Kurzgutachten zum ADCERT Datenschutzsiegel für NEXELLENT 3.0 der Deutschen Post AG

1 Allgemeine Beschreibung

Die **Deutsche Post AG** hat für das implementierte Datenschutzmanagementsystem im Rahmen des Markierungsverfahrens „NEXELLENT 3.0" bei der ADCERT Privacy Audit GmbH am 09.05.2016 eine **Cross-Zertifizierung** gemäß aktuell gültigem ADCERT Kriterienkatalog („ADCERT Criteria catalogue for privacy management systems" in der Version 1.0 vom 07.10.2016) beantragt und erteilt bekommen. Eine Cross-Zertifizierung setzt voraus, dass die zuvor bestehende Zertifizierung ausreichend Gewähr zur Datenschutzkonformität bietet und dass im Folgejahr ein Vollaudit nach dem ADCERT Kriterienkatalog erfolgreich absolviert wird. Sofern der Antragsteller dabei keine Hauptabweichung aufweist, wird mit dem Datum des Exit Meetings ein Zertifikat erteilt.

Als unabhängiger **Auditor** für Recht und Technik wurde in diesem Zertifizierungsverfahren Herr Dipl.-Inf. **Bernhard C. Witt** eingesetzt. Dieser ist

- Senior Consultant für Datenschutz und Informationssicherheit bei der it.sec GmbH & Co. KG seit 2005
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- zertifizierter ISO/IEC 27001 Lead Auditor (BSi)
- Certified in Risk and Information Systems Control (CRISC; ISACA)
- Prüfer für § 8a Abs. 3 BSIG mit zusätzlicher Prüfverfahrenskompetenz (AUDEG)
- Lehrbeauftragter für Datenschutz und IT-Sicherheit an der Universität Ulm (seit 2005)
- Autor der Bücher "IT-Sicherheit kompakt und verständlich" (2006) und "Datenschutz kompakt und verständlich" (2008 & 2010)
- Mitglied im DIN-Arbeitsausschuss "IT-Sicherheitsverfahren" (AK 1 & 4, seit 2011)

- Mitglied im Leitungsgremium der GI-Fachgruppe "Datenschutzfördernde Technik" (seit 2012)
- Mitglied im Leitungsgremium der GI-Fachgruppe "Management von Informationssicherheit" (seit 2007; als Sprecher von 02/2009 bis 11/2013)
- Mitglied im Leitungsgremium des GI-Fachbereichs "Sicherheit - Schutz und Zuverlässigkeit" (seit 2009; als Sprecher seit 11/2016)

Das **Vollaudit** wurde zu NEXELLENT 3.0 in zwei Stufen wie folgt durchgeführt:

- Stage-1-Audit (Dokumentenreview und Prüfung der Zertifizierungseignung): 4. – 6. Juli 2017 in den Räumen der Deutschen Post AG
- Stage-2-Audit (Wirksamkeitsprüfung): 21. – 25. August 2017 in den Räumen der Deutschen Post AG, der Deutschen Post Dialog Solutions GmbH und der Deutschen Post Direkt GmbH

Im Rahmen des Vollaudits wurde dem Antragsteller, Deutsche Post AG, vom Auditor für Recht und Technik attestiert, das ein **ausreichend wirksames Datenschutzmanagementsystem** für das Markierungsverfahren von NEXELLENT 3.0 **implementiert** wurde, welches insbesondere die Vorgaben aus dem EU-Datenschutzrecht erfüllt.

Von den 121 im Anhang A aufgelisteten Maßnahmen wurde durch den Antragsteller lediglich die Maßnahme A.3.1 zur Mobile Device Richtlinie mit folgender Begründung ausgeschlossen: Im Bereich des Markierungsverfahrens werden keine Handys / Mobile Devices genutzt. Es gibt keine Schnittstelle im Markierungsverfahren und/oder im Nexellent System, die mit diesen Geräten angesprochen werden können.

Das erteilte ADCERT Datenschutzsiegel ist für zwei Jahre bis zum 24. August 2019 gültig.

2 Detaillierte Angaben zum Zertifikat

Name des Verfahrens: NEXELLENT 3.0

Zertifikatsnummer: 012-01-01

Gültig bis: August 2019

Antragsteller: Deutsche Post AG, Zentrale, Geschäftsbereich 33 – Produktmanagement Dialogmarketing und Presse, Charles-de-Gaulle-Straße 20, 53113 Bonn

3 Beschreibung des Verfahrens

Gegenstand des zertifizierten Verfahrens ist die Markierung eines Nutzers, welches für die Use Cases, die nicht Gegenstand der Zertifizierung sind, benötigt wird. Relevant sind dabei die folgenden Prozessschritte (im Überblick):

- Der Login des Users auf einer Webseite eines angeschlossenen Adressmatchingpartners (AMP), der zwei parallel ablaufende Prozesse auslöst:
    - Der Weiterleitung der Anschrift des Users an die 3rd Party zum Abgleich mit der Mikrozellen-Datenbank der DP Direkt. Gleich zu Beginn dieses Abschnittes erstellt der AMP (sollte er das nicht wollen/können hilfsweise die 3rd Party) eine Vorgangs-ID, die für das spätere Zusammenführen der Daten benötigt wird.
    - Anfrage bei der 4th Party mit dem Ziel, ein Consentric Cookie und, soweit dies vom AMP erlaubt wurde, Cookies weiterer Trackingpartner im Browser des Nutzers zu setzen. Auch hierbei werden Vorgangs-IDs zur späteren Zusammenführung der Daten verwendet.
- In einem nachgelagerten Prozess melden die Trackingpartner (sofern sie an der Markierung beteiligt waren) ihre Cookies-IDs an die 3rd Party. Zur Zuordnung wird dabei

die Vorgangs-ID mit übertragen. In NEXELLENT 3.0 werden diese als „Partner-Cookies" bezeichnet.

