Short Public Report

1 Name und Version des IT-basierten Service

Europäische Meldeauskunft RISER
(im Weiteren als „RISER-Dienst“ bezeichnet, Version: Februar 2013)

2 Entwickler oder Betreiber des IT-basierten Service

Firmenname:
RISER ID Services GmbH
Adresse:
Charlottenstraße 79/80
10117 Berlin (DE)
Kontaktpersonen:
Hendrik Tamm

3 Zeitrahmen der Evaluation

Januar bis Mai 2013 sowie
Mai 2013 bis Februar 2014

4 EuroPriSe Expert der den IT-basierten Service evaluiert hat

Name des Experten (rechtlich/technisch):
Prof. Dr. Friedrich Holl
Adresse:
Hektorstraße 7
10711 Berlin

5 Zertifizierungsstelle

Name:
EuroPriSe Certification Authority

Adresse:
EuroPriSe GmbH
Joseph-Schumpeter-Allee 25
53227 Bonn
Germany
eMail: ca@european-privacy-seal.eu

6 Spezifikation des Zertifizierungsgegenstandes (ToE)

Die zum Dienst gehörigen Komponenten sind

- der RISER Internal Client (**Zweck**: System-, Kunden- und Lieferantenmanagement),
- das RISER Kundenportal (**Zweck**: Zugang zum RISER-System, um den eigenen Zugang managen, Anfragen auslösen und Ergebnisse abholen zu können),
- das RISER Lieferantenportal (**Zweck**: Batch-Zugang zum RISER-System, um Anfragen abholen und Ergebnisse übergeben bzw. hochladen zu können),
- das RISER Meldebehördenportal (**Zweck**: online-Zugang zum RISER-System, um den eigenen Zugang managen, Anfragen abholen und Ergebnisse übergeben bzw. hochladen zu können),
- Schnittstellen zu Kunden und Lieferanten per SFTP, SOAP, FTP, RISER Meldebehördenportal, RISER Lieferantenportal, Postalisch (Brief), Stadtportale[1], um Anfrage- und Ergebnisdaten übermitteln zu können sowie die Schnittstelle zur Umzugs- und Telefonverzeichnisdatenbank, die als solche die jedoch nicht zum Evaluierungsgegenstand gehört (s.u.),
- Führen von Logs als Verantwortliche Stelle,
- das Rollenkonzept.

1 Dies ist die abschließende Aufzählung der Schnittstellen

Neue Komponenten:

- EMA_Monitoring (**Zweck**: Information des Kunden bei zeitlich verzögerten Aktualisierungen im Melderegister)
- Archivierung (**Zweck**: abschließende Löschung bzw. Sicherstellung der Verfügbarkeit von Daten)
- Datenbank zur Auskunftserteilung über Verstorbene.
- Verarbeitung von erweiterten Melderegisterauskünften

Die zum Dienst gehörigen Prozesse sind:

- Prozesse zur Verarbeitung, Speicherung und Löschung der personenbezogenen Daten durch den RISER-Dienst (**Zweck**: Durchführung des RISER-Dienstes; einfache und erweiterte Melderegisterauskunft)
- Monitoring und Betrieb des RISER-Dienstes durch RISER (**Zweck**: Sicherstellung des RISER-Dienstes)
- Changeprozesse (Veranlassen und Produktivschalten eines Change) (**Zweck**: Fehlerbehebung und Weiterentwicklung des RISER-Dienstes)

Die Prozesse wurden nicht geändert und es wurden keine neuen Prozesse eingeführt.

Nicht zur Zertifizierung gehören folgende Komponenten:

- RISER Pre-Sales Web-Client (Interessentenverwaltung)
- die Verwendung sonstiger mobiler Hardware, die nicht für die Abwicklung des RISER-Dienstes genutzt werden darf.
- RISER -Newsletter
- Realtime-Anschriftenprüfung (ID-Check)
- Realtime-Altersverifikation (Age-Check)
- Auskunftserteilung über eine Umzugs- und Telefonverzeichnisdatenbank

7 Kurzbeschreibung des IT-basierten Service

Die RISER ID Services GmbH bietet einen zentralen Online-Dienst für Unternehmen an, über den europaweit Adressen abgefragt und verifiziert werden können. Kunden können diese Informationen entweder über eine Einzel- oder eine Sammelanfrage beauftragen.

