

Erklärung zur Auftragsdatenverarbeitung gemäß internationaler Datenschutzrichtlinien & deutschem Bundesdatenschutzgesetz (BDSG)

Stand vom 26. Oktober 2010

Hiermit gibt die AuthentiDate Deutschland GmbH (nachfolgend als „Auftragnehmer“ bezeichnet) nachfolgende Erklärung über die Verarbeitung von Daten von Auftraggebern im Rahmen der SIGNAMUS Webservices der AuthentiDate Deutschland GmbH (Auftragsdatenverarbeitung) ab. Diese Erklärung ist integraler Bestandteil einer Beauftragung eines Auftraggebers zur Auftragsdatenverarbeitung bei der AuthentiDate Deutschland GmbH im Rahmen der SIGNAMUS Webservices und beinhaltet die Rechte und Pflichten für Auftragnehmer und Auftraggeber.

1 Definitionen

Auftragnehmer im Sinne dieser Erklärung ist die AuthentiDate Deutschland GmbH.

Auftraggeber im Sinne dieser Erklärung sind gewerbliche Unternehmen, öffentliche und nichtöffentliche Organisationen und Institutionen welche mit dem Auftragnehmer einen schriftlichen Vertrag zur Erbringung von Dienstleistungen des SIGNAMUS Webservices geschlossen haben.

Auftragsdatenverarbeitung ist die Dienstleistung zur Verarbeitung von Daten, Dokumenten oder Unterlagen die im Rahmen eines schriftlichen Vertragsverhältnisses über die SIGNAMUS Webservices vereinbart werden.

2 International verbindliche Regelungen und nationale Datenschutzgesetze

Die SIGNAMUS Webservices verarbeiten Daten aus praktisch allen Staaten der Erde; d.h. weltweit. Daher werden alle Datenschutzmaßnahmen auch mit einem internationalen Fokus geplant und implementiert.

Leider bestehen aktuell keine international verbindlichen Regelungen zum Datenschutz (International Privacy). Bisher sind nur unverbindliche internationale Empfehlungen, Absichtserklärungen und Initiativen verfügbar. Ein aktueller Überblick über internationale Empfehlungen und nationale Regelungen zum Thema Datenschutz ist online unter www.privacyinternational.org online abrufbar.

Um trotz fehlender verbindlicher internationaler Regelungen für alle SIGNAMUS Kunden jederzeit den optimalen Datenschutz zu ermöglichen hat sich AuthentiDate an die gesetzlichen Datenschutzbestimmungen des Landes (Deutschland) gehalten, welches die weltweit führenden und strengsten Datenschutzbestimmungen hat. Die Erfüllung dieser weltweit strengsten Bestimmungen gewährleistet die Sicherheit der Daten weltweit.

Weitere Informationen zum Deutschen Bundesdatenschutzgesetz, sowie der Gesetzestext sind in deutscher und englischer Sprache online von der Website des Deutschen Bundesbeauftragten für Datenschutz und Informationsfreiheit unter www.bfdi.bund.de abrufbar.

Nachfolgend geht die Erklärung daher auf die besonderen Anforderungen dieser speziellen gesetzlichen Anforderungen ein.

3 Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag. Der Auftraggeber hat den Auftragnehmer im Rahmen der Sorgfaltspflichten des § 11 Deutsches Bundesdatenschutzgesetz (BDSG) als Dienstleister auszuwählen. Voraussetzung für die Zulässigkeit einer Datenverarbeitung im Auftrag ist, dass der Auftraggeber dem Auftragnehmer den Auftrag schriftlich erteilt. Dieser Vertrag enthält nach dem Willen der Parteien und insbesondere des Auftraggebers den schriftlichen Auftrag zur Auftrag i.S.d. § 11 Deutsches BDSG und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.

(2) Sofern in dieser Erklärung der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird damit allgemein die Verarbeitung von personenbezogenen Daten verstanden.

4 Gegenstand der Leistungen

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

Erstellung von elektronischen Signaturen, Prüfung von elektronischen Signaturen, Speicherung und Archivierung, sowie Konvertierung für Datensätze, Dokumente oder anderweitige Daten, welche personenbezogene Daten enthalten können.

5 Rechte & Pflichten des Auftraggebers

(1) Der Auftraggeber ist verantwortliche Stelle (§ 3 Abs. 7 Deutsches BDSG) für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber.

(2) Der Auftraggeber ist als verantwortliche Stelle für die Wahrung der Betroffenenrechte verantwortlich. Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen. Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen.

(3) Der Auftraggeber hat das Recht sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber ist verpflichtet, das Ergebnis in geeigneter Weise zu dokumentieren.

