



Fachkreis Administration

Outsourcing der Verwaltung von Zeitwertkonten:
Rechtskonforme Gestaltung unter Datenschutzaspekten



Nicolas Hoeltgen

Die Verwaltung von Zeitwertkonten unterliegt hohen gesetzlichen Anforderungen, die zuletzt im Gesetz zur Verbesserung der Rahmenbedingungen für die Absicherung flexibler Arbeitszeiten (Flexi II) novelliert wurden. Auf Grund der Komplexität der Materie beauftragen zahlreiche Unternehmen externe Spezialisten mit der

Administration dieser Konten. Argumente für ein solches Outsourcing sind neben der Schonung hauseigener Ressourcen vor allem der Rückgriff auf professionelle, mit der Materie vertraute Experten und die Etablierung transparenter Kostenstrukturen bei gleichzeitigem Profitieren von den Skaleneffekten des Anbieters.

Trotz dieser Vielzahl an offensichtlichen Vorteilen muss berücksichtigt werden, dass dabei personenbezogene Daten das Unternehmen verlassen und somit Risiken auch für das Unternehmen als Auftraggeber entstehen. Dazu folgendes Fallbeispiel:

Ein Unternehmen hat die technische Abwicklung der betrieblichen Zeitwertkonten im Rahmen eines Application-Services an einen Dienstleister ausgelagert. Die Datenverarbeitung findet so statt, dass Mitarbeiter des Dienstleisters im Zuge der Administration und Datensicherung auch Zugriff auf die Lohndaten nehmen können. Aus ungeklärter Ursache werden persönliche Daten von Mitarbeitern des Auftraggebers öffentlich zugänglich. Betroffene Mitarbeiter beschwerten sich bei der zuständigen Aufsichtsbehörde des jeweiligen Bundeslandes. Der Arbeitgeber hat im Dienstleistungsvertrag lediglich die Verfügbarkeit und das Wiederanlaufen des Dienstes der Zeitwertkontenadministration geregelt, nicht jedoch das Thema Datensicherheit. Damit verstößt der Arbeitgeber gegen die Vorschriften der zweiten Datenschutznovelle für Verträge, die nach dem 1. September 2009 in Kraft treten. Diese Novelle sieht Sanktionen bei nicht richtiger, nicht vollständiger oder nicht vorgeschriebener Weise erfolgter Erteilung eines Auftrages vor (vgl. § 43 Abs. 1 Nr. 2b und § 43 Abs. 3 des deutschen Bundesdatenschutzgesetzes). Konkret droht unserem Arbeitgeber ein Bußgeld von bis zu 50.000 Euro.

Wie also umgehen mit diesen Risiken? Was müssen Arbeitgeber berücksichtigen? Wie sollten vertragliche Vereinbarungen gefasst sein, um das Risiko für den Arbeitgeber zu minimieren?

Die Gesetzesgrundlage

Der Begriff der Auftragsdatenverarbeitung ist nicht endgültig im Gesetz definiert und ist deshalb von anderen Begriffen, wie zum Beispiel der Funktionsübertragung abzugrenzen.

Ein Hauptmerkmal der Auftragsdatenverarbeitung ist, dass der Auftraggeber für die Einhaltung der entsprechenden Vorschriften über den Datenschutz verantwortlich bleibt. Das bedeutet im Gegenzug, dass der Dienstleister weisungsgebunden ist und lediglich eine unterstützende Hilfsfunktion für den Auftraggeber (vgl. § 3 Abs. 7 und 8 Bundesdatenschutzgesetz, im Folgendem „BDSG“) übernimmt. Die Vergabe des Auftrags hat unter besonderer Berücksichtigung der technischen und organisatorischen Eignung des Auftragnehmers zu erfolgen. Der Auftrag hat schriftlich zu erfolgen, wobei die Datenverarbeitung selber sowie die zugehörigen technischen und organisatorischen Maßnahmen zu beschreiben sind. Zu diesen Maßnahmen gehört insbesondere auch die Gewährleistung der Auftragskontrolle. Der Auftragnehmer bleibt bezogen auf die Datenverarbeitung weisungsgebunden (vgl. Bundesamt für Sicherheit in der Informationstechnik, www.bsi.de).

Im Folgenden befassen wir uns primär mit dem für IT-Outsourcing maßgeblichen An-

forderungskatalog des geänderten § 11 des BDSG, der die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag regelt. Die unten genannte Fassung wurde mit der zweiten Datenschutznovelle verabschiedet und trat am 01.09.2009 in Kraft.

Wie ist nun der Wortlaut im § 11 BDSG, der sich explizit mit der „Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag“ beschäftigt? In Absatz 1 steht:

„Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben,

personenbezogener Daten (vgl. § 3 Abs. 5 BDSG). Daten über den Betroffenen können sowohl Betragsangaben und Investitionsziele individueller Wertguthaben sein, die dem einzelnen Arbeitnehmer zugeordnet werden, als auch personenbezogene Angaben, die z.B. für eine Abwicklung im Stör- od. Insolvenzfall benötigt werden.

