

Vorbewertung
gemäß
Trusted Cloud Datenschutzprofil Version 0.9
für
IDGARD der Uniscon GmbH

Version: 1.0
Dateiname: IDGARD_Vorbewertung_TCDP_V1.0

Prüfgegenstand IDGARD, Version 5.2

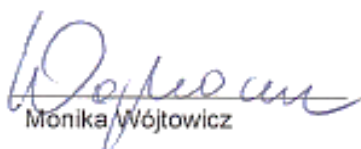
Anbieter Uniscon GmbH
Agnes-Pockels-Bogen 1
80992 München

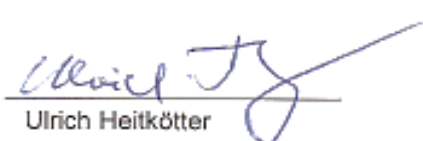
Prüforganisation: TÜV Informationstechnik GmbH
Prüfstelle für Datenschutz
Langemarckstraße 20
45141 Essen

Gutachter: Monika Wójtowicz, Ulrich Heitkötter

**Leiterin der Prüfstelle
(Recht):** Monika Wójtowicz

Datum: 05.06.2015


Monika Wójtowicz


Ulrich Heitkötter

1 Gesamtergebnis

Nach der durchgeführten Prüfung – gestützt auf die vorgelegten Dokumente, die geführten Gespräche, die Informationen und die weiteren von den verantwortlichen Mitarbeitern der Uniscon GmbH gemachten Angaben, die in den Abschnitten 4.6 bis 4.8 zusammengefasst wurden – sind die Auditoren zu dem Ergebnis gelangt, dass die Anforderungen des Trusted Cloud Datenschutzprofil (TCDP) Version 0.9 durch den Dienst IDGARD, Version 5.2, unter Berücksichtigung der ausgesprochenen Empfehlung (vgl. Abschnitt 4.4) als erfüllt anzusehen sind.

Damit entspricht der Dienst den gesetzlichen Anforderungen an die Datenverarbeitung im Auftrag i.S.d. § 11 BDSG, wie sie im TCDP, Version 0.9, konkretisiert wurden.

Der Schutz der Daten vor Verletzung der Vertraulichkeit und der Integrität entspricht der

TCDP-Schutzklasse III.

Der Schutz der Verfügbarkeit entspricht der

TCDP-Schutzklasse II.

Der Dienst IDGARD kann demnach für Daten mit dem Schutzbedarf I, II und III gemäß der Schutzbedarfsklassenbildung aus dem Arbeitspapier *Schutzklassen in der Datenschutz-Zertifizierung*¹ des Pilotprojekts Datenschutz-Zertifizierung von Cloud-Diensten des BMWi genutzt werden.

¹ Im Internet unter: http://www.trusted-cloud.de/media/content/150402_Arbpapier_Nr_9_Schutzklassen_Datenschutz_gesamt_RZ_Ansicht_EZ.pdf

2 Inhalt

1	GESAMTERGEBNIS	2
2	INHALT	3
3	ALLGEMEINES	6
3.1	Einleitung	6
3.2	Ziel und Charakter der Vorbewertung	8
3.3	Kurzbeschreibung des Prüfgegenstands	8
3.3.1	Netzplan	9
3.3.2	Referenzierte Dokumente	9
4	ZUSAMMENFASSUNG DER PRÜFERGEBNISSE	10
4.1	Gesamtergebnis	10
4.2	Auflagen, Empfehlungen, Hinweise	11
4.2.1	Begriffe Auflage – Empfehlung – Hinweis	11
4.2.1.1	Auflage	11
4.2.1.2	Empfehlung	11
4.2.1.3	Hinweis	11
4.3	Auflagen	11
4.4	Empfehlungen	11
4.5	Hinweise	11
4.6	Vertragliche Regelung der Auftragsdatenverarbeitung	12
4.6.1	TCDP Nr. 1 – Vertragliche Grundlage	12
4.6.2	TCDP Nr. 1.1 – Dienstleistung aufgrund eines Vertrags	12
4.6.2.1	Anforderung	12
4.6.3	TCDP Nr. 1.2 – Form des Vertrags	12
4.6.3.1	Anforderung	12
4.6.4	TCDP Nr. 1.3 – Gegenstand und Dauer des Auftrags	13
4.6.4.1	Anforderung	13
4.6.5	TCDP Nr. 1.4 – Art und Zweck der Datenverarbeitung	14
4.6.5.1	Anforderung	14
4.6.6	TCDP Nr. 1.5 – Technische und organisatorische Maßnahmen	14
4.6.6.1	Anforderung	14
4.6.7	TCDP Nr. 1.6 – Berichtigung, Löschung und Sperrung von Daten	15
4.6.7.1	Anforderung	15
4.6.8	TCDP Nr. 1.7 – Pflichten des Cloud-Anbieters	16
4.6.8.1	Anforderung	16
4.6.9	TCDP Nr. 1.8 – Unterauftragnehmer	16

