



**Nur per E-Mail**

[ivo.hurnik@bmas.bund.de](mailto:ivo.hurnik@bmas.bund.de)  
[juergen.mueller@bfdi.bund.de](mailto:juergen.mueller@bfdi.bund.de)  
[harald.flex@itsg.de](mailto:harald.flex@itsg.de)  
[robert.kronthaler@vdr.de](mailto:robert.kronthaler@vdr.de)

TEL.-ZENTRALE +49 30 18615 0  
FAX +49 30 18615 7010  
INTERNET [www.bmwi.de](http://www.bmwi.de)

BEARBEITET VON Jochen Puth-Weißenfels  
TEL +49 30 18615 7504  
FAX +49 30 18615 5113  
E-MAIL [Jochen.Puth-Weissenfels@bmwi.bund.de](mailto:Jochen.Puth-Weissenfels@bmwi.bund.de)  
AZ I C 5

DATUM Berlin, 1. Oktober 2008

BETREFF Umsetzung ELENA-Verfahren;  
HIER datenschutzrechtliche Grundsätze

Sehr geehrte Herren,

das BMWi ist - nicht nur vor dem Hintergrund der Diskussionen in den Gremien des Bundestages und des Bundesrates - an einer sachgerechten Umsetzung des ELENA-Verfahrens interessiert.

Hierzu gehört **zwingend** die Beachtung der in der Vergangenheit vereinbarten datenschutzrechtlichen Eckpunkte.

Der ordnungshalber füge ich diese noch einmal in der Anlage bei und bitte um Beachtung bei den weiteren Schritten. BMWi wird, in Abstimmung mit dem BfDI, die Beachtung der datenschutzrechtlichen Gesichtspunkte hinterfragen.

Mit freundlichem Gruß  
Jochen Puth-Weißenfels

**Eckpunkte aus datenschutzrechtlicher Sicht;**

1. Verschlüsselung sämtlicher Transportwege.
2. Verschlüsselung (Session-Master-Key) der Datensätze in der Datenbank.
3. Technische Aufteilung der ZSS in einen meldenden Zweig und einen abrufenden Zweig, in eine Innere und eine Äußere Schicht mit jeweils physikalischen Trennmöglichkeiten und Überwachungsmechanismen.
4. QSIG zur Signierung der Vollmacht (Erklärung zum Einverständnis für den Datenabruf) für den Abruf.
5. Vorhandensein einer "zum Zeitpunkt der Signatur gültigen Vollmacht (Einverständniserklärung zum Datenabruf)".
6. Speicherung der Daten in der Datenbank entweder unter der "ZID - Zertifikatsidentitätsnummer" oder der "vorläufigen Identitätsnummer (gebildet durch die RFV)".
7. Das Zwei-Karten-Prinzip für den Abruf der Daten (es muss immer eine Vollmacht vorliegen).
8. Trennung zwischen ZSS und RFV räumlich, organisatorisch, technisch und personell.
9. Trennung der Verfahren innerhalb der ZSS (wenn DRV Bund dann kein Zugriff auf Rentenversichertendaten); Physikalisch, Organisatorisch, Personell.
10. Zum Abruf muss immer Antrag und Vollmacht vorliegen (kein Abruf ohne Antrag, Ausnahme Selbstauskunft, da bei der Selbstauskunft nur ein Antrag zur Selbstauskunft auszufüllen ist und somit nicht direkt ein Zweck verfolgt wird).
11. (gezielte) Löschung der Daten oder Teilen von Daten unverzüglich bei Fristablauf.
12. Es können beliebig viele Signaturkarten pro Teilnehmer ins Verfahren eingebracht werden.
13. Trennung zwischen Datenspeichernde Stelle und Verschlüsselungsschlüssel (Masterkey) speichernde Stelle: Organisatorische und (rechtlich) verantwortliche Trennung.
14. Abruf nur der Datensatzteile die für die Aufgabenerfüllung erforderlich ist (inhaltliche wie zeitliche Begrenzung).

15. Kein Zugriff von Sicherheitsbehörden, Steuerbehörden, Zoll etc..
16. Kein Register der Arbeitnehmer, kein Register der Arbeitgeber.
17. Abruf nur von zugelassenen Behörden und berechtigten Mitarbeitern.
18. Protokollierung aller Datenbanktransaktionen, Abrufe etc. gemäß den vom Datenschutz vorgegebenen Fristen.
19. Speicherung der Vollmachten zum Abruf für Revisionszwecke mindestens so lange wie Protokolldaten zur Kontrolle!
20. Zuordnung RV/ZID-VID (Pseudonymisierung) nur in der RFV.