DDV
Die treibende Kraft der Data Driven Economy

2022/2023

URKUNDE

QUALITÄTSSIEGEL

Kompetenz-Center DirectMail Services

Für vorbildliche Qualität und Leistungen wird der Firma

Nuntius Marketing Logistik GmbH & Co. KG,
Korntal-Münchingen

das folgende *Qualitätssiegel* des
Deutschen Dialogmarketing Verbandes e.V. (DDV) erteilt:

Lettershop

QuLS
Qualitäts- und Leistungssiegel
DDV Deutscher Dialogmarketing Verband

Lettershop

Gültig bis 31. Dezember 2023

Das Prüf- und Zertifizierungsverfahren des Kompetenz-Centers hat ergeben, dass das Unternehmen die an die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) angepassten Qualitäts- und Leistungsstandards des Kompetenz-Centers erfüllt und die Gewähr für eine besonders gute, verbraucher- und auftraggebergerechte Arbeit bietet.

Auszüge aus dem Inhalt der Prüfung:

- Mitarbeiterschulungen, u. a. zu den relevanten Gesetzen
- Einhaltung des gesetzlich vorgeschriebenen Datenschutzes und der selbst auferlegten Datenschutzvorgaben
- Beachtung der Hinweispflichten (DS-GVO, Robinsonliste, Werbewidersprüche, etc.) gegenüber Adresseigentümern und Kunden
- Nennung der vorgeschriebenen Angaben bei Angeboten, Aufträgen und Auftragsbestätigungen
- Erfüllung der vorgeschriebenen Pflichten zur Steuerung von IT-Verarbeitungen
- Durchführung einer transparenten, zeitnahen Rechnungsstellung
- Beachtung des fairen Wettbewerbs

Frankfurt, im Oktober 2022

Paul Nachtsheim
Geschäftsführer DDV

RA Frederick Richter
Vorstand Stiftung Datenschutz
Vorsitzender der unabhängigen
Siegel-Kontrollkommission

Deutscher Dialogmarketing Verband e.V. DDV

Ehrenkodex des Councils DirectMail Services

Die im DDV, Deutscher Dialogmarketing Verband e.V., Wiesbaden, zusammengeschlossenen Firmen geben sich nachfolgenden Ehrenkodex:

Präambel

Die Mitglieder des Councils schaffen sich mit diesem Ehrenkodex einen Ordnungsrahmen für die Leistungen der Adressenmittler, Rechenzentren, Lettershops, Fulfillmentunternehmen und Druckereien.

Sie verpflichten sich, die jeweils geltenden gesetzlichen Vorschriften - insbesondere den Datenschutz, den Verbraucherschutz und die Wettbewerbsregeln - zu beachten.

Sie befolgen die Empfehlungen des Deutschen Industrie- und Handelstages sowie des DDV, Deutscher Dialogmarketing Verband.

Sie übernehmen nur Aufträge, für deren Bearbeitung die erforderlichen Fähigkeiten, Erfahrungen, Mitarbeiter und technischen Einrichtungen bereitgestellt werden können. Sie geben realistische Leistungs-, Termin- und Kostenangebote ab und halten diese ein. Sie unternehmen alle Anstrengungen, ihre Kenntnisse, ihre Fähigkeiten und die Qualität ihrer Leistungen ständig zu verbessern.

1. Datenschutz

Sie verpflichten sich und ihre Mitarbeiter auf die Einhaltung der gesetzlichen Datenschutzbestimmungen und verarbeiten Daten nur im jeweils gesetzlich zulässigen Rahmen.

Soweit gesetzlich erforderlich sind die Mitglieder bei den zuständigen Aufsichtsbehörden gemeldet und haben einen betrieblichen Datenschutzbeauftragten bestellt.

Sie weisen ihre Auftraggeber (Werbetreibende) auf die Informationspflichten nach § 28 Abs. 4 Bundesdatenschutzgesetz hin.

Darüber hinaus haben die Verarbeitungsunternehmen die DDV-Verpflichtungserklärung „Auftragsdatenverarbeitung und Datenumgang" mit weitreichenden Garantien in jeweils aktueller Fassung unterzeichnet und beim DDV hinterlegt.

2. Verbraucherschutz

Im Interesse der Verbraucher und der Direktmarketing-Anwender unterstützen die Mitglieder aktiv die Robinson-Datei.

Sie empfehlen ihren Kunden immer, soweit technisch möglich und wirtschaftlich vertretbar, den Abgleich gegen die Robinson-Datei.

Sie verpflichten sich darüber hinaus, alle Wünsche Betroffener nach Auskunft, Berichtigung, Löschung oder Sperrung von Daten schnellstens, zuvorkommend und ausführlich zu bearbeiten.

3. Qualitäts- und Leistungsstandards

Sie garantieren die Einhaltung der für die einzelnen Tätigkeitsbereiche detailliert festgelegten DDV- Qualitäts- und Leistungsstandards.

4. Vertraulichkeit

Sie behandeln alle internen Vorgänge und Informationen von Auftraggebern, die ihnen durch ihre Tätigkeit bekannt werden, streng vertraulich.

Sie geben Auftraggeber schriftlich als Referenzen nur an, wenn sie deren Zustimmung vorher eingeholt haben.

5. Sorgfaltspflicht

Sie verpflichten sich, bei der Erfüllung aller Leistungen ein Höchstmaß an Sorgfalt und Zuverlässigkeit zu erbringen.

6. Einmalige Nutzung

Sie verpflichten sich zur klaren Regelung, dass Adressen grundsätzlich nur für die einmalige Verwendung zur Nutzung überlassen werden.

Eine hiervon abweichende Nutzung ist schriftlich zu vereinbaren.

Für eine vertragswidrige Nutzung von Adressen eines Adressenverlages ist die Vertragsstrafe zu regeln.

b.w.

7. Porto für Werbesendungen

Porto-Beträge sind durchlaufende Posten und daher separat von den Leistungspreisen anzugeben bzw. abzurechnen.

Sofern quittierte Abrechnungen von der Post zur Verfügung gestellt werden, sind diese Belege den Rechnungen beizufügen.

Porto-Beträge sind jeweils vom Kunden im voraus anzufordern oder soweit möglich, direkt an die Post zu bezahlen.

Eine Kreditierung bzw. Stundung widerspricht dem Handelsbrauch der Branche.

8. Seriöse Werbung

Sie verpflichten sich zu seriösem Verhalten bei der eigenen Werbung und bei der Akquisition.

9. Kontrolle

Über die gesetzlich geregelte Überwachung durch die Aufsichtsbehörden hinaus unterwerfen sich die Mitglieder einer Überprüfung der Qualitäts- und Leistungsstandards durch eine unabhängige Kontrollinstanz.

10. Ahndung von Verstößen

Bekannt werdende Verstöße gegen die Grundsätze dieses Ehrenkodex werden von dem Kontrollorgan des Councils untersucht und geahndet. Das Kontrollorgan kann den Ausschluss aus dem Council beschließen sowie beim Präsidium und Vorstand des DDV den Ausschluss eines Mitglieds aus dem Verband schriftlich beantragen.

Wiesbaden, 28. März 2012

MUNTER LOGISTIK E. K. 70825 Korntal-Münchingen

Firmenstempel, Unterschrift

13/8/2012

Ort, Datum

Den Ehrenkodex bitte unterschrieben an den DDV zurücksenden:

Deutscher Dialogmarketing Verband e.V.
Hasengartenstraße 14
65189 Wiesbaden
Telefon: 0611/97793-0
Telefax: 0611/97793-99

Deutscher Dialogmarketing Verband e.V.