Bei einer Einzelanfrage werden die Daten direkt in eine Eingabemaske eingegeben, die an die Anforderungen der zuständigen nationalen oder regionalen Registerbehörde angepasst ist. Sammelanfragen werden durch die Übertragung einer Datei mit mehreren Anfragedatensätzen realisiert. RISER verbessert die vom Kunden gesandten Daten (qualifiziert sie) und passt sie an die von der Meldebehörden verwendeten Suchlogik an. Als Ergebnis werden der volle Name und die volle Adresse von der Registerbehörde übertragen. Zusätzlich können weitere Informationen, wie beispielsweise eine Namensänderung übermittelt werden.

Weiterhin können inzwischen erweiterte Melderegisteranfragen gestellt werden. Weist der Antragsteller besonderes Interesse nach, können ihm zusätzliche Daten, bspw. über frühere Vor- und Familiennamen, Tag und Ort der Geburt, gesetzlichen Vertreter, Staatsangehörig-

keiten, frühere Anschriften, Tag des Ein- und Auszugs, Familienstand, beschränkt auf die Angabe, ob verheiratet oder eine Lebenspartnerschaft führend oder nicht, Vor- und Familiennamen sowie Anschrift des Ehegatten oder Lebenspartners, Sterbetag und -ort nach dem Melderechtsrahmengesetz (MRRG) übermittelt werden (§ 21 (2) Nrn. 1 - 9 [MRRG]).

Mit dem EMA-Monitoring wird ein Zusatzservice zur Qualitätsverbesserung angeboten, mit dem Kunden bei zeitlich verzögerten Aktualisierungen im Melderegister erneut informiert werden. Der Kunde kann die Person dann noch einmal gezielt anfragen und ein aktuelles/neues Ergebnis erhalten. Im Zuge des eMA-Monitorings werden weder personenbezogene Anfrage- und Ergebnisdaten dauerhaft gespeichert noch an Dritte weitergegeben (sogenanntes Adresspooling).

Die Archivierung erlaubt das Archivieren und Löschen der aktuell gespeicherten Daten nach definierten Regeln in einem Archivierungsserver. Dies erfolgt nach einem mehrstufigen Archivierungskonzept und löscht Anfrage- und Ergebnisdateien im File-Transfer automatisiert. Die Aufbewahrungsfrist für Dateien ist auf 6 Monate festgelegt. Von dieser Voreinstellung können abweichende, kürzere Aufbewahrungsfristen eingerichtet werden.

Die RISER ID Services GmbH arbeitet als Auftragsdatenverarbeiter im Auftrag ihrer Kunden und speichert in ihren Datenbanken keine Daten für eigene Zwecke. Anfragen werden an offizielle Melderegisterbehörden in vielen Ländern Europas gestellt. Anfragen werden wie im Folgenden beschrieben bearbeitet:

Kundenanfragen für unterschiedliche Länder oder Kommunen werden über das zentrale Portal übermittelt. RISER verteilt die Anfragen an die entsprechenden Melderegister. Die Melderegister verarbeiten die Anfragen und senden die Ergebnisse zurück an RISER. Danach können die Kunden die Ergebnisse vom Webportal herunterladen.

Kunden des RISER-Dienstes können ausschließlich juristische Personen aus den Mitgliedstaaten der Europäischen Union werden.

8 Transnationale Rahmenbedingungen

Der RISER-Dienst verarbeitet personenbezogene Daten aus den folgenden sieben europäischen Ländern.

1. Deutschland
2. Österreich
3. Schweiz
4. Italien
5. Schweden
6. Estland
7. Litauen

Geplant ist, weitere Länder der Europäischen Union und des EWR an den RISER-Dienst anzubinden, in denen eine Auskunft aus öffentlichen Registern nach nationalem Recht möglich ist. Die Daten werden aus den nationalen bzw. lokalen Melde- oder Wählerregistern abgefragt.

Kunden des RISER-Dienstes sind ausschließlich juristische Personen aus Mitgliedsstaaten der Europäischen Union.

