ADP Privacy Code für Kundendatenverarbeitungsdienste

ADP Privacy Code für Kundendatenverarbeitungsdienste

Einleitung

ADP stellt ihren Kunden eine Vielzahl verschiedener Human Capital Management Services zur Verfügung. ADP hat sich im **ADP Kodex für Geschäftsverhalten und Ethik** zum Schutz Personenbezogener Daten verpflichtet.

In diesem ADP Privacy Code für Kundendatenverarbeitungsdienste wird erläutert, wie ADP die Verpflichtungen für die Verarbeitung von Personenbezogenen Daten, die sich auf die Beschäftigten des Kunden beziehen, im Zusammenhang mit der Bereitstellung von Kundenservices und Kundensupportservices umsetzt. In diesem Rahmen werden Kundendaten von ADP als Auftragsverarbeiter im Namen der Kunden verarbeitet.

Die Regeln, die für ADP als Datenverantwortliche bei der Verarbeitung Personenbezogener Daten von Betroffenen gelten, mit denen ADP eine Geschäftsbeziehung hat (z.B. Einzelpersonen, die im Namen des Kunden handeln, Zulieferer, Geschäftspartner, andere Geschäftskontakte und Verbraucher), und anderen Einzelpersonen, deren Personenbezogene Daten ADP im Zusammenhang mit ihren Geschäftsaktivitäten als Datenverantwortliche verarbeitet, finden Sie in den ***ADP Privacy Code für Geschäftsdaten***.

Artikel 1 – Umfang, Anwendbarkeit und Umsetzung

Umfang und Anwendbarkeit für EWR-Daten	**1.1**	Dieser Code betrifft die Verarbeitung von Personenbezogenen Daten durch ADP in ihrer Rolle als Auftragsverarbeiter für Kunden im Zuge der Erbringung von Kundenservices, wenn solche Personenbezogene Daten (a) anwendbarem EWR-Recht unterliegen (oder geltendem EWR-Recht unterlagen, bevor sie an eine andere Konzerngesellschaft in einem Land außerhalb des EWR übermittelt wurden, bei dem die zuständigen EU Institutionen nach Anwendbarem Recht nicht davon ausgehen, dass ein angemessenes Datenschutzniveau vorliegt); und (b) gemäß einem Servicevertrag verarbeitet werden, der ausdrücklich festlegt, dass dieser Code auf solche Personenbezogenen Daten anwendbar ist. Bei Fragen zur Anwendbarkeit dieses Codes wird sich der zuständige Privacy Steward mit dem Global Data Privacy and Governance Team in Verbindung setzen und beraten, bevor eine Verarbeitung stattfindet.
Elektronische und papierbasierte Verarbeitung	**1.2**	Dieser Code bezieht sich auf die Verarbeitung Personenbezogener Daten mit elektronischen Mitteln und in systematisch zugänglichen papierbasierten Ablagesystemen.
Anwendbarkeit von nationalem Recht	**1.3**	Keine der Bestimmungen in diesem Code enthält Einzelpersonen irgendwelche Rechte oder Rechtsbehelfe vor, die ihnen gemäß Anwendbarem Recht zustehen, und darf auch nicht so ausgelegt werden. Sofern Anwendbares Recht einen höheren Schutz bietet als dieser Code gelten die Bestimmungen des Anwendbaren Rechts. Sofern hingegen dieser Code einen höheren Schutz bietet als Anwendbares Recht oder zusätzliche Absicherungen, Rechte oder Abhilfen vorsieht, dann gilt dieser Code.

Standards und Leitlinien	**1.4**	ADP kann diesen Code durch verbindliche Richtlinien, Standards, Leitlinien und Anweisungen ergänzen, die mit diesem Code in Einklang stehen.
Verantwortlichkeit	**1.5**	Dieser Code ist für ADP verbindlich. Verantwortlich für dessen Einhaltung durch die Geschäftseinheiten sind die Verantwortlichen Führungskräfte. Die Belegschaft von ADP ist verpflichtet, diesen Code einzuhalten.
Datum des Inkrafttretens	**1.6**	Dieser Code wurde vom General Counsel nach Vorlage durch den Global Chief Privacy Officer genehmigt und vom ADP Führungskreis angenommen. Dieser Code gilt ab 11. April 2018 (Datum des Inkrafttretens). Der Code (einschließlich einer Liste der Konzerngesellschaften, die an der Verarbeitung von Kundendaten beteiligt sind) werden auf der Webseite www.adp.com veröffentlicht. Auf Anfrage kann er auch Einzelpersonen zur Verfügung gestellt werden. Die ADP Gruppe wird diesen Code entsprechend den in Artikel 16 angegebenen Zeitrahmen umsetzen.
Frühere Richtlinien	**1.7**	Dieser Code ergänzt die Datensicherheits- und Datenschutzvorgaben von ADP und ersetzt vorherige Erklärungen, soweit sie diesem Code widersprechen.
Rolle der Beauftragten ADP Konzerngesellschaft	**1.8**	Automatic Data Processing, Inc. hat ADP Nederland B.V. mit Sitz in Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Niederlande, als von ADP Beauftragte Konzerngesellschaft benannt und mit der Durchsetzung des Codes innerhalb der ADP Gruppe beauftragt. ADP Nederland, B.V. hat diesen Auftrag angenommen.

Artikel 2 – Servicevertrag

Servicevertrag, Unterauftrags-verarbeiter	**2.1**	ADP wird Kundendaten nur auf der Grundlage eines Servicevertrages verarbeiten, der die verbindlichen vertraglichen Anforderungen gemäß Anwendbarem Auftragsverarbeiter-Recht enthält, und nur für legitime Zwecke, wie in Artikel 4 angegeben. Die Vertragsschließende ADP Konzerngesellschaft nutzt Unterauftragsverarbeiter, d.h. sowohl ADP Unterauftragsverarbeiter als auch Externe Unterauftrags-verarbeiter zur regelmäßigen Erbringung von Kundenservices. ADP's Serviceverträge autorisieren die Nutzung solcher Unterauftragsverarbeiter, vorausgesetzt die Vertragsschließende ADP Konzerngesellschaft bleibt dem Kunden für die Leistung des Unterauftragsverarbeiters gemäß den Bedingungen des Servicevertrages haftbar. Für die Nutzung von Unterauftragsverarbeitern gelten ferner die Bestimmungen des Artikel 7.

Beendigung des Service-vertrages	**2.2**	Bei Beendigung der Kundenservices erfüllt ADP dem Kunden gegenüber ihre Verpflichtungen aus dem Servicevertrag im Hinblick auf die Rückgabe der Kundendaten, indem sie dem Kunden die Kundendaten herausgibt, die für die Kontinuität der Geschäftstätigkeiten erforderlich sind (falls die Daten nicht bereits vorher geliefert oder dem Kunden über eine entsprechende Produktfunktionalität zugänglich gemacht wurden, wie beispielsweise die Möglichkeit zum Herunterladen von Kundendaten). Nach Erfüllung der Verpflichtungen von ADP aus dem Servicevertrag, zerstört ADP die verbleibenden Kopien der Kundendaten sicher und erbringt (auf Ersuchen des Kunden) eine Bescheinigung darüber, dass dies geschehen ist. ADP darf eine Kopie von Kundendaten zurückbehalten, soweit dies nach Anwendbarem Recht gefordert ist, oder wie vom Kunden genehmigt oder wie zum Zwecke einer Streitbeilegung erforderlich. ADP darf diese Kundendaten nicht länger verarbeiten, als in dem Maß, in dem es für die vorgenannten Zwecke erforderlich ist. ADP‘s Vertraulichkeitspflichten nach dem entsprechenden Servicevertrag bleiben solange bestehen, wie ADP eine Kopie dieser Kundendaten vorhält.
Überprüfung von Beendigungsmaßnahmen	**2.3**	Innerhalb von 30 Tagen nach Beendigung des Servicevertrages (es sei denn, eine zuständige Aufsichtsbehörde fordert etwas anders) stellt ADP auf Antrag des Kunden oder der zuständigen Aufsichts-behörde ihre Datenverarbeitungseinrichtungen für ein Audit zur Verfügung gemäß Artikeln 11.2 oder 11.3 (falls anwendbar), um zu verifizieren, dass ADP ihre Verpflichtungen im Zusammenhang mit der Beendigung des Servicevertrages nach Artikel 2.2 erfüllt.

Artikel 3 – Verpflichtungen zur Einhaltung von Vorgaben

Weisungen des Kunden	**3.1**	ADP verarbeitet Kundendaten im Auftrag des Kunden ausschließlich in Übereinstimmung mit dem Servicevertrag, gemäß dokumentierter vom Kunden erhaltener Weisungen oder wie es Anwendbares Recht verlangt.
Einhaltung anwendbarer Rechtsvorschriften	**3.2**	ADP verarbeitet Kundendaten gemäß dem Anwendbaren Auftragsverarbeiter-Recht. Nach Maßgabe des Servicevertrages antwortet ADP unverzüglich und angemessen auf Hilfeersuchen des Kunden und ermöglicht es dem Kunden, seinen Verpflichtungen gemäß Anwendbarem Daten-verantwortlicher-Recht nachzukommen.
Nichteinhaltung von Vorgaben, erhebliche nachteilige Auswirkungen	**3.3**	Falls eine Konzerngesellschaft erfährt, dass das Anwendbare Auftragsverarbeiter-Recht eines Landes außerhalb des EWR oder eine Änderung des Anwendbaren Auftragsverarbeiter-Recht eines Landes außerhalb des EWR oder eine Weisung des Kunden wahrscheinlich eine erhebliche Beeinträchtigung der Fähigkeit von ADP darstellen würde, ihren Verpflichtungen nach 3.1., 3.2. oder 11.3 nachzukommen, wird diese Konzerngesellschaft die Beauftragte ADP

Konzerngesellschaft und den Kunden unverzüglich davon in Kenntnis setzen. In einem solchen Fall hat der Kunde gemäß diesem Code das Recht, die entsprechende Übermittlung von Kundendaten an ADP vorübergehend einzustellen, bis die Verarbeitung angepasst wurde, um die festgestellte Non-Compliance zu beheben. Sollte eine Anpassung nicht möglich sein, hat der Kunde das Recht, den entsprechenden Teil der Verarbeitung durch ADP gemäß den Bedingungen des Servicevertrages zu beenden. Diese Rechte und Pflichten bestehen nicht, wenn die Umstände oder eine Änderung im Anwendbaren Auftragsverarbeiter-Recht die Folge von Zwingenden Auflagen sind.