Regeln zur Auftragsverarbeitung

(DDV-Verpflichtungserklärung)

Dienstleister **Nuntius Marketing Logistik e.K.**

(**nachfolgend Dienstleister**)

Vertreter **Dietmar Müller**

Straße Hausnr. **Kornwestheimer Straße 228**

PLZ, Ort **70825 Korntal-Münchingen**

E-Mail-Adresse **d.mueller@nuntius.net**

Website **www.nuntius.net**

Diese DDV-Regeln zur Auftragsverarbeitung enthalten Mindestanforderungen zur Auftragsverarbeitung und Pflichten zum Datenumgang. Sie gelten für **Dienstleister** (im Folgenden auch **Auftragnehmer** genannt), die für Adresseigner (im Folgenden auch **Auftraggeber** genannt) im Auftrag personenbezogene Daten gemäß Datenschutz-Grundverordnung (im Folgenden **DSGVO**) verarbeiten. Der Adresseigner hat mit dem Dienstleister im Rahmen der Vereinbarung jedes Datenverarbeitungsauftrags eine nachweisbare Vereinbarung über eine Auftragsverarbeitung zu schließen.

Durch Zeichnung und Einreichung dieser „DDV-Regeln zur Auftragsverarbeitung“ erklärt der Dienstleister verbindlich, für jeden Auftrag zur Auftragsverarbeitung die nachfolgenden Regeln und damit die gesetzlichen Vertragspflichten der Auftragsverarbeitung einzuhalten. Zusammen mit dem gesonderten Adressauftrag, der ausdrücklich diese „DDV-Regeln zur Auftragsverarbeitung“ einbeziehen muss, erfüllt der Dienstleister die gesetzlichen Anforderungen an eine Auftragsverarbeitung. Der gesonderte Adressauftrag in Kombination mit den einbezogenen „DDV-Regeln zur Auftragsverarbeitung“ ermöglicht eine datenschutzkonforme Auftragsverarbeitung.

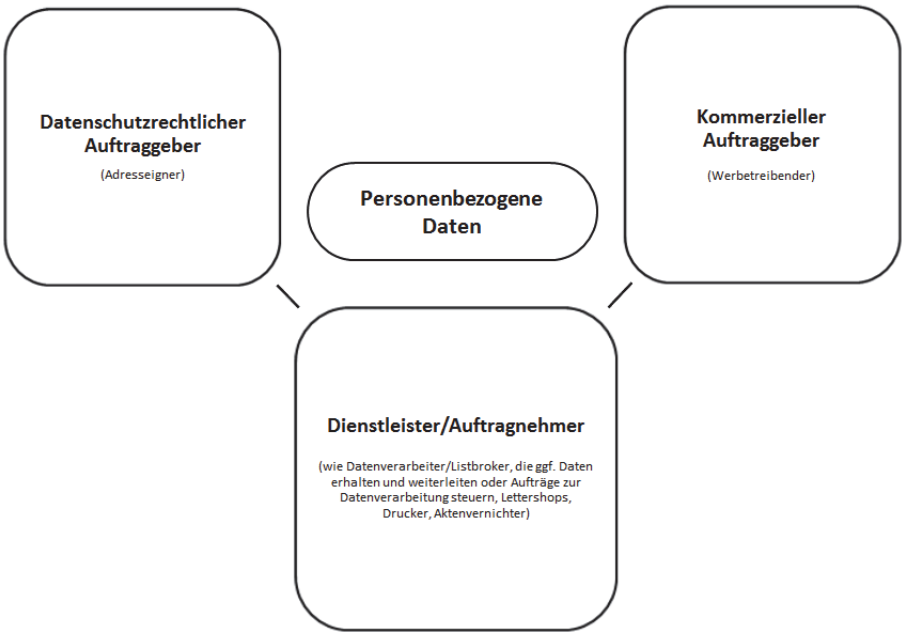
Für solche Unternehmen, die nur Teilbereiche der gesetzlichen Auftragsverarbeitung abdecken (beispielsweise Listbroker, die keine eigene Datenverarbeitung durchführen, aber Daten erhalten und weiterleiten oder Aufträge zur Datenverarbeitung steuern, oder Lettershops, die lediglich bereits adressiertes Material verarbeiten), gelten die „DDV-Regeln zur Auftragsverarbeitung“ nur soweit die betreffenden Unternehmen die vereinbarten Leistungen erbringen und dabei Adressdaten verarbeiten.

Vorbemerkung

Diese DDV-Regeln zur Auftragsverarbeitung (DDV-Verpflichtungserklärung) gelten für Dienstleistungen, bei denen der Dienstleister die Daten von natürlichen Personen (betroffene Personen nach Art. 4 Nr. 1 EU-Datenschutz-Grundverordnung, **DSGVO**; *insbesondere Kunden, Interessenten, Ansprechpartner von juristischen Personen, sonstige personenbezogene Daten*) für Auftraggeber verarbeitet und zwar unabhängig davon, ob die Datenverarbeitung und damit der Zugriff des Dienstleisters auf die Daten der betroffenen Personen Kernaufgabe des Auftragnehmers ist oder sonst als Auftragsverarbeitung nach Art. 28 DSGVO einzuordnen ist.

Die hier abgebildete Dienstleistung ist typischerweise eine des Dialogmarketings (*doch auch andere Dienstleistungen mit Bezug auf personenbezogene Daten können mit den Bedingungen dieser DDV-Regeln zur Auftragsverarbeitung datenschutzkonform erbracht werden*).

Bei Leistungen im Dialogmarketing sind datenschutzrechtlich in der Regel drei bzw. vier Beteiligte erfasst: Der **Werbetreibende**, der **Adresseigner**, der **Dienstleister** und der **potentielle Kunde**, der eine Werbemaßnahme empfängt. Der Werbetreibende stößt praktisch die Auftragsverarbeitung an, indem er das Ziel verfolgt, Kunden oder Neukunden (in Sinne dieser DDV-Regeln zur Auftragsverarbeitung „betroffene Personen“) werblich anzusprechen. Die werbliche Ansprache stellt eine Verarbeitung personenbezogener Daten (Name, Adresse und ggf. weitere Daten) des Adresseigners dar. Der Werbetreibende erhält die Nutzungsrechte an den personenbezogenen Daten vom Adresseigner und vergütet den Dienstleister, der diese Daten zwecks Dialogmarketings nach einer gesonderten Vereinbarung verarbeitet. Der Werbetreibende hat bei der hier vereinbarten Auftragsverarbeitung keinen Zugriff auf die personenbezogenen Daten der betroffenen Personen. Den Zugriff auf diese Daten steuert der Adresseigner als Herr der Daten, so dass dieser für die datenschutzkonforme Verarbeitung der personenbezogenen Daten verantwortlich ist (auch **datenschutzrechtlicher Auftraggeber**). [*Etwas anderes gilt dann, wenn die Daten verkauft werden und der Werbetreibende selbst datenschutzrechtlich verantwortlich wird.*] Die **datenschutzrechtliche Vertragsbeziehung** (auch **Auftragsverarbeitung**) besteht also zwischen dem Adresseigner und dem Dienstleister. Das folgende Schaubild macht die Beteiligten und deren Rechtsbeziehungen deutlich.



Wenn der **Adresseigner gleichzeitig Werbetreibender** ist, fließen die datenschutzrechtliche Verantwortung als Auftraggeber und das kommerzielle Innehaben der Nutzungsrechte in einem Unternehmen zusammen. Es gelten dann nur die Rechte und Pflichten dieses Vertrags, die für das Rechtsverhältnis zwischen Adresseigner und Dienstleister vorgesehen sind.

