Kurzgutachten

Zeitpunkt der Prüfung

Die Prüfung wurde im Zeitraum von Mai 2012 bis Juni 2012 durchgeführt.

Adresse des Antragstellers

TNT Post GmbH & Co. KG Rotenburger Straße 24 30659 Hannover

Auditierungsstelle

UIMCert GmbH Moltkestr. 19 42115 Wuppertal Tel.: 0202-309 87 39 E-Mail: certification@uimcert.de

Leiter der Prüfstelle

Dr. Heiko Haaz

Name Auditor

Jens Schirrmacher

Auditnummer UIMCert

F-116-02

Kurzbezeichnung des Projektes/Produktes

Die TNT Post GmbH & Co. KG, nachfolgend TNT Post genannt, bietet ihren Kunden umfangreiche Dienstleistungen im Zusammenhang mit der Beförderung von Briefsendungen an. Dieses Dienstleistungsangebot besteht aus zwei Kernelementen, nämlich

- „Prävention“ und
- „Erbringung von Postdienstleistungen“ (im Folgenden: "Leistungserbringungsprozess").

Das Dienstleistungsangebot Prävention findet in Zusammenarbeit mit weiteren Partnern statt und ist, da es nicht die Erbringung von Postdienstleistungen zum Gegenstand hat, nicht Bestandteil dieses Gutachtens und wird daher nicht weiter thematisiert.

Nachfolgend wird lediglich der Leistungserbringungsprozess untersucht und unter Datenschutzordnungsmäßigkeitsgesichtspunkten bewertet.

Der Leistungserbringungsprozess erfasst nicht nur den klassischen Versand von Briefsendungen, sondern auch die Vorbereitung der Adressdaten. Der Leistungserbringungsprozess beinhaltet die Prozessschritte Datenmanagement, Sortierung, Transport, Zustellung und Redressen.

Das Datenmanagement, in dessen Rahmen die Adressvorbereitung stattfindet, hat eine Sonderstellung, da es personenbezogene Daten als Hauptbestandteil enthält und in die anderen Teilprozesse mit eingreift.

Diese umfassenden Dienstleistungen werden dabei nicht vollständig durch TNT Post selbst erbracht. Hierbei spielen die unterschiedlichsten Geschäftspartner in der Ausführung der Tätigkeiten eine bedeutende Rolle. TNT Post arbeitet mit Transportdienstleistern und Zustellpartnern und im Rahmen der Leistungserbringung auch mit verschiedenen Lettershops zusammen und koordiniert deren Abläufe. Der datenschutzrelevante Kernbereich liegt im Datenmanagement.

TNT Post bleibt gegenüber seinen Kunden verantwortlich im Leistungserbringungsprozess.

Ziel dieses Gutachtens ist es demnach, den Leistungserbringungsprozess unter Datenschutzordnungsmäßigkeitsgesichtspunkten zu bewerten. Hierzu werden die genannten Prozessschritte und deren Verknüpfungen untereinander sowohl von der technisch-organisatorischen Seite als auch aus rechtlicher Sicht beurteilt.

Basis der Begutachtung ist die im Wiki-Portal der TNT Post-Seite hinterlegte Dokumentation zum Leistungserbringungsprozess.

Der Teilprozess Redressen wird im Gutachten nicht berücksichtigt. Die Redressenbearbeitung

stellt einen in sich abgeschlossenen Prozess dar. Da dieser Prozess dem Grundsatz nach von der eigentlichen, kundenbezogenen Zustellung unabhängig ist und in Zusammenarbeit mit weiteren Partnern durchgeführt wird, muss eine Prüfung und Bewertung des Redressprozesses in seiner Gesamtheit separat stattfinden.
Der Redressprozess ist ein nachgeschalteter Prozess, der nicht benötigt wird, um die Zustellung durchzuführen. Vielmehr stellt er ein zusätzliches Angebot der TNT Post dar.

