Gesetzeskonforme Durchführung von Auftragsdatenverarbeitung

März | 2014

Wichtige Datenschutzinformationen für Ihr Unternehmen

ebb

Inhalte | Datenschutzinformationen | März 2014

Inhaltsverzeichnis

Begrüßung | Ihr Datenschutzbeauftragter vor Ort

Enver Bastanoglu

Liebe Leserin, lieber Leser,

die gesetzlichen Vorgaben bei der Verarbeitung von personenbezogenen Daten im Auftrag sind alles andere als neu. Der § 11 des Bundesdatenschutzgesetzes wurde mit der Novelle II vom 14.08.2009 neu gefasst und trat bereits zum 01.09.2009 in Kraft. Die Vorgaben des § 11 galten sodann für alle neuen Verträge, Altverträge mussten angepasst werden. Somit dürfte es zum jetzigen Zeitpunkt keine Verhältnisse über Auftragsdatenverarbeitung mehr geben, die nicht den aktuellen Anforderungen des Gesetzes genügen.

Dennoch stellen wir im Alltag regelmäßig fest, dass es immer noch in vielen Unternehmen deutliche Abweichungen zwischen den Vorschriften des § 11 und der tatsächlichen Umsetzung gibt.

Dabei ist es leider nicht nur so, dass die Verträge oft nicht die „zehn wichtigen Punkte“ beinhalten. Sehr häufig werden die Auftragnehmer gar nicht oder nur unzureichend geprüft, und dann auch meist erst nach Beginn der Verarbeitung und nur einmalig. Von regelmäßigen Kontrollen kann ebenso wenig die Rede sein wie von einer aussagekräftigen Dokumentation einzelner Prüfungen oder gar der gesamten Beauftragung.

Bedingt durch diesen Umstand ist in Zukunft vermutlich mit einer erhöhten Kontrolle der Verhältnisse über Auftragsdatenverarbeitung durch die Landesdatenschutzbehörden zu rechnen. Wie nachteilig sich eine unzureichende Dokumentation des gesamten Auftragsverhältnisses bei einer Prüfung auswirken kann, ist mit Blick auf die Bußgeldvorschriften in § 43 (oder auf Seite 10) leicht festzustellen.

Falls Sie über diese Informationen hinaus eine ausführliche Beratung nutzen möchten, stehen wir Ihnen jederzeit sehr gerne zur Verfügung. Sie erreichen uns unter der Telefonnummer (08138) 6975251 oder per E-Mail enver@bastanoglu.de. Weiterführende Informationen zum Thema Datenschutz finden Sie auch auf meiner Internetseite www.bastanoglu.de

Mit besten Grüßen

Enver Bastanoglu
(nach DIN ISO EN 17024 zertifizierter Datenschutzbeauftragter)

Auftragsdatenverarbeitung | Was verbirgt sich dahinter?

Die Grundlage

Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten im Auftrag ist in § 11 BDSG klar geregelt. Demnach liegt eine Auftragsdaten-verarbeitung (kurz: ADV) immer dann vor, wenn personenbezogene Daten **weisungsabhängig** durch externe Stellen **im Auftrag** erhoben, verarbeitet oder genutzt werden. Klassische Beispiele für Auftragsdatenverarbeitung sind z.B. externe Auftragnehmer, die Lohn- und Gehaltsabrechnungen durchführen oder Lettershop-Dienstleister, die Werbemailings erstellen und versenden. Aber auch IT-Dienstleister gehören zur Gruppe der Auftragnehmer, wenn im Rahmen der Aufgabenstellung ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Weitere Beispiele für eine Auftragsdatenverarbeitung

- ✓ Nutzung von Rechenzentrumsdienstleistungen, wie z.B. gehostete E-Mail Server oder cloud-basierte Verarbeitung von personenbezogenen Daten,
- ✓ Einsatz eines Call Centers für z. B. Kontaktdatenerhebung oder Zufriedenheitsabfragen,
- ✓ Papier- und Altaktenentsorgung oder Datenträgervernichtung,
- ✓ Einsatz von Personalberatern zur Rekrutierung von Mitarbeitern,
- ✓ Versand eines Newsletters durch eine Marketingagentur,
- ✓ ausgelagerte Speicherung von Datensicherungen oder Archivierungen.