Antrag auf Offenlegung von Kundendaten

3.4 Wenn ADP von einer Strafverfolgungsbehörde oder Staatssicherheitsbehörde eines Landes außerhalb des EWR (Ersuchende Behörde) eine Aufforderung erhält, Kundendaten an sie weiterzugeben, nimmt ADP zunächst eine fallbezogene Prüfung vor, ob dieses Ersuchen rechtsgültig und für ADP verbindlich ist. ADP wird jedes Ersuchen, das nicht rechtsgültig und für ADP nicht bindend ist, in Einklang mit Anwendbarem Recht ablehnen.

Vorbehaltlich des nachfolgenden Absatzes informiert ADP den Kunden, die Führende Aufsichtsbehörde und die für den Kunden nach Artikel 11.3 zuständige Aufsichtsbehörde unverzüglich über ein solches rechtsgültiges und für ADP bindendes Ersuchen seitens einer Ersuchenden Behörde und verlangt von der Aufsichtsbehörde, dieses für einen angemessenen Zeitraum aufzuschieben, damit die Führende Aufsichtsbehörde eine Stellungnahme über die Rechtsgültigkeit der geforderten Offenlegung geben kann.

Sollte ein solches Aussetzen und/oder die Benachrichtigung über ein rechtsgültiges und für ADP bindendes Offenlegungsersuchen verboten sein, zum Beispiel gemäß strafrechtlichen Bestimmungen, um die Vertraulichkeit einer Untersuchung durch Strafverfolgungsbehörden zu wahren, wird ADP die Ersuchende Behörde auffordern, auf dieses Verbot zu verzichten, und entsprechend dokumentieren, dass ein solcher Antrag gestellt wurde. ADP wird der Führenden Aufsichtsbehörde jährlich allgemeine Informationen über Anzahl und Art von Offenlegungsersuchen, die sie in den letzten 12 Monaten erhalten hat, zukommen lassen.

Die Bestimmungen in diesem Artikel sind nicht anwendbar auf Ersuchen, die ADP von Behörden im Rahmen ihrer ordentlichen Geschäftstätigkeit als HCM Dienstleister erhält (wie Gerichtsbeschlüsse zur Lohnpfändung), denen ADP weiterhin nachkommen kann nach Maßgabe des Anwendbaren Rechtes, des Servicevertrages und der Weisungen des Kunden.

Kundenanfragen

3.5 ADP wird unverzüglich und angemessen auf Kundenanfragen im Zusammenhang mit der Verarbeitung von Kundendaten gemäß den Bestimmungen des Servicevertrages antworten.

Artikel 4 – Zwecke für die Verarbeitung Personenbezogener Daten

Berechtigte Geschäftszwecke

4.1 ADP verarbeitet Personenbezogene Daten (einschließlich Besonderer Datenkategorien) von Beschäftigten des Kunden, soweit dies erforderlich ist für die Erbringung von Kundenservices und Kundensupportservices und für die folgenden zusätzlichen Zwecke:

(a) Hosting, Speicherung und Verarbeitung, die für die Geschäftskontinuität und Notfallwiederherstellung notwendig sind, einschließlich der Erstellung von Sicherungs- und Archivkopien Personenbezogener Daten;

(b) System- und Netzwerkadministration und Sicherheit, einschließlich Überwachung der Infrastruktur, Verwaltung von Identitäts- und Berechtigungsnachweisen, Verifizierung und Authentifizierung und Zugangskontrolle;

(c) Überwachung und andere Kontrollen, die für die Gewährleistung der Sicherheit und Integrität der Transaktionen (z.B. Finanztransaktionen und Geldbewegungsaktivitäten) notwendig sind, einschließlich Due Diligence Prüfungen (wie z.B. die Überprüfung der Identität von Einzelpersonen und ob die Einzelperson zum Erhalt von Produkten und Dienstleistungen berechtigt ist oder wie z.B. die Überprüfung von Anstellungs- und Accountstatus);

(d) Durchsetzung von Verträgen und Schutz von ADP, ihren Mitarbeitern, Kunden, den Beschäftigten des Kunden und der Öffentlichkeit vor Diebstahl, Haftung, Betrug oder Missbrauch, einschließlich: (i) Erkennung, Untersuchung, Prävention und Abmilderung von Schäden durch tatsächlichen oder versuchten Finanzbetrug, Identitätsbetrug und andere Bedrohungen für finanzielle und physische Vermögenswerte, Zugangsberechtigungen und Informationssysteme, (ii) Teilnahme an Initiativen zur externen Cyber-Sicherheit, Bekämpfung von Betrug und Geldwäsche und (iii) je nach Erfordernis, zum Schutz von grundlegenden Interessen von Einzelpersonen, beispielsweise durch die Warnung vor bekannten Sicherheitsbedrohungen;

(e) interne Abwicklung von Geschäftsprozessen und Management durch ADP, die zwangsläufig zur Verarbeitung von Kundendaten führen zum Zwecke von:

(1) Internen Überprüfungen und konsolidierter Berichterstattung;

(2) Einhaltung gesetzlicher Vorschriften, einschließlich Archivierungspflichten, Pflichten zur Nutzung und Offenlegung von Informationen, die nach Anwendbarem Recht verlangt sind;

(3) Unkenntlichmachung von Daten und Zusammenfassung von unkenntlich gemachten Daten zur Datenminimierung und Analyse von Services;

(4) Nutzung von unkenntlich gemachten und zusammengefassten Daten, wie von den Kunden erlaubt, zur Erstellung von Analysen, Bewahrung von Kontinuität und Verbesserung von Produkten und Services der ADP; und

(5) Unterstützen der Unternehmensführung einschließlich Zusammenschlüsse, Übernahmen, Veräußerungen und Joint Ventures.

Artikel 5 – Sicherheitsanforderungen

Datensicherheit **5.1** ADP ergreift kommerziell angemessene und geeignete technische, physische und organisatorische Maßnahmen, die die Anforderungen gemäß Anwendbarem EWR-Recht oder strengere Anforderungen nach Maßgabe des Servicevertrages erfüllen, um die Kundendaten während der Verarbeitung vor Missbrauch oder versehentlichen, unrechtmäßigen oder nicht genehmigten Vorgängen, wie Vernichtung, Verlust, Änderung, Offenlegung, Erwerb oder Zugang zu schützen. ADP ergreift in jedem Fall die in **Annex 2** dieses Codes aufgeführten Maßnahmen, die ADP ändern kann, vorausgesetzt solche Änderungen stellen keine erhebliche Minderung des Sicherheitsniveaus für Kundendaten gemäß **Annex 2** dar.

Zugriff auf Personenbezogene Daten und Vertraulichkeit **5.2** Die Belegschaft ist zum Zugriff auf Kundendaten nur in dem Maße berechtigt, als dies für die anwendbaren Verarbeitungszwecke gemäß Artikel 4 erforderlich ist. ADP legt den Mitarbeitern der Belegschaft, die Zugang zu Kundendaten haben, Geheimhaltungspflichten auf.

Meldung von Datensicherheits-verletzungen **5.3** ADP informiert den Kunden unverzüglich, sobald ihr zur Kenntnis gelangt, dass sich eine Datensicherheitsverletzung ereignet hat, es sei denn, ein Mitarbeiter der Strafverfolgungsbehörden oder eine Aufsichtsbehörde bestimmt, dass eine Mitteilung ein Ermittlungs-verfahren behindern oder die nationale Sicherheit gefährden oder einen Vertrauensbruch im Industriesektor darstellen würde. In diesem Fall wird die Benachrichtigung so lange verzögert, wie von der Strafverfolgungsbehörde oder Aufsichtsbehörde verlangt. ADP antwortet unverzüglich auf Kundenanfragen im Zusammenhang mit einer solchen Datensicherheitsverletzung.

Artikel 6 – Transparenz gegenüber Beschäftigten des Kunden

Sonstige Anfragen von Beschäftigten des Kunden **6.1** ADP unterrichtet den Kunden unverzüglich über Anfragen oder Beschwerden im Zusammenhang mit der Verarbeitung Personenbezogener Daten durch ADP, die ADP direkt von Beschäftigten des Kunden erhalten hat, ohne auf solche Anfragen oder Beschwerden zu antworten, es sei denn, der Servicevertrag oder Weisungen des Kunden sehen etwas anderes vor.

Soweit ein Kunde ADP im Servicevertrag verpflichtet, auf Anfragen und Beschwerden von Beschäftigten des Kunden zu antworten, stellt ADP sicher, dass den Beschäftigten des Kunden alle angeforderten und vernünftigerweise notwendigen Informationen zur Verfügung gestellt werden (wie z.B. Ansprechpartner und Verfahren), damit der

Beschäftigten des Kunden die Anfrage oder Beschwerde wirkungsvoll einreichen bzw. erheben kann.

Die Bestimmungen von Artikel 6.1. gelten nicht für Anfragen, die ADP im Rahmen der üblichen Erbringung von Kundenservices und Kundensupportservices bearbeitet.

Artikel 7 – Unterauftragsverarbeiter

Vereinbarungen mit Externen Unterauftrags-verarbeitern

7.1 Externe Unterauftragsverarbeiter dürfen Kundendaten nur im Einklang mit einem Unterauftragsverarbeitervertrag verarbeiten. Der Unterauftragsverarbeitervertrag legt dem Externen Unterauftrags-verarbeiter für die Verarbeitung vergleichbare Datenschutzvorgaben auf, die nicht weniger Schutz bieten als die Vorgaben, die für die Vertragschließende ADP Konzerngesellschaft aufgrund des Service-vertrages und dieses Codes gelten.

Veröffentlichung einer Liste der Unterauftrags-verarbeiter

7.2 ADP veröffentlicht auf einer geeigneten ADP-Webseite eine Aufstellung der Kategorien von Unterauftragsverarbeitern, die zur Erbringung der entsprechenden Kundenservices eingeschaltet sind. Diese Aufstellung wird im Falle von Änderungen unverzüglich aktualisiert.

Mitteilung neuer Unterauftrags-verarbeiter und Recht auf Widerspruch

7.3 ADP informiert den Kunden, wenn neue Unterauftragsverarbeiter von ADP für die Bereitstellung von Kundenservices herangezogen werden. Der Kunde kann innerhalb von 30 Tagen nach Erhalt der Bekanntmachung gegen einen solchen Unterauftragsverarbeiter bei ADP schriftlich Widerspruch einlegen unter Angabe von sachlich gerechtfertigten Gründen in Bezug auf die Unfähigkeit des Unterauftragsverarbeiters zum Datenschutz der Kundendaten gemäß den Verpflichtungen aus dem Unterauftragsverarbeitervertrag, wie in Artikel 7.1 dargelegt. Für den Fall, dass die Parteien keine einvernehmliche Lösung finden können, hat ADP die Option, dem Unterauftragsverarbeiter nicht länger Zugang zu den Kundendaten zu gewähren oder dem Kunden die Möglichkeit zu geben, die betroffenen Kundenservices gemäß den Bestimmungen des Servicevertrages zu beenden.

