## Kurzgutachten

### Zeitpunkt der Prüfung

Die Prüfung wurde im Zeitraum von Dezember 2014 bis Februar 2016 durchgeführt.

### Adresse des Antragstellers

Postcon National 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, Timo Noll

### Auditnummer UIMCert

F-116-03

# 1 Kurzbezeichnung des IT-Produktes

Postcon bietet ihren Kunden umfangreiche Dienstleistungen im Zusammenhang mit der Beförderung von Briefsendungen an. Dieses Dienstleistungsangebot besteht aus zwei Kernelementen, nämlich

- der Prävention und
- der 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 Postcon selbst erbracht. Hierbei spielen die unterschiedlichsten Geschäftspartner in der Ausführung der Tätigkeiten eine bedeutende Rolle. Postcon 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.

Postcon 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 Postcon-Seite hinterlegte Dokumentation zum Leistungserbringungsprozess.

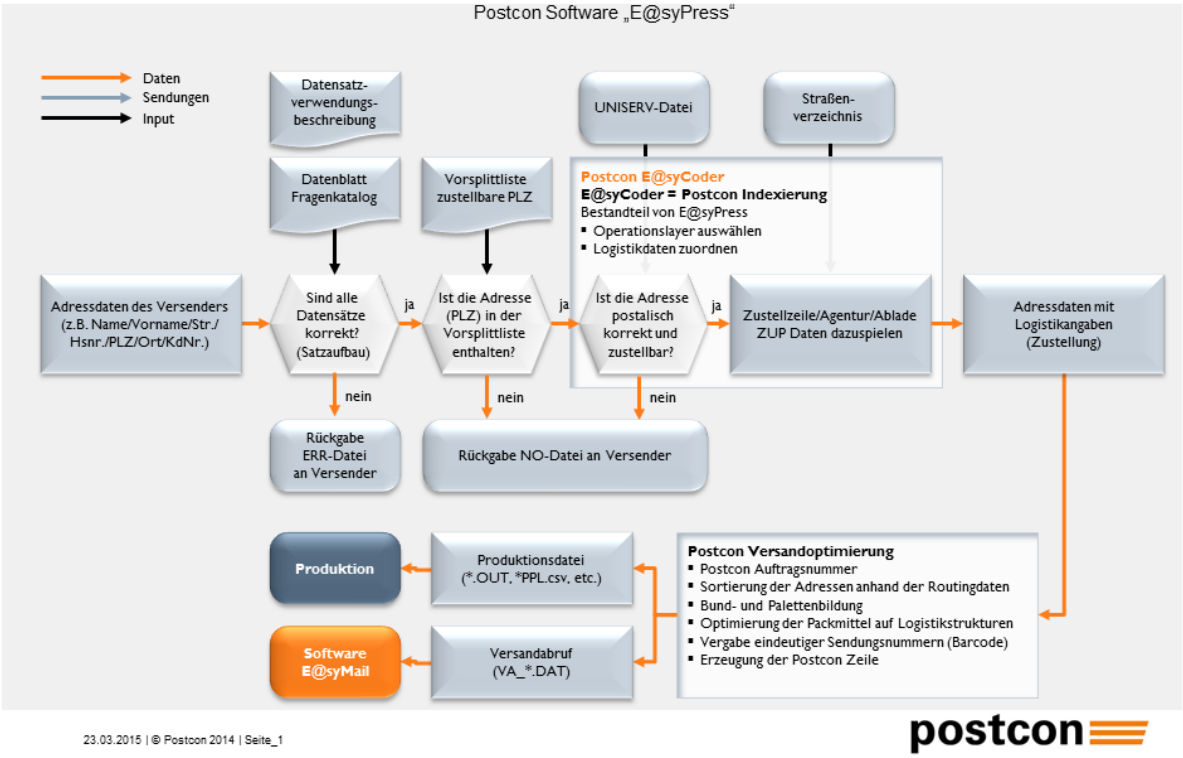
Der Teilprozess Redressen wird im Gutachten nicht berücksichtigt. Die Redressenbearbeitung stellt einen in sich abgeschlossenen Prozess dar. Da dieser Prozess dem Grundsatz nach von der eigentlichen, kundenbezogenen Zustellung unabhängig ist und in Zusammenarbeit mit weiteren Partnern durchgeführt wird, 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 von Postcon dar.