9 Verwendete Werkzeuge

Hardware:

Hewlett-Packard (HP) -

- ProLiant DL380G7
- ProLiant DL380G6
- ProLiant DL360G4
- ProLiant DL380G3
- ProLiant DL140G3
- ProLiant DL320s

Software:

• Tomcat	• Apache 2.0.49
• SUN Java 1.6	• MaxDB 64Bit version 7.6.06
• RISER-Applikation	• Linux Debian Version 4.0
• WinSCP	• openBSD
• Nagios 3.0.3	• Suse Linux Enterprise Server v.11
• MySQL	• Suse Linux Enterprise Server v.9
• Mantis	• Phproject
• Eclipse	• Typo3
• CVS	• Putty
• SQL-Studio	• Jasper-Reports

10 Version der für die Evaluation verwendeten EuroPriSe Kriterien

201111_EuroPriSe Criteria

11 Ergebnisse der Evaluation

Bei der Betrachtung der „grundlegenden Aspekte der Verarbeitung" kann festgestellt werden, dass die RISER ID Services GmbH ein System entwickelt hat, das die Grundlagen des Datenschutzes in äußerst positiver Weise umsetzt. Obwohl die RISER ID Services GmbH Auftragsdatenverarbeiter für die zu verarbeitenden Daten ist zeigt sich, dass insbesondere die Zwecke der Datenverarbeitung eindeutig und klar definiert und sämtliche zu verarbeitenden Daten genau spezifiziert sind. Bei der Übermittlung personenbezogener Daten an Drittländer ist anzumerken, dass die einbezogenen Drittstaaten (bisher nur die Schweiz) das europäische Datenschutzniveau gemäß Richtlinie 95/46/EC bei der Verarbeitung vollständig einhalten. Aus Sicht der Betroffenen sollte der RISER-Service insofern von allen Beteiligten datenschutzrechtlich adäquat umgesetzt werden (können).

Bei der Evaluation der „Grundlegenden technische Konstruktion" des RISER-Service konnte der Bereich der „Datenvermeidung und Minimierung" als besonders gelungen bewertet werden. Die RISER ID Services GmbH vermeidet die Übermittlung nicht erforderlicher Daten, wo immer es möglich ist. Zweck des RISER-Service ist es, einfache und erweiterte Melderegisterauskünfte europaweit zur Verfügung zu stellen. Deshalb werden von der RISER ID Services GmbH nur die Daten an den Anfragenden übermittelt, die im jeweiligen Prozess notwendig sind. Zusätzliche Daten, die gegebenenfalls von Registerstellen unterschiedlicher Länder aufgrund der landesspezifischen Gesetze übermittelt werden, werden auf die Daten einer einfachen Melderegisterauskunft reduziert, wenn keine erweiterte Auskunft (mit Angabe des besonderen Interesses) gestellt wurde. Die Beschreibung des Service, unter anderem durch die Datenschutzerklärung, führt zu einer umfassenden Transparenz des RISER-Service, sowohl für die Kunden als auch die Betroffenen.

Die Zulässigkeit der Verarbeitung durch die RISER ID Services GmbH bestimmt sich im wesentlichen aus der Europäischen Datenschutzrichtlinie 95/46/EC und den jeweiligen landesspezifischen Melderegistergesetzten. Aus der Tatsache, dass RISER als Auftragsdatenverarbeiter tätig wird ergibt sich zudem, dass der Auftraggeber als verantwortliche Stelle fungiert und nicht die RISER ID Services GmbH. Die grundsätzliche Zulässigkeit einer Melderegisterauskunft von Seiten des Auftraggebers ergeben sich vorrangig aus dem Vorliegen eines Vertrags (Art. 7 b) Richtlinie 95/46/EC) oder aus der Erforderlichkeit zur Verwirklichung berechtigter Interessen (Art. 7 f) Richtlinie 95/46/EC). Die RISER ID Services GmbH kann (muss) insofern davon ausgehen, dass eine der möglichen Voraussetzungen für die Zulässigkeit der Datenverarbeitung durch den Auftraggeber vorliegen und der Kunde rechtmäßig handelt. Aufgrund dieser Abhängigkeit sind die Verträge mit den Auftraggebern so verfasst, dass die RISER ID Services GmbH die Verträge nur abschließt, wenn ihre datenschutzrechtlichen Vorgaben auch vom Kunden akzeptiert bzw. erfüllt werden und im Falle einer unrechtmäßigen Verarbeitung der Daten durch den Auftraggeber, der Vertrag gekündigt werden kann.

Insgesamt ist festzustellen, dass das Geschäftsmodell der RISER ID Services GmbH aus rechtlicher Sicht in keiner Weise zu beanstanden ist und dass die in diesem Kontext geschlossenen Verträge die rechtlichen Vorgaben umsetzen. Die Prüfung ergab zudem, dass die daten-

schutzrechtlichen Rahmenbedingungen, wie beispielsweise die Umsetzung der technisch-organisatorischen Maßnahmen, in diesen Verträgen in hervorragender Weise abgebildet werden.