Verantwortung und Haftung können nicht abgegeben werden

Bei einer Datenverarbeitung im Auftrag ist der Auftraggeber für die Einhaltung der Vorschriften und Gesetze verantwortlich, der Auftragnehmer wird hierbei als Teil der verantwortlichen Stelle angesehen. Der Auftraggeber bleibt somit Herr der Daten und haftet für Schäden, die den Betroffenen durch die Datenverarbeitung beim Auftragnehmer entstehen können. Auch die Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung und Sperrung bleiben unberührt und richten sich einzig und allein an den Auftraggeber.

Umso wichtiger ist es, bei der Auswahl der Auftragnehmer sorgfältig vorzugehen und diese vor Auftragsvergabe auf die Einhaltung gesetzlicher Pflichten zu prüfen.

Keine Auftragsdatenverarbeitung

Werden Tätigkeiten durch externe Stellen in Anspruch genommen, die nicht die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten zum Gegenstand haben, liegt keine Auftragsdatenverarbeitung vor.

Selbst dann nicht, wenn ein Kontakt mit personenbezogenen Daten bei der Auftragserfüllung unvermeidlich ist oder zumindest nicht ausgeschlossen werden kann. Es muss allerdings klar erkennbar sein, dass der Umgang mit personenbezogenen Daten nicht Kernaufgabe der Leistungserbringung ist.

Nicht unter Auftragsdatenverarbeitung fallen somit in der Regel Dienstleistungen wie Gebäudereinigungen, Objektbewachungsdienste sowie Einsätze von Handwerksunternehmen.

Aber auch Transportleistungen von Post-, Kurier- und Speditionsdiensten sind nicht als Auftragsdatenverarbeitung zu bewerten, ebenso wenig Bank- oder Telekommunikationsdienstleistungen.

Geheimhaltung ist trotzdem notwendig

Obschon man in solchen Fällen auf ein Vertragswerk gemäß § 11 BDSG verzichten kann, ist es dennoch notwendig, die externen Personen schriftlich auf Geheimhaltung zu verpflichten. Solche Vereinbarungen sollten sich inhaltlich an die Verpflichtung auf das Datengeheimnis nach § 5 BDSG anlehnen und können separat abgeschlossen oder auch in den bestehenden Dienstleistungsvertrag integriert werden.

Der Abschluss einer Geheimhaltungsvereinbarung ist dann entbehrlich, wenn der externe Dienstleister bereits einer gesetzlichen Pflicht zur Geheimhaltung unterliegt, wie z.B. dem Post- und Bankgeheimnis oder dem Telekommunikations- bzw. Fernmeldegeheimnis.

Manchmal kann es aber je nach Zweck der Verarbeitung dennoch notwendig oder sinnvoll sein, die vertragliche Regelung mit dem Auftragnehmer inhaltlich an den Vorgaben des § 11 BDSG zu orientieren.

Funktionsübertragung | Abgrenzung zur Auftragsdatenverarbeitung

Funktionsübertragung

Nicht jede Verarbeitung von personenbezogenen Daten durch externe Stellen ist auch automatisch als Auftragsdatenverarbeitung einzustufen. Denn sobald das beauftragte Unternehmen im Rahmen des Auftrags **eigenverantwortlich** Funktionen ausübt oder **selbsttätig** Entscheidungen trifft, ist dies als Funktionsübertragung einzustufen. Die Weisungsbindung des Auftraggebers entfällt hierbei, der Auftrag geht in der Regel weit über Hilfstätigkeiten hinaus. Der Auftragnehmer hat somit als Daten verarbeitende Stelle die Verantwortung zu tragen und die Zulässigkeit und Richtigkeit der Datenverarbeitung sicherzustellen.