Die schriftliche Festlegung zumindest für Verträge nach dem 01.09.2009 wird im Einzelnen durch einen Maßnahmenkatalog in § 11 Abs. 2 geregelt. Das Erfordernis einer Anpassung von Altverträgen wird in der Literatur teilweise verneint (vgl. Hanloser, MMR 2009, 594, 597).

Ein Hauptmerkmal der Auftragsdatenverarbeitung ist, dass der Auftraggeber für die Einhaltung der entsprechenden Vorschriften über den Datenschutz verantwortlich bleibt. Das bedeutet im Gegenzug, dass der Dienstleister weisungsgebunden ist und lediglich eine unterstützende Hilfsfunktion für den Auftraggeber übernimmt.

verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich.“

Unter Erheben versteht der Gesetzgeber das Beschaffen von Daten über den Betroffenen (vgl. § 3 Abs. 3 BDSG). Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen von personenbezogenen Daten (vgl. § 3 Abs. 4 BDSG), Nutzung bezieht sich auf die Verwendung

Der Anforderungskatalog im Einzelnen

Die vom Gesetzgeber vorgegebenen Mindestinhalte eines Vertrages zur Auftragsdatenverarbeitung nach § 11, Abs. 2 werden im Folgenden genauer betrachtet.

Festzuhalten ist, dass alle Punkte zwingend in der vertraglichen Vereinbarung enthalten sein müssen.



1. Der Gegenstand und die Dauer des Auftrags.

Dieser Punkt wird zwischen den Parteien üblicherweise im Rahmen eines Dienstvertrags geregelt. Im Fall von Zeitwertkonten ist der Gegenstand der Vereinbarung die Verwaltung der betrieblichen Zeitwertkonten über einen bestimmten Zeitraum. In der Regel wird ein fester Zeitraum vereinbart, der sich im Folgenden laufend verlängert.

2. Der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen

Eine schriftliche Konkretisierung des Auftrags ist Bestandteil eines Leistungsverzeichnisses, während hierbei eine konkrete Schnittstellenbeschreibung eindeutige Angaben zur Art der Daten macht. Da gerade am Anfang eines Projektes das entsprechende Datenmodell noch nicht fest definiert ist, kann es ratsam sein die Daten abstrakt festzulegen, um sie später genauer zu spezifizieren.

3. Die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen

Der Gesetzgeber hat hierbei kein bestimmtes Produkt oder einen Standard genannt. Vielmehr soll das Verhältnis von Maßnahmen zum Schutzzweck sichergestellt sein. Da bei der Administration von Zeitwertkonten sehr sensible Personaldaten verwaltet werden, sind entsprechende IT-Standards Pflicht. Hierzu gehört die Verpflichtung zur Einführung von Zutritts-, Zugangs- und Zugriffskontrollen. Kern dieser Punkte ist die Sicherstel-

lung dass unberechtigte Personen keinen Zutritt, Zugang und Zugriff auf die personenbezogenen Daten erhalten. Dies ist unter anderem durch ein umfangreiches Berechtigungskonzept des ausgewählten Administrators sicherzustellen. In diesem Konzept sollten Maßnahmen zum Schutz der Gebäude, Räume, Betriebssysteme, Server und Datenbanken beschrieben sein. In der Praxis erfolgt dies regelmäßig durch eine wirksame Identifikation und anschließende Authentifikation von Zugriffsberechtigten.

Die Weitergabekontrolle stellt sicher, dass personenbezogene Daten bei Ihrer Übertragung entsprechend gesichert sind. Hierbei ist die oftmals genutzte verschlüsselte Exceltabelle via E-Mail sicherlich kein adäquates Mittel. Vielmehr empfehlenswert sind technisch sicherere Verfahren, wie beispielsweise das VPN (Virtual Private Network)-Verfahren oder ein gesichertes HTTPS Verfahren mit einer jeweiligen an die aktuellen technischen Verhältnisse angepassten Verschlüsselung. Bei der Eingabekontrolle muss in nachvollziehbarer Weise einsehbar sein, wer wann welche personenbezogenen Daten erfasst, geändert oder gelöscht hat. Dies erfolgt in der Regel durch Logdateien der Anwendungssoftware und der Datenbanken.

Die Auftrags- und Zweckbindungskontrolle stellt zwingend sicher, dass die dem Auftragnehmer überlassenen Daten nur zu dem vertraglichen Zweck verwendet werden. Hierzu kann unter anderem das interne Kontrollsystem mit den standardisierten Vertragswerken abgeglichen werden. Eine weitere wichtige Prüfung erfolgt durch die Verfügbarkeitskontrolle, die

sicherstellen soll, dass personenbezogene Daten vor Zerstörung geschützt sind. Hierzu sollte der Dienstleister ein umfangreiches Backup- und Recoverykonzept vorhalten. Der Auftraggeber sollte sich vor Auftragsvergabe einen Blick über die Dokumentation machen. Gibt es z.B. ein „Notfall-Handbuch“ das Fragen zum Schutz der Daten beantwortet und einen Plan auf mögliche Szenarien beinhaltet?