Ausnahme

7.4 Die Bestimmungen in diesem Artikel 7 gelten nicht in Fällen, in denen der Kunde ADP anweist, es einem Dritten zu erlauben, die Kundendaten gemäß einem zwischen dem Kunden und einem Dritten (z.B. einem externen Leistungsanbieter) direkt abgeschlossen Vertrag zu verarbeiten.

Artikel 8 – Aufsicht und Einhaltung von Vorgaben

Global Chief Privacy Officer **8.1** Die ADP Gruppe setzt einen Global Chief Privacy Officer ein, der folgende Aufgaben hat:

(a) Leitung der Sitzungen des Privacy Leadership Council;
(b) Beaufsichtigung der Einhaltung dieses Codes;
(c) Beaufsichtigen, Koordinieren und Beratung mit den verantwortlichen Mitgliedern des Privacy Network betreffend Fragestellungen zum Schutz der Privatsphäre und Datenschutz;
(d) Erstellen von Jahresberichten über Datenschutz- und Datensicherheitsrisiken und Compliance-Themen für den ADP Führungskreis;
(e) Koordinieren offizieller Untersuchungen von oder Erhebungen über die Verarbeitung von Kundendaten durch eine Regierungsbehörde in Zusammenarbeit mit den verantwortlichen Mitgliedern des Privacy Network und der Rechtsabteilung von ADP;
(f) Auseinandersetzung mit Widersprüchen zwischen diesem Code und Anwendbarem Recht;
(g) Überwachen der Durchführung von Datenschutz-Folgenabschätzungen (DFSA) bzw. deren Überprüfung;
(h) Überwachen der Dokumentation sowie der Meldung und Kommunikation von Datensicherheitsverletzungen;
(i) Beratung zu den Datenverwaltungsprozessen, Systemen und Werkzeugen zur Umsetzung des Rahmenplans zum Datensicherheits- und Datenschutzmanagement wie vom Privacy Leadership Council vorgesehen, einschließlich:
    (1) Pflege, Aktualisieren und Veröffentlichen dieses Codes sowie darauf bezogener verbindlicher Richtlinien und Standards;
    (2) Beraten über Werkzeuge zur Sammlung, Pflege und Aktualisierung von Bestandsverzeichnissen mit Informationen über Struktur und Funktionsweise der zur Verarbeitung von Kundendaten eingesetzten Systeme;
    (3) Durchführen, Unterstützen oder beratende Begleitung von Datenschutzschulungen für die Belegschaft, damit diese ihre Aufgaben und Verantwortlichkeiten gemäß diesem Code kennt und wahrnimmt;
    (4) Zusammenarbeit mit der Internal Audit Abteilung von ADP und anderen, um ein geeignetes Qualitätssicherungsprogramm zu entwickeln und zu pflegen, mit dem die Einhaltung dieses Codes überwacht, geprüft und berichtet wird, und sicherstellen, dass ADP die Einhaltung des Codes bei Bedarf verifizieren und bestätigen kann;
    (5) Einführen von Verfahrensstandards zur Bearbeitung von Anfragen, Bedenken und Beschwerden im Hinblick auf Datensicherheit und Datenschutz; und
    (6) Beratung in Bezug auf geeignete Sanktionen bei Verletzung dieses Codes (z.B. Disziplinarstrafen).

Privacy Network **8.2** ADP etabliert ein Privacy Network, das geeignet ist, die Einhaltung dieses Codes in der gesamten ADP Organisation zu lenken.

Das Privacy Network etabliert und pflegt einen Rahmenplan, um den Global Chief Privacy Officer zu unterstützen und verschafft sich Überblick über die Aufgaben gemäß Artikel 8.1 und andere Aufgaben, die angemessen sind, um diesen Code umzusetzen und zu aktualisieren. Je nach ihrer Funktion in der Region oder Organisation, haben die Mitglieder des Privacy Network folgende zusätzliche Aufgaben:

(a) Beaufsichtigen der Einführung der Datenverwaltungsprozesse, Systeme und Werkzeuge, die die Einhaltung dieses Codes durch die Konzerngesellschaften in ihren jeweiligen Regionen und Organisationen ermöglichen;
(b) Unterstützen und Bewerten des übergreifenden Datensicherheits- und Datenschutzmanagements und der Compliance der Konzerngesellschaften in ihren Regionen;
(c) Regelmäßige Beratung der Privacy Stewards und des Global Chief Privacy Officer in Hinblick auf regionale oder lokale Datenschutzrisiken und Compliance Themen;
(d) Überprüfen, dass angemessene Verzeichnisse geführt werden über Systeme, die Kundendaten verarbeiten;
(e) Verfügbarkeit für Anfragen nach datenschutzrechtlicher Freigabe oder Beratung;
(f) Beschaffung der Informationen, die der Global Chief Privacy Officer für seinen Jahresbericht zu Datensicherheits- und Datenschutzthemen benötigt;
(g) Unterstützen des Global Chief Privacy Officer bei etwaigen offiziellen Untersuchungen oder Anfragen durch Behörden;
(h) Entwickeln und Veröffentlichen von Datenschutzrichtlinien und -standards für ihre jeweiligen Regionen oder Organisationen;
(i) Beratung von Konzerngesellschaften bezüglich der Aufbewahrung oder Vernichtung von Daten;
(j) Benachrichtigung des Global Chief Privacy Officer über Beschwerden und Unterstützung bei der Bearbeitung dieser Beschwerden; und
(k) Unterstützen des Global Chief Privacy Officer, anderer Mitglieder des Privacy Network, der Privacy Stewards und Anderer, damit sie:
    (1) die Konzerngesellschaften oder Organisationen unterstützen, diesen Code einzuhalten unter Anwendung der hierfür entwickelten Anleitungen, Werkzeuge und Schulungen ;
    (2) Best Practice im Datensicherheits- und Datenschutz-management an die Regionen weitergegeben;
    (3) sicherstellen, dass Datensicherheits- und Datenschutzvorgaben bei der Einführung neuer Produkte und Services bei Konzerngesellschaften oder Organisationen einbezogen werden; und
    (4) die Privacy Stewards, Konzerngesellschaften, Geschäftseinheiten, Funktionsbereiche und die Einkaufsabteilung beim Einsatz von Unter-auftragsverarbeitern unterstützen.

Privacy Stewards **8.3** Privacy Stewards sind Führungskräfte der ADP, die von einer Verantwortlichen Führungskraft und/oder vom ADP Führungskreis damit beauftragt wurden, diesen Code in einer Geschäftseinheit oder einem Funktionsbereich von ADP einzuführen und umzusetzen. Privacy Stewards sind für die effektive Umsetzung der Vorschriften in der jeweiligen Geschäftseinheit oder dem Funktionsbereich verantwortlich. Die Privacy Stewards müssen insbesondere überprüfen, ob wirksame Kontrollen für das Datensicherheits- und Datenschutzmanagement in allen Geschäftsbereichen, die mit Kundendaten zu tun haben, integriert sind und ob angemessene Ressourcen und Budgets für die Erfüllung der Verpflichtungen nach diesem Code zur Verfügung stehen. Die Privacy Stewards können bei Bedarf Aufgaben delegieren und angemessene Ressourcen zuweisen, um ihre Verantwortlichkeiten zu erfüllen und die Compliance-Ziele zu erreichen.

Die Privacy Stewards haben u.a. folgende Aufgaben:

(a) Überwachen des übergreifendenden Datensicherheits- und Datenschutzmanagements und der Compliance in ihrer Konzerngesellschaft, Geschäftseinheit oder ihrem Funktionsbereich und Überprüfen, dass alle vom Global Data Privacy and Governance Team zur Verfügung gestellten Prozesse, Systeme und Werkzeuge wirksam eingesetzt werden;

(b) Sicherstellen, dass das Datensicherheits- und Datenschutzmanagement und die Compliance-Aufgaben während der regulären Geschäftstätigkeit sowie während und nach einer organisatorischen Umstrukturierung, einem Outsourcing, Fusionen, Übernahmen und Veräußerungen angemessen delegiert werden;

(c) Zusammenarbeit mit dem Global Chief Privacy Officer und den jeweiligen Mitgliedern des Privacy Network, um neue gesetzliche Anforderungen zu verstehen und umzusetzen, und sicherzustellen, und zu überprüfen, dass die Datensicherheits- und Datenschutzmanagementprozesse aktualisiert werden, um veränderten Umständen und gesetzlichen und behördlichen Anforderungen gerecht zu werden;

(d) Beratung mit dem Global Chief Privacy Officer und den jeweiligen Mitgliedern des Privacy Network in all den Fällen, in denen ein tatsächlicher oder möglicher Widerspruch zwischen dem Anwendbaren Recht und diesem Code zutage tritt;

(e) Überwachen von Unterauftragsverarbeitern, die von der Konzerngesellschaft, Geschäftseinheit oder einem Funktionsbereich eingesetzt werden, um fortwährende Compliance der Unterauftragsverarbeiter mit diesem Code und dem Unterauftragsverarbeitervertrag zu gewährleisten:

(f) Sicherstellen, dass die Belegschaft der Konzerngesellschaft, Geschäftseinheit oder des Funktionsbereichs die Pflichtschulungen zu Datensicherheit und Datenschutz absolviert haben; und

(g) Steuerung, dass aufbewahrte Kundendaten gemäß Artikel 2.2 gelöscht, vernichtet, unkenntlich gemacht oder übertragen werden.

Verantwortliche Führungskräfte

8.4 Die Verantwortlichen Führungskräfte sind als Leiter von Geschäftseinheiten oder Funktionsbereichen dafür verantwortlich, dass in ihren Organisationen effizientes Datensicherheits- und Datenschutzmanagement implementiert wird. Jede Verantwortliche Führungskraft setzt (a) geeignete Privacy Stewards ein, (b) sorgt dafür, dass angemessene Ressourcen und Mittel für Compliance bereitgestellt werden, und (c) unterstützt bei Bedarf den Privacy Steward dabei, Compliance-Schwächen zu adressieren und Risiken anzugehen.