(4) Der Auftraggeber hat das Recht, Weisungen über Art, Umfang und Verfahren der Datenverarbeitung zu erteilen. Mündliche Weisungen oder Weisungen in Textform (z.B. E-Mail) sind unverzüglich vom Auftraggeber schriftlich zu bestätigen.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern sensitive Daten vom Auftragnehmer für den Auftraggeber verarbeitet werden, wird der Auftraggeber weisungsberechtigte Personen konkret benennen

Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer wird den Auftraggeber bei der Durchführung von Kontrollen durch den Auftraggeber unterstützen und an der vollständigen und zügigen Abwicklung der Kontrolle mitwirken.

(3) Nicht mehr benötigte Unterlagen, bzw. Datensätze mit personenbezogenen Daten und Dateien werden unaufgefordert an den Arbeitgeber zurückgegeben oder werden datenschutzgerecht vernichtet.

(4) Ist der Auftragnehmer verpflichtet i.S.d. § 4f Deutsches BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen, bestätigt er dessen Bestellung mit dieser Erklärung und wird diesen auf Verlangen gegenüber dem Auftraggeber schriftlich oder in Textform (z.B. E-Mail) benennen.

(5) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden (vgl. Ziff. 8 der Anlage zu § 9 Deutsches BDSG).

(6) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.

(7) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer

ist berechtigt, die Durchführung der betreffenden Weisung(en) solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

(8) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers unverzüglich mitzuteilen, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist.

(9) Bei einer Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder bei Subunternehmern ist der Auftragnehmer verpflichtet den Auftraggeber entsprechend zu informieren. Der Auftragnehmer hat zu gewährleisten, dass auch in diesem Fall die entsprechenden Regelungen des BDSG eingehalten werden.

(10) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, auf geeignete Weise kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der Auftragnehmer die Daten mit dem jeweiligen Zweck kennzeichnen.

(11) An der Erstellung der Verfahrensverzeichnisse durch den Auftraggeber wird der Auftragnehmer mitwirken. Er wird dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitteilen.

(12) Der Auftragnehmer kann dem Auftraggeber Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind.

(13) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Anforderungen des Auftraggebers an den Auftragnehmer entstehen, bleiben unberührt.

7 Umfang der Weisungsbefugnis

(1) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen. Die Weisungen müssen schriftlich erfolgen. Dem Auftragnehmer soll eine angemessene Frist zur Umsetzung der Weisungen gesetzt werden.

(2) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

8 Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht unabhängige Dritte, wie z.B. Wirtschaftsprüfer, oder Unternehmen, welche auf Datenschutzaudits spezialisiert sind, mit der Überprüfung der die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer zu beauftragen. Die Kosten der Beauftragung Dritter zur Überprüfung trägt der Auftraggeber.

(2) Der Auftraggeber hat zu gewährleisten, dass der unabhängige Dritte alle Informationen und Ergebnisse, welche dieser im Rahmen der Überprüfung erhält vertraulich behandelt. Unternehmen, welche vollständig oder teilweise im Wettbewerb zum Auftragnehmer stehen, sind von einer Beauftragung durch den Auftraggeber zur Überprüfung gemäß Absatz 1 ausgeschlossen.

(3) Der Auftragnehmer ist dem vom Auftraggeber beauftragten unabhängigen Dritten gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(4) Der vom Auftraggeber beauftragte Dritte kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die Dokumentation zu den verwendeten Datenverarbeitungssystemen verlangen.

(5) Der vom Auftraggeber beauftragte unabhängige Dritte kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Störungen der Betriebsabläufe sind zu vermeiden.

9 Datengeheimnis

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des § 5 Deutsches BDSG verpflichtet. Der Auftragnehmer verpflichtet sich, die glei-

chen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis i.S.d. § 5 Deutsches BDSG verpflichtet werden.

10 Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

11 Geheimhaltungspflichten

(1) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

12 Technische & organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind (vergl. dazu auch Anforderungen gemäß Anlage zum §9 Deutsches BDSG):

a) Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

Der Zutritt zu den SIGNAMUS Systemen ist durch ein mehrschichtiges Zonenmodell geschützt. Um Zutritt zu den SIGNAMUS Systemen zu erlangen, müssen die Zonen von außen nach innen passiert werden.

Jede Zone ist mit elektronischen oder physikalischen Zutrittskontrollmechanismen versehen, die nur zutrittsberechtigtes Personal passieren lässt. Die Berechtigungen werden von der äusseren zur inneren Zone immer restriktiver.

