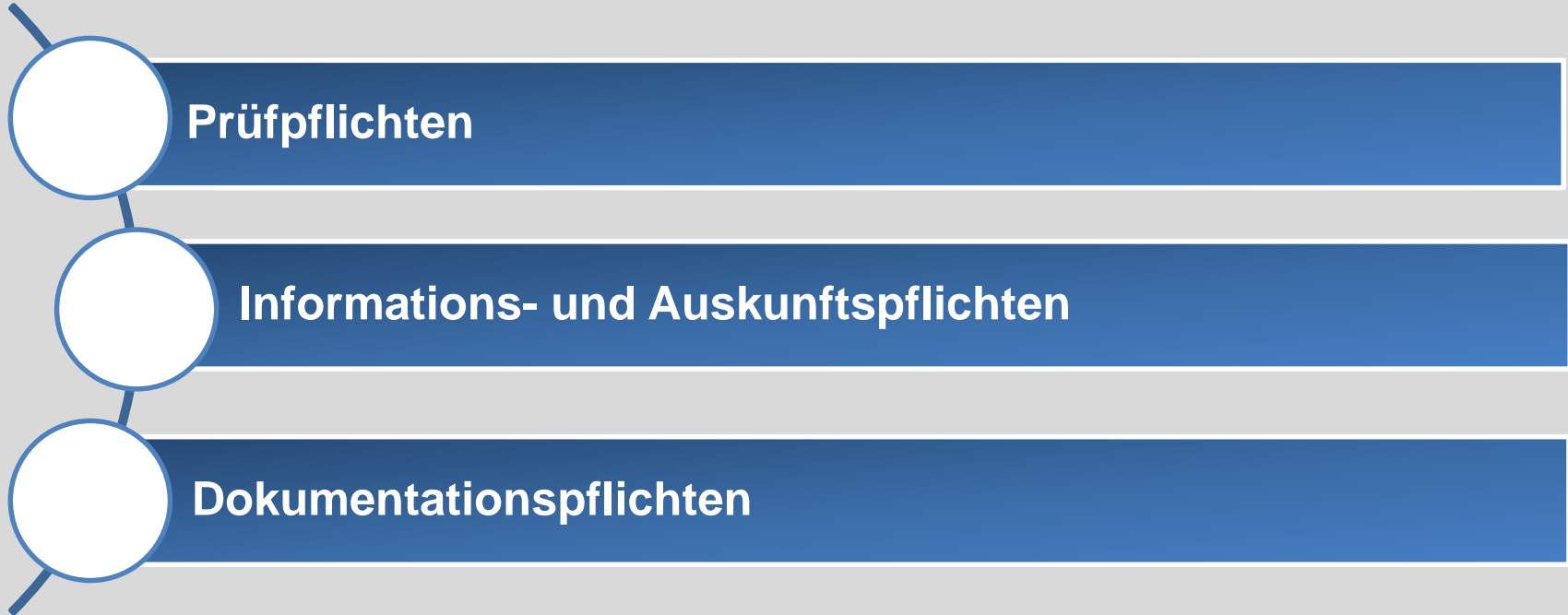
Beschreibung der ergriffenen Maßnahmen

Benennung des Datenschutzbeauftragten



Das kommt auf die Unternehmen zu...