4.6.9.1	Anforderung	16
4.6.10	TCDP Nr. 1.9 – Kontrollrechte des Cloud-Nutzers	17
4.6.10.1	Anforderung	17
4.6.11	TCDP Nr. 1.10 – Mitteilung bei Verstößen	17
4.6.11.1	Anforderung	17
4.6.12	TCDP Nr. 1.11 – Weisungsbefugnisse des Cloud-Nutzers	17
4.6.12.1	Anforderung	17
4.6.13	TCDP Nr. 1.12 – Rückgabe und Löschung von Daten	18
4.6.13.1	Anforderung	18
4.7	Verhältnis zwischen Cloud-Anbieter und Cloud-Nutzer	19
4.7.1	TCDP Nr. 2 – Weisungsgebundenheit des Cloud-Anbieters	19
4.7.1.1	Anforderung	19
4.7.2	TCDP Nr. 3 – Remonstrationspflicht	20
4.7.2.1	Anforderung	20
4.7.3	TCDP Nr. 4 – Unterauftragnehmer	20
4.7.3.1	Erläuterung	20
4.7.4	TCDP Nr. 4.1 – Grundlage der Einschaltung von Unterauftragnehmern	21
4.7.4.1	Anforderung	21
4.7.5	TCDP Nr. 4.2 – Information des Cloud-Nutzers	21
4.7.5.1	Anforderung	21
4.7.6	TCDP Nr. 4.3 – Vertragliche Grundlage der Unterbeauftragung	22
4.7.6.1	Anforderung	22
4.7.7	TCDP Nr. 4.4 – Auswahl und Kontrolle der Unterauftragnehmer	23
4.7.7.1	Anforderung	23
4.7.8	TCDP Nr. 4.5 – Weisungen des Cloud-Nutzers	23
4.7.8.1	Anforderung	23
4.7.9	TCDP Nr. 5 – Betrieblicher Datenschutzbeauftragter und gesetzliche Anforderungen	24
4.7.9.1	Anforderung	24
4.7.10	TCDP Nr. 6 – Berichtigung, Löschung, Sperrung von Daten	25
4.7.10.1	Anforderung	25
4.7.11	TCDP Nr. 7 – Mitteilungspflicht bei Datenschutzverstößen	26
4.7.11.1	Anforderung	26
4.7.12	TCDP Nr. 8 – Unterstützung der Kontrollen durch den Cloud-Nutzer	26
4.7.12.1	Anforderung	26
4.7.13	TCDP Nr. 9 – Rückgabe und Löschung von Daten	27
4.7.13.1	Anforderung	27
4.7.14	TCDP Nr. 10 – Datengeheimnis	27
4.7.14.1	Anforderung	27
4.8	Technische und organisatorische Maßnahmen	29
4.8.1	TCDP Nr. 21 – Sicherheitsbereich und Zutrittskontrolle	29
4.8.1.1	Anforderung	29

4.8.2	TCDP Nr. 22 – Logischer Zugang zu Datenverarbeitungsanlagen und Zugriff auf Daten	29
4.8.2.1	Anforderung	29
4.8.2.2	Technische Stellungnahme zur Bewertung der Einhaltung der TCDP Nr. 22 des durch IDGARD	31
4.8.3	TCDP Nr. 23 – Übertragung und Speicherung von Daten	31
4.8.3.1	Anforderung	31
4.8.4	TCDP Nr. 24 – Nachvollziehbarkeit der Datenverarbeitung	32
4.8.4.1	Anforderung	32
4.8.5	TCDP Nr. 25 – Auftragskontrolle	33
4.8.5.1	Anforderung	33
4.8.6	TCDP Nr. 26 – Verfügbarkeit von Daten	33
4.8.6.1	Anforderung	33
4.8.7	TCDP Nr. 27 – Getrennte Verarbeitung	34
4.8.7.1	Anforderung	34
4.8.8	TCDP Nr. 28 – Kryptographie	34
4.8.8.1	Anforderung	34
4.9	Konventionen	36

Tabellen

Tabelle 1: Für den Bericht verwendete Dokumente	10
---	----

Abbildungen

Abbildung 1: Verhältnis der Normen	7
Abbildung 2: Scope der Vorbewertung	8
Abbildung 2: Netzplan	9

3 Allgemeines

3.1 Einleitung

Die Uniscon GmbH² betreibt mit Ihrem Web Privacy Service IDGARD³ einen Dienst, der gemäß seiner Konzeption und auf Grund einer neuartigen Basistechnologie (Sealed Cloud) eine betreibersichere Datenverarbeitung im Internet bieten soll.

Die Uniscon will gegenüber ihren Kunden und Geschäftspartnern einen Nachweis darüber erbringen, dass sie mit IDGARD die Anforderungen des TCDP (Trusted Cloud Data Protection Profile), Version 0.9⁴, an die rechtskonformen Cloud-Dienste erfüllt.

Das TDCP wurde im Rahmen des Pilotprojekts Datenschutzzertifizierung von Cloud-Diensten des Bundeswirtschaftsministeriums erarbeitet. Bei TCDP handelt es sich um einen Kriterienkatalog, der die datenschutzrechtlichen Anforderungen des Bundesdatenschutzgesetzes an Cloud-Dienste konkretisiert und die Umsetzungsempfehlungen des internationalen Standards ISO/IEC 27018: 2014 zur sicheren und datenschutzkonformen Umsetzung von Cloud-Diensten zu verpflichtenden Anforderungen des TCDP macht.

Dieser Katalog definiert drei Schutzklassen für unterschiedliche Schutzbedarfe der Anwender und ordnet die Umsetzungsempfehlungen des genannten Standards (ISO/IEC 27018:2014) entsprechend den Anforderungen des Bundesdatenschutzgesetzes zur Erreichung des für die definierten Schutzklassen erforderlichen Sicherheitsniveaus zu. Das TCDP erweitert den Anforderungskatalog, wo dies zur Abdeckung der gesetzlichen Normen erforderlich ist.

² Im Folgenden Uniscon oder Anbieter genannt.

³ Im Folgenden „IDGARD“ genannt.

⁴ Im Folgenden „TCDP“ genannt.