Grundsätzlich wird das Prinzip der Least-Privileges angewandt, so dass Personen Zutrittsberechtigungen nur für die Zonen erhalten, die sie für die Ausübung ihrer Tätigkeit unbedingt benötigen.

Die erhobenen elektronischen Zutrittsprotokolle werden gespeichert und können bei Bedarf unter Einbeziehung des betrieblichen Datenschutzbeauftragten ausgewertet werden.

b) Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

Der Zugang zu den SIGNAMUS Systemen ist durch mehrere Ebenen geschützt. Zugang ist nur nach erfolgreicher Authentifizierung am Betriebssystem möglich. Jeder Operator verfügt über ein eigenes Benutzerkonto, dessen Passwort nur ihm bekannt ist. Für Passwörter wird eine Komplexitätsrichtlinie angewendet, die die Qualität der verwendeten Passwörter sicherstellt.

Erfolgreiche und fehlgeschlagene Anmeldeversuche an den Systemen werden protokolliert.

Die SIGNAMUS Systeme sind durch eine zuverlässige Firewallarchitektur gegen unauthorisierte Netzwerkverbindungen geschützt. Administrativer Remotezugang ist nur berechtigten Administratoren mittels einer verschlüsselten Verbindung mit 2-Faktor-Authentifizierung möglich.

c) Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsbeziehung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

Da SIGNAMUS eine automatisierte Datenverarbeitung im Auftrag durchführt, ist ein Zugriff auf die personenbezogenen Daten durch Personal der AuthentiDate International AG zur Verarbeitung, Nutzung und Speicherung im Normalfall nicht notwendig.

Ein Zugriff auf diese Daten erfolgt ggf. ausschließlich im Falle einer eventuell notwendigen Fehlersuche.

Es werden entsprechende Dateisystemberechtigungen verwendet, die den Zugriff auf die Daten auf das für die Verarbeitung notwendig Maß einschränken.

d) Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Alle Daten, die durch externe Datenübertragung, z.B. Internet, übermittelt werden, werden bei der Übertragung an und von den SIGNAMUS Systemen verschlüsselt. Alle Datenübertragungen werden elektronisch protokolliert.

Das unbefugte Lesen, kopieren oder verändern der Daten wird durch die Zutritts-, Zugangs-, und Zugriffskontrolle und deren Schutzmechanismen verhindert.

e) Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

Eine anonyme manuelle Eingabe oder Erfassung von Daten zur Weiterverarbeitung in das SIGNAMUS System ist systemtechnisch ausgeschlossen. Die Übermittlung von Daten an das SIGNAMUS System zur Weiterverarbeitung erfordert eine vorherige erfolgreiche Authentifizierung. Alle Datenübermittlungen werden elektronisch protokolliert.

Nicht autorisierte Übermittlungen werden vor Annahme der Daten abgelehnt. Eine Veränderung oder Löschung von Daten durch externe Systeme ist systemtechnisch ausgeschlossen.

f) Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

Alle Daten die an das SIGNAMUS System übermittelt werden, werden auftragsbezogen gekennzeichnet. Dadurch ist gewährleistet, dass diese nur nach den Weisungen des Auftraggebers und gemäß dem ausgehandelten Vertragszweck verarbeitet werden. Die Verarbeitung wird elektronisch protokolliert.

g) Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Alle Daten die an die SIGNAMUS System zur Weiterverarbeitung gesendet werden, werden während der Verarbeitung und/oder zur Archivierung (wenn beauftragt) redundant gespeichert. Ebenfalls werden alle Daten periodisch auf Datenträger gesichert und eine Kopie extern sicher ausgelagert. Damit wird der Verlust oder eine Zerstörung von Daten verhindert.

h) Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Alle Daten werden vom Auftraggeber über getrennte Eingabeverzeichnisse, für die nur der jeweilige Auftraggeber über die Zugangsdaten verfügt, übermittelt. Die Daten unterschiedlicher Auftraggeber werden logisch voneinander getrennt gespeichert und verarbeitet. Ein Auftraggeber hat keine Möglichkeit auf die Daten anderer Auftraggeber zuzugreifen oder diese einzusehen.

13 Beendigung

Nach Beendigung einer Beauftragung hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen. Die Datenträger des Auftragnehmers sind danach physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen.

14 Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

(3) Die Einrede des Zurückbehaltungsrechts i.S.v. § 273 Deutsches BGB wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Düsseldorf, den 26. Oktober 2010



Jan C. Wendenburg
Geschäftsführer

AuthentiDate Deutschland GmbH (Auftragnehmer)
Rethelstrasse 47
40237 Düsseldorf