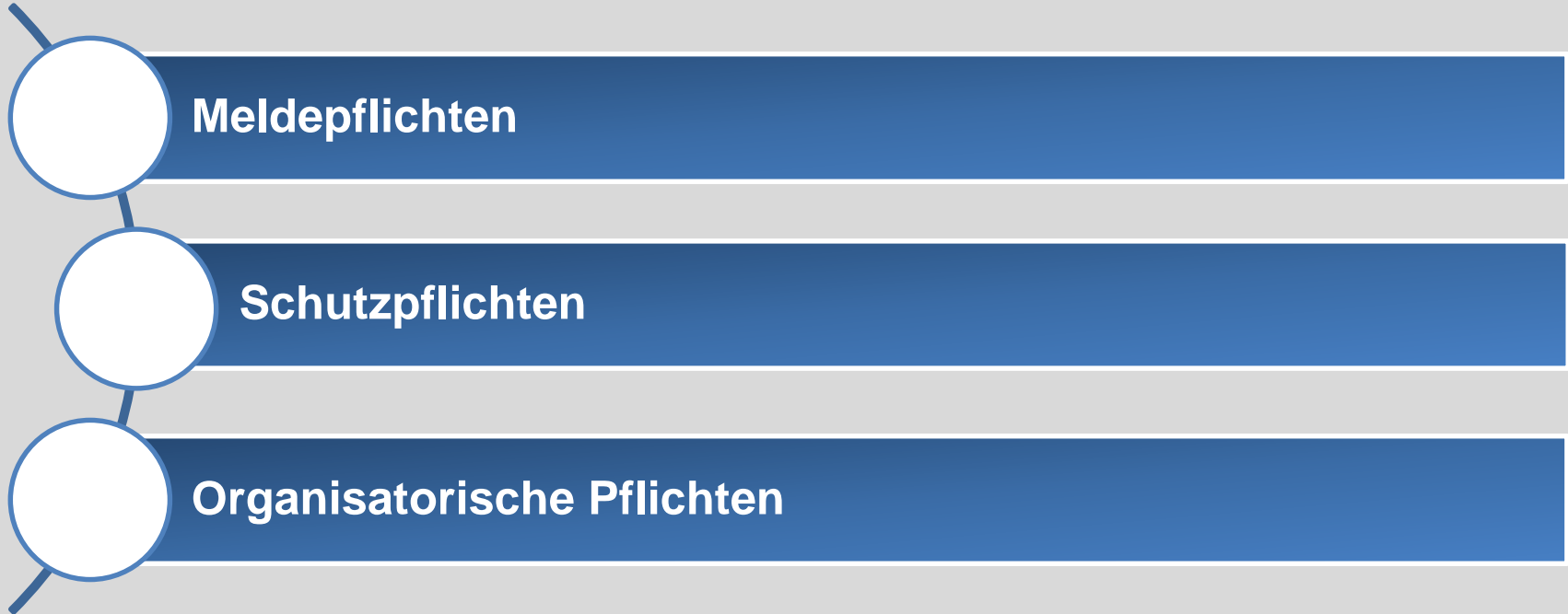
Seite 23
15.02.2018





Das kommt auf die Unternehmen zu...

Seite 24
15.02.2018





Sofortmaßnahmen...

- **Datenschutzerklärung anpassen!**
- **Verfahrensverzeichnis erstellen!**
- **Auftragsdatenvereinbarung anpassen!**
- **Einwilligungserklärung überprüfen!**
- **Technischen Datenschutz prüfen!**
- **Datenschutzbeauftragten bestellen!**



Zusammenfassung

Deutliche Verschärfung der Anforderungen

Hohe Bußgelder bei Verstößen

Datenschutzkonzept notwendig

Regelmäßige Auditierung/Zertifizierung



Die Landesbeauftragte für den Datenschutz Niedersachsen

Barbara Thiel, Prinzenstraße 5, 30159 Hannover,

Tel. 0511/120-4500

Telefax: 0511/120-4599

E-Mail: poststelle@lfd.niedersachsen.de



Weiterführende Links

- www.Ida.niedersachsen.de (Nds. Datenschutzbeauftragte)
- www.Ida.Bayern.de (Bay. Landesamt für Datenschutzaufsicht)
- www.datenschutz.hessen.de (Hess. Datenschutzbeauftragte)