Das Gutachten bezieht sich auf die Prozessschritte:

- Datenmanagement
- Produktion/Sortierung
- Transport
- Zustellung

Damit setzt sich das begutachtete IT-Produkt aus dem Leistungserbringungsprozess von Postcon 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 den Gutachten zu den Audits aus 2009/2010 und 2012. Das von Postcon angebotene Verfahren wurde seit der Erstzertifizierung nicht wesentlich verändert. Wenngleich das überwiegende notwendige Softwarepaket gleich geblieben ist, gibt es Veränderungen bei der Adressvalidierung und eine Erweiterung des Labeldruckprogramms.
Darüber hinaus gibt es im Wesentlichen nur Softwareupdates.

## 2 Modellierung des Datenflusses




## 3 Zweck und Einsatzbereich

Der oben beschriebene Leistungserbringungsprozess von Postcon dient der Aufbereitung von Adressdaten zur Vorbereitung und Durchführung der ordnungsgemäßen Beförderung von Postsendungen.

## 4 Normen und Gesetze, die der Prüfung zugrunde gelegt wurden

Folgende Gesetze finden Anwendung:

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

# 5 Zusammenfassung der Prüfungsergebnisse

## 5.1 Komplex 1: Grundsätzliche technische Ausgestaltung von IT-Produkten

Die IT-Sicherheits- und Datenschutz-Schutzziele wie Verfügbarkeit, Integrität, Vertraulichkeit, Nicht-Verkettbarkeit, Transparenz und Intervenierbarkeit werden durch die Postcon GmbH durch umfangreiche Maßnahmen sowohl im technischen, wie auch im organisatorischen Bereich bis hin zu Sensibilisierung der Kunden und Dokumentation der eigenen Prozesse realisiert. Dabei erfolgt der Leistungserbringungsprozess im Sinne des § 4 LDSG SH unter Berücksichtigung der Datenvermeidung und Datensparsamkeit.

## 5.2 Komplex 2: Zulässigkeit der Datenverarbeitung

Die Bewertung der Zulässigkeit der Datenverarbeitung hat sich im Vergleich zu 2012 nicht geändert.
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.

## 5.3 Komplex 3: Technisch-organisatorische Maßnahmen

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 Postcon eine Vielzahl an technischen und organisatorischen Maßnahmen ein. Darunter fallen der Einsatz eines Berechtigungskonzepts in Verbindung mit der Implementierung eines Passwortkonzepts, der speziell gesicherte Zutritt zu Datenverarbeitungsanlagen und Logistik-Prozessen sowie die gesicherte Datenübertragung von und zu Kunden.

Das Berechtigungskonzept, besonders im Hinblick auf den Leistungserbringungsprozess, wurde im Rahmen einer ISO 27001 Zertifizierung geprüft und anerkannt bzw. für normkonform befunden.

### 5.4 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. Die Kunden (Versender) scheiden als Betroffene aus, da es sich fast ausnahmslos um juristische Personen des privaten oder öffentlichen Rechts handelt, auf die § 6 BDSG nicht anwendbar ist (§ 3 Abs. 1 BDSG).
Da Postcon die personenbezogenen Daten der Empfänger von Postsendungen von den Kunden zum Zweck der eigenverantwortlichen Erledigung des Versandauftrags übermittelt werden, ist Postcon als "verantwortliche Stelle" zur Wahrung der Rechte der Betroffenen verpflichtet, und zwar so lange, wie Postcon über diese Daten verfügt, d. h. sie speichert.
Über die Verfahrensweise bei der Geltendmachung von Betroffenenrechten sind alle Mitarbeiter durch ein "Datenschutz-Merkblatt" unterrichtet worden. Die Durchführung der Maßnahmen erfolgt im Einvernehmen mit dem betrieblichen Datenschutzbeauftragten.
Die Betroffenen können weiterhin ihre Rechte gegenüber den Kunden als weitere "verantwortliche Stelle" geltend machen. Die Abwicklung erfolgt über den Datenschutzbeauftragten.