Privacy Leadership Council

8.5 Der Global Chief Privacy Officer leitet die Sitzungen des Privacy Leadership Council bestehend aus den Privacy Stewards, den vom Global Chief Privacy Officer ausgewählten Mitgliedern des Privacy Network und Anderen, die zur Unterstützung seiner Aufgabe erforderlich sind. Der Privacy Leadership Council wird einen Rahmenplan zur Unterstützung der Konzerngesellschaften, Geschäftseinheiten und Funktionsbereiche bei ihren Aufgaben zur Erfüllung dieses Codes und zur Unterstützung der Arbeit des Global Chief Privacy Officer erarbeiten und pflegen.

Nichtbesetzung von Mitgliedern des Privacy Network und Privacy Stewards

8.6 Sollte zu einem Zeitpunkt kein Global Chief Privacy Officer ernannt oder in der Lage sein, die Funktionen, die dieser Rolle zugewiesen sind, auszufüllen, dann ernennt der General Counsel eine Person interimsweise zum Global Chief Privacy Officer. Wenn es zu einem Zeitpunkt für eine bestimmte Region oder Organisation kein Mitglied im Privacy Network gibt, übernimmt der Global Chief Privacy Officer die in Artikel 8.2 beschriebenen Aufgaben eines solchen Mitglieds.

Wenn es zu einem Zeitpunkt keinen Privacy Steward für eine Konzerngesellschaft, eine Geschäftseinheit oder einen Funktionsbereich gibt, beauftragt die Verantwortliche Führungskraft eine geeignete Person damit, die in Artikel 8.3 beschriebenen Aufgaben zu übernehmen.

Gesetzlich vorgeschriebene Funktionen **8.7** Sofern Mitglieder des Privacy Network, z.B. Datenschutzbeauftragte gemäß innerhalb des EWR geltenden Rechts, ihre Positionen aufgrund gesetzlicher Vorschriften wahrnehmen, führen sie ihre Stellenaufgaben soweit aus, als dies nicht ihren gesetzlichen Verpflichtungen widerspricht.

Artikel 9 – Richtlinien und Verfahren

Richtlinien und Verfahren **9.1** ADP erarbeitet zur Einhaltung dieses Codes verbindliche Richtlinien, Standards, Leitlinien und Verfahren und setzt diese um.

System-informationen **9.2** ADP etabliert einfach verfügbare Informationen bezüglich Struktur und Funktionsweise aller Systeme und Prozesse zur Verarbeitung von Kundendaten wie Verzeichnisse von Systemen und Prozessen, die sich auf Kundendaten auswirken, zusammen mit im Rahmen von Datenschutz-Folgenabschätzungen (DFSA) gewonnenen Informationen. Eine Kopie dieser Informationen wird der Führenden Aufsichtsbehörde oder auf Anfrage einer für den Kunden gemäß Artikel 11.3 zuständigen Aufsichtsbehörde zur Verfügung gestellt.

Artikel 10 – Schulungen

Schulungen **10.1** ADP führt Schulungen über die Pflichten und Grundsätze gemäß diesem Code und Datensicherheits- und Datenschutzpflichten für die Belegschaft durch, die Zugang zu Kundendaten oder Verantwortlichkeiten im Zusammenhang mit der Verarbeitung von Kundendaten haben.

Artikel 11 – Compliance Überwachung und Überprüfung

Interne Audits **11.1** ADP wird Geschäftsprozesse und -verfahren, bei denen Kundendaten verarbeitet werden, regelmäßig daraufhin auditieren, ob sie mit diesem Code übereinstimmen. Dies bedeutet insbesondere:

(a) die Audits können im Verlauf der regelmäßigen Tätigkeit der Innenrevision von ADP (auch unter Einsatz unabhängiger Dritter) oder durch interne mit der Qualitätssicherung betraute Teams oder ad hoc im Auftrag des Global Chief Privacy Officer durchgeführt werden;

(b) der Global Chief Privacy Officer kann auch eine Überprüfung durch einen externen Sachverständigen verlangen und informiert die Verantwortliche Führungskraft der jeweiligen Geschäftseinheit und/oder den ADP Führungskreis entsprechend;

(c) im Rahmen des Überprüfungsprozesses werden die einschlägigen berufsrechtlichen Vorgaben bezüglich Unabhängigkeit, Integrität und Vertraulichkeit angewendet;

(d) der Global Chief Privacy Officer und das zuständige Mitglied des Privacy Network werden über die Ergebnisse der Überprüfung informiert;

(e) falls bei der Überprüfung Verstöße gegen diesen Code festgestellt werden, werden diese an den zuständigen Privacy Steward und die Verantwortlichen Führungskräfte berichtet. Die Privacy Stewards arbeiten mit dem Global Data Privacy and Governance Team zusammen, um einen geeigneten Plan zur Beseitigung der festgestellten Verstöße zu entwickeln und umzusetzen.

(f) eine Kopie der Auditergebnisse hinsichtlich der Einhaltung dieses Codes wird auf Anfrage der Führenden Aufsichtsbehörde oder der zuständigen Aufsichtsbehörde gemäß Artikel 11.3 zur Verfügung gestellt.

Kundenaudits

11.2 ADP befasst sich mit Auditanfragen des Kunden, wie in Artikel 11.2 beschrieben. ADP beantwortet Fragen des Kunden über die Verarbeitung von Kundendaten durch ADP. Für den Fall, dass der Kunde einen berechtigten Grund zur Annahme hat, dass die von ADP bereitgestellten Antworten einer weiteren Analyse bedürfen, wird ADP im Einvernehmen mit den Kunden entweder:

(a) die Einrichtungen, die sie für die Verarbeitung von Kundendaten nutzt, für ein Audit durch einen qualifizierten, unabhängigen externen Prüfer zugänglich machen, der von ADP vernünftigerweise zu akzeptieren, an Vertraulichkeitsvereinbarungen gebunden und vom Kunden beauftragt ist. Der Kunde stellt dem Global Chief Privacy Officer eine Kopie des Prüfberichts zur Verfügung, der als vertrauliche Information der ADP behandelt wird. Audits werden nicht häufiger als einmal pro Jahr pro Kunde während der Laufzeit des Servicevertrages während der normalen Geschäftszeiten durchgeführt und erfordern (i) einen schriftlichen Antrag, der mindestens 45 Tage vor dem vorgeschlagenen Audittermin bei ADP eingereicht wird; (ii) einen detaillierten, schriftlichen Auditplan, der von der Konzernsicherheitsorganisation der ADP überprüft und genehmigt wurde und (iii) den vor Ort einzuhaltenden Sicherheitsstandards der ADP. Solche Audits finden nur in Anwesenheit eines Vertreters der Konzernsicherheitsorganisation von ADP, des Global Data Privacy & Governance Team von ADP oder einer von einem zuständigen Vertreter benannten Person statt. Die Audits dürfen weder die Verarbeitungsaktivitäten von ADP noch die Sicherheit und Vertraulichkeit von Personenbezogenen Daten anderer Kunden der ADP beeinträchtigen; oder

(b) dem Kunden eine Erklärung eines qualifizierten, unabhängigen, externen Prüfers vorlegen, in der bestätigt wird, dass die von ADP etablierten Geschäftsprozesse und Verfahren, die mit der Verarbeitung von Kundendaten verbunden sind, in Einklang mit diesem Code sind.

ADP kann Kunden für solche Audits eine angemessene Gebühr in Rechnung stellen.

Dieser Artikel 11.2 ergänzt und erklärt die Auditrechte, die Kunden gemäß Anwendbarem Recht und den Serviceverträgen zustehen. Im

Falle eines Widerspruchs haben das Anwendbare Recht und der Servicevertrag Vorrang.

Audits durch Aufsichtsbehörden

11.3 Jede Aufsichtsbehörde eines EWR-Landes, die für die Auditierung eines Kunden der ADP zuständig ist, wird autorisiert, die betreffende Datenübertragung auf Compliance mit diesem Code zu denselben Bedingungen zu überprüfen, wie sie nach dem für sie Anwendbaren Datenverantwortlichen-Recht für ein Audit des Kunden selbst gelten würden.

Eine solche Überprüfung wird wie folgt ermöglicht:

(a) In dem Bestreben, dem Ersuchen nachzukommen, arbeiten ADP und der Kunde in gutem Glauben zusammen, indem sie der Aufsichtsbehörde Informationen zur Verfügung stellen, wie z.B. interne Auditberichte und indem sie Gespräche ermöglichen zwischen der Aufsichtsbehörde, dem Kunden und den Fachexperten der ADP, die die Sicherheit, den Datenschutz und die vorhandenen operativen Kontrollen beurteilen können. Der Kunde erhält Zugang zu den Kundendaten gemäß Servicevertrag und kann den Zugang an Vertreter der Aufsichtsbehörde delegieren;

(b) Falls die über die vorgenannten Mechanismen verfügbarbaren Informationen unzureichend sind, um den von der Aufsichtsbehörde formulierten Zielvorgaben gerecht zu werden, ermöglicht ADP der Aufsichtsbehörde, mit dem Prüfer von ADP zu sprechen;

(c) Falls dies unzureichend ist, räumt ADP der Aufsichtsbehörde unmittelbar das Recht ein, ADP's Datenverarbeitungseinrichtungen, die für die Verarbeitung der Kundendaten genutzt werden, zu untersuchen nach angemessener Vorankündigung und während der Geschäftszeiten und unter vollständiger Beachtung der Vertraulichkeit der erlangten Informationen und der Geschäftsgeheimnisse von ADP. Die Aufsichtsbehörde erhält nur Zugang zu solchen Kundendaten, die den entsprechenden Kunden betreffen.

Dieser Artikel 11.3 ergänzt und erklärt die Auditrechte, die Aufsichtsbehörden gemäß Anwendbarem Recht und den Serviceverträgen zustehen können. Im Falle eines Widerspruchs haben die Vorschriften des Anwendbaren Rechtes Vorrang.

Jahresbericht

11.4 Der Global Chief Privacy Officer erstellt einen Jahresbericht für den ADP Führungskreis über die Einhaltung dieses Codes, etwaige Datensicherheits- und Datenschutzrisiken und andere relevante Themen. In diesen Bericht fließen Informationen ein, die unter anderem das Privacy Network über lokale Entwicklungen und spezifische Angelegenheiten innerhalb der Konzerngesellschaften liefert.

Abhilfemaßnahmen **11.5** ADP ergreift geeignete Maßnahmen, um Abhilfe zu leisten in allen Fällen von Non-Compliance mit diesem Code, die während Compliance-Audits festgestellt werden.