Achtung: Diese DDV-Regeln zur Auftragsverarbeitung berücksichtigen insbesondere die Anforderungen nach Art. 28 DSGVO und sind in den konkreten Auftrag des Adresseigners (**gesonderter Adressauftrag**) einzubeziehen. In dem gesonderten Adressauftrag sind vor allem auch Gegenstand und die Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sowie ggf. etwaige Empfänger oder Empfängerkategorien festzulegen.

1. Begriffsbestimmungen

Adresseigner (= Listeigner):	Das Unternehmen, das die personenbezogenen Adressdaten selbst erhoben oder in sonstiger Weise erworben hat, und ohne dessen datenschutzrechtlichen Auftrag die Datenverarbeitung durch den Dienstleister nicht vorgenommen werden darf.
Adressdaten (-sätze):	Personenbezogene Daten, deren Verarbeitung den datenschutzrechtlichen Anforderungen unterlieg und die bei der Verwendung dieser Adresseigners ausschließlich mit Erteilung eines Auftrags nach Art. 28 DSGVO durch den Dienstleister verarbeitet werden dürfen. Es kann sich um Namen, Postadressen, Kommunikationsdaten und sonstige personenbezogene Daten handeln.
Datenschutzrechtlicher Auftraggeber:	Verantwortlicher nach Art. 4 Nr. 7 DSGVO und Inhaber der Daten, der den Auftrag zur Datenverarbeitung nach Art. 28 DSGVO an den Dienstleister erteilt. Er muss mit dem Werbetreibenden nicht identisch sein, in dessen wirtschaftlichen Interesse der datenschutzrechtliche Auftrag erteilt wird. Bei Werbung für eigene Produkte und/oder Leistungen fallen datenschutzrechtlicher Auftraggeber und Werbetreibender zusammen.
DDV:	Deutscher Dialogmarketing Verband e.V., Hahnstraße 70, 60528 Frankfurt, www.ddv.de.
Dienstleister:	Auftragsverarbeiter nach Art. 4 Nr. 8 DSGVO, der die Adressdaten zwecks Dialogmarketing oder der sonstige personenbezogene Daten (beispielsweise zwecks Aktenvernichtung, Rechenzentrumsdienstleistung, Listbroking oder Call-Center-Dienstleistungen) im Auftrag des Adresseigners verarbeitet und unterzeichnende Partei des gesonderten Adressauftrags einschließlich der einbezogenen DDV-Regeln zur Auftragsverarbeitung ist.
DSGVO:	EU-Datenschutz-Grundverordnung.
Gesonderter Adressauftrag:	Vereinbarung zwischen Adresseigner und Dienstleister mit Weisungen für den Gegenstand und die Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sowie ggf. etwaige Kategorien von Empfängern oder Empfänger. Der gesonderte Adressauftrag in Kombination mit den einbezogenen DDV-Regeln zur Auftragsverarbeitung ermöglichen eine datenschutzkonforme Auftragsverarbeitung.
Listbroker:	Das Unternehmen, das das Nutzungsrecht an den Adressdaten (nicht die Adressdaten selbst) vom Adresseigner erhält und direkt

	oder indirekt über einen anderen Listbroker einem Werbetreibenden zur Durchführung einer Werbemaßnahme einräumt.
Werbeaktion:	Die Werbemaßnahme, die mit den Adressdaten vorgenommen wird (beispielsweise ein ausgesendetes Mailing/ein ausgesendeter Katalog, ein E-Mail-Newsletter, ein werblicher Anruf oder eine Datenaufbereitung/-weiterverarbeitung).
Werbetreibender:	Der kommerzielle Auftraggeber, der als wirtschaftlicher Auftraggeber die Adressdaten für seine Zwecke über den Dienstleister nur mit Zustimmung des Adresseigners nutzen darf.

2. Allgemeine Pflichten des Dienstleisters

(1) Der Adresseigner räumt in einem *gesonderten Adressauftrag* Nutzungsrechte an Adressdaten ein. Der Werbetreibende erwirbt diese Nutzungsrechte zur Durchführung einer konkret definierten Werbeaktion direkt oder über einen Listbroker. Der Dienstleister, bezahlt vom Werbetreibenden, wird für den Adresseigner als Auftragsverarbeiter tätig, um bei der Werbeaktion Dienstleistungen unter Zugriff auf die vom Adresseigner gehaltenen, im gesonderten Adressauftrag genannten Adressdaten zu erbringen. Der Dienstleister wird die Adressdaten ausschließlich dem jeweils gesonderten Adressauftrag, sonstigen Weisungen des Adresseigners für die erforderlichen auftragsbezogenen Dienstleistungen wie IT- (beispielsweise Analyse, postalische Korrektur, Abgleich, Porto-Optimierung und Ausdruck), Druck-, Lettershop- oder Call-Center-Arbeiten und den einbezogenen DDV-Regeln zur Auftragsverarbeitung verarbeiten. Der Dienstleister wird eine darüberhinausgehende Verarbeitung (beispielsweise Speicherung von Daten in anonymisierter Form, zur Auftragserfassung, History-Files oder Optimierungsanalysen) nur dann durchführen, wenn dies datenschutzrechtlich zulässig ist und die dazu notwendigen Weisungen des Adresseigners oder eine zwingende gesetzliche Verpflichtung des Dienstleisters vorliegen. Die Weisungen sind grundsätzlich in Textform zu erteilen; im Ausnahmefall erforderliche mündliche Weisungen sind vom Adresseigner unverzüglich in Textform zu bestätigen.

(2) Der Gegenstand und die Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sowie ggf. etwaige Kategorien von Empfängern oder Empfänger sind – sofern nicht mit diesen DDV-Regeln zur Auftragsverarbeitung bestimmt – im jeweiligen Adressauftrag festgelegt.

(3) Der Dienstleister wird die Adressdaten getrennt von Datenbeständen, die nicht im Zusammenhang mit dem gesonderten Adressauftrag stehen, verarbeiten. Damit soll eine unbefugte Verarbeitung für andere, nicht erlaubte Zwecke ausgeschlossen werden.

(4) Soweit der Dienstleister die Adressdaten auf portablen Speichermedien erhält, wird er diese Daten zur ordnungsmäßigen Abwicklung des gesonderten Adressauftrags kopieren. Die übergebenen Originaldatenträger sind erst nach Zustimmung des Adresseigners zu löschen und bis dahin nicht mehr zu verarbeiten (Einschränkung der Verarbeitung). Der damit für den Dienstleister verbundene Aufwand wird vom Adresseigner vergütet.

(5) Nach Abschluss der vertraglichen Arbeiten hat der Dienstleister die im Rahmen des Adressauftrags in seinen Besitz gelangten Adressdaten nach Weisung des Adresseigners an den Adresseigner oder an einen von ihm schriftlich benannten Dritten herauszugeben oder nach DSGVO datenschutzkonform zu löschen. Das gilt auch für Verarbeitungsergebnisse, die im Rahmen des gesonderten Adressauftrags erstellt worden sind, sowie für Test- und Ausschussmaterial. Makulatur mit personenbezogenen Daten ist gemäß Sicherheitsstufe 3 der DIN 66399-2 entweder durch hausinterne Aktenvernichter oder von spezialisierten Auftragsverarbeitern zu vernichten. Der Dienstleister hat dafür Sorge zu tragen, dass Datensätze mit personenbezogenen Adressdaten nicht als E-Mail-Anhang, auf Kommunikationsservern, Clients, Produktionsrechnern, in Datensicherungen über den Löschtermin hinaus bestehen bleiben. Sofern nicht der Adresseigner eine andere Weisung, beispielsweise für Treuhandbestände, gegeben hat, muss die Löschung dieser Daten spätestens im siebenten