Wesentliche Merkmale einer Funktionsübertragung

- ✓ Übernahme der Verantwortung für die Zulässigkeit und Richtigkeit der Datenverarbeitung,
- ✓ fehlender Einfluss des Auftraggebers auf Teile der Erhebung, Verarbeitung oder Nutzung der Daten,
- ✓ die Daten verarbeitende Stelle erhält Nutzungsrechte an den Daten,
- ✓ keine gesetzliche Privilegierung für die Weitergabe und Verarbeitung von personenbezogenen Daten durch einen externen Dienstleister.

Beispiele für eine Funktionsübertragung

Es gibt nicht wenige Dienstleistungen, die aufgrund der jeweiligen Aufgabenstellung mit eigenverantwortlicher Wahrnehmung und der fehlenden Weisungsabhängigkeit durch den Auftraggeber keine Auftragsdatenverarbeitung darstellen, z.B. externe Dienstleister für folgende Aufgaben/ Bereiche:

- ✓ Unternehmensberatung und Wirtschaftsprüfung,
- ✓ Personalverwaltung, Mitarbeiterrekrutierung,
- ✓ Finanz- und Steuerberatung,
- ✓ Vertragskundenbetreuung,
- ✓ Inkassomanagement mit Forderungsübertragung.

Wie geht man nun korrekt vor?

Die richtige Vorgehensweise bei der Durchführung von Auftragsdatenverarbeitung wird durch das Bundesdatenschutzgesetz vorgegeben. Hier heißt es in § 11 Absatz 2 Satz 1 und 2 BDSG: ***Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen…***

Weiterhin finden wir in § 11 Absatz 2 Satz 4 und 5 BDSG folgende Aussagen: ***Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.***

Somit ergibt sich also folgender chronologischer Ablauf zur Umsetzung der gesetzlichen Vorgaben:

1. Auswahl des Auftragnehmers und Begutachtung der von ihm getroffenen technischen und organisatorischen Maßnahmen.

2. Abschluss eines Vertrages mit dem Auftragnehmer gemäß § 11 BDSG. Der Vertragsabschluss muss noch **vor** Beginn der Verarbeitung erfolgen.

3. Prüfung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen und Dokumentation der Prüfung. Beides muss ebenfalls **vor** Beginn der Verarbeitung durchgeführt werden.

4. Zukünftig ist eine regelmäßige Prüfung des Auftragnehmers auf Einhaltung der vertraglich vereinbarten technischen und organisatorischen Maßnahmen erforderlich. Das Ergebnis der Prüfung muss ebenfalls dokumentiert werden.

Die vertragliche Verpflichtung und Prüfung des Auftragnehmers müssen in jedem Fall vor Beginn der Verarbeitung erledigt sein!

Details zu den inhaltlichen Vorgaben eines solchen Vertrages sowie zur Durchführung von Prüfungen und Kontrollen des Auftragnehmers finden Sie auf den nachfolgenden Seiten.

Vertrag nach § 11 BDSG | Was muss geregelt werden?

Der Gesetzgeber schreibt den Regelungsumfang eines Vertrages über Auftragsdatenverarbeitung in § 11 Absatz 2 Satz 2 Nrn. 1 bis 10 BDSG genau vor. Demnach sind folgende Punkte mit dem Auftragnehmer zu regeln:

1. ***Gegenstand und Dauer des Auftrags***
   1) Welche Leistung ist Gegenstand des Auftrags?
      - ✓ Gehaltsabrechnung, Werbemailing, Papierentsorgung etc.

   2) Wie lange soll der Auftrag ausgeführt werden? Einmalig, dauerhaft?
      - ✓ Befristet bis…, läuft auf unbestimmte Zeit und ist kündbar zum…

2. ***Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen***
   1) Welche Leistungen sind im Detail zu erbringen? Dauer der Speicherung der Daten? Welche Besonderheiten sind zu beachten?
   2) Personaldaten, Kundendaten, Protokollierungsdaten etc.
   3) Mitarbeiter, Kunden, Interessenten, Lieferanten, Messekontakte etc.

