

Verwaltungsabkommen zwischen
den Ländern

Freie und Hansestadt Hamburg,
vertreten durch den Senat

und

Schleswig-Holstein,
endvertreten durch
den Minister für Wirtschaft, Arbeit,
Verkehr und Technologie
des Landes Schleswig-Holstein,

über die Führung eines gemeinsamen Registers
zum Schutz fairen Wettbewerbs.

§ 1 Ziele

(1) Die Länder Schleswig-Holstein und die Freie und Hansestadt Hamburg sind sich darüber einig, gemeinsam ein automatisiertes Register zum Schutz fairen Wettbewerbs (im folgenden: Register) zu führen. Das gemeinsame Register dient dem Ziel, den öffentlichen Auftraggebern in den beteiligten Ländern die Prüfung und Feststellung zu erleichtern, dass öffentliche Aufträge nur an gesetzestreue und zuverlässige Unternehmen vergeben werden. Mit der Einrichtung des gemeinsamen Registers wird für öffentliche Auftraggeber im Gebiet der beteiligten Länder die Möglichkeit gegeben, sich im Rahmen der Überprüfung der Zuverlässigkeit potenzieller Vertragspartner gezielt über schwere Verfehlungen von Unternehmen zu informieren, um die Vergabe öffentlicher Aufträge an unzuverlässige Unternehmen zu verhindern.

(2) Das Verwaltungsabkommen wird auf der Basis des hamburgischen Gesetzes zur Einrichtung eines Registers zum Schutz fairen Wettbewerbs – GRfW – vom 17.9.2013, HmbGVBl. S.417 und des schleswig-holsteinischen Gesetzes zur Einrichtung eines Registers zum Schutz fairen Wettbewerbs – GRfW – vom 13.11.2013, GVOBl. Schl.-H., S. 405 abgeschlossen. Bei Änderungen der gesetzlichen Vorschriften ist das Verwaltungsabkommen gegebenenfalls anzupassen, neu zu fassen oder aufzuheben.

(3) Um ein in sich konsistentes Register zu gewährleisten, werden die beteiligten Länder darauf hinwirken, dass die für ein gemeinsames Register notwendigen Regelungen einheitlich getroffen werden.

(4) Soweit in diesem Verwaltungsabkommen das GRfW genannt wird, sind die Vorschriften der Gesetze beider Länder gemeint.

§ 2 Organisation

(1) Sitzland des gemeinsamen Registers (§ 10 Abs. 2 Nr. 1 GRfW) ist Hamburg. Es wird bei der Finanzbehörde der Freien und Hansestadt Hamburg eingerichtet und geführt (Registerstelle). Es unterliegt gemäß § 10 Abs. 5 Satz 1 GRfW der Überwachung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit.

(2) Zur Verarbeitung von Daten im gemeinsamen Register sind diejenigen Stellen befugt, die nach den Vorschriften des jeweiligen GRfW zur Datenverarbeitung im gemeinsamen Register ermächtigt sind.

(3) Die Freie und Hansestadt Hamburg und das Land Schleswig-Holstein richten je eine Zentrale Informationsstelle (§ 2 Absatz 1 GRfW) für ihren Zuständigkeitsbereich ein. Diese Zentralen Informationsstellen nehmen die Meldungen Dritter entgegen und entscheiden eigenständig über den Eintrag in das gemeinsame Register. Die jeweils andere Zentrale Informationsstelle ist über den Eintrag unverzüglich zu unterrichten.

(4) Das für die Registerführung erforderliche IT-Verfahren wird vom gemeinsamen IT-Dienstleister Dataport AöR gestellt und betrieben (Auftragsdatenverarbeitung). Der Entwicklungsauftrag auf Grundlage einer zwischen den beteiligten Ländern abgestimmten Verfahrensbeschreibung und eines Lastenhefts wird durch die Freie und Hansestadt Hamburg erteilt. Der entsprechende Vertrag und mögliche Änderungen bedürfen der Zustimmung von Schleswig-Holstein.

