EU-DSGVO & BDSG-neu | START 25. Mai 2018!

Januar | 2018

Wichtige Datenschutzinformationen für Ihr Unternehmen

premiumstore

Inhaltsverzeichnis

v

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Thomas Müller

Liebe Leserin, lieber Leser,

mit der Verabschiedung der europäischen Datenschutz-Grundverordnung (EU-DSGVO), die europäische und nationale Regelungen zum Datenschutz einheitlich novelliert, wurde es notwendig auch das Bundesdatenschutzgesetz (BDSG) an die neuen Gegebenheiten der EU-DSGVO anzupassen.

Beschlossen wurde das *„Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680*“, mit dem das „alte“ Bundesdatenschutzgesetz mit den neuen Vorgaben in Einklang gebracht wurde.

Das Ergebnis trägt wieder den Namen „Bundesdatenschutzgesetz“ nur jetzt mit dem Zusatz „neu“ (kurz: BDSG-neu). Es wird das „alte“ Bundesdatenschutzgesetz (BDSG-alt) am 25. Mai 2018 ablösen!

Somit wird der 25. Mai 2018 zu einem sehr wichtigen Stichtag für alle Unternehmen in Deutschland und in Europa, da genau ab diesem Zeitpunkt nur noch und ausschließlich die neuen Datenschutz-Verordnungen und -Gesetze zur Geltung kommen.

Grund genug, die wichtigsten Informationen, des ab Mai gültigen Bundesdatenschutzgesetzes (BDSG-neu) in Verbindung mit der europäischen Datenschutz-Grundverordnung in den Fokus dieser Ausgabe zu stellen.

Sollten Sie darüber hinaus weitere Informationen benötigen oder eine ausführliche Beratung in Anspruch nehmen wollen, stehen wir Ihnen jederzeit sehr gerne zur Verfügung.

Sie erreichen uns unter der Telefonnummer +49 (5221) 99 33 2 77 oder per E-Mail an info@eu-dsgvo.nrw .

Mit besten Grüßen

Thomas Müller
Externer Datenschutzberater DSVGO

Ziele und allgemeine Informationen zu den neuen Vorgaben

Ziel der Neuerungen ist es, ein einheitliches Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten in allen europäischen Mitgliedstaaten zu gewährleisten - Ein Gesetz, welches für alle gültig ist!

Alles in allem erst einmal eine gute Idee - einheitliches Schutzniveau und gleiche Regeln für alle Staaten der europäischen Union. Nur so ganz einfach ist das dann doch nicht, weil jedes Mitgliedsland eigene nationale Interessen hat und auch diese in den neustrukturierten Datenschutzvorgaben ihren Platz haben müssen.

Die Lösung: ***Konkretisierungsklauseln*** (auch *Öffnungsklauseln* genannt)

Mit den diesen *Klauseln zur Konkretisierung* erhalten die Mitgliedstaaten die Möglichkeit, nationale Datenschutzregelungen mit einzubringen, die dann für das jeweilige Land gültig sind. Diese Regelungen können vielfältig sein und ermöglichen so sehr große Handlungsspielräume für die einzelnen nationalen Belange.

Wichtig hierbei ist nur, dass die Vorgaben der europäischen Datenschutzgrundverordnung immer vor den nationalen Interessen stehen und somit zwingend eingehalten werden müssen.

Genau hier kommt das Bundesdatenschutzgesetz ins Spiel, welches in 2017 durch das „*Gesetz zur Anpassung des Datenschutzrechts …*“ auf die EU-DSGVO angepasst wurde und ab jetzt ***Bundesdatenschutzgesetz neu (BDSG-neu)*** benannt wird.

Das BDSG-neu tritt am 25. Mai 2018 in Kraft und löst zeitgleich das BDSG-alt ab. Es regelt die nationalen Datenschutzvorgaben auf Basis der EU-DSGVO und ist für alle bindend, die in Deutschland personenbezogene Daten[1] verarbeiten!