3. ***Nach § 9 zu treffende technische und organisatorische Maßnahmen***
   Hier wird Bezug auf die Anlage zu § 9 Satz 1 BDSG genommen, erforderlich ist jedoch die Nennung konkreter Maßnahmen, die den Auftrag betreffen, zum Beispiel:
   - ✓ Art der Übermittlung und Sicherheit bei der Übertragung der Daten,
   - ✓ Art der Speicherung (Trennungsgebot) der Daten,
   - ✓ Sicherung/Backup der Daten beim Auftragnehmer sowie Vereinbarungen zur sicheren Löschung/Vernichtung,
   - ✓ Maßnahmen zur Ausfallsicherheit der Systeme des Auftragnehmers.

4. ***Die Berichtigung, Löschung und Sperrung der Daten***
   Es muss festgelegt werden, wann und wie Daten gesperrt oder gelöscht werden sollen. Ferner hat der Auftragnehmer eine Mitwirkungspflicht zur Bearbeitung von Anfragen Betroffener bei der Ausübung ihrer Rechte auf Auskunft, Berichtigung, Sperrung oder Löschung.

5. ***Nach Absatz 4 bestehende Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen***

   Folgende Pflichten ergeben sich für den Auftragnehmer aus dem § 11 Absatz 4 BDSG:

   - ✓ Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 5)
   - ✓ Umsetzung geeigneter Maßnahmen zur Datensicherheit (§ 9)
   - ✓ Bestellung eines Datenschutzbeauftragten, wenn zutreffend (§§ 4f, 4g)

   Weiterhin muss der Auftragnehmer durch eigene Kontrollen die ordnungsgemäße Verarbeitung sicherstellen und die getroffenen technischen und organisatorischen Maßnahmen überprüfen. Die Kontrollen müssen nachweisbar sein und können auf vielfältige Weise durchgeführt werden, z.B. durch die interne Revision, den eigenen Datenschutzbeauftragten oder externe Audits.

   Werden Subunternehmer eingesetzt, erstreckt sich die Pflicht zur Kontrolle auch auf diese.

6. ***Etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen***

   Es sollten Festlegungen hinsichtlich des Einsatzes von Subunternehmern getroffen werden. Ist die Vergabe an Unterauftragnehmer notwendig oder gewünscht, sollte in jedem Fall geregelt werden, unter welchen Voraussetzungen dies geschehen soll, z.B.:

   - ✓ Nur nach vorheriger Genehmigung des Auftraggebers,
   - ✓ nur Subunternehmer aus dem Inland und/oder EU bzw. EWR,
   - ✓ Subunternehmer übernimmt nur Teile der Verarbeitung,
   - ✓ Auftragnehmer muss mit Subunternehmer gleichartigen Vertrag gemäß § 11 schließen.

7. ***Kontrollrechte des Auftraggebers und Duldungs- und Mitwirkungspflichten des Auftragnehmers***

   Der Auftraggeber muss sich dem Sachverhalt angemessene Kontrollrechte beim Auftragnehmer vertraglich einräumen, da er ja verpflichtet ist, sich regelmäßig von der Einhaltung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.
   Gleichzeitig muss der Auftragnehmer die vereinbarten Kontrollen nicht nur dulden, sondern hat an deren Durchführung auch mitzuwirken.

8. ***Mitzuteilende Verstöße des Auftragnehmers gegen Vorschriften zum Datenschutz oder gegen die im Auftrag getroffenen Festlegungen***
   Der Auftragnehmer muss verpflichtet werden, alle Verstöße, die bei der Verarbeitung der im Auftrag definierten Daten des Auftraggebers vorfallen, innerhalb einer definierten Frist zu melden. Handelt es sich um Daten, die der Informationspflicht des Auftraggebers nach §42a unterliegen, sollte der Auftragnehmer darauf gesondert hingewiesen werden.

