

Präambel

Die BPS EDV-Service GmbH ist als Rechenzentrum und Dienstleister von kaufmännischen Anwendungen mit der Verarbeitung von personenbezogenen Daten beauftragt. Das zentrale Geschäftsfeld der Heuer- und Gehaltsabrechnung benötigt zur Abwicklung ihrem Wesen nach umfangreiche persönliche Angaben über Mitarbeiter und Angestellte der Auftraggeber. Für diese Informationen besteht ein besonders schutzwürdiges Interesse, welches durch Einhaltung der Regelungen im geltenden Datenschutzgesetz zu wahren ist. Gemäß dem Bundesdatenschutzgesetz sind technisch-organisatorische Maßnahmen zur Erreichung eines möglichst hohen Datenschutzniveaus und zu Wahrung der Informationssicherheit einzurichten. Im Folgenden werden diese Maßnahmen auf Unternehmens- und Anwendungsebene, sowie Grundsätze zum Datenschutz dargelegt.

1. Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung

Die BPS EDV-Service GmbH unterwirft sich dem Grundsatz der Datensparsamkeit und erhebt, verarbeitet und nutzt so wenig personenbezogene Daten wie möglich. Personenbezogene Daten werden erhoben, um entgeltabrechnungsrelevante Mitarbeiterdaten in der EDV zu erfassen und Entgeltabrechnungen, sowie personalwirtschaftliche Auswertungen zu erstellen. Im Auftrag erhobene Daten werden im Rahmen einer kundenindividuellen Dienstleistungsvereinbarung nach dem gleichen Grundsatz behandelt und weisungsgebunden verarbeitet. Zum Zwecke der Datenerhebung stellt die BPS EDV-Service GmbH jedem Anwender eine spezielle Software zur Verfügung, die den Datenaustausch über das Internet nach dem Client/Server-Prinzip realisiert. Neben der Erfassung der abrechnungsrelevanten, personenbezogenen Daten ermöglicht das Programm (im Folgenden Client-Anwendung genannt) den Abruf durchgeführter Abrechnungen oder personalwirtschaftlicher Auswertungen.

2. Schutzbedarfsbestimmung

Die Erreichung eines angemessenen Schutzniveaus bedarf einer vorausgehenden Ermittlung möglicher Gefahren und Risiken für die durch das EDV-System verarbeiteten Daten. Das zentrale Schutzziel für das Entgeltabrechnungssystem sind die personenbezogenen Daten, deren Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität durch Einrichtung und Aufrechterhaltung geeigneter betrieblicher und technischer Maßnahmen gewahrt werden sollen.

Vertraulichkeit als Systemeigenschaft beschreibt den Schutz vor unbefugter Preisgabe von Informationen. Für die Client-Anwendung und das Abrechnungssystem bedeutet dies, dass nur solche Personen Zugang zu den Personaldaten erhalten, die zur Kenntnisnahme berechtigt sind. Dieses Schutzziel bezieht sich im Wesentlichen auf

die Nutzung der Software, sowie auf den Datenaustausch zwischen Erfassungsprogramm und BPS-Server. Mögliche Gefahren sind die unerlaubte Nutzung der Datenerfassung und das Ausspähen von Daten bei der Übermittlung. Die Bereitstellung von Online-Kommunikationsschnittstellen und die damit verbundene permanente Anbindung an das Internet erfordern, dass auch das Unternehmensnetzwerk gegen Missbrauch geschützt wird.

Die Integrität von Daten in der EDV fasst die Unverfälschtheit, Vollständigkeit und Konsistenz der Daten während des gesamten Verarbeitungsprozesses in einem Begriff zusammen. Zu diesem Zweck muss die Authentizität der Daten, also die Möglichkeit der Zuordnung der Daten zu ihrem jeweiligen Ursprung (z.B. im Rahmen des Datenaustausches), gewährleistet sein. Ebenso muss die Revisionsfähigkeit gegeben sein, die sicherstellt, dass Datenmanipulationen (z.B. Änderung an den Personaldaten) in ihrer Art und Weise nachvollzogen und ihrem Ursprung (z.B. dem Nutzer der Änderungen durchführt) zugeordnet werden können. Die Integrität wird in der Hauptsache durch Fehlbedienung des Erfassungsprogramms, technische Fehler, Fehler in der Software oder auch durch Brand- und Elementarschäden bedroht.

