Kurzgutachten zum ADCERT Datenschutzsiegel für NEXELLENT 4 der Deutschen Post AG

1 Allgemeine Beschreibung

Die **Deutsche Post AG** hat für das Markierungsverfahren „NEXELLENT 4“ bei der ADCERT Privacy Audit GmbH am 28.05.2019 die **Re-Zertifizierung** gemäß aktuell gültigem ADCERT Kriterienkatalog („ADCERT Criteria Catalogue for Privacy Preserving Processes and/or Products“ in der Version 2.0 vom 13.05.2019) beantragt.

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

- Principal 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)
- Co-Autor der Bücher "Managementsysteme für Informationssicherheit (ISMS) mit DIN EN ISO/IEC 27001 betreiben und verbessern" (2018) und "Formularhandbuch Datenschutzrecht", 2. Auflage (2018)
- 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 **Re-Zertifizierungs-Audit** wurde zu NEXELLENT 4 vom 27. bis 30. August 2019 in den Räumen der Deutschen Post AG, der Deutschen Post Direkt GmbH und der SEVEN PRINCIPLES AG durchgeführt.

Im Rahmen des Re-Zertifizierungs-Audits wurde dem Antragsteller, Deutsche Post AG, vom Auditor für Recht und Technik attestiert, dass für das Markierungsverfahren von NEXELLENT 4 **die Privatheit wirksam erhaltende Prozesse implementiert** wurden, welche insbesondere die Vorgaben aus dem EU-Datenschutzrecht erfüllen.

Von den 125 im Anhang A aufgelisteten Maßnahmen wurde durch den Antragsteller lediglich folgende Maßnahmen mit folgender Begründung ausgeschlossen:

- Maßnahme A.3.1 zur Mobile Device Richtlinie: Im Bereich der Administration des Markierungsverfahrens werden keine Handys / Mobile Devices genutzt. Es gibt keine administrativen Schnittstellen im Markierungsverfahren und/oder im Nexellent System, die mit diesen Geräten angesprochen werden.
- Maßnahme A.5.1.2 zu Werten außerhalb der EU: Im Bereich des Markierungsverfahren findet keine Datenverarbeitung außerhalb der EU statt.

Gegenüber dem Zertifizierungsgegenstand „NEXELLENT 3.0“ aus 2017 gab es 2019 folgende Änderungen:

- Aufgabe des selbst gestellten Datenschutzziels der informationellen Gewaltenteilung, um einen kosteneffizienteren Betrieb zu ermöglichen
- Wechsel in der System-Architektur hin zu Microservices
- Entwicklung und Betrieb nach dem DevOps-Verfahren
- Abschaltung der ursprünglich genutzten AWS Cloud Infrastruktur

Diese Änderungen beeinträchtigen nicht die Gültigkeit und Aussagekraft des erteilten ADCERT Datenschutzsiegels nach Ansicht des Auditors für Recht und Technik. Im Rahmen der durchgeführten Audits wurde ausdrücklich überprüft, ob ein angemessenes Schutzniveau gemäß ADCERT Kriterienkatalog erreicht wird, mit dem zugleich unbegründete die Privatheit gefährdende Risiken nachweislich vermieden werden.

Das erteilte ADCERT Datenschutzsiegel ist für zwei Jahre bis zum 30. August 2021 gültig.

2 Detaillierte Angaben zum Zertifikat

Name des Verfahrens: NEXELLENT 4
Zertifikatsnummer: 012-01-01
Gültig bis: August 2021
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 Third 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 Third Party) eine Vorgangs-ID, die für das spätere Zusammenführen der Daten benötigt wird.
    - Anfrage beim HUB 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 den Tokenstore. Zur Zuordnung wird dabei die Vorgangs-ID mit übertragen. In NEXELLENT 4 werden diese als „Partner-Cookies“ bezeichnet.
- Ein Nutzer, der durch dieses Verfahren „markiert“ wurde, wird im System durch ein eindeutiges „Token“ repräsentiert. Mit dem Token sind die weiteren im HUB vorgehaltenen Kennziffern verknüpft.
- 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

Anstelle personenbezogener Daten werden im Verfahren NEXELLENT 4 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 4 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 4 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.

Für das Verfahren NEXELLENT 4 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 nachweislich implementiert, so dass nach derzeitigem Sachstand bei diesem Verfahren kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zu erwarten ist.

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. Die eingerichteten Prozesse gewährleisten in ausreichender Weise, dass die Privatheit in Form der informationellen Selbstbestimmung durchgängig erhalten bleibt. Im Zuge des implementierten Risikomanagements wird bei NEXELLENT 4 sogar ein höheres Schutzniveau erreicht, als dies nach eigenen Vorgaben nötig wäre.

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.

Das implementierte Datenschutzmanagementsystem, das zur Steuerung der die Privatheit erhaltenden Prozesse eingesetzt wird, 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 4 berücksichtigt insoweit vollumfänglich die Anforderungen aus der Datenschutz-Grundverordnung.

Berlin, den 29.03.2020

gez.
Holger Heimann
(Geschäftsführer der ADCERT Privacy Audit GmbH)

Erstellt durch:	Erstellt am:	Letzte Änderung:	Version:	Review durch:	Freigabe durch:
Bernhard C. Witt	25.10.2019	29.03.2020	0.1	Holger Heimann	Holger Heimann
				Status: Freigegeben	