[1] Personenbezogene Daten sind „*Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person*" (u.a. Name, Alter, Geburtsdatum, Anschrift, Telefonnummer, E-Mail, Bankdaten, Familienstand, Bildungsstand, Kenntnisse, Fähigkeiten, Erfahrungen, Lohn- und Gehaltsdaten, Urlaubsdaten, Krankentage, die Hautfarbe, uvm. … einer natürlichen Person).

Bestellung eines Datenschutzbeauftragten

Anders als in der europäischen Datenschutzgrundverordnung (EU-DSGVO) ist die Anzahl der Mitarbeiter, ab der ein betrieblicher oder externer Datenschutzbeauftragter bestellt werden muss, in Deutschland deutlich niedriger.

Laut BDSG-neu muss ein Datenschutzbeauftragter bestellt werden:

> *„… wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, wenn wegen eines hohen Risikos für die Rechte und Freiheiten der von der Datenverarbeitung Betroffenen eine Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO notwendig ist oder geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden (vgl. § 38 Abs. 1 BDSG-neu) …“.*

Kündigungsschutz eines Datenschutzbeauftragten

Auch beim erhöhten Kündigungsschutz des Datenschutzbeauftragten weicht das BDSG-neu deutlich von den Vorgaben der EU-DSGVO ab. Wo die europäische Verordnung keinen besonderen Schutz vorsieht, setzt das BDSG-neu ein deutliches Zeichen und schützt den Datenschutzbeauftragten vor unzulässiger Entlassung. Im Rahmen dieses sehr hohen Schutzniveaus können Kündigungen nur „aus wichtigem Grund" ausgesprochen werden. Dieser erhöhte Schutz wirkt sogar bei einer gültigen Abberufung vom Amt des Datenschutzbeauftragten nach. In diesem Fall gelten die Schutzmechanismen für weitere 12 Monate!

Schmerzensgeldanspruch für Verbraucher

Im BDSG-neu hinzugekommen ist der „Schmerzensgeldanspruch für Verbraucher“, der auch für Arbeitnehmer und Arbeitnehmerinnen Gültigkeit hat.

Im Gegensatz zur EU-DSGVO können, laut BDSG-neu, jetzt auch betroffene Personen eine Entschädigung verlangen, die keinen Vermögensschaden erlitten haben, was speziell für Unternehmen relevant werden könnte, da hier hohe finanzielle Risiken lauern!

Mehr Befugnisse für die Datenschutz-Aufsichtsbehörden

Mit den Neuregelungen durch die europäische Datenschutz-Grundverordnung (EU-DSGVO) und dem Bundesdatenschutzgesetz neu (BDSG-neu) kommen auf die Datenschutz-Aufsichtsbehörden deutlich mehr Aufgaben zu.

Hierfür wird die Personaldecke der einzelnen Behörden verstärkt und sie erhalten mehr Rechte und viel mehr Sanktionsmöglichkeiten. Es wurde auch schon davon gesprochen, dass *„… die Datenschutz-Aufsichtsbehörden durch die EU-DSGVO Zähne bekommen …*“, was zur Folge hat, dass die die Anzahl der aktiven Datenschutz-Kontrollen deutlich steigern wird!

Zudem werden die Bußgelder deutlich angepasst. Waren bislang Strafen von bis 300.000,00 EUR möglich, werden diese ab 25. Mai 2018 auf bis zu 20 Millionen angehoben und sollte das als Sanktion nicht ausreichend sein, könnten sogar bis zu 4% des weltweiten Konzernumsatzes geltend gemacht werden!

Neuerung bei der Beweislast

Mit Einführung der EU-DSGVO unterliegt jedes Unternehmen der sogenannten „Rechenschaftspflicht“, so dass ab jetzt nicht nur die Sicherstellung der Datenschutzvorgaben nachzuweisen sind, sondern auch proaktiv die Gewährleistung der Angemessenheit des Datenschutzniveaus. Durch diese Rechenschaftspflicht wird die bisherige Lastenverteilung umgedreht und Sie müssen nun aktiv nachweisen, dass Ihr Datenschutz funktioniert und das unabhängig davon, ob Schaden entstanden ist oder nicht. Genau das macht es für Aufsichtsbehörden zukünftig deutlich einfacher entsprechende Kontrollen durchzuführen.