Ein Qualitätskriterium, das Aufschluss darüber gibt, mit welcher Wahrscheinlichkeit Daten in einem bestimmten Zeitrahmen durch ein Datenverarbeitungssystem zur Verfügung gestellt und ordnungsgemäß verarbeitet werden können, ist die Verfügbarkeit. In Bezug auf das Abrechnungssystem bedeutet dies, dass Kunden die von BPS bereitgestellten Dienste und Funktionen des Abrechnungssystems zum geforderten Zeitpunkt beanspruchen können. Dabei bilden Systemausfälle auf Grund von technischem Defekt, Stromausfall, Malware-Befall oder Brand- und Elementarschäden die grundlegenden Gefährdungen der Verfügbarkeit.

Nicht alle Risiken, insbesondere derer, die durch höhere Gewalt (z.B. Brand wegen Blitzeinschlag) begründet sind, können unterbunden werden. Darüber hinaus muss die Verhältnismäßigkeit und Wirtschaftlichkeit der Maßnahmen zur Erreichung eines möglichst hohen Schutzniveaus gewahrt werden. Unter diesen Aspekten hat die BPS diverse Vorkehrungen getroffen, um einen möglichst hohen und umfassenden Schutz der Informationen und Daten umzusetzen. Diese Maßnahmen beziehen sich auf technisch-organisatorische Umsetzungen im Unternehmen, sowie auf Mechanismen, die auf Anwendungsebene implementiert wurden.

3 Technisch-organisatorische Maßnahmen

3.1 Betriebliche Regelungen

Organisatorische Vorgehensweisen und vorgeschriebene Verhaltensweisen der Mitarbeiter sind ein zentraler Aspekt des Datenschutzes der BPS. So existiert

über die obligatorische Verpflichtung auf das Datengeheimnis hinaus ein Verbot, dass Mitarbeitern untersagt, personenbezogene Daten und Akten aus den Räumlichkeiten des Unternehmens zu transportieren. Weiterhin existiert die Vorgabe, Arbeitsplatzrechner bei Abwesenheiten zu sperren, um eine nicht autorisierte Verarbeitung bzw. Kenntnisnahme von personen- und unternehmensbezogenen Daten zu verhindern.

3.2 Zutritt zu den Datenverarbeitungssystemen

BPS ist ein eigenständiges Rechenzentrum, welches die zur Durchführung der angebotenen Dienstleistungen benötigten Datenverarbeitungssysteme selbstständig betreibt. Die Anlagen befinden sich in einem separaten Raum am Unternehmenssitz. Die Zugänge zum Gebäude des Unternehmenssitzes sind stets geschlossen und können nur von Mitarbeiter mittels Sicherheitsschlüssel oder über eine biometrische Zutrittskontrolle geöffnet werden. Betriebsfremde werden grundsätzlich persönlich am Eingang abgeholt und während ihrem Aufenthalt von Mitarbeitern der BPS begleitet. Nicht autorisierte Personen haben keinen Zugang zu den Server-Räumen.

3.3 Softwarezugriff und technische Zugangskontrollen

Unbefugten ist der Zugang zu den Datenverarbeitungssystemen durch Einrichtung von Zugangskontrollen nicht gestattet. Mögliche Außenzugänge sind mit einer wirksamen technischen Zugangskontrolle versehen. Ebenso existieren als Kommunikationsschnittstelle für die Client-Anwendung zugangskontrollierte Dienste.

Das Unternehmensnetzwerk ist über ein Hardware-Firewall-System vom Internet bis auf den notwendigen Datenaustausch abgeschottet. Dieses System überprüft den gesamten ein- und ausgehenden Datenverkehr auf Malware und erkennt und unterbindet selbstständig böswillige Attacken und Angriffsversuche aus dem Internet. Gleichzeitig werden durch eine dezidierte Portfreigabe mögliche Angriffspunkte auf das Mindestmaß reduziert.