## 6 Ergebniszusammenfassung

Das grundsätzliche Fazit entspricht dem von 2012/2013. Ein ordnungsgemäßer Leistungserbringungsprozess von Postcon, 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 in Hinblick auf die Schutzziele, 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) Berücksichtigung. Die vertraglichen Situationen sind im Hinblick auf die datenschutzrechtlichen Aspekte ebenfalls als vorbildlich zu bezeichnen. Postcon 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 Postcon adäquat positioniert. Die zu schützenden personenbezogenen Daten sind keine, die das Gesetz als besondere Arten personenbezogener Daten definiert und die damit besonders schützenswert wären.

Postcon verarbeitet im 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. Hierzu trägt auch die ISO/IEC 27001 Zertifizierung bei. Das Überwachungsaudit 2014 bestätigt das weiterhin normorientierte ISMS.

In der Summe zeigt sich, dass der Leistungserbringungsprozess von Postcon datenschutzordnungsgemäß organisiert ist und darüber hinaus aktuellen Gegebenheiten angepasst wird. Darüber hinaus trägt der Gütesiegelprozess zu einer stetigen Verbesserung der Umsetzung der Datenschutzanforderungen bei, wie in Kapitel 8 beschrieben wird.
Es wird empfohlen das Gütesiegel zu erteilen.

# 7 Sofern das Projekt/Produkt einen Teil der Anforderungen nur unzureichend erfüllt: Beschreibung, wie dies ausgeglichen wird

Postcon bietet die Möglichkeit der unsicheren Datenanlieferung durch Bestandskunden. Da es rein technisch dem Kunden obliegt, wie er Daten versendet/anliefert, hat Postcon nur begrenzt Einfluss auf die Datenanlieferung.
Sollte der Kunde ausdrücklich eine Rücksendung der Daten (Out-Datei) auch auf unsicherem Wege fordern, würde sich Postcon dem beugen.
Postcon klärt seine Kunden über die unsicheren Datenanlieferungsmethoden, wie beispielsweise „E-Mail“ und die damit verbundenen Risiken auf. Seit Erteilung des ursprünglichen ULD-Gütesiegels, macht sich diese Aufklärungsarbeit bezahlt, da mittlerweile 95% der Kunden (und 98% des Datenvolumens) per sFTP angeliefert werden und so die fragewürdige Anlieferung der Daten per E-Mail keine nennenswerte Rolle mehr spielt.
Weiterhin werden derzeit administrative Tätigkeiten ausschließlich manuell protokolliert. Dies soll im laufe des Jahres 2016 geändert werden.
Es seitens Postcon aktuell (Mai 2016) ein Projekt zur finalen Auswahl einer geeigneten Protokollierungssoftware aufgesetzt worden. Es ist geplant, dass die Auswahl und Implementierung Ende August 2016 abgeschlossen sein wird.

# 8 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 Postcon 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.

Die Zustellpartner werden von Postcon-Außendienstmitarbeitern betreut. Jeder der 9 Außendienstmitarbeiter betreut ca. 15 Zustellpartner. Die Außendienstler prüfen regelmäßig die Einhaltung der Postcon Vorgaben.

Sobald hierbei Vorfälle bekannt werden, die den Datenschutz berühren, findet eine ausführliche Überprüfung des Sachverhalts durch Postcon statt. Im Rahmen einer regelmäßigen Lieferantenbewertung führt Postcon 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 Postcon geprüft.
Darüber hinaus ist die Aufrechterhaltung der ISO 27001 Zertifizierung nennenswert, das Informationssicherheitsmanagementsystem einhergeht mit sicherheitsrelevanten und letztlich auch datenschutzrelevanten Anforderungen.

**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 04.07.2016

gez. H. Haaz

Prüfstellenleiter Dr. H. Haaz

gez. T. Noll

Sachverständiger T. Noll

gez. J. Schirrmacher

Sachverständiger J. Schirrmacher