Das Datenschutz-Managementsystems (DSMS)

Mit der Einführung der neuen Regelungen wird es unumgänglich, Prozesse umfangreich zu dokumentieren und eine Erfolgsmessung einzuführen. Nur so kann der Nachweis erfolgen, dass die Grundsätze der Datenverarbeitung nach EU-DSGVO eingehalten werden. Zudem ermöglicht ein solches System schnellere Reaktionszeiten, falls es einmal zu einer Datenschutzpanne kommen sollte.

Eine unzureichende Dokumentation kann sich hingegen sehr negativ auswirken, vor allem wenn es um die Festlegung eines möglichen Bußgeldes geht. Somit ist die Einführung eines Datenschutz-Managementsystems (DSMS) nach EU-DSGVO für jedes Unternehmen so gut wie unumgänglich!

Für mehr Informationen zum Thema DSMS können Sie unsere Datenschutzzeitung vom Oktober 2017 nutzen.

Die wichtigsten Schritte, die von jedem Unternehmen bis zum 25.05.2018 umgesetzt sein müssen

- ✓ Bestellung eines Datenschutzbeauftragten (DSB)
  Wenn die Vorgaben (Seite 5, oben) zur Bestellung eines Datenschutzbeauftragten erfüllt sind, muss zwingend und unverzüglich eine Bestellung eines betrieblichen oder externen DSB erfolgen.
- ✓ Erstellung eines „Verzeichnis zu Verarbeitungstätigkeit"
  Jedes Unternehmen muss ein Verzeichnis von Verarbeitungstätigkeiten erstellen, in dem unter anderem Verantwortlichkeiten und Zwecke der Verarbeitung von personenbezogenen Daten festgelegt werden.
- ✓ „Auftragsverarbeiter" – Es müssen Verträge geschlossen werden
  Arbeitet man mit externen Personen/Unternehmen, die Zugriff auf personenbezogene Daten erhalten (z.B. IT-Dienstleister, …), müssen entsprechende Verträge geschlossen werden. Die EU-DSGVO spricht hier vom *Auftragsverarbeiter* und vom *für die Verarbeitung Verantwortlichen*. Wie in der früheren Auftragsdatenverarbeitung ist auch jetzt eine vertragliche Regelung erforderlich, die allerdings nicht mehr schriftlich vorliegen muss. Die Vereinbarung wird auch in elektronischer Form von den Aufsichtsbehörden akzeptiert.
- ✓ Erstellung eines Verfahren zur Meldung von Datenschutzverstößen
  Legen Sie einen Prozess fest, so dass eine Schadensmeldung innerhalb von 72 Stunden nach Kenntnisnahme des Verstoßes gewährleistet ist.
- ✓ Erstellung einer Datenschutz-Folgenabschätzung (DSFA)
  Laut EU-DSGVO ist eine DSFA grundsätzlich immer dann durchzuführen wenn: *„… eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat …*".
- ✓ Überarbeitung und Anpassung aller vorhandenen Dokumente
  Alle Datenschutzerklärungen sollten überarbeitet werden, da unter anderem Meldepflichten teilweise deutlich verschärft wurden. Speziell allgemein verfügbare Erklärungen (z.B. über das Internet veröffentlichte Dokumente) sollten hierbei bevorzugt überarbeitet werden, da hier eine Abmahnwelle drohen könnte.

Die neuen Datenschutzvorgaben ziehen Auswirkungen nach sich, die nahezu alle Unternehmen in Europa betreffen. Somit ist es für alle Unternehmensführungen wichtig, Verfahren, mit denen personenbezogene Daten verarbeitet werden, auf einen möglichen Anpassungsbedarf überprüfen zu lassen.

Das Projekt zur Umsetzung (EU-DSGVO & BDSG-neu)

1. Der aktuelle Stand (Ist)

Um das aktuelle Datenschutzniveau festzustellen (Ist-Zustand), empfiehlt sich ein Audit, in dem alle relevanten Datenschutzprozesse analysiert werden. Dies betrifft u. a.