Der Zugriff auf Anwendungsebene und somit auf personenbezogene Daten wird über mehrstufige Sicherheitsmechanismen hergestellt. Dabei ist der Einsatz von X.509-Zertifikaten ein zentraler Bestandteil des Autorisierungsverfahrens für den Zugriff auf die bereitgestellten Online-Dienste. BPS betreibt für die Bereitstellung dieser Zertifikate eine eigene Public-Key-Infrastructure (PKI), in der sie als Stammzertifizierungsstelle auftritt und kundenindividuelle Zertifikate ausgibt. Ein gültiges Zertifikat muss auf jedem Anwender-PC installiert sein und ist zusammen mit der Eingabe einer gültigen Kombination aus Benutzername und Passwort die Voraussetzung für eine erfolgreiche Anmeldung am Datenaustausch-Server der BPS. Grundsätzlich ist technisch sichergestellt, dass ein Datenaustausch ausschließlich

mit Besitzern von BPS ausgegebenen und zum Zeitpunkt der Kommunikation gültigen Zertifikaten initiiert werden kann. Die programmatische Benutzeridentifizierung erfolgt zweistufig, wobei zunächst der jeweilige Kunde über das eingesetzte Zertifikat und im zweiten Schritt der jeweilige Anwender über die Benutzername-Passwort-Kombination ermittelt wird.

3.4 Rollen-/Ressourcenmanagement und Eingabekontrolle

Aufbauend auf der eindeutigen Identifizierung von Anwendern ist in dem Abrechnungssystem ein Rollen- und Ressourcenmanagement implementiert. Einzelnen Benutzern können Rechte und Ressourcen zugewiesen und entzogen werden, sodass der Zugriff auf personenbezogene Daten den Erfordernissen des Arbeitsbereiches eines Anwenders angepasst werden können. Für die Einrichtung neuer Benutzer und der Zuteilung von Rechten und Ressourcen bedarf es eines speziellen Anwenders, der auch über die zu diesem Zweck erforderlichen Rechte verfügt.

Die Identifizierung einzelner Anwender wird weiterhin für die Revisionsfähigkeit des Systems herangezogen. Änderungen an Personaldaten können auf den angemeldeten Benutzer zurückgeführt werden, da Datenmanipulationen in ihrer Art und Weise zeitpunkt- und anwenderbezogen mitsamt den Zuständen vor und nach der Speicherung einer Änderung protokolliert werden. Der Auftraggeber erhält bei Bedarf einen monatlichen Ausdruck des Protokolls.

3.5 Sicherung der Datenübertragung

Der Austausch der Daten zwischen dem Datenaustausch-Server der BPS und der Client-Anwendungen erfolgt über gesicherte Einrichtungen zur Datenübertragung. Die Vertraulichkeit und Integrität der Daten wird auf dem Übertragungsweg durch den Einsatz von Verschlüsselungstechniken und einer Signatur der Daten erreicht. Abgefangene Daten aus dem Datenverkehr sind somit auf Grund ihrer Nichtlesbarkeit für potentielle Angreifer unbrauchbar. Durch die Signatur der Übertragungsdaten mit Hilfe der bereits genannten Software-Zertifikate werden unbefugte Datenmanipulationen aufgedeckt und ggf. die übertragenen Daten verworfen.

Die Datenverschlüsselung erfolgt als Kombination aus symmetrischem und asymmetrischem Kryptographieverfahren, einer Vorgehensweise, die als hybride Verschlüsselung bezeichnet wird. Jedes Zertifikat kapselt neben diversen Informationen einen Kryptographieschlüssel, der für den Austausch eines Sitzungsschlüssels pro Kommunikationsvorgang mit dem Kommunikationspartner herangezogen wird. Dieser Sitzungsschlüssel wird dann für den eigentlichen Datenaustausch herangezogen. Die Zertifikate werden darüber hinaus für das digitale Signaturverfahren eingesetzt, wobei über die Datenmenge in einem im Zertifikat festgelegten Verfahren eine eindeutige Zahl

(Signatur) berechnet wird. Diese Zahl wird vom Absender mit den eigentlichen Nutzdaten verschlüsselt und übertragen. Der Empfänger der Nachricht entschlüsselt die Daten (mit dem Sitzungsschlüssel) und berechnet erneut die Signatur über die entschlüsselten Nutzdaten und vergleicht diese mit der mitgesendeten Signatur des Absenders. Werden Abweichung dieser Werte festgestellt werden empfangenen Daten verworfen, da eine Datenmanipulation aufgedeckt wurde, ansonsten erfolgt eine Verarbeitung der empfangenen Daten.

Die eingesetzten Kryptographie- und Signaturalgorithmen sowie ihre jeweiligen Schlüsselstärken werden entsprechend den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik in der jeweiligen aktuellen technischen Richtlinie angepasst.