Monat nach Postauflieferung nachweislich erfolgt sein. Die Kalenderwoche (ISO 8601) der letzten Postauflieferung ist dem Dienstleister mitzuteilen, wenn sie sich nicht aus dem gesondertem Adressauftrag ergibt. Der Dienstleister wird dem Adresseigner und seinem Vertreter auf deren Wunsch die eigene Löschung oder die Löschung durch Auftragnehmer in Textform innerhalb von fünf Werktagen bestätigen. Auf Wunsch stellt der Dienstleister dem Adresseigner und seinem Vertreter ein Löschprotokoll bzw. einen Vernichtungsbeleg zur Verfügung. Vorzulegen ist ein Protokoll, das die Tatsache der Löschung mit Datums- und Zeitangabe, Löschart und verantwortliche Person für fünf Jahre dokumentiert. Der mit den vorherig genannten Pflichten zur Herausgabe und Löschung für den Dienstleister verbundene Aufwand wird vom Adresseigner gemäß des gesonderten Adressauftrags vergütet. Die Verpflichtung zur Herausgabe oder zur Löschung gilt nicht, wenn der Dienstleister gesetzlich zu einer Aufbewahrung oder in sonstiger Weise zur Speicherung der konkreten Daten verpflichtet ist. Eine sonstige Weitergabe der Daten ist nur laut gesondertem Adressauftrag oder Weisung des Adresseigners erlaubt.

(6) Die Einschaltung von Unterauftragnehmern zur Erfüllung des gesonderten Adressauftrags (Dienstleister mit vereinbartem Datenzugriff) setzt die vorherige schriftliche Zustimmung des Adresseigners voraus. Der Dienstleister kann ohne schriftliche Zustimmung Unterauftragnehmer zur Vertragsdurchführung unter Wahrung seiner Pflicht zur Auftragskontrolle und nachweislich geschlossener Vereinbarungen gemäß Art. 28 DSGVO einschalten, wenn es sich um Dienstleistungen der Auftragsverarbeitung handelt, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen beispielsweise erweiterte Telekommunikationsleistungen oder Reinigungskräfte, die zugleich mit der Entsorgung von Datenträgern betraut sind. Eine Zustimmung wird allerdings dann erforderlich, wenn die genannte Leistung selbst ganz oder zumindest in wesentlichen Teilen die mit dem Auftragnehmer vereinbarte Dienstleistung darstellt. In jedem Fall sind bei den genannten (Unter-)Beauftragungen die Inhalte dieser DDV-Regeln zur Auftragsverarbeitung entsprechend vorzusehen. Auf Wunsch erhalten der Adresseigner und ein abweichender Werbetreibender eine Liste aller Unterauftragnehmer, einschließlich solcher, zu deren Einsatz der Auftraggeber zugestimmt hat. Diese Vorgaben gelten entsprechend für die Einschaltung von Freiberuflern/Freelancern, die für den Dienstleister tätig sind, ohne dabei wie ein Arbeitnehmer in dessen Unternehmen eingegliedert zu sein und wesentliche Leistungen für den gesonderten Adressauftrag erbringen.

(7) Der Dienstleister wird in seinem Verantwortungsbereich technische und organisatorische Maßnahmen zum angemessenen Schutz der Adressdaten des Adresseigners vor allem gegen ungewollten oder unbefugten Abfluss treffen (geeignete technische und organisatorische Datensicherheitsmaßnahmen, um ein dem Risiko angemessenes Schutzniveau zu schaffen; nach Art. 32 DSGVO) und den Auftraggeber bei der gegebenenfalls gebotenen Datenschutz-Folgenabschätzung bezogen auf seine Sphäre und mit Rücksicht auf die ihm vom Auftraggeber zur Verfügung gestellten Informationen unterstützen. Der Dienstleister kann für diese Unterstützung eine angemessene Vergütung und die Erstattung von Aufwendungen verlangen. Der Dienstleister unterstützt den Adresseigner unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Mittel und Informationen unverzüglich bei der Einhaltung dessen Pflichten zur Information der Betroffenen und zur Auskunftserteilung sowie zur Berichtigung, Löschung oder Einschränkung der Verarbeitung sowie sonstiger Betroffenenrechte nach den geltenden Datenschutzvorschriften. Der damit für den Dienstleister verbundene Aufwand wird vom Adresseigner laut des gesonderten Adressauftrags vergütet. Nach Art. 30 Abs. 2 DSGVO führt der Dienstleister ein Verzeichnis über die von ihm durchgeführten Verarbeitungen. Dieses ist auf Wunsch dem Adresseigner und seinem Vertreter in Kopie herauszugeben, soweit dessen Inhalt im Zusammenhang mit dem gesonderten Adressauftrag steht.

(8) Bei der Abwehr geltend gemachter Ansprüche betroffener Personen auf Schadensersatz wirkt der Dienstleister mit, sofern ihm die Mitwirkung ohne weiteren wesentlichen Aufwand möglich ist. Soweit sich die betroffene Person an den Dienstleister wendet, um Betroffenenrechte geltend zu machen, wird der Dienstleister die betroffene Person formal, oh-

ne inhaltliche Vorbeantwortung, an den Adresseigner verweisen und diesem die Anfrage übergeben. Eine Beantwortung durch den Dienstleister im Auftrag ist nur dann vorzunehmen, wenn der Adresseigner dies gegen Vergütung des damit verbundenen Aufwandes beim Dienstleister im Rahmen der Auftragsverarbeitung beauftragt hat.

(9) Der Adresseigner ist verpflichtet, ungewollte oder unrechtmäßige gesetzlich relevante Datenabflüsse an Dritte oder sonstige Datenschutzverletzungen, die zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen, der zuständigen Datenschutzaufsichtsbehörde und – bei hohem Risiko für die Rechte und Freiheiten der betroffenen Person – den betroffenen Personen unverzüglich mitzuteilen. Soweit derartige Verletzungen dem Dienstleister in seiner Sphäre bekannt werden, unterrichtet er den Adresseigner unverzüglich. Der Dienstleister wird in diesem Fall einstweilig und nach pflichtgemäßen Ermessen in seinem Verantwortungsbereich angemessene Maßnahmen zum Schutze der Adressdaten des Adresseigners und zur Minderung möglicher nachteiliger Folgen (geeignete technische und organisatorische Datensicherheitsmaßnahmen, um ein dem Risiko angemessenes Schutzniveau zu schaffen; nach Art. 32 DSGVO) treffen. Der Dienstleister informiert den Adresseigner über etwaige von ihm getroffene Maßnahmen möglichst zeitnah.

(10) Der Dienstleister unterrichtet den Auftraggeber unverzüglich, wenn eine vom Adresseigner erteilte Weisung nach seiner Meinung – die keine umfassende rechtliche Prüfung voraussetzt – zu einem Verstoß gegen gesetzliche Vorschriften führen kann. Die Weisung braucht nicht befolgt zu werden, wenn sie nicht geändert oder vom Adresseigner ausdrücklich bestätigt wird.

(11) Der Dienstleister benennt einen einheitlichen Ansprechpartner für sich, mit dem der Adresseigner oder sein Vertreter Fragen im Zusammenhang mit dem gesonderten Adressauftrag klären kann. Der Dienstleister hat unter den gesetzlichen Voraussetzungen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten bestellt. Über einen Wechsel der Ansprechpartner wird der Dienstleister den Adresseigner unverzüglich in Textform informieren.