4. Die Berichtigung, Löschung und Sperrung von Daten

Der Auftraggeber muss die Möglichkeit schriftlich fixieren, dass er bei Bedarf die Berechtigung, Löschung und Sperrung der Daten veranlassen kann. Soweit sich ein Betroffener direkt an den Auftragnehmer wendet, hat er die Anfrage unverzüglich an den Auftraggeber weiterzuleiten. Wichtig ist in diesem Zusammenhang etwaige gesetzliche Aufbewahrungsfristen zu kennen und einzuhalten.

5. Die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen

Im Rahmen der Auftragskontrolle hat der Auftraggeber die ordnungsgemäße Umsetzung der im Satz 4 genannten Pflichten zu prüfen und gegenüber dem Auftragnehmer schriftlich zu fixieren. In der Praxis werden solche Prüfungen gelegentlich durch unabhängige Instanzen, wie bspw. Wirtschaftsprüfer im Auftrag durchgeführt. Wünschenswert ist es, dass der Auftragnehmer eine gewisse Affinität gegenüber dem technischen Fortschritt beweist, um zeitnah an der ständig weiterlaufenden Entwicklung in der Informationsverarbeitung zu partizipieren.

6. Die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen

Ein Unterauftragsverhältnis im Sinne der Ziffer 6 ist eine Beauftragung, die unmittelbar mit der Erfüllung des Auftrags notwendig ist (vgl. GDD Arbeitskreis „Datenschutz-Praxis“). Ein Beispiel könnte sein, dass ein Kapitalanlageinstitut einem Arbeitgeber nicht nur die Kapitalanlage sondern auch die Administration von Zeitwertkonten vertraglich anbietet, für die Verwaltung aber ein Unterauftragsverhältnis eingeht. Dann sollte zumindest die Berechtigung hierzu schriftlich erfolgt sein.

7. Die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers

Da der Arbeitgeber weiterhin auch bei der Auftragsdatenverarbeitung alle Pflichten behält, muß er sich etwaige Kontrollbefugnisse explizit bestätigen lassen. Der Auftragnehmer duldet diese Kontrollpflicht und unterstützt den Auftraggeber.

8. Mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen

Es ist unrealistisch davon auszugehen, dass der Auftraggeber die Datenverarbeitung permanent überwachen kann. Andererseits können auch zwischen den einzelnen Überwachungsterminen Fehler auftreten, die bis hin zu Verletzungen des BDSG führen. Dies hat der Auftragnehmer dem Auftraggeber unverzüglich mitzuteilen.

9. Der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält

Als Beispiel für eine Weisung soll das Trennungsgebot dienen. Hiermit ist die Separation des Datenbestandes des Auftraggebers von dem anderer Auftraggeber innerhalb des Systems der Auftragnehmer gemeint. In der Regel wird ein Administrator eine Vielzahl von Datenverarbeitungstätigkeiten auch für weitere Auftraggeber vornehmen, so gilt natürlich auch hier das Trennungsgebot. Es ist also durchaus im Sinne des Auftraggebers, sich derartige Weisungsbefugnisse vorzubehalten.

Außerdem kann sich der Auftraggeber beispielsweise das Recht einräumen lassen, während der Vertragslaufzeit dem Auftragnehmer weitere Weisungen bezüglich Zweck, Art und Umfang der Verarbeitung von Daten an den Auftragnehmer zu erteilen.

10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Viele der in der Praxis regelmäßig zu beobachtenden Verstöße gegen das Datenschutzgesetz wurden durch das Fehlen von Regelungen zu Überlassung- und Rückgabe sowie entsprechender Erklärungen der Parteien erst möglich. Ganze Datenbanken wurden nach Beendigung des Auftrags zweckentfremdet und gewinnbringend an weitere Unternehmen verkauft. Daher wird nun gefordert, den Auftragnehmer auf die Rückgabe oder Löschung der Daten nach Beendigung

des Auftrags zu verpflichten. Aufzuführen ist hierbei welche Daten zurückgegeben werden sowie wie die Löschung zu erfolgen hat. Empfehlenswert ist auch eine Dokumentation der durchgeführten Maßnahmen.

Fazit:

Festzuhalten ist, dass die externe Administration von betrieblichen Zeitwertkonten in jedem Fall eine Auftragsdatenverarbeitung gemäß Bundesdatenschutzgesetz ist. Daraus folgt zwingend, dass eine schriftliche Vereinbarung zwischen den Vertragsparteien erfolgen muss, die den Maßnahmenkatalog des § 11 Abs. 2 beinhaltet. Es ist im Eigeninteresse des beauftragenden Arbeitgebers den Dienstleister zu verpflichten, die Entwicklung und konkrete Ausgestaltung des Maßnahmenkatalogs periodisch nachzuweisen. Dies erleichtert die Kontrolle und ggfs. die Einleitung von Prozesskorrekturen. Eine entsprechende vertragliche Gestaltung ermöglicht es dem Arbeitgeber, von den unbestreitbaren Vorteilen der Auslagerung zu profitieren ohne auf dem Feld des Datenschutzes unnötige Risiken einzugehen.