- ✓ Prozesse, in denen personenbezogene Daten verarbeitet werden
- ✓ Prüfung aktueller Rechtsgrundlagen (Zulässigkeit der Verarbeitung)
- ✓ Prüfung des Schutzniveaus
- ✓ Prüfung der aktuellen Verträge (Auftragsdatenverarbeitung)
- ✓ Prüfung aller Dokumentationen
- ✓ Prüfung individueller Betriebsvereinbarungen

2. Der zu erreichende Status (Soll)

Nachdem das aktuelle Datenschutzniveau festgestellt wurde, muss der Handlungsbedarf zur Erreichung der Rechtskonformität ermittelt werden: *Lückenanalyse*. Folgend die wichtigsten Punkte, die zu berücksichtigen sind:

- ✓ Wurden alle Rechtsgrundlagen eingehalten?
  Für die Verarbeitung von personenbezogener Daten ist eine Legitimationsgrundlage erforderlich. Folglich ist zu prüfen, ob für alle Prozesse eine Rechtsgrundlage besteht.

- ✓ Sind alle Betroffenenrechte berücksichtigt?
  Mit den neuen Datenschutzvorgaben werden die Rechte betroffener deutlich gestärkt. Hierzu gehören Informationspflichten, Auskunftsrechte, das Recht auf Berichtigung, das Recht auf Löschung, das neue Recht auf Datenübertragbarkeit und das Widerspruchsrecht. Wurden alle Vorgaben berücksichtigt?

- ✓ Wurden datenschutzfreundliche Voreinstellungen realisiert?
  Laut Art. 25 EU-DSGVO sind bei der Prozessgestaltung „datenschutzfreundliche Voreinstellungen“ umzusetzen (Data Protection by design und Data Protection by default). Wurden diese in alle Abläufe integrieret?

- ✓ Bestehen Datenschutzrelevante Dienstleistungsbeziehungen?
  Falls ja, müssen alle bestehenden Vereinbarungen mit Auftragsverarbeitern geprüft, bzw. noch nicht vorhandene Verträge geschlossen werden.

- ✓ Sind alle Dokumentationspflichten erfüllt?
  In der EU-DSGVO ist eine Rechenschaftspflicht verankert, mit der der Nachweis geführt werden muss, dass personenbezogene Daten rechtmäßig verarbeitet werden. Sind hier alle Dokumentationspflichten erfüllt?

- ✓ Die Datenschutz-Folgenabschätzung
  Im BDSG-alt gab es eine Vorabkontrolle. Diese wird durch die Datenschutz-Folgenabschätzung abgelöst, was eine umfangreiche Dokumentation nach sich zieht. Wurde eine die Datenschutz-Folgenabschätzung durchgeführt und wenn ja, wurde diese bestmöglich dokumentiert?

- ✓ Meldepflicht des Datenschutzbeauftragten an die Aufsichtsbehörde
  Nach Art. 37 Abs. 7 EU-DSGVO müssen unter anderem die Kontaktdaten des Datenschutzbeauftragten an die zuständige Aufsichtsbehörde gemeldet werden. Wurden die notwendigen Meldungen durchgeführt?

- ✓ Sicherheit der Verarbeitung
  Art. 32 DSGVO: *„… unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten …*“. Ist die Sicherheit der Verarbeitung sichergestellt?

- ✓ Optionale Prüfung durch eine akkreditierte Zertifizierungsstelle
  Um eine offizielle Bestätigung zu haben, dass alle Datenschutzvorgaben erfüllt wurden, besteht im Rahmen eines Zertifizierungsverfahrens die Möglichkeit, den Nachweis zu erbringen, dass die Datenverarbeitung im Einklang mit der EU-DSGVO und dem BDSG-neu erfolgt.