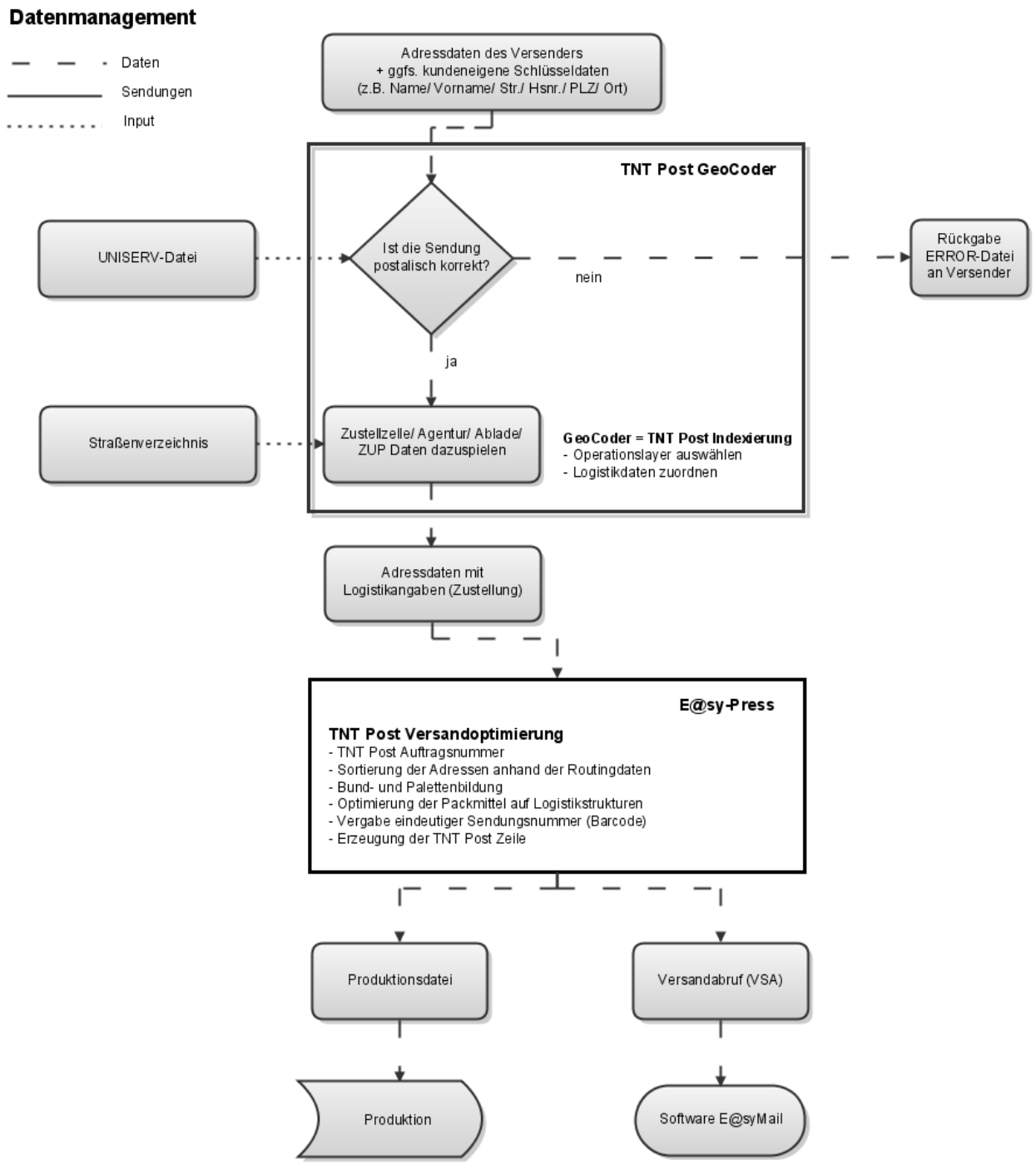
Damit bezieht sich das Gutachten auf die von TNT Post erbrachten Bestandteile der Prozessschritte:

- Datenmanagement
- Produktion/Sortierung
- Transport
- Zustellung

Damit setzt sich das begutachtete IT Produkt aus dem Leistungserbringungsprozess der TNT Post zusammen. Dieser wird unter anderem mit Hilfe von Software-Produkten realisiert. Die Softwareprodukte selbst sind nicht Zertifizierungsgegenstand, da sie als „Tools, die zur Herstellung des IT-Produktes verwendet wurden“ anzusehen sind.