Checkliste der Nds. Aufsichtsbehörde

1. Datenschutz ist Chefsache

- Haben Sie sich als Geschäftsleitung schon mit den neuen Anforderungen der DS-GVO und des BDSG (neu) befasst? Kennen Sie insbesondere die neuen Regelungen
 - zur Rechenschaftspflicht über die Einhaltung der Grundsätze der Datenverarbeitung (Art. 5 Absatz 2 DS-GVO)?
 - zu den Informationspflichten gegenüber den Betroffenen, deren Daten Sie verarbeiten (Art. 12 - 14 DS-GVO)?
 - zu den Rechten der Betroffenen auf Datenübertragbarkeit (Art. 20 DS-GVO)?
 - zur technischen und organisatorischen Sicherheit der Datenverarbeitung Art. 32 DSGVO?
 - zur Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)?
 - zur Meldung von Datenschutzverstößen (Art. 33 DS-GVO)?
- Wer ist in Ihrem Unternehmen neben der Geschäftsleitung für Datenschutzthemen zuständig? Haben Sie einen Datenschutzbeauftragten bestellt (Art. 37 DS-GVO, § 38 BDSG neu)?
- Wurden Ihre Beschäftigten über die neuen Datenschutzregelungen informiert und/oder geschult?



Checkliste II

2. Bestandsaufnahme

- Haben Sie alle Ihre Geschäftsabläufe, bei denen personenbezogene Daten¹ verarbeitet werden, in ein Verzeichnis von Verarbeitungstätigkeiten aufgenommen (Art. 30 DS-GVO)²? Denken Sie hierbei insbesondere an die
 - Verarbeitung von Kundendaten
 - Verarbeitung von Beschäftigtendaten
 - Verarbeitung von Daten von Kindern
 - Verarbeitung von Daten für Dritte als Auftragsverarbeiter
 - Wird dieses Verzeichnis regelmäßig aktualisiert? Wer ist hierfür in Ihrem Unternehmen zuständig?



Checkliste III

3. Betroffenenrechte und Informationspflichten

- Die Betroffenen sind über die Verarbeitung ihrer Daten zu informieren. Dies hat insbesondere in einer transparenten, leicht zugänglichen Form sowie in einer klaren und einfachen Sprache zu erfolgen (Art. 12 DS-GVO).
- Wie stellen Sie diese datenschutzkonforme Information der Betroffenen über alle in Art. 13 und 14 DS-GVO genannten Punkte sicher?
- Besonders wichtig sind in diesem Zusammenhang folgende Informationen:
 - Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
 - Zwecke und Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten
 - Dauer der Speicherung, ggf. Kriterien für die Festlegung der Speicherdauer
 - Hinweis auf Betroffenenrechte
 - Bei Datenverarbeitung auf Basis von Einwilligungen: Hinweis auf Recht zum Widerruf der Einwilligung
 - Recht auf Beschwerde bei der Aufsichtsbehörde
 - Herkunft der Daten
- Wie stellen Sie die weiteren Betroffenenrechte sicher (Art. 15-22 DS-GVO)? Denken Sie dabei insbesondere an folgende Rechte:
 - Recht auf Auskunft
 - Recht auf Berichtigung
 - Recht auf fristgemäße Löschung der verarbeiteten Daten
 - Recht auf Einschränkung der Verarbeitung
 - Recht auf Datenübertragbarkeit



Checkliste IV

4. Personenbezogene Daten von Kindern

- Verarbeiten Sie auch personenbezogene Daten von Kindern in Bezug auf Dienste der Informationsgesellschaft³?
- Wenn ja, haben Sie in diesen Fällen an die besonderen Anforderungen an die Einwilligung gedacht (Art. 8 DS-GVO)?

5. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

- Setzen Sie oder Ihre Dienstleister technische und organisatorische Maßnahmen ein, die ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten (Art. 32 DS-GVO)? Haben Sie Ihre diesbezügliche Schutzbedarfsklassifizierung⁴ dokumentiert?
- Setzen Sie Pseudonymisierungs- oder Verschlüsselungsverfahren ein? In welchen Fällen?
- Haben Sie für die von Ihnen eingesetzten IT-Anwendungen jeweils ein dokumentiertes Rollen- und Berechtigungskonzept?
- Wie stellen Sie sicher, dass bei der Änderung oder Neuentwicklung von Produkten oder Dienstleistungen Datenschutzanforderungen von Anfang an mit berücksichtigt werden (Art. 25 DS-GVO)?