- Ein Nutzer, der durch dieses Verfahren „markiert" wurde, wird im System durch ein eindeutiges „Token" repräsentiert. Jedem Token ist zudem für jeden beteiligten Trackingpartner ein PartnerToken zugeordnet.
- Die 3rd Party speichert eine Referenzdatei für weitergehende Datenabgleiche zwischen Token und Mikrozelle. Außerdem wird eine Zuordnung von Partner-Cookies und PartnerToken gespeichert.
- Bei der 4th Party wird die Zuordnung zwischen Token und PartnerToken abgelegt. Außerdem die Zuordnung von Consentric-Cookie und Token.
- Die Vorgangs-IDs werden nach Abschluss des Verfahrens nicht mehr benötigt und aus allen Systemen gelöscht.

4 Gegenstand der Zertifizierung

Gegenstand des Verfahrens ist ein System zur Übertragung der Strukturelemente der Mikrozellendatenbank der Deutschen Post Direkt GmbH (DP Direkt) in das Internet. Die Reaktion einer Mikrozelle im Internet auf die Zusendung eines postalischen Werbeschreibens kann durch dieses Messverfahren aufgezeigt werden. Der zertifizierte Teilbereich umfasst die Markierung eines Users, welche Voraussetzung für das anschließende Messverfahren ist.

5 Bewertungen im Rahmen der Zertifizierung

Im Rahmen von NEXELLENT 3.0 ist durchgängig das Prinzip der sog. „informationellen Gewaltenteilung" implementiert, d.h. die einzelnen Dienstleister, die zur Abwicklung dieses Verfahrens eingesetzt werden, verfügen nur über ein begrenztes Wissen hinsichtlich der zu

verwendenden Daten. Keine Stelle ist dabei dazu in der Lage, sämtliche Daten zusammenzuführen und gespeicherte Daten für ein umfassendes Persönlichkeitsprofil einsetzen zu können.

Anstelle personenbezogener Daten werden in diesem Verfahren anhand der vom Adressmatchingpartner stammenden Adressen sog. Mikrozellen verwendet, für die mind. fünf Adressen aggregiert werden. Auf diese Weise lässt sich im Markierungsverfahren kein Personenbezug mehr feststellen. Das angewendete Messverfahren selbst basiert auf einer reinen Maschine-zu-Maschine-Kommunikation. In NEXELLENT 3.0 wird insoweit das Prinzip der Datenminimierung unter frühzeitiger Entfernung personenidentifizierender Angaben als auch das Prinzip „Datenschutz by Design" konsequent anwendet.

Durch entsprechende Vorlagen für Vereinbarungen, die mit Adressmatchingpartnern getroffen werden, welche am Verfahren NEXELLENT 3.0 partizipieren möchten, ist sichergestellt, dass an der Stelle, in denen es eingangs noch einen Personenbezug geben kann, das Prinzip der Rechtmäßigkeit und das Prinzip der Transparenz gewahrt wird.

Zum Schutz der verarbeiteten Daten wurde bei der Deutschen Post AG ein umfassendes und ausreichend wirksames Datenschutzmanagementsystem eingerichtet, welches nachweislich die aktuell bestehenden Anforderungen an Datenschutz und Datensicherheit im Einklang mit dem diesem Audit zugrunde liegenden ADCERT Kriterienkatalog berücksichtigt. Im Rahmen der durchgeführten Prüfungen, sowohl bei der Deutschen Post AG, als auch bei den eingesetzten Auftragsverarbeitern, konnte keine Hauptabweichung gegenüber dem ADCERT Kriterienkatalog festgestellt werden. Die von den beteiligten Stellen implementierten Maßnahmen gewährleisten insoweit einen ausreichenden Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Für das Verfahren NEXELLENT 3.0 wurde bei der Deutschen Post AG eine Datenschutz-Folgenabschätzung unter Berücksichtigung der Kritikalität der Daten durchgeführt sowie geeignete, ausreichend wirksame und dem Stand der Technik genügend entsprechende technische und organisatorische Maßnahmen festgelegt und implementiert, so dass nach derzeitigem Sachstand kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zu erwarten ist.

Das implementierte Datenschutzmanagementsystem stellt darüber hinaus sicher, dass jedes ggf. beibehaltene Risiko wohlbegründet ist und regelmäßig einer erneuten Überprüfung unterzogen wird, ob es weiterhin beibehalten werden kann.

Das Verfahren NEXELLENT 3.0 berücksichtigt insoweit nicht nur Anforderungen aus der Datenschutz-Richtlinie der EU, sondern auch bereits die Anforderungen aus der Datenschutz-Grundverordnung.

Berlin, den 12.10.2017

gez.

Holger Heimann

(Geschäftsführer der ADCERT Privacy Audit GmbH)