Dieses Gutachten zum Rezertifizierungsprozess basiert auf dem Gutachten zum ursprünglichen Rezertifizierungsprozess 2009/2010, da das eigentliche Produkt/Verfahren nicht verändert wurde.
Im rechtlichen Teil des Gutachtens wird die Beziehung zwischen TNT Post und den Zustellpartnern nochmals ausführlicher betrachtet. Es wird eine Neubewertung aus rechtlicher Sicht auf Basis der aktuellen Interpretation der Zustellpartner als eigene Postdienstleister und nicht als Auftragsdatenverarbeiter für TNT Post durchgeführt.

Datenfluss


Datenmanagement
Daten
Sendungen
Input
Adressdaten des Versenders
+ ggfs. kundeneigene Schlüsseldaten
(z.B. Name/ Vorname/ Str./ Hsnr./ PLZ/ Ort)
TNT Post GeoCoder
UNISERV-Datei
Ist die Sendung postalisch korrekt?
nein
Rückgabe ERROR-Datei an Versender
ja
Straßenverzeichnis
Zustellzelle/ Agentur/ Ablade/ ZUP Daten dazuspielen
GeoCoder = TNT Post Indexierung
- Operationslayer auswählen
- Logistikdaten zuordnen
Adressdaten mit Logistikangaben (Zustellung)
E@sy-Press
TNT Post Versandoptimierung
- TNT Post Auftragsnummer
- Sortierung der Adressen anhand der Routingdaten
- Bund- und Palettenbildung
- Optimierung der Packmittel auf Logistikstrukturen
- Vergabe eindeutiger Sendungsnummer (Barcode)
- Erzeugung der TNT Post Zeile
Produktionsdatei
Versandabruf (VSA)
Produktion
Software E@syMail

Zweck und Einsatzbereich

Der Leistungserbringungsprozess der TNT Post dient der Vorbereitung von gegebenen/ vorhandenen Adressdaten, sowie der ordnungsgemäßen Beförderung von Postsendungen.

Normen und Gesetze, die der Prüfung zugrunde gelegt wurden

Bundesdatenschutzgesetz (BDSG)
Postdienste-Datenschutzverordnung (PDSV)
Postgesetz (PostG)
Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH)

Zusammenfassung der Prüfungsergebnisse

1 **Komplex 1:** Grundsätzliche technische Ausgestaltung von IT-Produkten

In Komplex 1 haben sich seit dem ersten Gutachten 2009/2010 keine Änderungen ergeben.
Der Leistungserbringungsprozess erfolgt im Sinne des § 4 LDSG SH unter Berücksichtigung der Datenvermeidung und Datensparsamkeit. Darüber hinaus werden personenbezogene Daten im Dateneingang, im Datenmanagement sowie im Datenausgang nach bestimmten Vorgaben gelöscht.
Die Produktionsdaten (Out-Datei, Error-Datei, No-Datei) werden TNT Post-seitig nach einer Woche gelöscht. Die durch den Kunden eingelieferten Originaldaten (VSA) in E@syMail eingelesen nach 4 Monaten gelöscht, da erfahrungsgemäß über diesen Zeitraum noch Rückfragen eingehen. Zu diesem Zeitpunkt werden auch den Namensbezug und die Hausnummern aus E@syMail gelöscht. Eine Komplettlöschung aus E@syMail erfolgt aus abrechnungstechnischen Gründen nach einem Jahr.
Die Vorgaben sind in einer Löschroutine als Arbeitsanweisung definiert. Durch den Einsatz der Löschroutinen wird gewährleistet, dass immer nur die Adressdaten der Versandempfänger vorgehalten werden, die zur Erfüllung der Aufgaben erforderlich sind.
Die Dokumentation wird in Form eines Wikis aufbewahrt und verwaltet.