9. ***Umfang der Weisungsbefugnisse des Auftraggebers***
   Die Weisungsbefugnisse ergeben sich in der Regel bereits aus dem Auftrag selbst. Es empfiehlt sich aber immer eine namentliche Nennung der Weisung gebenden und Weisung empfangenden Mitarbeiter. Sind darüber hinaus weitere Weisungsbefugnisse notwendig, sollten diese schriftlich fixiert werden.

10. ***Rückgabe überlassener Datenträger und Löschung der Daten beim Auftragnehmer***
    Dieser Punkt ist besonders wichtig und wird oft vernachlässigt. Es ist genau zu regeln, wie die Daten und/oder Datenträger zu löschen bzw. zurückzugeben sind. Bei der Löschung von Daten, die auf den Systemen des Auftragnehmers gespeichert sind, sind auch die Datensicherungen und eventuelle Archivierungen des Auftragnehmers zu berücksichtigen.

Mögliche Bußgelder nach § 43 BDSG

Wer einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt, handelt ordnungswidrig und ist dem Risiko eines Bußgeldes bis zu 50.000,00 Euro ausgesetzt.

Wer ist zuständig und verantwortet die Prüfung?

Zuständig ist zunächst immer die verantwortliche Stelle. Deren Leiter wird diese Aufgaben in der Regel ganz oder teilweise an Personen übertragen, die unmittelbar mit dem Auftrag beschäftigt sind oder über die nötige Sicherheit in der Anwendung des § 11 verfügen, z.B. entsprechende Fachabteilungen oder der Datenschutzbeauftragte selbst. Aber auch externe Dienstleister können eingesetzt werden, sofern diese über die nötige Fachkompetenz verfügen.

Müssen Kontrollen vor Ort durchgeführt werden?

Zur Umsetzung der vom Gesetzgeber geforderten Kontrollen, die erstmalig vor Beginn der Verarbeitung und sodann regelmäßig vorgenommen werden müssen, stehen dem Auftraggeber mehrere Möglichkeiten zur Verfügung. Die Durchführung von Vor-Ort-Kontrollen ist nicht als ausdrückliche Pflicht im Gesetz verankert. Es können auch andere geeignete Maßnahmen angewendet werden:

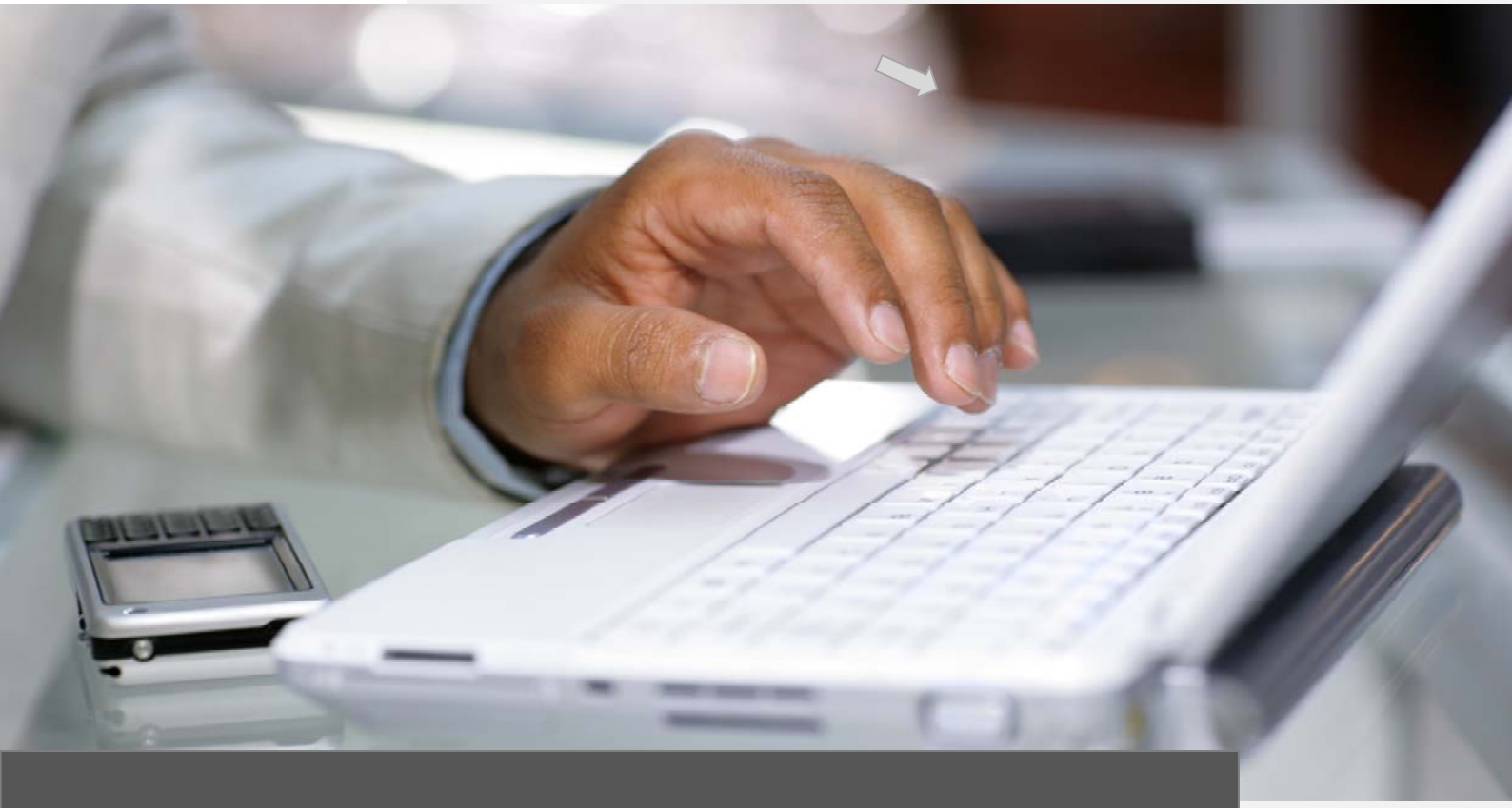
- ✓ Beantwortung eines Fragebogens des Auftraggebers
- ✓ Internes Datenschutzkonzept des Auftragnehmers
- ✓ Interne Prüfberichte des Datenschutzbeauftragten des Auftragnehmers
- ✓ Zertifizierung / Datenschutz-Audit durch externe Stellen
- ✓ Nachweis der Zertifizierung einer ISO 27001 (nach BSI Grundschutz)

Wichtig ist aber in jedem Falle, die Kontrollen und die Begründung für die getroffene Bewertung entsprechend zu dokumentieren.

Festlegung der Regelmäßigkeit von Kontrollen

In laufenden Auftragsverhältnissen muss der Auftraggeber regelmäßig prüfen, ob der Auftragnehmer die getroffenen Maßnahmen auch tatsächlich einhält. Im Gesetz finden sich richtigerweise keine definierten Vorgaben oder Fristen, denn die Vielfalt an möglichen Verarbeitungen von personenbezogenen Daten im Auftrag ist nahezu unbegrenzt. Hier muss der Prüfungsrhythmus je nach Sachlage individuell und unter Berücksichtigung der Art und Weise der zu verarbeitenden Daten bestimmt werden. Als Richtwert werden häufig Fristen zwischen ein bis drei Jahren genannt. Generell gilt aber, dass der Prüfungsturnus mit steigender Sensibilität der Daten im Zweifel eher kürzer zu wählen ist.

März | 2014



Impressum

Enver Bastanoglu

Kastanienweg 1a

85253 Erdweg

Telefon: 08138 6975251
Telefax: 08138 6975259

www: bastanoglu.de
E-Mail: enver@bastanoglu.de

Sitz der Gesellschaft: Erdweg Ust-Id: DE 218 553 335
Vertreten durch: Enver Bastanoglu

Redaktion:
Enver Bastanoglu

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.

ebb