Artikel 12 – Rechtsfragen

Rechte der Beschäftigten des Kunden **12.1** Wenn ADP gegen den Code verstößt in Bezug auf Personenbezogene Daten eines unter diesen Code fallenden Beschäftigten des Kunden, kann der Beschäftigte des Kunden als begünstigter Dritter die Artikel 1.5, 1.6, 2.1, 2.2, 3, 5, 6, 7.1, 7.3, 7.4, 11.2, 11.3, 12.1, 12.2, 12.3, 12.5, 12.7, 12.8 und 14.3 dieses Codes gegen die Vertragsschließende ADP Konzerngesellschaft durchsetzen.

Soweit der Beschäftigte des Kunden solche Rechte gegen die Vertragsschließende ADP Konzerngesellschaft durchsetzen kann, darf sich die Vertragsschließende ADP Konzerngesellschaft zur Vermeidung der Haftung nicht darauf berufen, dass ein Verstoß ihrer Pflichten durch einen Unterauftragsverarbeiter erfolgt ist, es sei denn, dass ein Einwand des Unterauftragsverarbeiters zugleich einen Einwand für ADP darstellt. ADP kann indes Einwände oder Rechte geltend machen, auf die sich auch der Kunde hätte berufen können. ADP kann zudem alle Einwände geltend machen, die ADP gegen den Kunden hätte geltend machen können (wie beispielsweise Mitverschulden). Für die Abwehr von Forderungen der betroffenen Einzelperson kann ADP auch alle Einwände geltend machen, die ADP gegen den Kunden hätte geltend machen können.

Beschwerdeverfahren **12.2** Die Beschäftigten des Kunden können eine schriftliche Beschwerde im Hinblick auf jeden Anspruch, den sie gemäß Artikel 12.1 haben, gegenüber dem Global Data Privacy and Governance Team per Post oder E-Mail an die am Ende dieses Codes angegebene Adresse richten. Der Beschäftigte des Kunden kann zudem eine Beschwerde oder eine Klage vor den Behörden oder Gerichten nach Maßgabe von Art. 12.3 dieses Codes einlegen.

Das Global Data Privacy and Governance Team ist für die Bearbeitung von Beschwerden verantwortlich. Jede Beschwerde wird einem geeigneten Mitarbeiter (entweder innerhalb des Global Data Privacy and Governance Team oder der zuständigen Geschäftseinheit oder des Funktionsbereichs) zugewiesen. Die Belegschaft wird:

(a) den Eingang der Beschwerde unverzüglich bestätigen;
(b) die Beschwerde prüfen und, falls erforderlich, eine Untersuchung starten;
(c) den zuständigen Privacy Steward und das zuständige Mitglied des Privacy Network unterrichten, falls die Beschwerde begründet ist, damit ein Abhilfeplan entwickelt und umgesetzt werden kann; und

(d) alle eingegangenen Beschwerden, die erfolgten Antworten und die von ADP unternommenen Abhilfemaßnahmen dokumentieren.

ADP wird angemessene Vorkehrungen treffen, Beschwerden unverzüglich zu bearbeiten, so dass der Beschäftigte des Kunden innerhalb von vier Wochen nach Einreichung der Beschwerde eine Antwort erhält. Die Antwort erfolgt schriftlich und wird dem Beschäftigten des Kunden über den von ihm für den Kontakt mit ADP verwendeten Weg (z.B. Post oder E-Mail) zugesandt. In der Antwort wird erklärt, welche Schritte ADP unternommen hat, um der Beschwerde nachzugehen, und ADP's Entscheidung, ob und wenn ja, welche Schritte sie als Reaktion auf die Beschwerde unternimmt.

Für den Fall, dass ADP ihre Untersuchung und Antwort nicht innerhalb von vier Wochen in angemessener Art und Weise abschließen kann, informiert sie den Beschäftigten des Kunden innerhalb von vier Wochen, dass die Untersuchung noch nicht abgeschlossen ist und dass eine Antwort innerhalb der nächsten acht Wochen erfolgen wird.

Falls die Reaktion von ADP auf die Beschwerde für den Beschäftigten des Kunden nicht zufriedenstellend ist (z.B. bei Ablehnung des Antrags) oder ADP die Bedingungen des Beschwerdeverfahrens gemäß Artikel 12.2 nicht einhält, kann der Beschäftigte des Kunden gemäß Artikel 12.3 bei den Behörden oder Gerichten eine Beschwerde bzw. Klage einreichen.

Gerichtsbarkeit für Ansprüche von Beschäftigten des Kunden

12.3 Beschäftigte des Kunden werden gebeten, zunächst das in Artikel 12.2 dieses Codes beschriebene Beschwerdeverfahren zu befolgen, ehe sie bei Behörden oder Gerichten eine Beschwerde oder Klage einreichen.

Beschäftigte des Kunden können nach eigenem Ermessen Ansprüche nach Artikel 12.1 geltend machen, indem sie Beschwerde einreichen bei

(i) der Aufsichtsbehörde des Landes, in dem sie ihren gewöhnlichen Wohnsitz oder Arbeitsplatz haben, oder wo der Verstoß stattfand, gegen die Vertragsschließende ADP Konzerngesellschaft oder die Beauftragte ADP Konzerngesellschaft; oder
(ii) der Führenden Aufsichtsbehörde oder den Gerichten in den Niederlanden, in diesem Fall aber nur gegen die Beauftragte ADP Konzerngesellschaft.

Beschäftigte des Kunden können nach eigenem Ermessen Ansprüche nach Artikel 12.1 geltend machen, indem sie eine Beschwerde einreichen bei:

(i) Gerichten des Landes, in dem sie ihren gewöhnlichen Wohnsitz haben, oder des Herkunftslands der gemäß diesem Code übermittelten Daten gegen die die Vertragsschließende ADP Konzerngesellschaft oder die Beauftragte ADP Konzerngesellschaft; oder

(ii) der Führenden Aufsichtsbehörde oder den Gerichten in den Niederlanden, in diesem Fall aber nur gegen die Beauftragte ADP Konzerngesellschaft.

Die Aufsichtsbehörden und Gerichte handeln gemäß ihrem jeweils anwendbaren materiellen und prozessualen Recht. Die vorgenannten Entscheidungsmöglichkeiten des Beschäftigten des Kunden lassen die materiellen und prozessualen Rechte, die den Parteien laut Anwendbarem Recht zustehen, unberührt.

Rechte der Kunden

12.4 Der Kunde kann diesen Code gegen (i) die Vertragsschließende ADP Konzerngesellschaft oder (ii) die Beauftragte ADP Konzerngesellschaft vor der Führenden Aufsichtsbehörde oder den Gerichten in den Niederlanden durchsetzen, aber nur, wenn die Vertragsschließende ADP Konzerngesellschaft ihren Sitz außerhalb des EWR hat. Die Beauftragte ADP Konzerngesellschaft stellt sicher, dass angemessene Maßnahmen ergriffen werden, um Verstöße gegen diesen Code durch die Vertragsschließende ADP Konzerngesellschaft oder eine Konzerngesellschaft zu beheben.

Die Vertragsschließende ADP Konzerngesellschaft und die Beauftragte ADP Konzerngesellschaft dürfen sich nicht auf einen Verstoß gegen ihre Pflichten seitens einer anderen Konzerngesellschaft oder eines Unterauftragsverarbeiters berufen, um der Haftung zu entgehen, es sei denn, ein Einwand dieser Konzerngesellschaft oder dieses Unterauftragsverarbeiters würde auch von ADP als eigener Einwand geltend gemacht werden können.

Zur Verfügung stehende Rechtsbehelfe, Beweislast für Beschäftigte des Kunden

12.5 Im Fall, dass ein Beschäftigter des Kunden einen Anspruch nach Artikel 12.1 geltend machen kann, hat der Beschäftigte des Kunden das Recht auf Schadensersatz für Schäden, soweit das Anwendbare EWR-Recht dies vorsieht.

Fordert ein Beschäftigter des Kunden Schadenersatz für einen Schaden gemäß Artikel 12.1, muss dieser Beschäftigte des Kunden nachweisen, dass er einen Schaden erlitten hat und dass dieser Schaden nachvollziehbar entstanden ist aufgrund einer Verletzung dieses Codes. Folglich trägt die ADP Vertragsschließende Konzerngesellschaft (oder ggf. die Beauftragte ADP Konzerngesellschaft) die Beweislast dafür, dass die Schäden, die dem Beschäftigten des Kunden aufgrund einer Verletzung dieses Codes entstanden sind, nicht auf die entsprechende Konzerngesellschaft oder einen Unterauftragsverarbeiter zurückzuführen sind, bzw. muss andere zutreffende Einwände vorbringen.

Recht des Kunden auf Schadenersatz

12.6 Im Falle eines Verstoßes gegen diesen Code und nach Maßgabe der Bestimmungen des Servicevertrages haben Kunden das Recht auf Schadensersatz in Bezug auf direkte Schäden entsprechend den Bestimmungen des Servicevertrages.

Gegenseitige Unterstützung	**12.7**	Alle Konzerngesellschaften arbeiten bei Bedarf zusammen (a) für die Bearbeitung einer Anfrage, einer Beschwerde oder Forderung durch einen Kunden oder einen Beschäftigten des Kunden oder (b) bei einer gesetzlichen Untersuchung oder Ersuchen einer zuständigen Regierungsbehörde und unterstützen sich, soweit vernünftigerweise zumutbar. Die Konzerngesellschaft, die ein Auskunftsersuchen gemäß Artikel 6.1 oder eine Beschwerde oder Forderung gemäß Artikel 12.2 oder 12.3 erhält, ist verantwortlich für die Durchführung der Kommunikation mit dem Kunden oder dem Beschäftigten des Kunden hinsichtlich des Ersuchens oder der Forderung, es sei denn, die Umstände erfordern etwas anderes oder das Global Data Privacy and Governance Team gibt etwas anderes vor.
Empfehlungen und verbindliche Entscheidungen von Aufsichtsbehörden	**12.8**	ADP wird nach Treu und Glauben mit der Führenden Aufsichtsbehörde und der zuständigen Aufsichtsbehörde gemäß Artikel 12.3 zusammenarbeiten und alle zumutbaren Anstrengungen unternehmen, den Ratschlägen dieser Behörden zur Interpretation und Anwendung dieses Codes zu folgen. ADP hält sich an verbindliche Entscheidungen der zuständigen Aufsichtsbehörden.
Auf diesen Code anwendbares Recht	**12.9**	Dieser Code unterliegt niederländischem Recht und wird gemäß niederländischem Recht ausgelegt.

Artikel 13 – Sanktionen für Non-Compliance

Nichteinhaltung des Codes	**13.1**	Die Nichteinhaltung dieses Codes durch die Belegschaft kann zu angemessenen Disziplinarmaßnahmen führen nach Maßgabe des Anwendbaren Rechtes und Richtlinien der ADP bis hin zur Kündigung eines Anstellungsvertrages oder Vertrages.