3. Sicherheitspflichten des Dienstleisters

(1) Der Dienstleister gewährleistet in seinem Verantwortungsbereich, dass er die Adressdaten nach dem Stand der Technik, den Implementierungskosten, ihrer Art, ihrem Umfang, den Umständen und den Zwecken der mit dem gesonderten Adressauftrag in Zusammenhang stehenden Verarbeitung, nach der Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen hinreichend technisch und organisatorisch sicher im Sinne der Art. 32 DSGVO verarbeitet (Datensicherheitseinrichtungen). Auf Wunsch des Adresseigners gibt der Dienstleister dem Adresseigner und seinem Vertreter auch nach Erteilung des Auftrags sein aktuelles Datensicherheitskonzept heraus und ermöglicht dem Datenschutzbeauftragten des Adresseigners oder einem zur Berufsverschwiegenheit verpflichteten vom Adresseigner benannten Prüfer die Einsicht in das Datensicherheitskonzept, ebenso dessen Prüfung. Das Datensicherheitskonzept beinhaltet hinreichende Erläuterungen zu den Themen Zutrittskontrolle zum Gebäude, Zugangskontrolle zum System, Zugriffskontrolle zu den Anwendungen, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und getrennte Verarbeitung. Soweit vom Adresseigner Änderungen gewünscht sind, wird der Dienstleister diese implementieren; auf schriftliche vorherige Ankündigung und auf Kosten des Adresseigners, soweit sie den gesetzlich geforderten Stand der Technik überschreiten.

(2) Adressdaten, die auf elektronischem Wege weitergegeben werden müssen, dürfen vom Dienstleister nur in nach dem Stand der Technik sicherer, nämlich verschlüsselter Form weisungsgemäß weitergegeben werden, sofern nicht der Adresseigner etwas anderes wünscht.

(3) Der Dienstleister ist nicht befugt, bei der Entwicklung von Software oder bei sonstigen Tests – außerhalb des gesetzlich Zulässigen – Echtdaten des Adresseigners zu verwenden. Es ist mit anonymisierten Original- oder fiktiven Testdaten zu arbeiten.

(4) Der Dienstleister speichert und verarbeitet die Adressdaten getrennt nach Aufträgen und erlaubt Zugriff durch Mitarbeiter nur, soweit dies zur Durchführung des gesonderten Adressauftrags erforderlich ist. Zudem erlaubt er nur solchen Mitarbeitern Zugriff auf die Daten, die auf Geheimhaltung gesondert und ausdrücklich verpflichtet sind und regelmäßig in für die Adressverarbeitung relevanten Datenschutz- und Datensicherheitsvorschriften und -verfahren geschult sind.

4. Pflichten des Dienstleisters zur Duldung von Kontrollen

(1) Der Adresseigner ist gesetzlich verpflichtet, sich von der Wirksamkeit der Datensicherheitseinrichtungen beim Dienstleister zu überzeugen. Der Dienstleister duldet daher, dass der Adresseigner die Verarbeitung der von ihm überlassenen Daten durch Einsichtnahme und Prüfung der mit dieser Vereinbarung in Zusammenhang stehenden Datenverarbeitungseinrichtungen, der gespeicherten Daten, der Datenverarbeitungsprogramme vor Ort und der Dokumentation der Datenschutzorganisation, einschließlich Arbeitsanweisungen, in der Regel einmal jährlich kontrolliert. Der Dienstleister hat die mit dem gesonderten Adressauftrag in Zusammenhang stehenden Dokumente zur Einsicht bereit zu halten und Antworten auf Fragen in angemessener Frist zu geben. Die Einsicht ist dem Datenschutzbeauftragten des Adresseigners und von ihm beauftragten zur gesetzlichen Berufsverschwiegenheit verpflichteten Personen zu gewähren.

(2) Der Adresseigner kann sich ohne eigene Kontrollen von den nach dem Stand der Technik hinreichenden Datensicherheitseinrichtungen auch dadurch überzeugen, dass ihm der Dienstleister entsprechende Nachweise wie Prüfungsberichte zur Informationssicherheit oder die Angaben zur Erlangung der DDV-Gütesiegel der Kompetenz-Center DirectMail Services (DMS) und Zielgruppenmarketing (ZGM) vorlegt.

5. Abgleichprotokoll/Kontrolladressen

(1) Wenn auftragsgemäß Abgleiche mit Einsatz von Fremddaten durchgeführt werden, hat der Dienstleister ein lückenloses und nachvollziehbares Protokoll mit nachfolgend festgelegten Inhalten zu erstellen.

DDV-Standard „Abrechnungsprotokoll	
Erstellungsdatum	
Bezeichnung der Werbeaktion	
Listenbezeichnung pro Datei	
Zahl der gelieferten Adressdaten	
./.	Adressdaten, die sich aus postalischer Prüfung (unter anderem Korrekturen) ergeben
=	Bruttomenge für den Abgleich (Abgleich-Input)
./.	Adressdaten, die durch den Dubletten-Abgleich eliminiert worden sind
=	Nettomenge nach Abgleich (Abgleich-Output)
./.	Reduzierung nach Auftrag des Kunden
=	Einsatzmenge

(2) Zur Kontrolle und zum Schutz vor vertragswidriger Verwendung dürfen Kontrolladressen in die jeweiligen Datensätze eingefügt werden. Kann der Adresseigner eine nicht mit ihm

vereinbarte Werbung an eine Kontrolladresse vorlegen, wobei diese Kontrolladresse eindeutig allein dem Bestand zuzuordnen ist, der nur für die jeweilige Werbeaktion zur Verarbeitung überlassen worden ist, so wird vermutet, dass eine unbefugte Verwendung erfolgt ist. Der Dienstleister ist verpflichtet, dem Adresseigner und seinem Vertreter eine von sich aus erkannte unbefugte Verwendung von Daten unverzüglich mitzuteilen. Eine solche Mitteilung hat mindestens in Textform zu erfolgen.

6. Sonstiges

(1) Im Falle der Weitergabe von Fremddaten (elektronisch oder in gedruckter Form) ist der Empfänger darüber zu unterrichten, dass die Adressdaten von einem oder– unter Umständen – von verschiedenen Verantwortlichen stammen und nur für den Zweck verarbeitet werden dürfen, für den sie geliefert wurden.

(2) Werden Abgleiche unter Einsatz von Fremddaten im Verbraucher-Bereich (Business to Consumer) durchgeführt, wird derjenige Dienstleister, der für die Fremdabgleiche zuständig ist, die aktuelle (Update monatlich) DDV-Robinsonliste einsetzen, es sei denn, der/die Verantwortliche(n) hat/haben schriftlich auf den Einsatz verzichtet.

(3) Der Umstand, dass sich ein Unternehmen den „DDV-Regeln zur Auftragsverarbeitung" durch Zeichnung unterworfen hat, wird auf der Website des DDV veröffentlicht. Dem DDV sind dazu die gezeichneten „DDV-Regeln zur Auftragsverarbeitung" zur Hinterlegung einzureichen. Jedem Auftraggeber, Listbroker oder jedem anderen beteiligten Dienstleister wird der Dienstleister auf Wunsch eine Kopie der gezeichneten „DDV-Regeln zur Auftragsverarbeitung" zur Verfügung stellen. Soweit irgendwelche tatsächlichen Umstände beim Dienstleister den gezeichneten Vorgaben der „DDV-Regeln zur Auftragsverarbeitung" nicht mehr entsprechen, wird das der Dienstleister dem DDV unverzüglich schriftlich mitteilen. Die Veröffentlichung der Information, dass das betreffende Mitglied die „DDV-Regeln zur Auftragsverarbeitung" gezeichnet hat, wird dann rückgängig gemacht.