(5) Das IT-Verfahren muss dem durch die Risikoanalyse festgestellten hohen Schutzbedarf genügen. Um über die heterogenen Organisationsgrenzen hinweg Registerpflege und Registerabfrage zu ermöglichen, wird die vorhandene Infrastruktur des GovernmentGateways genutzt. Dataport wird verpflichtet werden, mit dem „MasterUserKonzept“ ein Registrierungstool zur Verfügung zu stellen, das den datenschutzrechtlichen Erfordernissen Rechnung trägt. Um Doppelregistrierungen zu vermeiden, werden die jeweiligen Länder-Mandanten des GovernmentGateways verwendet. Der Zugang zum Verfahren für öffentliche Auftraggeber erfolgt unter Nutzung des Internets über das jeweilige Dienste-Portal (Schleswig-Holstein-Service und HamburgService). Dataport ist für den sicheren Betrieb (u.a. Verfügbarkeit, Vertraulichkeit, Integrität) vertraglich verantwortlich zu machen. Test und Freigabe des IT-Verfahrens erfolgen in einem dreistufigen Verfahren (Test, Freigabeverfahren, Produktion). Die Auftraggeber sind jederzeit berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme.

(6) Es wird eine Lenkungsgruppe eingerichtet, der je eine Vertreterin oder ein Vertreter der beteiligten Länder angehören. Die Datenschutzbeauftragten der beteiligten Länder haben je einen Sitz mit beratender Stimme in der Lenkungsgruppe. Eine Vertreterin oder Vertreter von Dataport nimmt an den Sitzungen mit beratender Stimme teil.

(7) Die Lenkungsgruppe regelt grundsätzliche Fragen der Planung, Umsetzung, Realisierung und des Controllings der Arbeits- und Projektmaßnahmen. Den Mitgliedern obliegt weiterhin die Aufgabe, sich in ihren jeweiligen Ländern bei den fachlich beteiligten Stellen für die erforderlichen Maßnahmen zur Erreichung der Projektziele einzusetzen. Die Lenkungsgruppe kann zu ihren Sitzungen sachverständige Personen hinzuziehen. Der Vorsitz in der Lenkungsgruppe wechselt alle zwei Jahre, beginnend mit Schleswig-Holstein.

(8) Die Finanzbehörde der Freien und Hansestadt Hamburg übernimmt für das IT-Verfahren die Aufgaben der Fachlichen Leitstelle (§ 10 Abs. 2 Nr. 1 GRfW) im Sinne der Hamburgischen Freigaberichtlinie. Diese Aufgaben umfassen:

- Entwicklungsplanung,
- fachliche und technische (organisatorische) Steuerung des IT-Verfahrens,
- Festlegung fachlicher Anforderungen in enger Abstimmung mit Schleswig-Holstein,
- Dokumentation,
- Freigabe der Software.

Die Fachliche Leitstelle ist verfahrensverantwortende Stelle gemäß § 8 Abs. 2 LDSG SH und § 10 HmbDSG.

§ 3 Umfang der Verarbeitungsbefugnis

(1) Die Stellen gemäß § 2 Absatz 2 und Absatz 3 sind zur Verarbeitung der Daten im gemeinsamen Register nur insoweit befugt, wie dies erforderlich und gemäß den GRfW der Vertragsländer übereinstimmend zulässig ist.

(2) Die Stellen gemäß § 2 Absatz 2 und Absatz 3 sind zum lesenden Zugriff auf die Daten befugt. Im Rahmen ihrer fachlichen Zuständigkeit sind die Stellen gemäß § 2 Absatz 3 auch zum schreibenden Zugriff auf die Daten ihres Landes befugt.

(3) Die Stellen gemäß § 2 Absatz 2 und Absatz 3 dürfen Daten des gemeinsamen Registers automatisiert abrufen, soweit die Verarbeitung dieser Daten übereinstimmend nach den GRfW der Vertragsländer erforderlich und zulässig ist.

§ 4 Maßnahmen zur Datensicherheit und Datenschutzkontrolle

(1) Die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit und Datenschutzkontrolle gemäß § 10 Abs. 2 Nr. 2 und § 9 Abs. 2 und 3 GRfW trifft die Registerstelle (§ 2 Absatz 1).

(2) Durch geeignete technische Vorkehrungen, insbesondere durch Vergabe personenbezogener Kennungen und differenzierter Berechtigungen nach organisatorischen und funktionalen Kriterien, ist sicherzustellen, dass der Zugriff auf die Daten nur durch autorisierte, fachlich zuständige Personen und nur in dem jeweils erforderlichen und gesetzlich zulässigen Umfang erfolgt.

(3) Der durch die Berechtigungen ermöglichte Funktionsumfang wird von der Registerstelle (§ 2 Absatz 1) allgemein vorgegeben. Die zentralen Informationsstellen gemäß § 2 Absatz 3 können nur im Rahmen dieses Funktionsumfangs Berechtigungen vergeben.

(4) Die zentralen Informationsstellen gemäß § 2 Absatz 3 entscheiden innerhalb ihres Aufgabenbereiches eigenverantwortlich über die Vergabe der Berechtigungen.

