Kurzgutachten

Zeitpunkt der Prüfung

Die Prüfung wurde im Zeitraum von Mai 2009 bis Juni 2010 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

Prof. Dr. Reinhard Voßbein

Name Auditor

Jens Schirrmacher
Timo Noll

Auditnummer UIMCert

F-116-01

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

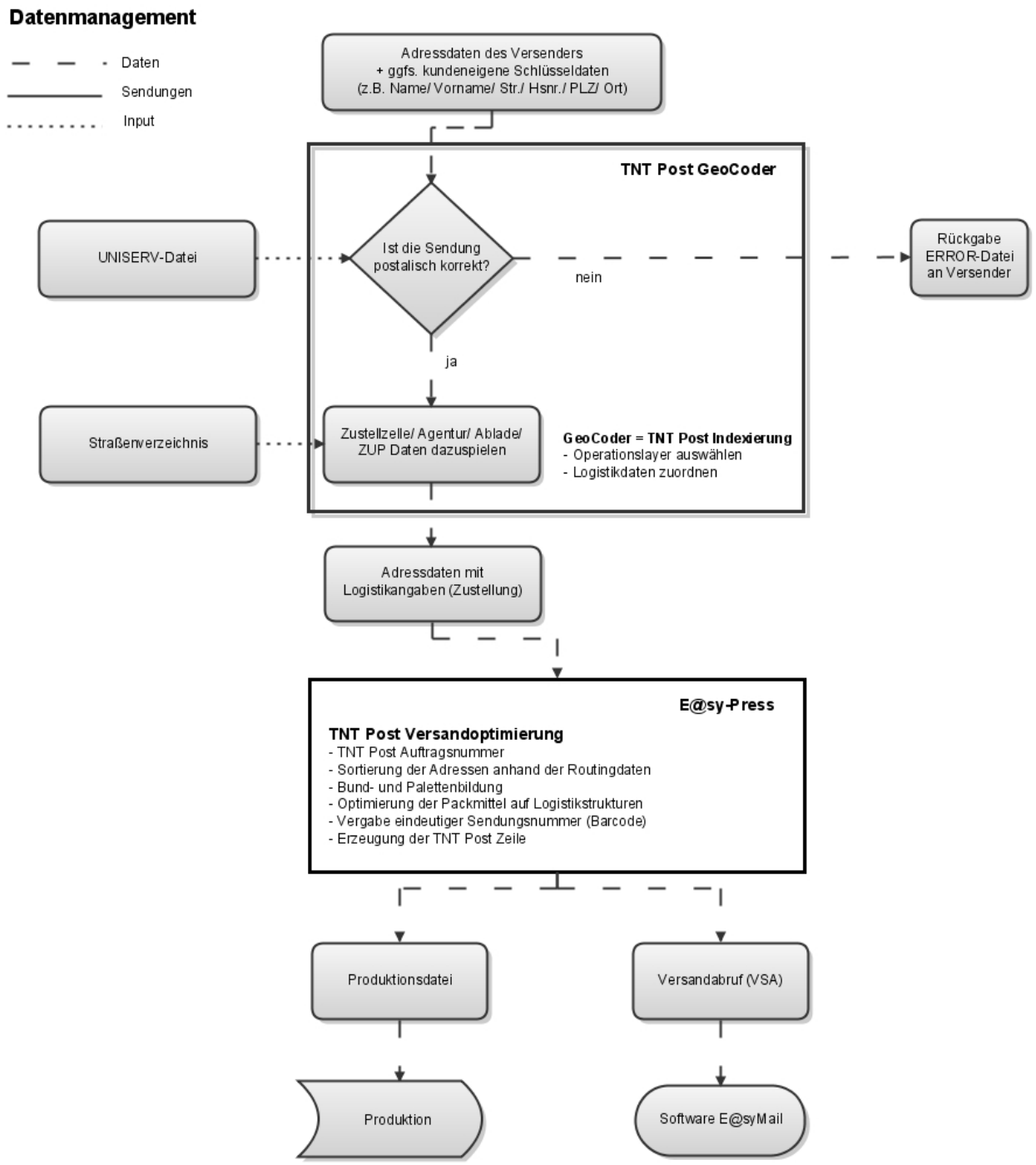
stellt einen in sich abgeschlossenen Prozess dar. Da dieser Prozess dem Grundsatz nach von der eigentlichen, kundenbezogenen Zustellung unabhängig ist und in Zusammenarbeit mit weiteren Partnern durchgeführt wird, muss eine Prüfung und Bewertung des Redressprozesses in seiner Gesamtheit separat stattfinden.
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.

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

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 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

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 Passwort-

konzepts (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.

4 **Komplex 4:** Rechte der Betroffenen

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

Ein ordnungsgemäßer Leistungserbringungsprozess der TNT Post, bestehend aus den betrachteten Prozessschritten Datenmanagement, Transport und Zustellung, muss die Ordnungsmäßigkeitskriterien der Datenschutzgesetzgebung 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 eine zeitnahe Berücksichtigung. Die vertraglichen Situationen sind im Hinblick auf die datenschutzrechtlichen Aspekte als vorbildlich zu bezeichnen. Einzige Ausnahme hierzu bilden die Zusatzverträge zur Auftragsdatenverarbeitung. Diese wurden erst nachträglich geschlossen.
Auch auf Seiten der technisch organisatorischen Maßnahmen ist die TNT Post adäquat positioniert. Bei den hier verarbeiteten personenbezogenen Daten handelt sich in der Regel nicht

um besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG. Die für besondere Arten personenbezogener Daten geltenden Sondervorschriften sind hier somit nicht einschlägig.
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 als Auftragsdatenverarbeiter eingebundenen Zustellpartner beispielsweise müssen die Adressdaten einsehen, um sie zustellen zu können. In jedem Falle 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. Die Datenanlieferung und Datenversendung sollen nur PGP-verschlüsselt erfolgen. TNT Post-seitig ist dies realisiert und ist in letzter Instanz vom jeweiligen Kunden abhängig.
In der Summe zeigt sich, dass der Leistungserbringungsprozess der TNT Post datenschutzordnungsgemäß 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 Kunden 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 zukünftig 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.

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

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 Regelungen 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. Es gibt 10 Betreuer der TNT Post für die Zustellpartner in der Fläche. Diese kontrollieren die Einhaltung der TNT Post Vorgaben im Tagesgeschäft. Bei Auffälligkeiten bzgl. der unzustellbaren Sendungen empfiehlt/ fordert TNT Post vom ZUP nach Abwägung der Umstände eine Kontrolle der Einhaltung des Datenschutzes durch sachverständige Dritte.

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 07.07.2010

Gez. R. Voßbein

Prüfstellenleiter Prof. Dr. R. Voßbein

Gez. J. Schirrmacher

Sachverständiger J. Schirrmacher