3. Umsetzung des Handlungsbedarfes bis zum 25. Mai 2018!

Bei der Umsetzung der neuen Vorgaben durch die neue europäische Datenschutz-Grundverordnung (EU-DSGVO) und des neuen Bundesdatenschutzgesetzes (BDSG-neu) sollten unter anderem folgende Punkte berücksichtigt werden:

- ✓ Anpassung der betroffenen Prozesse und Strukturen
- ✓ Festlegung der Rechtsgrundlagen und des Zwecks der Datenverarbeitung sowie der Dokumentation von Interessenabwägungen
- ✓ Implementierung von Informationspflichten, Betroffenenrechten und Löschkonzepten
- ✓ Anpassung der Datenschutzorganisation
- ✓ Bestellung eines Datenschutzbeauftragten
- ✓ Reaktionsmechanismen auf Datenpannen
- ✓ Organisation von Meldepflichten
- ✓ Anpassung der Dienstleistungsbeziehungen
- ✓ Aufbau der Dokumentation
- ✓ Anpassung der IT-Sicherheit
- ✓ Anpassung der Betriebsvereinbarungen

Quelle: Die Grundlage für diesen Maßnahmenkatalog bildet die Veröffentlichung *„Kurzpapier Nr. 8, Maßnahmenplan „DS-GVO“ für Unternehmen“* des Bayerisches Landesamt für Datenschutzaufsicht.

Die akkreditierte Datenschutzzertifizierung

Sind wir datenschutzkonform?

Viele verantwortliche Unternehmer und Unternehmerinnen stellen sich aktuell, auf Basis der vielen Veränderungen durch die EU-DSGVO und dem BDSG-neu, die Frage „… *sind wir durch unsere getroffenen Maßnahmen in Sachen Datenschutz jetzt zu 100% rechtssicher aufgestellt?*“.

Die Lösung: Eine offizielle Zertifizierung!

Mit den Artikeln 42 und 43 der EU-DSGVO legt der Gesetzgeber jetzt einen rechtlichen Grundstein für europäisch einheitliche Lösung: Ein Akkreditierungs- und Zertifizierungsverfahren, mit dem man die Einhaltung der Datenschutzvorgaben rechtssicher nachweisen kann.

Vorteile einer Zertifizierung

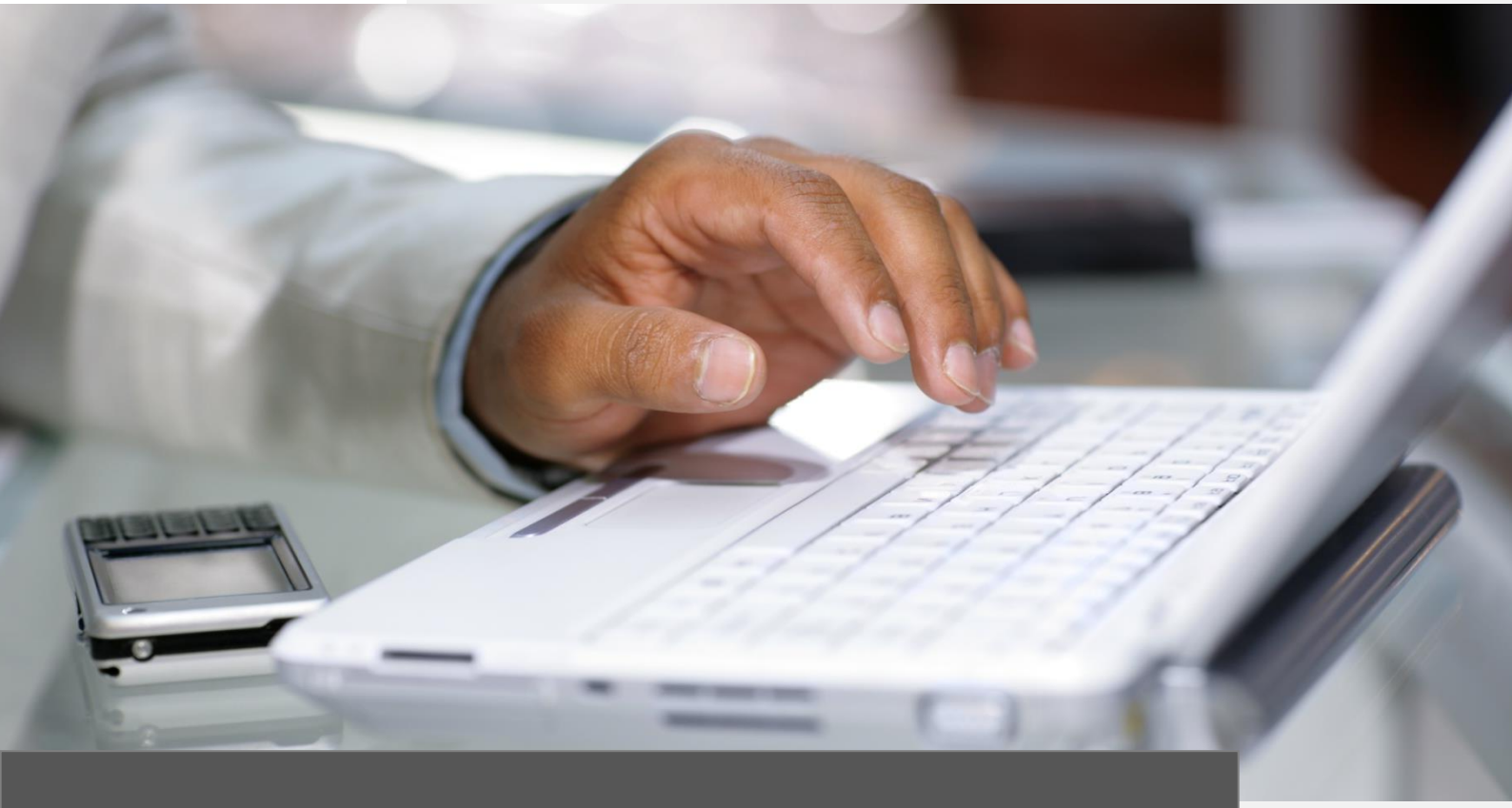
Die EU-DSGVO nennt explizit einige Anwendungsbereiche, bei denen eine Zertifizierung für den Nachweis der Einhaltung der Grundverordnung als Faktor mit herangezogen werden kann:

- ✓ Erfüllung der Pflichten des Verantwortlichen (Art. 24 Abs. 3)
- ✓ Erfüllung der Anforderungen an Technikgestaltung und datenschutzfreundliche Voreinstellungen des Art. 25 Abs. 1 und 2 (vgl. Abs. 3)
- ✓ Garantien des Auftragsverarbeiters nach Art. 28 (vgl. Abs. 5 und 6)
- ✓ Sicherheit der Verarbeitung (Art. 32 Abs. 3)
- ✓ Datenübermittlung an ein Drittland (Art. 46 Abs. 2 lit. f)
- ✓ Datenschutz-Folgeabschätzung (ErwGr. 90)

Daneben kann ein Zertifikat auch für Marketingzwecke genutzt werden, um sowohl Geschäftskunden, Verbrauchern als auch Bürgern gegenüber die Beachtung des Datenschutzrechts darzustellen.

Wichtig! Eine genehmigte Zertifizierung ist immer nur eine Momentaufnahme. Sie ist von Vorteil und erleichtert die Prüfung durch die Aufsichtsbehörden. Allerdings befreit sie nicht von der Verantwortung für die Einhaltung der Datenschutzverordnungen und –gesetze! Ebenso bleiben die Aufgaben und Befugnisse der zuständigen Aufsichtsbehörden von einer Zertifizierung unberührt.

Januar | 2018



Impressum

premiumstore, Inhaber Thomas Müller e.K.
Salzufler Str. 179a
32052 Herford

Tel.: +49 (5221) 9933277
Fax: +49 (5221) 689851
Web: www.eu-dsgvo.nrw
E-Mail: info@eu-dsgvo.nrw

Amtsgericht Bad Oeynhausen, HRA 3793
Ust-IdNr.: DE201550075

Redaktion:
Thomas Müller

Bildnachweise:
Diese Datenschutzbroschüre wurde in unserem Auftrag von der Firma ITKservice GmbH & Co. KG, Fuchsstädter Weg 2, 97491 Aidhausen erstellt. Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei der Firma ccvision.de gekauft und lizensiert.