Artikel 14 – Widersprüche zwischen diesem Code und Anwendbarem Auftragsverarbeiter-Recht

Widerspruch zwischen diesem Code und Recht	**14.1**	Wenn ein Widerspruch zwischen dem Anwendbaren Auftragsverarbeiter-Recht und diesem Code auftritt, beraten sich die Verantwortliche Führungskraft oder der Privacy Steward mit dem Global Chief Privacy Officer, den zuständigen Mitgliedern des Privacy Networks (soweit zweckdienlich) und der Rechtsabteilung der Geschäftseinheit darüber, wie dieser Code eingehalten und der Widerspruch, soweit dies angesichts der für ADP geltenden rechtlichen Anforderungen durchführbar ist, aufgelöst werden kann.

Neue widersprechende gesetzliche Anforderungen

14.2 Mitglieder der Rechtsabteilung, die Sicherheitsbeauftragten der ADP und die Privacy Stewards informieren das Global Data Privacy and Governance Team unverzüglich über etwaige ihnen bekannt werdende neue rechtliche Anforderungen, die der Einhaltung dieses Codes durch ADP entgegenstehen könnten.

Die zuständigen Privacy Stewards werden nach Beratung mit der Rechtsabteilung die Verantwortlichen Führungskräfte unverzüglich über etwaige neue rechtliche Anforderungen informieren, die ADP außer Lage setzen könnten, diesen Code einzuhalten.

Berichterstattung an die Führende Aufsichtsbehörde

14.3 Wenn ADP Kenntnis erlangt, dass Anwendbares Auftragsverarbeiter-Recht oder eine Änderung im Anwendbaren Auftragsverarbeiter-Recht ihre Fähigkeit, die Verpflichtungen nach 3.1, 3.2 oder 11.3 zu erfüllen, wahrscheinlich in erheblichem Umfang beeinträchtigen wird, informiert ADP die Führende Aufsichtsbehörde.

Artikel 15 – Änderungen zu diesem Code

Genehmigung für Änderungen

15.1 Alle wesentlichen Änderungen dieses Codes erfordern die vorherige Freigabe des Global Chief Privacy Officer und des General Counsel sowie die Annahme durch den ADP Führungskreis und werden anschließend den Konzerngesellschaften mitgeteilt. Unwesentliche Änderungen dieses Codes können nach vorheriger Freigabe durch den Global Chief Privacy Officer vorgenommen werden. Die Beauftragte ADP Konzerngesellschaft setzt die Führende Aufsichtsbehörde jährlich über Änderungen dieses Codes in Kenntnis.

Falls eine Änderung dieses Codes eine erhebliche Auswirkung auf die Verarbeitungsbedingungen der Kundenservices hat, unterrichtet ADP die Führende Aufsichtsbehörde unverzüglich, einschließlich einer kurzen Begründung, warum diese Änderung erfolgt ist, und informiert den Kunden über diese Änderung. Der Kunde kann dieser Änderung innerhalb von 30 Tagen nach Erhalt der Mitteilung durch schriftliche Erklärung an ADP widersprechen. Für den Fall, dass die Parteien keine einvernehmliche Lösung finden können, richtet ADP eine alternative Lösung für die Datenübermittlung ein. Für den Fall, dass keine alternative Lösung für die Datenübermittlung eingerichtet werden kann, hat der Kunden nach diesem Code das Recht, die entsprechende Datenübermittlung von Kundendaten an ADP auszusetzen. In dem Fall, dass eine Aussetzung der Datenübermittlung nicht möglich ist, ermöglicht ADP dem Kunden die Beendigung der entsprechenden Kundenservices nach Maßgabe der Bedingungen des Servicevertrages.

Datum des Inkrafttretens von Änderungen

15.2 Jede Änderung tritt mit ihrer Genehmigung gemäß Artikel 15.1 und Veröffentlichung auf der Website **www.adp.com** und Mitteilung an die Kunden unmittelbar in Kraft.

Frühere Versionen

15.3 Jede Anfrage, Beschwerde oder Forderung eines Beschäftigten des Kunden in Zusammenhang mit diesem Code wird entsprechend der Version des Codes behandelt, die zum Zeitpunkt, als das Anliegen, die Beschwerde oder Forderung gestellt wurde, gültig war.

Artikel 16 – Implementierung und Übergangszeiten

Implementierung

16.1 Die Implementierung dieses Codes wird von den Privacy Stewards mit Unterstützung des Global Privacy and Governance Team überwacht. Von den unten genannten Ausnahmen abgesehen, gibt es für die Einhaltung dieses Codes eine Übergangszeit von achtzehn Monaten ab dem Datum des Inkrafttretens (gemäß Artikel 1.6).

Das heißt, sofern nicht anders angegeben, erfolgt die Verarbeitung von Kundendaten innerhalb von achtzehn Monaten ab Datum des Inkrafttretens vollständig in Übereinstimmung mit diesem Code und dieser Code erlangt somit seine volle Gültigkeit. Während der Übergangszeit gilt dieser Code für eine Konzerngesellschaft, sobald diese Konzerngesellschaft die erforderlichen Aufgaben für die volle Implementierung abgeschlossen und sie den Global Chief Privacy Officer entsprechend informiert hat.

Neue Konzerngesellschaften

16.2 Jedes Unternehmen, das nach dem Datum des Inkrafttretens zur Konzerngesellschaft wird, muss diesen Code innerhalb von zwei Jahren nach ihrer Aufnahme als Konzerngesellschaft befolgen.

Veräußerte Unternehmen

16.3 Für ein veräußertes Unternehmen gilt dieser Code auch nach ihrer Veräußerung für den Zeitraum fort, den ADP benötigt, um die Verarbeitung von Kundendaten durch das veräußerte Unternehmen zu beenden.

Übergangszeit für bestehende Vereinbarungen

16.4 Sofern es bestehende Vereinbarungen mit Unterauftragsverarbeitern und sonstigen Dritten gibt, auf die sich dieser Code auswirkt, gelten die Bestimmungen der Vereinbarungen weiter, bis die Vereinbarungen im normalen Geschäftsverlauf erneuert werden, vorausgesetzt dass alle bestehenden Vereinbarungen innerhalb von achtzehn Monaten ab dem Datum des Inkrafttretens mit diesem Code in Einklang stehen.

Kontaktdaten

ADP Global Data Privacy and Governance Team:
privacy@adp.com

Führende ADP Konzerngesellschaft:
ADP Nederland B.V.
Lylantse Baan 1, 2908
LG CAPELLE AAN DEN IJSSEL
NIEDERLANDE

Auslegung

AUSLEGUNG DIESES CODES

(i) Sofern aus dem Kontext nichts anderes hervorgeht, sind alle Bezugnahmen auf einen bestimmten Artikel oder Annex Bezugnahmen auf den Artikel oder Annex in diesem Dokument wie von Zeit zu Zeit geändert;
(ii) Überschriften dienen nur der besseren Orientierung und sind nicht zur Auslegung einer Bestimmung dieses Codes heranzuziehen;
(iii) Wird für ein Wort oder einen Begriff eine Definition angegeben, so haben alle anderen grammatikalischen Formen die entsprechende Bedeutung;
(iv) Die männliche Form schließt die weibliche mit ein;
(v) Die Verwendung von Begriffen wie „zum Beispiel“, „insbesondere“, „einschließlich“ und die darauffolgenden Begriffe sind nicht als Beschränkung der vorangehenden allgemeinen, generischen Begriffe oder Konzepte aufzufassen, und umgekehrt;
(vi) Das Wort „schriftlich“ umfasst alle dokumentierten Kommunikationen, Schreiben, Verträge, elektronischen Aufzeichnungen, elektronischen Unterschriften, Reproduktionen oder sonstigen rechtsgültigen und durchsetzbaren Urkunden unabhängig von ihrem Format;
(vii) Die Bezugnahme auf ein Dokument (z.B. auf diesen Code) bezieht sich auf das Dokument in seiner jeweils gültigen Fassung einschließlich Ergänzungen, Änderungen oder Ersatzdokumenten, es sei denn, in diesem Code oder dem betreffenden Dokument ist dies ausgeschlossen; und
(viii) Eine Bezugnahme auf gesetzliche Bestimmungen umfasst auch regulatorische Anforderungen, Industriestandards und Best Practices, die durch zuständige nationale und internationale Kontrollbehörden oder andere Institutionen herausgegeben werden.

ANNEX 1 – BCR Definitionen

ADP (ADP Gruppe)	ADP (die ADP Gruppe) umfasst Automatic Data Processing, Inc. (die Muttergesellschaft) und die Konzerngesellschaften, einschließlich ADP, Inc.
ADP Unterauftragsverarbeiter	Für den Zweck des Privacy Code für Kundendaten-verarbeitungsdienste bedeutet ADP Unterauftragsverarbeiter eine KONZERNGESELLSCHAFT, die von einer anderen KONZERNGESELLSCHAFT als Unterauftragsverarbeiter für KUNDENDATEN beauftragt wird.
ADP Führungskreis	ADP FÜHRUNGSKREIS bezieht sich auf das Vorstands-gremium, bestehend aus (i) dem Chief Executive Officer (CEO) der Automatic Data Processing, Inc. und (ii) den anderen Direktoren, die dem CEO direkt unterstellt sind und die gemeinsam für das Geschäft der KONZERNGESELL-SCHAFTEN der ADP verantwortlich sind.
Anderer Zweck	ANDERER ZWECK bedeutet ein Zweck, der nicht der ursprüngliche Zweck ist, für den die PERSONEN-BEZOGENEN DATEN weiterverarbeitet werden.
Angehöriger	ANGEHÖRIGER bedeutet der Ehegatte, Partner, das Kind oder der Begünstigte eines MITARBEITERS oder der Notfallkontakt eines MITARBEITERS oder ein VORÜBER-GEHEND BESCHÄFTIGTER.
Angemessenheitsbeschluss	ANGEMESSENHEITSBESCHLUSS bedeutet die Entscheidung einer AUFSICHTSBEHÖRDE oder einer anderen zuständigen Stelle, dass ein Land, eine Region oder ein Empfänger bei der Übertragung PERSONENBEZOGENER DATEN ein angemessenes Schutzniveau bietet. Die unter einen Angemessenheitsbeschluss fallenden Rechtsträger umfassen sowohl Empfänger in Ländern, von denen nach ANWENDBAREM RECHT davon ausgegangen wird, dass sie ein angemessenes Datenschutzniveau bieten, als auch Empfänger, die an andere Regelwerke gebunden sind (zum Beispiel Binding Corporate Rules), die durch eine zuständige Aufsichtsbehörde oder eine andere befugte Stelle genehmigt wurden. Hinsichtlich der Vereinigten Staaten sind Unternehmen vom Angemessenheitsbeschluss abgedeckt, die sich nach US-EWR und/oder US-Schweizer Datenschutzabkommen zertifizieren lassen.
Angestellter im Mitarbeiter-Sharing	ANGESTELLTER IM MITARBEITER-SHARING („Co-Employed Individual“) ist ein Angestellter eines US-Kunden, der von einer indirekten US-Tochtergesellschaft von Automatic Data Processing, Inc. als Teil des Arbeitgeberserviceangebots in den USA angestellt ist.
Anwendbares Auftragsverarbeiter-Recht	Für den Zweck des Privacy Code für Kundendaten-verarbeitungsdienste bedeutet Anwendbares Auftrags-verarbeiter-Recht alle Rechtsvorschriften zum Schutz der Privatsphäre oder Datenschutzgesetze, die auf ADP als