2 **Komplex 2:** Zulässigkeit der Datenverarbeitung

Die Bewertung der Zulässigkeit der Datenverarbeitung hat sich nicht grundlegend geändert. Allerdings wird die rechtliche Einordnung zum Teil neu bewertet. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat sich als für TNT Post zuständige Aufsichtsbehörde zu der Frage des Vertragsverhältnisses zwischen TNT Post und den Zustellpartnern geäußert und die Ansicht vertreten, dass er die ZUP als eigenverantwortliche Postdienstleister bzw. als an der Erbringung von Postdienstleistungen Mitwirkende (vgl. § 1 Abs. 1 PDSV) ansehe. Demzufolge sei die Weitergabe der Daten (Briefe) von TNT Post an seine ZUP als Datenübermittlung zu qualifizieren. Aufgrund der Stellungnahme des BFDI, der Aufarbeitungen von Herrn Dr. Wronka für TNT Post, der rechtlichen Würdigung durch die UIMCert als Auditor und nicht zuletzt auf Wunsch von TNT Post wurde dieser Sachverhalt erneut thematisiert und die Bewertung des Vertragsverhältnisses zwischen TNT Post und den ZUP entsprechend der Bewertung der zuständigen Aufsichtsbehörde angepasst.

Die Datenverarbeitung erfolgt auf Basis und gemäß den Vorschriften der PDSV, des BDSG, LDSG SH und PostG. Da beispielsweise Adressdaten nur zur Erfüllung des Versandauftrags genutzt werden, ist die Zweckbindung sichergestellt. Die Umsetzung der gesetzlichen Anforderungen erfolgt durch geeignete technische und organisatorische Maßnahmen durchgehend adäquat bis vorbildlich. Hierunter fällt auch die Einhaltung der inhaltlichen Forderungen der DSVO, auch wenn die Dokumentation formal nicht an den Vorgaben der DSVO ausgerichtet ist.

3 **Komplex 3:** Technisch-organisatorische Maßnahmen: Begleitmaßnahmen zum Schutz der Betroffenen

Die eingesetzten beschriebenen technischen und organisatorischen Maßnahmen wurden nicht verändert und haben nach wie vor Gültigkeit. Änderungsnotwendigkeiten haben sich in den vergangenen zwei Jahren nicht ergeben.
Um einen datenschutzrechtlich ordnungsmäßigen Prozessablauf zu gewährleisten, setzt TNT Post eine Vielzahl an technischen und organisatorischen Maßnahmen ein. Darunter fallen der Einsatz eines Berechtigungskonzepts in Verbindung mit der Implementierung eines Passwortkonzepts (technisch und organisatorisch), der speziell gesicherte Zutritt zu Datenverarbeitungsanlagen und Logistik-Prozessen, sowie das TNT Post-seitige Angebot zur sicheren Datenanlieferung mittels sFTP und PGP-Verschlüsselung von und zu Kunden.
Das Berechtigungskonzept, besonders im Hinblick auf den Leistungserbringungsprozess, wurde neben der Vor-Ort-Prüfung 2010 auch im Rahmen einer ISO 27001 Zertifizierung und des 2011er Überwachungsaudits geprüft und anerkannt bzw. für normkonform befunden.

4 **Komplex 4:** Rechte der Betroffenen

Die Bewertung der Wahrung der Rechte der betroffenen Personen hat sich nicht geändert.
Betroffene im Rahmen des Leistungserbringungsprozesses sind im Wesentlichen die Adressaten der Postsendungen. Da TNT Post die personenbezogenen Daten der Empfänger von Postsendungen von den Kunden zum Zweck der eigenverantwortlichen Erledigung des Versandauftrags übermittelt werden, ist TNT Post als "verantwortliche Stelle" zur Wahrung der Rechte der Betroffenen verpflichtet, und zwar so lange, wie TNT Post über diese Daten verfügt, d.h. sie speichert.
Zur Sicherstellung der Rechte der Betroffenen wurde eine Verfahrenweise entwickelt, über die alle Mitarbeiter durch ein "Datenschutz-Merkblatt" unterrichtet wurden. Die Durchführung der Maßnahmen erfolgt im Einvernehmen mit dem betrieblichen Datenschutzbeauftragten.

5 Ergebniszusammenfassung

Das grundsätzliche Fazit enspricht dem von 2010. Ein ordnungsgemäßer Leistungserbringungsprozess der TNT Post, bestehend aus den betrachteten Prozessschritten Datenmanagement, Transport und Zustellung, muss die Ordnungsmäßigkeitskriterien des Datenschutzrechts erfüllen. Bei der Prüfung durch die UIMCert wurden sowohl die vertraglichen Bindungen zu den an den Prozessschritten beteiligten Dritten, als auch die technisch organisatorischen Maßnahmen, sowohl innerhalb der einzelnen Prozessschritte, als auch untereinander, geprüft und bewertet.