(4) Die Verbindlichkeit der „DDV-Regeln zur Auftragsverarbeitung" für das zeichnende Mitglied bleibt bestehen bis zum Widerruf, den das Mitglied per Einschreiben an den DDV zu richten hat. Der Widerruf gilt 6 Wochen nach Eingang mit Wirkung für die Zukunft. Für die Laufzeiten der vor Ablauf der vorgenannten 6-Wochen-Frist bereits erteilen gesonderten Adressaufträge gelten die „DDV-Regeln zur Auftragsverarbeitung" fort.

(5) Mit Unterzeichnung bestätigt der Dienstleister zusätzlich die Übereinstimmung des vorstehenden Textes mit der vom DDV vorgegebenen Textfassung der DDV-Regeln zur Auftragsverarbeitung (Stand: 10/2017).

(6) Die Schriftformerfordernisse im Sinne der DDV-Regeln zur Auftragsverarbeitung können mit Ausnahme des Schriftformerfordernisses für die Auftragserteilung auch durch Textform (insbesondere per E-Mail) erfüllt werden.

(7) Vereinbarungen auf der Basis der DDV-Regeln zur Auftragsverarbeitung unterliegen deutschem Recht. Es gilt der Gerichtsstand des jeweiligen Auftrags, soweit zulässig vereinbar.

Korntal-Münchingen, den 7. März 2018

NUNTIUS MARKETING LOGISTIK e.K. • Kornweathener Str. 228 - 70825 Korntal-Münchingen •

Firmenstempel oder Firmenname

(Dietmar Müller) (_____)

Unterzeichner Druckbuchstaben ggf. 2. Unterzeichner Druckbuchstaben

Beschreibung der technischen und organisatorischen Maßnahmen (§ 32 DS-GVO und § 64 BDSG)

Name der Firma: Nuntius Marketing Logistik GmbH & Co. KG

Kornwestheimer Str. 228

70825 Korntal-Münchingen

Inhaber: Dietmar Müller

d.mueller@nuntius.net

Telefon: 07150.9129-10

Datenschutzbeauftragter

Holger Hanke

h.hanke@nuntius.net

Telefon: 07150.9129-31

1. Organisatorische Maßnahmen

1.1 Ein interner Datenschutzbeauftragter ist bestellt.

1.2 Das Unternehmen unterliegt nicht der Meldepflicht.

1.3 Alle Mitarbeiter sind nachweislich auf die Vertraulichkeit (§ 28 Abs. 3 DS-GVO) und auf das Datengeheimnis (§ 53 BDSG - neu) sowie auf die Wahrung von Geschäftsgeheimnissen verpflichtet worden.

1.4 Alle Mitarbeiter sind nachweislich auf das Fernmeldegeheimnis (§ 88 TKG i.V. mit § 206 StGB) verpflichtet.

1.5 Alle Mitarbeiter werden regelmäßig zu Datenschutz-Themen geschult.

1.6 Das Unternehmen wird regelmäßig in unabhängigen Sicherheitsüberprüfungen durch den Deutschen Dialogmarketing Verband e.V. unterzogen.

1.7 Die Datenverarbeitung findet innerhalb Deutschland statt.

1.8 Es existieren definierte Prozesse zur Meldung und Behandlung von IT-Sicherheitsvorfällen und Datenschutzpannen.

2. Zutrittskontrolle

2.1 Es gibt schriftliche Regelungen zum Gebäudezutritt, insbesondere für den Zutritt zu
Räumen mit Datenverarbeitungsanlagen und Datenträgerarchiven
(Wer hat wann Zutritt, Regelungen für Besucher).

2.2 Der Zutritt zum Gebäude ist mittels Sicherheitsschloss gesichert.

2.3 Der Zutritt zu den Datenverarbeitungsanlagen ist mittels Sicherheitsschloss gesichert.

3. Zugangskontrolle

3.1 Es gibt schriftliche Regelungen zur Benutzung von Datenverarbeitungsanlagen
(Wer hat wann und wie Zugang zu den Daten).

3.2 Es gibt schriftliche Regelungen zur Sperrung von Benutzerkonten
(nach Anzahl von fehlgeschlagenen Anmeldeversuchen, bei Abwesenheit durch Bildschirmschoner).

3.3 Der logische Zugang zu den relevanten DV-Systemen ist wie folgt gesichert:
- Passwortverfahren mit wenigstens 8 Zeichen, drei Zeichenklassen und erzwungenem Passwortwechsel nach spätestens drei Monaten
- Automatische Sperrung von Kennungen nach maximal 5 Fehlversuchen
- Passwortdateien sind gegen unbefugte Zugriffe geschützt
- Benutzerkonten für nicht mehr Berechtigte (z. B. ausgeschiedene Mitarbeiter) werden umgehend gesperrt
- Benutzer-Accounts sind personifiziert

3.4 Es gibt einen geregelten Prozess für Benutzer-Accounts und Kennwörter
(Vergabe, Rücksetzen und Löschen, Zuständigkeiten).

3.5 Es gibt getrennte Benutzerkonten für die Systemadministration und die regulären Benutzer.

3.6 Es existiert ein geregelter Patch-Management Prozess zur Versorgung der Systeme
mit Updates und gibt es eine Sicherheitsüberprüfung.

4. Zugriffskontrolle

4.1 Es gibt ein differenziertes, schriftliches Berechtigungskonzept (dokumentierte Berechtigungsvergabe, regelmäßige Prüfung bestehender Berechtigungen), um die Nutzung von Profilen bzw. Rollen und Transaktionen zu regeln.

4.2 Es gibt schriftliche Regelungen zur Nutzung mobiler Datenträger (CD, DVD, USB-Stick, Notebooks, etc.) deren Einhaltung überprüft wird und die u. a. beinhalten: Nur dienstliche Nutzung zulässig, verschlüsselte Datenablage bei entsprechender Vertraulichkeitsstufe.

4.3 Es erfolgt eine kontrollierte Vernichtung/Entsorgung von Datenträgern und elektronischen Daten des Auftraggebers.

5. Weitergabekontrolle

5.1 Es gibt schriftliche Regelungen zum Versand und zur Übertragung von Daten.

5.2 Die Daten werden bei der Übertragung mittels Verschlüsselung (Passwort, PGP-Verschlüsselung, VPN-Tunnel, Verschlüsselungssoftware) geschützt.

6. Eingabekontrolle

6.1 Es gibt schriftliche, dokumentierte Regelungen zur Durchführung einer Eingabekontrolle (Bei der Erfassung oder Veränderung von Daten des Auftraggebers: Wer, was, wann).

7. Auftragskontrolle

7.1 Alle Teile der Auftragsverarbeitung werden am Standort (Inhouse) durchgeführt.

7.2 Es werden keine Subauftragnehmer oder externer Firmen zur Auftragsverarbeitung eingesetzt.

8. Verfügbarkeitskontrolle

8.1 Die Daten werden gegen zufällige Zerstörung oder Verlust wie folgt geschützt:
- Tägliche Datensicherung
- Datensicherung in anderem Zyklus

- Spiegelung von Daten
- Einsatz von USV
- Einsatz einer Brandmeldeanlage
- Getrennte Aufbewahrung von Produktivdaten und Datensicherungen
- Stichprobenartige Prüfung von Datensicherungen

8.2 Die Daten werden gegen vorsätzliche Zerstörung oder Verlust wie folgt geschützt:
- Einsatz von Virenscannern auf Arbeitsstationen
- Einsatz von Virenscannern auf Servern
- Einsatz von Firewalls zur Absicherung von Netzwerkübergängen

9. Trennungskontrolle

9.1 Es existieren schriftliche Regelungen zur Trennung der Daten des Auftraggebers
von eigenen/anderen Auftragsdaten (Mandantentrennung)

9.2 Es existieren schriftliche Regelungen zur Funktionstrennung (Test/Entwicklung/Produktion)

9.3 Das Daten vertraulich und nur zum vorgesehenen Zweck verarbeitet und genutzt
werden, wir wie folgt sichergestellt:
- Die Daten werden nach Mandanten getrennt verarbeitet
- Es gibt eine Trennung zwischen Entwicklung, Test und Produktion
- Datentrennung durch ein differenziertes Benutzerkonzept

NUNTIUS
MARKETING LOGISTIK

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management

• Es gelten die Grundsätze:

- Datenschutz ist Aufgabe des gesamten Unternehmens.
- Es werden datenschutzfreundliche Technologien eingesetzt, wo immer das
- möglich und wirtschaftlich ist.
- Die IT-Sicherheit muss auf dem aktuellen Stand der Technik sein.