	DATENVERARBEITER im Auftrag eines KUNDEN, der der DATENVERANTWORTLICHE ist, anwendbar sind.
Anwendbares Datenverantwortlicher-Recht	Für den Zweck des Privacy Code für Kundendaten-verarbeitungsdienste bedeutet Anwendbares Daten-verantwortlicher-Recht alle Rechtsvorschriften zum Schutz der Privatsphäre oder Datenschutzgesetze, die auf einen KUNDEN als DATENVERANTWORTLICHEN dieser KUNDENDATEN anwendbar sind.
Anwendbares EWR-Recht	ANWENDBARES EWR-RECHT bezeichnet die Anforderungen nach dem jeweils ANWENDBAREM RECHT im EWR, das für alle PERSONENBEZOGENEN DATEN gilt, die ursprünglich im Zusammenhang mit den Aktivitäten einer im EWR ansässigen KONZERNGESELLSCHAFT gesammelt wurden (auch wenn diese dann an eine andere, außerhalb des EWR ansässige KONZERNGESELLSCHAFT übermittelt wurden).
Anwendbares Recht	ANWENDBARES RECHT bedeutet alle Rechtsvorschriften zum Schutz der Privatsphäre oder Datenschutzgesetze, die auf bestimmte Verarbeitungsaktivitäten anwendbar sind.
Archiv	ARCHIV bezeichnet eine Sammlung von PERSONEN-BEZOGENEN DATEN, die nicht mehr notwendig sind, um die Ziele zu erreichen, für die diese DATEN ursprünglich gesammelt wurden oder die nicht länger für allgemeine geschäftliche Aktivitäten genutzt werden, die aber möglicherweise noch für historische, wissenschaftliche oder statistische Zwecke, zur Streitbelegung, für Untersuchungen oder allgemeine Archivierungszwecke genutzt werden. Der Zugang auf ein Archiv ist nur Systemadministratoren und anderen vorbehalten, deren Arbeit Zugang zum Archiv ausdrücklich erfordert.
Aufsichtsbehörde oder AB	AUFSICHTSBEHÖRDE ODER AB bezeichnet eine für den Datenschutz oder den Schutz der Privatsphäre zuständige Kontroll- oder Aufsichtsbehörde in einem Land, in dem eine KONZERNGESELLSCHAFT ihren Sitz hat.
Auftragsverarbeiter	AUFTRAGSVERARBEITER bezeichnet die juristische Person oder natürliche Einzelperson, die im Auftrag eines DATENVERANTWORTLICHEN PERSONENBEZOGENE DATEN verarbeitet.
Auftragsverarbeitervertrag	AUFTRAGSVERARBEITERVERTRAG ist ein Vertrag für die Verarbeitung von PERSONENBEZOGENEN DATEN, der zwischen ADP und einem EXTERNEN AUFTRAGS-VERARBEITER abgeschlossen wird.
Automatic Data Processing, Inc.	AUTOMATIC DATA PROCESSING, INC. ist die Mutter-gesellschaft der ADP GRUPPE. Sie wurde in Delaware (USA) gegründet und hat ihren Firmensitz in One ADP Boulevard, Roseland, New Jersey, 07068-1728, USA.
Beauftragte ADP Konzerngesellschaft	Die BEAUFTRAGTE ADP KONZERNGESELLSCHAFT ist die ADP Nederland, B.V. mit Sitz in Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, the Netherlands.

Belegschaft	BELEGSCHAFT bezeichnet als Gesamtheit die derzeit angestellten MITARBEITER der ADP sowie alle Beschäftigte mit Zeitvertrag, die derzeit für ADP arbeiten.
Beschäftigte des Kunden	BESCHÄFTIGTE DES KUNDEN sind alle PERSONEN, deren PERSONENBEZOGENE DATEN von ADP als AUFTRAGSVERARBEITER für einen KUNDEN gemäß einem SERVICEVERTRAG verarbeitet werden. Der Klarheit halber sind BESCHÄFTIGTE DES KUNDEN alle EINZELPERSONEN, deren PERSONENBEZOGENE DATEN von ADP im Zuge der Erbringung von KUNDENSERVICES verarbeitet werden (ungeachtet der Rechtsnatur der Beziehung zwischen der EINZELPERSON und dem KUNDEN). GESCHÄFTSKONTAKTE, deren PERSONENBEZOGENE DATEN ADP im Zusammenhang mit ihrer direkten Beziehung zum KUNDEN verarbeitet, sind hierin nicht mit eingeschlossen. Zum Beispiel: ADP verarbeitet PERSONENBEZOGENE DATEN eines GESCHÄFTS-KONTAKTES im HR Bereich, um einen Vertrag mit dem KUNDEN abzuschließen - diese DATEN unterliegen dem Privacy Code für Geschäftsdaten. Wenn ADP aber dessen DATEN für den KUNDEN zur Lohnabrechnung verarbeitet (z.B. Erstellen von Gehaltsabrechnungen, Support bei der Nutzung eines ADP Systems), dann werden die DATEN dieser EINZELPERSON als KUNDENDATEN verarbeitet.
Besondere Datenkategorien	BESONDERE DATENKATEGORIEN sind PERSONEN-BEZOGENE DATEN, die Auskunft geben über eine EINZELPERSON im Hinblick auf Rasse oder ethnische Herkunft, politische Gesinnung oder Mitgliedschaft in politischen Parteien oder ähnlichen Organisationen, religiöse oder philosophische Überzeugungen, Mitgliedschaft in einem Berufsverband oder in einer Gewerkschaft, körperliche oder geistige Gesundheit einschließlich jeglicher diesbezüglicher Meinung, Behinderungen, den genetischen Code, Suchtkrankheiten, Sexualleben, Straftaten, Strafregister oder Verfahren hinsichtlich Straftaten oder unrechtmäßigem Verhalten.
Bewerber	BEWERBER ist jede EINZELPERSON, die ADP PERSONENBEZOGENE DATEN zur Verfügung stellt im Zusammenhang mit ihrer Bewerbung auf eine MITARBEITER Stelle bei ADP.
Binding Corporate Rules (BCR)	BINDING CORPORATE RULES sind verbindliche Datenschutzrichtlinien innerhalb einer Unternehmensgruppe, die für die Übermittlung PERSONENBEZOGENER DATEN in dieser Gruppe nach ANWENDBAREM RECHT ein angemessenes Schutzniveau bieten.
Code	CODE bedeutet (wo anwendbar) der ADP Privacy Code für Geschäftsdaten, der ADP Privacy Code für den Arbeitsplatz (ADP-intern) und der ADP Privacy Code für Kundendatenverarbeitungsdienste, diese werden gemeinsam als Codes bezeichnet.

Datenschutzfolgen-abschätzung (DSFA)	DATENSCHUTZFOLGENABSCHÄTZUNG (DSFA) ist ein Verfahren zur Durchführung und Dokumentation einer vorangegangenen Bewertung der Auswirkungen, die eine bestimmte VERARBEITUNG auf den Schutz der PERSONEN-BEZOGENEN DATEN haben kann, wo eine solche VERARBEITUNG voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten von EINZELPERSONEN verbunden ist, insbesondere dort, wo neue Technologien eingesetzt werden. Eine DSFA soll Folgendes beinhalten: (i) Eine Beschreibung von: a) Umfang und Kontext der VERARBEITUNG; b) GESCHÄFTSZWECKE, für die die PERSONEN-BEZOGENEN DATEN verarbeitet werden; c) spezifische Zwecke, für die BESONDERE DATEN-KATEGORIEN verarbeitet werden; d) Kategorien von Empfängern für PERSONEN-BEZOGENE DATEN, einschließlich Empfänger, für die kein Angemessenheitsbeschluss besteht; e) Speicherzeiträume für PERSONENBEZOGENE DATEN; ii) Eine Beurteilung der: a) Notwendigkeit und Verhältnismäßigkeit der VERARBEITUNG; b) Risiken für die Datenschutzrechte von EINZELPERSONEN; und die Maßnahmen zur Minderung dieser Risiken, einschließlich Schutzmaßnahmen, Sicherheitsmaßnahmen und andere Mechanismen (wie z.B. „Privacy by Design“ bzw. „eingebauter Datenschutz“) zum Schutz Personenbezogener Daten.
Datensicherheitsverletzung	DATENSICHERHEITSVERLETZUNG bezeichnet jeden Vorfall, der sich auf die Vertraulichkeit, Integrität oder Verfügbarkeit von PERSONENBEZOGENEN DATEN auswirkt, wie beispielsweise die unbefugte Nutzung oder Offenlegung von PERSONENBEZOGENEN DATEN oder der unautorisierte Zugriff, der die Vertraulichkeit oder die Sicherheit der PERSONENBEZOGENEN DATEN beeinträchtigt.
Datenverantwortlicher	DATENVERANTWORTLICHER bezeichnet die juristische oder natürliche EINZELPERSON, die die Zwecke und Mittel der VERARBEITUNG von PERSONENBEZOGENEN DATEN alleine oder gemeinsam mit anderen festlegt.
Datenverantwortlicher Dritter	DATENVERANTWORTLICHER DRITTER bezeichnet einen DRITTEN, der PERSONENBEZOGENE DATEN verarbeitet und die Zwecke und Mittel der VERARBEITUNG bestimmt.
Datum des Inkrafttretens	DATUM DES INKRAFTTRETENS ist der Tag, an dem die CODES in Kraft treten gemäß Artikel 1 der CODES.