Bei der Beurteilung der "Anforderungen an unterschiedliche Phasen der Verarbeitung" des RISER-Dienstes ist insbesondere der interne Zugang zu Daten bemerkenswert: Hier wird ein sehr granulares Rollenkonzepts angeboten, das eine optimale Anpassung der Zugänge an die Anforderungen des Dienstes erlaubt.

Die „Löschung der Daten nach Beendigung der Voraussetzung“ wird gleichfalls positiv gelöst. Ergebnisdaten werden nur eine sehr begrenzte Zeit (sechs Wochen) für eine direkte Abholung durch den Auftraggeber bereitgehalten. Danach werden die Daten in Stufen anonymisiert und archiviert.

Die RISER ID Services GmbH hat die „Einhaltung aller Datenschutzgrundsätze und –Pflichten“ zu einem ihrer wesentlichen unternehmerischen Ziele gemacht. Die Evaluation hat in diesem Bereich deshalb auch hervorragende Ergebnisse erzielt. Sowohl bei der "Spezifikation und Begrenzung des Zwecks“,, bei der "Proportionalität" als auch der "Qualität der Daten" wurde festgestellt, dass der Dienst die in diesen Bereichen gestellten Anforderungen exzellent umgesetzt hat. So sind die Zwecke für die die Daten genutzt werden können sehr gut dokumentiert, die Daten-Minimierung ist sehr gut umgesetzt worden und es werden nur Daten verarbeitet, die, bezogen auf die Zwecke für die sie erhoben wurden, wirklich erforderlich sind.

Gleichfalls hervorzuheben ist die Umsetzung der Regelungen zur Auftragsdatenverarbeitung. Die RISER ID Service GmbH versucht hier als Auftragsdatenverarbeiter die von ihr entwickelten unternehmerischen Standards auch gegenüber ihren Auftraggebern durchzusetzen – ein eher unüblicher Vorgang, da die Auftraggeber grundsätzlich verpflichtet sind, ihre Vorstellungen bezüglich der datenschutzrechtlich umzusetzenden Maßnahmen im Vertrag zu formulieren. Da jedoch die von der RISER ID Services GmbH entwickelten Standards sehr hoch und als vorbildlich zu bezeichnen sind, ist es als besonders positiv zu bewerten, dass Verträge nur auf dieser Basis abgeschlossen werden. Dabei wird einer Übermittlung der Daten in Drittländer aus Sicht der RISER-ID Services GmbH gleichfalls nur unter diesen Datenschutz-Rahmenbedingungen zugestimmt.

Weiterhin sind die einzuhaltenden Formalitäten und hier insbesondere die „Pflicht zur Meldung bei der Kontrollstelle“ in exzellenter Weise umgesetzt.

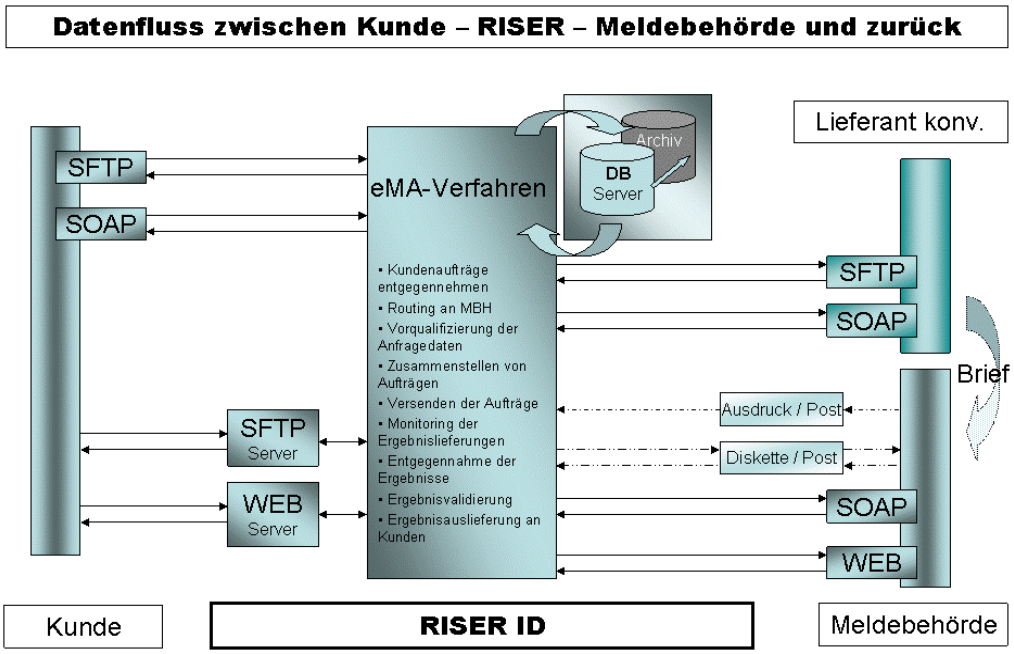
Als Auftragsdatenverarbeiter sind natürlich insbesondere die technisch-organisatorischen Maßnahmen elementar für die Abwicklung eines Service. Die RISER ID Services GmbH hat im technischen Bereich grundsätzlich ebenfalls sehr gute Arbeit geleistet. So sind nicht nur die Zugangskontrolle, der Zugang zu Daten, Programmen und Geräten oder das Logging der Verarbeitung von personenbezogenen Daten adäquat umgesetzt. Gleiches gilt für den Backup und Recovery-Bereich und für den Bereich "Datenschutz und Security Management".