Wie aus den Einzelangaben der Prüfergebnisse ersichtlich, werden die Anforderungen von der rechtlichen Seite vorbildlich erfüllt. So finden auch aktuelle Gesetzesänderungen ebenso wie Anregungen des ULD Schleswig-Holstein oder rechtliche Würdigungen der Aufsichtsbehörde (BfDI) eine zeitnahe Berücksichtigung. Die vertraglichen Situationen sind im Hinblick auf die datenschutzrechtlichen Aspekte ebenfalls als vorbildlich zu bezeichnen. Die TNT Post beschäftigt sich intensiv mit der Thematik des Datenschutzes und der Einhaltung der entsprechenden Gesetze und holt im Bedarfsfall externe Gutachten ein.

Auch auf Seiten der technisch organisatorischen Maßnahmen ist die TNT Post adäquat positioniert. Die zu schützenden personenbezogenen Daten sind keine, die das Gesetz als besondere Arten personenbezogener Daten definiert und die damit besonders schützenswert wären. TNT Post verarbeitet ihm Rahmen ihrer Tätigkeiten Adressdaten. Eindeutige Berechtigungsstrukturen legen fest, wer auf diese personenbezogene Daten zugreifen darf und kann und wer nicht. Darüber hinaus sind viele Datenverarbeitungsprozesse dergestalt, dass ein Zugriff durch Personen nicht nötig und entsprechend nur eingeschränkt möglich ist.

In anderen Prozessschritten hingegen ist die Einsichtnahme von Daten entweder durch weitere technische oder organisatorische Maßnahmen unterbunden (z. B. geschlossene Transportcontainer) oder nicht notwendig. Die Zustellpartner beispielsweise müssen die Adressdaten einsehen, um sie zustellen zu können. In jedem Fall ist der zugriffsberechtigte Personenkreis auf die zur Aufgabenerfüllung notwendigen Personen eingeschränkt.

In Zukunft wird die Sicherheit besonders im Rahmen der Adresszuleitung durch die Kunden noch weiter erhöht. Im Allgemeinen wird dies durch den PDCA (Plan-Do-Check-Act)-Zyklus als Bestandteil eines Informationssicherheitsmanagementsystems erreicht. Eine entsprechende ISO27001 Zertifizierung erfolgte 2010,das Überwachungsaudit 2011 bestätigt das weiterhin normorientierte ISMS.

In der Summe zeigt sich, dass der Leistungserbringungsprozess der TNT Post datenschutz-

ordnungsgemäß organisiert ist und darüber hinaus aktuellen Gegebenheiten angepasst wird. Es wird empfohlen das Gütesiegel zu erteilen.

Sofern das Projekt/Produkt einen Teil der Anforderungen nur unzureichend erfüllt:
Beschreibung, wie dies ausgeglichen wird[1]

TNT Post bietet u. a. die Möglichkeit der Datenanlieferung durch Bastandskunden per FTP. Da es rein technisch dem Kunden obliegt, ob er die Daten verschlüsselt versendet, muss diese Art der Datenanlieferung als unsicher angesehen werden.
Ausgeglichen wird dies TNT Post-seitig dadurch, dass zum einen die Übertragung per sFTP ermöglicht wird und zum anderen dadurch, dass TNT Post ihre Kunden sowohl über die unsichere Datenanlieferung per FTP aufklärt, als auch die Verschlüsselung der Daten ausdrücklich empfiehlt. Der Umgang mit verschlüsselten Daten wird durch TNT Post unterstützt. Die Bereitstellung der Daten für Kunden erfolgt ausschließlich verschlüsselt.

Beschreibung, wie das Projekt/Produkt den Datenschutz oder die IT-Sicherheit fördert

Hoher Automatisierungsgrad
Die Verarbeitung der Daten im Bereich des Leistungserbringungsprozesses läuft weitestgehend automatisch ab. Durch den hohen Automatisierungsgrad ist eine Einsichtnahme in die Daten nur noch an sehr wenigen Stellen möglich. Durch die automatische Datenverarbeitung wird eine missbräuchliche Nutzung der personenbezogenen Daten sehr stark eingeschränkt.