Checkliste V

6. Verträge prüfen

- Haben Sie Ihre bestehenden Verträge mit Auftragsverarbeitern, d.h. mit Unternehmen, die in Ihrem Auftrag personenbezogene Daten verarbeiten, an die neuen Regelungen (Art. 26 - 28 DS-GVO) angepasst?
- Dokumentieren Sie Anpassungen, die Sie Ihren Auftragsverarbeitern geben?
- Bestehen für alle Verarbeitungen, bei denen eine Übermittlung personenbezogener Daten in ein Drittland⁵ möglich ist⁶, entsprechende zusätzliche Garantien/Nvereinbarungen⁷?
 - EU-Standardvertragsklauseln
 - Binding Corporate Rules
 - Privacy Shield (nur für die USA)



Checkliste V

7. Datenschutz-Folgenabschätzung

- Führt Ihr Unternehmen Verarbeitungen mit einem voraussichtlich hohen Risiko für die Rechte und Freiheiten der Betroffenen durch (Art. 35 DS-GVO)? Dies gilt z.B. bei einer umfangreichen Verarbeitung besonderer Kategorien⁹ personenbezogener Daten.
- Falls ja, haben Sie für die in diesen Fällen erforderliche Datenschutz-Folgenabschätzung in Ihrem Unternehmen einen Prozess eingeführt?
- Wer ist für diesen Prozess zuständig?



Checkliste VI

8. Meldepflichten

- Haben Sie in Ihrem Unternehmen einen Prozess zur Meldung von Datenschutzverstößen an die Aufsichtsbehörde eingeführt (Art. 33 DS-GVO)?
 - Haben Sie dabei insbesondere auch die Einhaltung der Meldefrist von 72-Stunden beachtet?
 - Wer ist in Ihrem Unternehmen für die Meldung zuständig?
- Falls Sie einen Datenschutzbeauftragten bestellt haben, denken Sie an die Meldung von seinen/ihren Kontaktdaten an die Aufsichtsbehörde.

9. Dokumentation

- Können Sie die Einhaltung aller vorstehend genannten Pflichten/Anforderungen (schriftlich) nachweisen?
- Wie stellen Sie sicher, dass Ihre Dokumentation immer auf dem neuesten Stand ist?

Quelle:

https://www.lfd.niedersachsen.de/startseite/dsgvo/fragen_zur_vorbereitung_auf_dsgvo/



Disclaimer

Dieser Vortrag dient der unverbindlichen Information und hat – insbesondere vor dem Hintergrund der sich aktuell noch entwickelnden Rechtslage – keinen Anspruch auf Vollständigkeit und Richtigkeit. Er kann und will auch keine rechtliche Beratung für den Einzelfall ersetzen. Im Zweifel sollte ein Rechtsanwalt / Rechtsanwältin konsultiert werden.



Vielen Dank für Ihre Aufmerksamkeit!

Seite 37
15.02.2018

Für die Beantwortung Ihrer Fragen stehe ich Ihnen gern zur Verfügung!



Dr. jur. Björn Schreier
Rechtsanwalt
Fachanwalt für Handels- und
Gesellschaftsrecht
Fachanwalt für Steuerrecht
dr-schreier@ksh-recht.de

KAPPUHNE · SCHREIER · HERBOTE
PARTNERSCHAFTSGESELLSCHAFT · RECHTSANWÄLTE

Am Münster 28
37154 Northeim
Telefon: 05551 / 97 60-0
Telefax: 05551 / 97 60-50

Düstere-Eichen-Weg 50
37073 Göttingen
Telefon: 0551 / 48 862-85
Telefax: 0551 / 48 862-86

www.ksh-recht.de

Diese Bilder dürfen nur im Zusammenhang mit diesem Vortrag benutzt werden. Copyright KAPPUHNE · SCHREIER · HERBOTE.
Der Inhalt dieser Präsentation ist urheberrechtlich geschützt und darf nicht vervielfältigt werden.