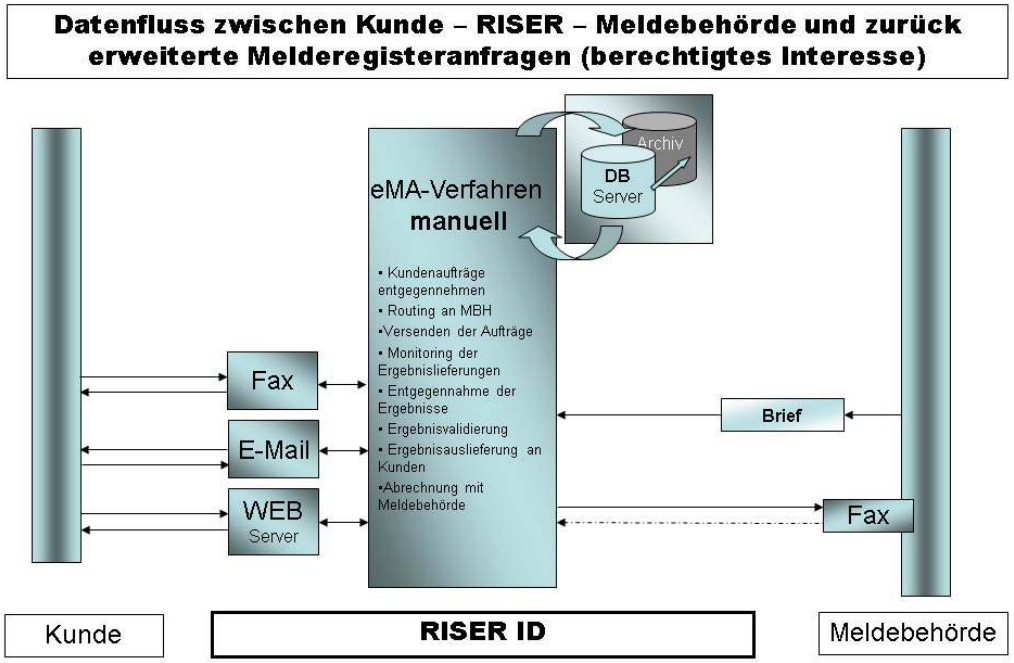
Obwohl die RISER ID Services GmbH noch als junges Unternehmen zu bezeichnen ist, hat sich der unternehmerische Reifegrad weiter entwickelt und es finden sich nur sehr wenige Aspekte, hinsichtlich derer noch Verbesserungspotential besteht.

Bei der Beurteilung der Einhaltung der Rechte unter der Richtlinie 95/46/EC sowie der bezogen auf die Richtlinie 2002/58/EC wurde bei der Evaluation eine insgesamt adäquate Umsetzung der Rechte ermittelt.

Zusammenfassend ist festzustellen, dass der von der RISER ID Services GmbH angebotene RISER-Dienst als konform mit den Anforderungen an Datenschutz und Datensicherheit gemäß den EuroPriSe-Vorgaben zu bewerten ist. Insgesamt setzt die RISER-ID Services GmbH darauf, Datenschutz und Datensicherheit als wesentliches Element ihres Angebots umzusetzen. Dies gelingt ihr in vorbildlicher Weise.