Qualität der Organisationslösungen
Die gesamten Organisationslösungen zur Erfüllung des Kerngeschäfts der Postdienstleistung sind vorbildlich. Dies zeigt sich auch in der Dokumentation der einzelnen Prozesse sowie in den datenschutzrechtlich relevanten Organisationsanweisungen. Es herrscht ein hoher Sensibilisierungsgrad bei den Mitarbeitern und diese sind angewiesen, mögliche Vorfälle mit Datenschutzbezug sofort an die entsprechenden Stellen zu melden.

Überwachung und Kontrollen
Die durch die TNT Post getroffenen technischen, organisatorischen und rechtlichen Regelun-

[1] Die wertende Gesamtbetrachtung muss mit den Normen bzw. Gesetzen vereinbar sein.

gen werden überwacht und regelmäßig auf ihre Einhaltung hin kontrolliert. Die Überwachung der technischen Regelungen wird revisionssicher protokolliert. Diese Protokolle dienen als Grundlage für die Kontrolle der Einhaltung und damit der Wirksamkeit der entsprechenden Regelungen.
Die Zustellpartner werden von TNT Post Außendienstmitarbeitern betreut. Jeder der 9 Außendienstmitarbeiter betreut ca. 15 Zustellpartner. Die Außendienstler prüfen regelmäßig die Einhaltung der TNT Post Vorgaben.
Sobald hierbei Vorfälle bekannt werden, die den Datenschutz berühren, findet eine ausführliche Überprüfung des Sachverhalts durch TNT Post statt. Im Rahmen einer regelmäßigen Lieferantenbewertung führt die TNT Post auch regelmäßige Zustellpartner-Audits durch. Diese dauern 1-2 Tage an und werden anhand eines vorgegebenen strukturierten Interviews/Fragebogens und eines daraus folgenden Punktesystems durch die Gebietsleiter, die hierfür zu internen Auditoren weitergebildet wurden, durchgeführt. Im Laufe des Audits wird auch eine Begehung der Prozesse bei den zu auditierenden Zustellpartnern vorgenommen (z. B. Produktion/Sortierung, Zustellung etc.). Die ZUP-Audits finden je nach Größe, Umsatz und Bedeutung der ZUP in definierten Zeitintervallen zumeist einmal im Jahr statt. Mit Hilfe dieser Audits wird die Umsetzung der Vorgaben der TNT Post geprüft.

Unkritische personenbezogene Daten / keine sensiblen Daten
Im Leistungserbringungsprozess werden keine kritischen personenbezogenen Daten verarbeitet. Es werden lediglich Adressdaten benötigt, um die Aufgabe der Zustellung von Postsendungen zu erfüllen. Darüber hinaus werden keine Daten benötigt. Durch den sehr geringen Anteil an personenbezogenen Daten und den Verzicht auf die Erhebung weiterer personenbezogener Daten wird die Datensparsamkeit besonders gewährleistet.

Anreicherung der Adressdaten um Logistikinformationen ohne zusätzliche personenbezogene Daten
Es werden keinerlei personenbezogene Daten erhoben, welche nicht zwingend für die Erfüllung der Transportdienstleistung notwendig sind. Die Logistikinformationen, um welche die Adressdaten für eine effizientere Zustellung angereichert werden, enthalten keine personenbezogenen Daten.
Verschlossene Transportkisten
Die Sendungen werden bei jedem Transportvorgang in verschlossenen Transportbehältern

aufbewahrt. Nur zu Zwecken der Sortierung werden die Postsendungen den verschlossenen Behältern entnommen. Dadurch ist gewährleistet, dass Unbefugte keinen Einblick in die Adressdaten bekommen können. Insgesamt ist durch die geschlossene Logistikkette außer in besonderen Fällen keinerlei Sendung von außen einsehbar.

Wuppertal, den 02.10.2012

gez. H. Haaz

Prüfstellenleiter Dr. H. Haaz

gez. J. Schirrmacher

Sachverständiger J. Schirrmacher