• Das Unternehmen legt Strategien fest hinsichtlich:

- Zuweisung von Zuständigkeiten.
- Risikobewertung.
- Durchführung von Kontrollen.
- Sensibilisierung und Schulung der Mitarbeiter.

• Wenn immer das erforderlich ist, werden die eingesetzten Verfahren einer dokumentierten Datenschutz-Folgenabschatzung unterzogen, bestehend aus:

- Schutzbedarfsfeststellung.
- Risikoanalyse.
- Sicherheitskonzept.

• Durchgeführte Verarbeitungstätigkeiten – auch als Auftragsverarbeiter – werden einheitlich und nachweisbar dokumentiert.

• Weisungen von Kunden im Rahmen einer Auftragsverarbeitung werden kundenbezogen
dokumentiert.

• Ausgeführte Tätigkeiten im Rahmen der Auftragsverarbeitung werden kundenbezogen
dokumentiert.

Incident-Response-Management

Es bestehen interne Richtlinien, Handlungsanweisungen und Prozesse zum Datenschutz, die bei Bedarf oder sich ändernden Voraussetzungen erweitert bzw. ergänzt werden.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

• Es werden für den jeweiligen Verarbeitungszweck geeignete technische und organisatorische Maßnahmen getroffen, die jedem Auftraggeber im Rahmen der Vereinbarung einer Auftragsverarbeitung zugesichert werden. Spätere Änderungen dieser Maßnahmen können nur zu besseren Zuständen führen, niemals zu einer Verschlechterung.

• Es gilt stets die höchste Schutzstufe bei der Erstellung neuer Objekte in der Berechtigungs- und Zugriffsverwaltung. So hat beispielsweise eine neu erstellte Kennung zunächst keinerlei Rechte im System und erhält diese erst, wenn ihr ein Profil (Sammlung von Rechten) zugeordnet wird.

• Berechtigungsobjekte ohne Zuordnung einer Satzebenen-Berechtigung dürfen zunächst keine Daten-Inhalte sehen. Erst durch Zuweisung einer Satzebene werden die dort definierten Dateninhalte zur Benutzung freigegeben.

• Erstellte Auswertungsergebnisse und Listen – ob im Einzelfall oder fallübergreifend – können nur von daraufhin berechtigten Personen eingesehen werden.

Auftragskontrolle

• Im Rahmen der Geschäftsprozesse liegt es in der Verantwortung der Führungskräfte, in deren Aufgabenbereich die jeweiligen datenschutzrelevanten Dienstleistungen fallen, sicherzustellen, dass personenbezogene Daten nur entsprechend der Weisungen der Auftraggeber (grundsätzlich schriftlich vereinbart) und in Einklang mit den geltenden Rechtsvorschriften verarbeitet werden.

• Darüber hinaus stellt auch der betriebliche Datenschutzbeauftragte sicher, dass der Auftragskontrolle genüge getan wird.

• Schriftliche Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO mit Regelungen zum Auftragsablauf.

• Eindeutige Regelung der Zuständigkeiten und Verantwortlichkeiten sowie zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers.

• Sorgfältige Auswahl von Lieferanten und Unterauftragnehmern. Die angemessene Etablierung und die Einhaltung eines Datenschutz-Managements sind – nach Möglichkeit – durch die Einhaltung von Verhaltensregeln und / oder Zertifizierungen nachzuweisen.

• Alle Mitarbeiter werden regelmäßig geschult, um die Einhaltung der Vorschriften der DS-GVO und die Einhaltung von Weisungen sicherzustellen. Es erfolgen regelmäßig Nachschulungen.

• Regelmäßige Prüfung der vereinbarten Regelungen durch den betrieblichen Datenschutzbeauftragten.

• Ansprechpartner und verantwortliche Projektmanager werden für den konkreten Auftrag bestimmt und schriftlich festgehalten.

DDV

Deutscher Dialogmarketing Verband e.V.

Mitgliedsurkunde des DDV

Nuntius Marketing Logistik e. K.

Mitglied seit **03.11.2009**

Der DDV vertritt als größter nationaler Zusammenschluss von Dialogmarketing-Unternehmen in Europa und als einer der Spitzenverbände der Kommunikationswirtschaft in Deutschland die Interessen von Anwendern und Dienstleistern im Dialogmarketing. Der Verband ist der freiheitlichen Kommunikation, der Nachwuchsförderung, einem sinnvollen Daten- und Verbraucherschutz und der Qualitätssicherung im Dialogmarketing verpflichtet.

Wiesbaden, den 17.11.2009

Präsident

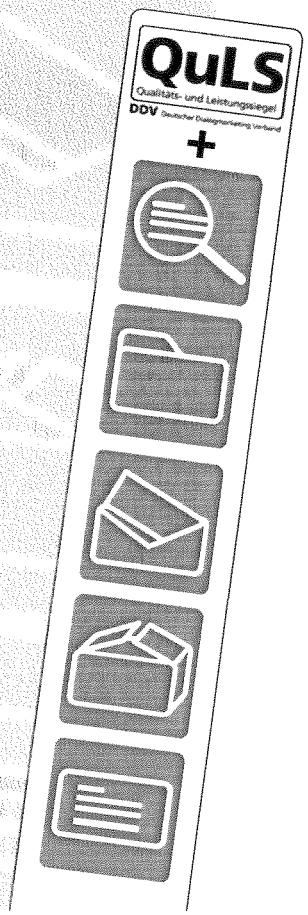
Geschäftsführer

DDV Deutscher Dialogmarketing Verband e.V. · Hasengartenstraße 14, 65189 Wiesbaden
Tel.: 0611/97793-0 · Fax: 0611/97793-99 · Internet: http://www.ddv.de · eMail: info@ddv.de

Sicherheit, Transparenz und Datenschutz

Die Qualitätssiegel des DDV bei Adressdienstleistungs-Unternehmen

www.ddv.de



DDV

Setzen Sie auf Nummer Sicher

Die Adressdienstleister in den drei DDV-Councils DirectMail Services, List Council und Print und Service haben sich verpflichtet, im Bereich Datenschutz weitreichende und über die gesetzlichen Anforderungen hinausgehende Qualitäts- und Leistungsstandards (QuLS) zu beachten. Die Einhaltung dieser Vorgaben wird durch ein externes Datenschutz-Prüfunternehmen vor Ort bei den Unternehmen und zudem jährlich durch Auswertung einer Online-Selbstverpflichtungserklärung (SVE) geprüft.

Der DDV erteilt nach bestandener Prüfung – abhängig vom Tätigkeitsbereich – eines oder mehrere Qualitätssiegel, bezogen auf das Kalenderjahr.

Die geprüften Unternehmen setzen das Logo des jeweiligen Siegels werblich gegenüber Kunden und Auftraggebern ein.