12 Schematische Darstellung der Systemarchitektur und des Datenflusses





13 Datenschutz verbesserde Funktionalitäten

RISER verarbeitet die Daten ausschließlich zum vertraglich festgelegten Zweck und nach den vertraglich festgelegten, datenschutzkonformen Verfahren. RISER verwendet die Ergebnisdaten nicht für eigene Zwecke, wie andere Konkurrenzunternehmen, die die einmal ermittelten Daten selbst speichern. Die so agierenden Unternehmen können hierdurch bei Personen, die mehrfach angefragt werden, Rationalisierungs- und Kosteneinsparungseffekte auf der Basis unsicherer Daten erzielen, da eine erneute Anfrage bei der Registerbehörde nicht mehr nötig ist bzw. nötig zu sein scheint. RISER verzichtet auf eine derartige Vorgehensweise, weil so nicht sichergestellt werden kann, dass die wirklich aktuellen Daten der Betroffenen übermittelt werden.

Weiterhin versucht RISER so wenige Daten wie möglich zur Verarbeitung zu nutzen bzw. zu übermitteln. So werden beispielsweise Ergebnisdaten, die von ausländischen Registern kommen und die mehr Daten enthalten als die einer "einfachen Melderegisterauskunft", grundsätzlich auf diese Daten reduziert.

RISER hält umfassende Informationen für Betroffene und potentielle Kunden über die einzuhaltenden Datenschutzmaßnahmen bereit. Weiterhin versucht RISER die Auftraggeber an das hohe Datenschutzniveau anzupassen, das RISER als Auftragnehmer einhält. So definiert RISER von sich aus die Vorgaben für die technisch-organisatorischen Maßnahmen, die für den Abschluss eines Datenverarbeitungsvertrags notwendig sind und die eigentlich vom Auftraggeber vorgegeben werden müssten. RISER stellt dabei vertragliche Datenschutz-Mindeststandards sicher. Ohne deren Umsetzung würde ein Vertrag nicht abgeschlossen.

14 Bereiche, die besondere Aufmerksamkeit der Nutzer bedingen

entfällt

15 Kompensation von Schwachstellen

entfällt

16 Ergebnistabelle der relevanten Anforderungen

EuroPriSe Requirement	*Decision*	*Remarks*
Data Avoidance and Minimisation	excellent	Der Dienst nutzt nur das Minimum der erforderlichen Daten. Personenbezogene Anfrage- und Ergebnisdaten werden weder dauerhaft für eigene Zwecke gespeichert noch an Dritte weitergegeben (sogenanntes Adresspooling).
Transparency	adequate	Dokumentation und Datenschutzerklärung sind informativ, up-to date und verständlich
Technical-Organisational Measures	adequate	Zugangsschutz, die vorhandenen Loggingmechanismen und die Maßnahmen zum Schutz vor versehentlichen Verlust von Daten sind mit sehr gut zu bewerten. Back-up- und Recovery-Mechanismen sind etabliert und werden exzellent betrieben. Das Datenschutz- und Sicherheitsmanagement ist in Teilen exzellent gelöst, ist insgesamt aber nur als adäquat zu bewerten.
Data Subjects' Rights	adequate	RISER ist als Auftragsdatenverarbeiter nur für einen kleinen Bereich verantwortlich, in dem Rechte der Betroffenen explizit zu berücksichtigen sind. In diesen Fällen sind adäquate Maßnahmen getroffen worden.

Gutachter Statement

Ich versichere, dass der oben genannte IT-basierte Service nach den EuroPriSe-Kriterien, Regeln und Prinzipien evaluiert wurde und dass die oben beschriebenen Ergebnisse das Resultat dieser Evaluierung sind.

Berlin, 17.02.2014	Prof. Dr. Friedrich Holl	
Ort, Datum	Name des rechtlichen / technischen Gutachters	Unterschrift

Ergebnis der Zertifizierung

Der oben genannte IT-basierte Service hat die EuroPriSe-Evaluierung bestanden.

Hiermit wird bescheinigt, dass der oben genannte IT-basierte Service eine Nutzung nach den Europäischen Vorgaben für Datenschutz ermöglicht.

	EuroPriSe Certification Authority EuroPriSe GmbH, Bonn	
Ort, Datum	Name der Zertifizierungsstelle	Unterschrift