3.6 Verfügbarkeit und Datensicherung

Die EDV-Systeme sind durch verschiedene Maßnahmen gegen Datenverlust und Systemausfall geschützt. Tägliche Datensicherungen garantieren, dass bei Verlust der Funktionsfähigkeit des Systems keine Daten verloren gehen. Für den Fall von Brand- und Elementarschaden oder anderen schädigenden Ereignissen werden diese Sicherungen außerhalb der Räumlichkeiten der BPS aufbewahrt. Derzeitig kann ein Datenbestand zu dem Schaden bzw. dem Verlust vorangehenden Werktag rekonstruiert werden.

Technische Ausfälle an Speichermedien werden über sogenannte RAID-Systeme (Festplattenspiegelung) abgefangen und unterbrechen nicht den Betrieb des EDV-Systems. Stromausfälle werden über eine unterbrechungsfreie Stromversorgung abgefangen und garantieren bei längerem Ausfall das ordnungsgemäße Herunterfahren der Server, um Datenverlust vorzubeugen.

Bei Brand- und Elementarschaden, die nicht durch geeignete Maßnahmen verhindert werden können und bei denen die gesamte Datenverarbeitungsanlage zerstört wird, müssen längere Ausfallzeiten kalkuliert werden. Die Ausfallzeit beläuft sich auf die Wiederbeschaffung geeigneter Hardware, sowie auf die Inbetriebnahme dieser. Durch die außerhäusliche Lagerung der Datensicherungen kann ein zumindest in der Leistungsfähigkeit eingeschränkter Betrieb erfolgen. Auf Grund der Wahrscheinlichkeit des Eintretens eines solchen Schadenfalls wird die Ausfallzeit als akzeptabel angesehen.

4. Verantwortung des Anwenders

Die Client-Anwendung nimmt keine eigenständige persistente Speicherung von personen- oder unternehmensbezogenen Daten auf dem Arbeitsplatzrechners eines Anwenders vor. Der Abruf von solchen Daten erfolgt manuell durch den Anwender, wobei diesem jegliche Verantwortung bezüglich Umgang und Speicherort dieser Daten obliegt. Jeder Anwender ist zu einem verantwortungsbewussten Umgang mit diesen Daten und mit seinen individuellen Zugangsdaten für die Anwendung angehalten.

5. Datenübermittlung an Dritte

Zur Erfüllung steuerrechtlicher und sozialversicherungsrechtlicher Pflichten ist abhängig von der jeweiligen Dienstleistungsvereinbarung die Übermittlung personenbezogener Daten an Dritte notwendig. Empfänger dieser Daten sind Finanzbehörden oder Institutionen der Sozialversicherungsträger. Für die Übermittlung dieser Daten setzt BPS externe und zugelassene Software ein, deren Sicherheit in Bezug auf die Datenübertragung von den jeweiligen verantwortlichen Stellen reguliert wird und nicht von BPS beeinflusst werden kann.

Neben diesen Datenübermittlungen werden Datenexporte bereitgestellt deren Weitergabe nicht in den Verantwortungsbereich der BPS fällt. Der abrufende Anwender hat für den Umgang mit diesen Daten Sorge zu tragen.

Datenübermittlungen in Drittstaaten ergeben sich nur im Rahmen der Vertragserfüllung, erforderlicher Kommunikation sowie anderer im BDSG ausdrücklich vorgesehener Ausnahmen. Im Übrigen erfolgt keine Übermittlung in Drittstaaten; eine solche ist auch nicht geplant.

6. Unterbeauftragung

Sofern sonstige Dienstleister bzw. Unterauftragnehmer von BPS beansprucht werden und diese Beauftragung den Umgang mit personenbezogenen Daten erforderlich macht, ist es unerlässlich, dass seitens der jeweiligen Unternehmen eine unterzeichnete Datenschutzverpflichtungserklärung nach BDSG vorliegt. Sofern die Erteilung solcher Auftragsverhältnisse die Zustimmung eines Dritten erfordert, wird BPS diese Zustimmung über den Auftraggeber einholen.

7. Löschung von Daten und Aufbewahrungsfristen

BPS behält sich vor, personen- und unternehmensbezogene Daten aus dem EDV-System zu löschen. Eine Löschung erfolgt frühestens nach Ablauf einer Frist von zehn Jahren, spätestens jedoch nach Ablauf der darüber hinaus gehenden gesetzlichen Aufbewahrungsfristen. Für die Löschung der Daten bedarf es keiner Einwilligung des Auftraggebers oder der betroffenen Person.