Die Qualitätssiegel des DDV

QuLS
Qualitäts- und Leistungssiegel
DDV Deutscher Dialogmarketing Verband

+

→ Siegel **Listbroker**
(List Council)

→ Siegel **Datenverarbeitung**
(Council DirectMail Services, Print und Service)

→ Siegel **Lettershop**
(Council DirectMail Services, Print und Service)

→ Siegel **Fulfillment**
(Council DirectMail Services, Print und Service)

→ Siegel **Adressverlag**
(Council DirectMail Services)

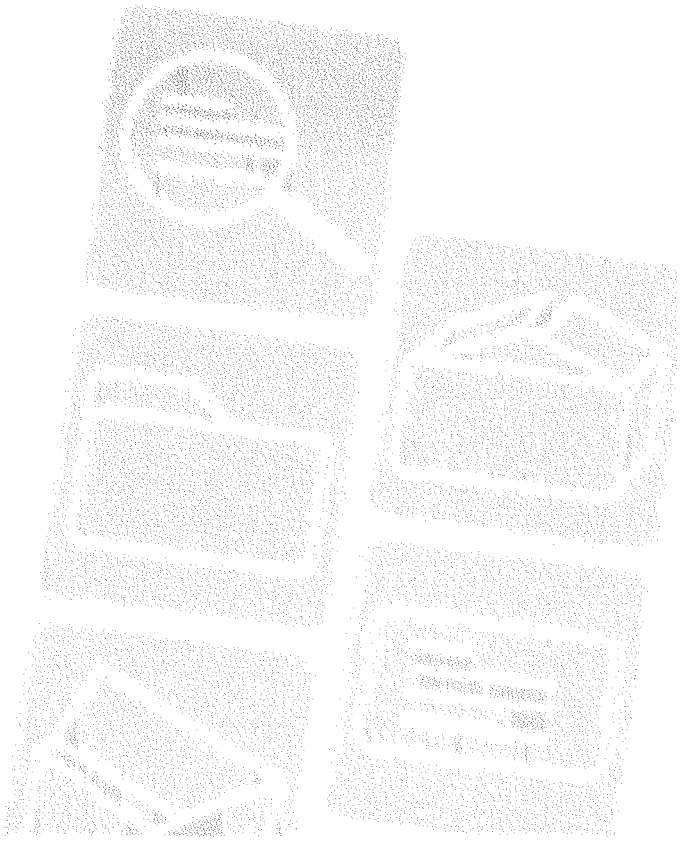
1. Wem nutzt das Qualitätssiegel?

→ **Kunden / Auftraggebern**
Das Qualitätssiegel erleichtert es dem Auftraggeber (z.B. werbungtreibende Unternehmen, Listeigner), seiner gesetzlich vorgeschriebenen Prüfungspflicht bezüglich des eingeschalteten Dienstleisters nachzukommen: Nach § 11 Abs. 2 Satz 1 BDSG hat der Auftraggeber einen geeigneten Dienstleister sorgfältig auszuwählen. Zudem muss er sich nach § 11 Abs.2 Satz 4 BDSG „vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen". Das Prüfergebnis hat er zu dokumentieren.

Wer DDV-geprüfte Unternehmen beauftragt, stützt sich auf eine gute, systematische Prüfungsgrundlage mit sehr strengen und umfangreichen Anforderungen. Für den Kunden / Auftraggeber stellt dies eine weitreichende Absicherung gegen das Risiko einer Pflichtverletzung dar.

Geprüfte Unternehmen haben darüber hinaus für die Umsetzung der Prüfungsanforderungen in der Tagespraxis standardisierte Verfahrensabläufe und Dokumente entwickelt. Sie stellen bei der Kommunikation mit Geschäftspartnern ein hohes Maß belegbarer Qualität sicher und unterstützen diese bei der Einhaltung ihrer Pflichten in Bezug auf Daten- und Verbraucherschutz.

→ **Siegelinhabern**
Durch die Vor-Ort-Prüfungen und die alljährliche Selbstverpflichtungserklärung sind die Siegelinhaber gezwungen, die Qualitäts-, Datenschutz- und Sicherheitsmaßnahmen permanent zu überprüfen und auf aktuellem Niveau zu halten. Das erteilte Qualitätssiegel belegt, dass sich der Dienstleister durch geprüfte Qualität von anderen Unternehmen am Markt abhebt. Wer auf das Siegel verweisen kann, hat damit einen deutlichen Wettbewerbsvorteil – dies schon deshalb, weil er dem Auftraggeber die gesetzlich vergebenen Prüfungen vereinfacht.



2. Was wird geprüft?

Anhand einer mehr als 140 Fragen umfassenden Checkliste – bezogen auf die besonderen Anforderungen bei Adressdienstleistungen – wird die Einhaltung der gesetzlichen Vorgaben zum Schutz der Daten der verschiedenen Geschäftspartner überprüft. Dazu zählen z.B. der Nachweis eines umfassenden Datensicherheitskonzeptes, regelmäßige Mitarbeiterschulungen, oder die Bestellung eines von der Geschäftsführung unabhängigen Datenschutzbeauftragten.

Die Prüfungen umfassen darüber hinaus eine Vielzahl spezieller Anforderungen, die in systematisch aufbereiteten Themenabschnitten darauf ausgerichtet sind, den Verbraucher zu schützen und Kunden sowie Adresslieferanten bei der Einhaltung ihrer gesetzlichen Verpflichtungen zu unterstützen.

3. Wie und wann wird geprüft?

Bevor das Siegel erstmalig erteilt wird, erfolgt eine umfangreiche **Vor-Ort-Prüfung**, dann nach drei Jahren und weiter in regelmäßigen Abständen eine Wiederholungsprüfung. Anlassbezogene Sonderprüfungen vor Ort sind bei Verdacht jederzeit möglich. Die Vor-Ort-Prüfung umfasst zwei Stufen: Nach erfolgter Kontrolle im Unternehmen wird der dazu erstellte Prüfbericht vor Siegelerteilung einer Kontrollkommission unter Vorsitz des Hauptgeschäftsführers der IHK Wiesbaden vorgelegt.

Ergänzt werden die Vor-Ort-Prüfungen durch eine alljährliche **Selbstverpflichtungserklärung** (SVE), bei der das siegelführende Unternehmen gegenüber dem Prüfer Eigenerklärungen zu einem detaillierten Online-Fragebogen abgibt. Besondere Qualität erlangt die SVE dadurch, dass nicht allein die zutreffende Antwort ausreicht. Vielmehr muss diese durch aktuelle Dokumente belegt werden können.

Das Siegel wird als Jahressiegel, bezogen auf das Kalenderjahr, vergeben. Die Prüfungen sind kostenpflichtig. Wird das Prüfungsziel nicht erreicht, so wird das Jahressiegel nicht erteilt und das Unternehmen aus dem jeweiligen Council ausgeschlossen. Details regeln beschlossene Rahmenbedingungen.

4. Wer führt die Prüfung durch?

Das Prüf- und Zertifizierungsverfahren zur Erlangung des Qualitätssiegels wird durch ein unabhängiges Datenschutz-Prüfunternehmen durchgeführt:

Beratungsbüro Gliss & Kramer KG
Erik-Blumenfeld-Platz 27a
22587 Hamburg
Tel. +49-(0)40-39906032
www.gliss-kramer.de

Durch die interne Organisation des Beratungsbüros und strikte Abgrenzung ist sichergestellt, dass keine Prüfungen durch Personen erfolgen können, die mit dem geprüften Unternehmen bereits als Berater in Verbindung stehen.

Kontakt
Deutscher Dialogmarketing
Verband e.V.
Hasengartenstraße 14
65189 Wiesbaden
Hans-Jürgen Schäfer
Telefon +49 611 97793-31
Fax: +49 611 97793-99
E-Mail: info@ddv.de

weitere Informationen
www.ddv.de