(5) Neben den in § 9 Abs. 3 Satz 5 GRfW festgelegten Protokolldaten zum Registerabruf sind sämtliche schreibenden Zugriffe auf das gemeinsame Register zu protokollieren (wann, durch wen und in welcher Weise wurden Daten verändert). Die Protokolldaten sind revisions sicher vorzuhalten und sechs Monate aufzubewahren. Die nach § 2 Abs. 1 dieses Abkommens zuständige Stelle führt regelmäßig Stichprobenkontrollen der Protokolldaten durch, um unzulässige schreibende und lesende Zugriffe aufzudecken bzw. präventiv zu verhindern.

§ 5 Datenschutzrechtliche Verantwortung

(1) Die Verantwortung für die Einhaltung der Maßnahmen zur Datensicherheit und die datenschutzrechtliche Verantwortung gegenüber den Betroffenen tragen die Registerstelle (§ 2 Absatz 1) bezüglich des Gesamtsystems und die Zentralen Informationsstellen (§ 2 Absatz 3) in ihrem jeweiligen Zuständigkeitsbereich. Dies gilt auch für die Rechte der Betroffenen auf Auskunft, Berichtigung, Löschung und Sperrung.

(2) Für die Zulässigkeit der Datenverarbeitung trägt nach Maßgabe des § 10 Abs. 4 GRfW die jeweils Daten verarbeitende Stelle die Verantwortung. Für die Zulässigkeit der Datenübermittlung trägt die übermittelnde Stelle die Verantwortung. Für die Zulässigkeit des Abrufes von Daten trägt die empfangende Stelle die Verantwortung.

(3) Die Löschung von Einträgen aus dem gemeinsamen Register richtet sich nach den übereinstimmenden Vorschriften der GRfW.

§ 6 Test und Abnahme

Die erforderlichen Tests des von Dataport zu erstellenden IT-Verfahrens werden in den beteiligten Ländern parallel durchgeführt werden. Die Abnahme erfolgt im Einvernehmen mit den beteiligten Ländern durch die fachliche Leitstelle (§ 2 abs. 8).

§ 7 Kostenverteilung

Die Kosten für die Entwicklung des IT-Verfahrens und des Betriebs des gemeinsamen Registers einschließlich der Kosten der fachlichen Leitstelle nach § 2 Absatz 8 tragen die beteiligten Länder je zur Hälfte. Den zur Abfrage verpflichteten Stellen entstehen keine Kosten für die Nutzung des IT-Verfahrens.

§ 8 Beitritt weiterer Länder

Nach gemeinsamer Entschließung der beteiligten Länder können dem gemeinsamen Register weitere Länder beitreten. Deren Beteiligung am Entwicklungsaufwand für das IT-Verfahren wird in einem gesonderten Beitrittsabkommen festgelegt.

§ 9 Nutzungs- und Verwertungsrechte

Die Nutzungs- und Verwertungsrechte an dem entwickelten IT-Verfahren stehen jedem an diesem Abkommen beteiligten Land entsprechend der Kostenverteilung nach § 7 zu. Sie sind nur gemeinsam berechtigt, anderen Ländern oder dem Bund das Verfahren oder Teile davon zur Nutzung zu überlassen; insoweit erzielte Erträge stehen den beteiligten Ländern zu gleichen Teilen zu.

§ 10 Pflege des Systems

Die beteiligten Länder werden die fachlich oder rechtlich notwendige Fortentwicklung des IT-Verfahrens nach Abnahme gemeinsam durch Dataport durchführen lassen. Die Aufwendungen sind entsprechend § 7 zu verteilen.

§ 11 Transparenz

Dieses Abkommen ist im Amtsblatt für Schleswig-Holstein zu veröffentlichen. Die Freie und Hansestadt Hamburg kann das Abkommen nach den Bestimmungen des Hamburgischen Transparenzgesetzes veröffentlichen.

§ 12 Kündigung

Dieses Abkommen kann mit einer Frist von drei Monaten zum Jahresende gekündigt werden. Im Fall der Kündigung sind die Registerdaten zu trennen.

§ 13 Inkrafttreten, Außerkrafttreten

Das Abkommen tritt mit der Unterzeichnung in Kraft. Es tritt mit Inkrafttreten eines bundesweiten Korruptionsregistergesetzes außer Kraft.

Hamburg/Kiel, den

Freie und Hansestadt Hamburg

Für den Senat, vertreten durch
die Finanzbehörde

Land Schleswig-Holstein

endvertreten durch
den Minister für Wirtschaft, Arbeit, Verkehr und
Technologie