Dritter	DRITTER bezeichnet eine Person, private Organisation oder eine Regierungsbehörde, die keine KONZERN-GESELLSCHAFT ist.
Einzelperson	Eine EINZELPERSON bezeichnet eine identifizierte oder identifizierbare natürliche Person, deren PERSONEN-BEZOGENE DATEN von ADP entweder als AUFTRAGS-VERARBEITER oder DATENVERANTWORTLICHER verarbeitet werden, mit Ausnahme von ANGESTELLTEN IM MITARBEITER-SHARING. Bitte beachten Sie: Der Privacy Code für Geschäftsdaten und der Privacy Code für den Arbeitsplatz sind deshalb nicht auf die Verarbeitung von PERSONENBEZOGENEN DATEN von ANGESTELLTEN IM MITARBEITER-SHARING anwendbar.
EWR	EWR oder EUROPÄISCHER WIRTSCHAFTSRAUM bezeichnet alle Mitgliedsstaaten der Europäischen Union sowie Norwegen, Island und Liechtenstein, und, für die Zwecke dieses Codes, auch die Schweiz und das Vereinigten Königreich nach seinem Austritt aus der Europäischen Union. Nach einer Entscheidung des General Counsel – die auf www.adp.com veröffentlicht wird - kann dies auch andere Länder mit Datenschutzge-setzen mit einschließen, die den EWR-Datenübermittlungsbeschränkungen entsprechende Beschränkungen für die Datenübermittlung haben.
EWR-Datenübermittlungs-beschränkung	EWR-DATENÜBERMITTLUNGSBESCHRÄNKUNG bezeichnet jegliche Beschränkungen im Zusammenhang mit der grenzüberschreitenden Übermittlung von PERSONEN-BEZOGENEN DATEN gemäß den Datenschutzgesetzen eines Landes des EWR.
Externer Auftragsverarbeiter	EXTERNER AUFTRAGSVERARBEITER ist ein DRITTER, der im Auftrag von ADP PERSONENBEZOGENE DATEN verarbeitet und nicht der direkten Führung von ADP untersteht.
Externer Unterauftragsverarbeiter	EXTERNER UNTERAUFTRAGSVERARBEITER ist jeder DRITTE, der von ADP als UNTERAUFTRAGSVERARBEITER beauftragt wurde.
Führende Aufsichtsbehörde	Die FÜHRENDE AUFSICHTSBEHÖRDE ist die niederländische Aufsichtsbehörde.
Geschäftskontakt	GESCHÄFTSKONTAKT bezeichnet jede PERSON (außer einem MITARBEITER), die mit ADP in beruflicher oder geschäftlicher Eigenschaft direkt im Kontakt steht. Zum Beispiel gehören zu den Geschäftskontakten Mitglieder der Personalabteilung des KUNDEN, die mit ADP als Nutzer ihrer Produkte oder Services zusammenarbeiten. Zu den Geschäftskontakten gehören auch Account-Inhaber der KUNDEN, ZULIEFERER und GESCHÄFTSPARTNER, geschäftliche Kontaktpersonen, Gewerkschaftsmitarbeiter, Vertreter von Aufsichtsbehörden, Medienkontakte und andere Einzelpersonen, die mit ADP beruflich zusammenarbeiten.
General Counsel	GENERAL COUNSEL bezeichnet den Leiter der Rechtsabteilung von Automatic Data Processing, Inc.

Global Chief Privacy Officer	GLOBAL CHIEF PRIVACY OFFICER bezeichnet den MITARBEITER der ADP, der die Stelle als Konzerndaten-schutzbeauftrager bei Automatic Data Processing, Inc. innehat.
Global Data Privacy and Governance Team	Als GLOBAL DATA PRIVACY AND GOVERNANCE TEAM wird ADP's Abteilung für Datenschutz und Datensteuerung bezeichnet. Die Abteilung für Datenschutz und Datensteuerung wird vom Global Chief Privacy Officer geleitet und besteht aus Datenschutzbeauftragen, Daten-schutzmanagern und anderen Mitarbeitern mit Berichtslinien an den Global Chief Privacy Officer oder den Datenschutzbeauftragten oder den Datenschutzmanagern.
Geschäftliche Kontaktdaten	GESCHÄFTLICHE KONTAKTDATEN sind sämtliche DATEN eines Berufstätigen, die sich typischerweise auf einer Visitenkarte oder in einer E-Mail-Signatur finden.
Geschäftspartner	GESCHÄFTSPARTNER sind alle DRITTEN, außer KUNDEN und ZULIEFERER, die eine geschäftliche Beziehung oder strategische Allianz mit ADP haben bzw. hatten (z.B. Marketingpartner, Joint Venture- oder Entwicklungspartnerschaften).
Geschäftszweck	Der GESCHÄFTSZWECK ist ein legitimer Zweck für die VERARBEITUNG PERSONENBEZOGENER DATEN gemäß Artikel 2, 3 oder 4 jedes CODES oder für die VERARBEITUNG BESONDERER DATENKATEGORIEN gemäß Artikel 4 jedes CODES.
Interner Auftragsverarbeiter	INTERNER AUFTRAGSVERARBEITER bezieht sich auf eine KONZERNGESELLSCHAFT, die PERSONENBEZOGENE DATEN im Auftrag einer anderen KONZERNGESELLSCHAFT verarbeitet, die der DATENVERANTWORTLICHE ist.
Kinder	Für die Zwecke der Datensammlung und -vermarktung sind unter KINDER solche EINZELPERSONEN zu verstehen, die nach ANWENDBAREM RECHT unter dem Mindestalter sind, um ihre Einwilligung zu Datenerfassung und/oder Marketing abgeben zu können.
Konzerngesellschaft	KONZERNGESELLSCHAFT bezeichnet eine juristische Person, die eine Tochtergesellschaft von Automatic Data Processing, Inc. und/oder ADP, Inc. ist, wenn entweder Automatic Data Processing, Inc. oder ADP, Inc. direkt oder indirekt mehr als 50% der ausgegebenen Anteile besitzt, 50% oder mehr der Stimmrechte bei Gesellschafterversammlungen innehat, die Befugnis hat, die Mehrheit der Direktoren zu ernennen oder auf andere Weise die Aktivitäten einer solchen juristischen Person leitet.
Kunde	KUNDE bedeutet ein DRITTER, der ein oder mehrere Produkte oder Services der ADP für sein eigenes Unternehmen nutzt.

Kundendaten	KUNDENDATEN sind PERSONENBEZOGENE DATEN von BESCHÄFTIGTEN DES KUNDEN (einschließlich zukünftiger Beschäftigter, ehemaliger Beschäftigter und Angehöriger von Beschäftigten), die von ADP im Zusammenhang mit der Bereitstellung von KUNDENSERVICES verarbeitet werden.
Kundenservices	KUNDENSERVICES sind Human Capital Management Services, die ADP für KUNDEN erbringt, wie beispielsweise die Einstellung von BESCHÄFTIGTEN, Lohn- und Gehaltsabrechnung und Spesenabrechnung, Talent-management, Einzelpersonalmanagement, Consulting und Analytics und Altersvorsorgeprodukte.
Kundensupportservices	KUNDENSUPPORTSERVICES sind die von ADP zur Unterstützung der Bereitstellung von Produkten und Services der ADP durchgeführte Verarbeitungsaktivitäten. Beispiele für Kundensupportservices sind Schulungen für GESCHÄFTSKONTAKTE, Beantwortung von Fragen über die Services, Öffnen und Lösen von Support-Tickets, Bereitstellung von Informationen zu Produkten und Services (einschließlich Updates und Compliance-Warnungen), Qualitätskontrolle und -überwachung und damit verbundene Aktivitäten, die zur effektiven Nutzung von Produkten und Services der ADP beitragen.
Mitarbeiter	MITARBEITER bezeichnet einen BEWERBER, einen derzeitiger Mitarbeiter oder einen früheren Mitarbeiter von ADP mit Ausnahme von Angestellten im Mitarbeiter-Sharing („Co-Employed Individuals“). Bitte beachten: Der Privacy Code für den Arbeitsplatz findet deshalb keine Anwendung auf die Verarbeitung Personenbezogener Daten von Angestellten im Mitarbeiter-Sharing.
Personenbezogene Daten oder Daten	PERSONENBEZOGENE DATEN oder DATEN sind sämtliche Informationen, die sich auf eine identifizierte oder identifizierbare EINZELPERSON beziehen. PERSONENBE-ZOGENE DATEN können in Richtlinien und Standards, die die CODES umsetzen, auch als persönliche Daten bezeichnet werden.
Privacy Leadership Council	PRIVACY LEADERSHIP COUNCIL ist ein Gremium, das vom Global Chief Privacy Officer geleitet wird und das aus Privacy Stewards, den vom Global Chief Privacy Officer ausgewählten Mitgliedern des Privacy Networks und anderen besteht, die das Gremium möglicherweise bei seinen Aufgaben unterstützen können.
Privacy Network	PRIVACY NETWORK bezieht sich auf die Mitglieder des GLOBAL DATA PRIVACY AND GOVERNANCE TEAM und andere Mitglieder der Rechtsabteilung, einschließlich Compliance-Experten und Datenschutzbeauftragte, die für Compliance im Datenschutz innerhalb der entsprechenden Regionen, Länder, Geschäftseinheiten oder Funktionsein-heiten zuständig sind.

Privacy Steward	PRIVACY STEWARD bezeichnet eine Führungskraft der ADP, die von einer VERANTWORTLICHEN FÜHRUNGSKRAFT und/oder dem ADP FÜHRUNGSKREIS beauftragt wurde, die CODES innerhalb einer ADP-Geschäftseinheit zu implementieren und durchzusetzen.
Servicevertrag	SERVICEVERTRAG bezeichnet einen Vertrag, eine Vereinbarung oder Bestimmungen, gemäß derer ADP für einen KUNDEN KUNDENSERVICES erbringt.
Übergeordnetes Interesse	ÜBERGEORDNETES INTERESSE bedeutet das vordringliche Interesse gemäß Artikel 13.1 des Privacy Codes für den Arbeitsplatz und des Privacy Codes für Geschäftsdaten, auf dessen Basis die Pflichten von ADP oder Rechte von EINZELPERSONEN, wie in Artikel 13.2 und 13.3 der CODES dargelegt, unter bestimmten Umständen außer Kraft gesetzt werden können, wenn ein solches vordringliches Interesse den Schutzinteressen der Einzelperson überzuordnen ist.
Unterauftragsverarbeiter	UNTERAUFTRAGSVERARBEITER bezeichnet alle ADP UNTERAUFTRAGSVERARBEITER und EXTERNE UNTER-AUFTRAGSVERARBEITER.
Unterauftragsverarbeiter-vertrag	Der UNTERAUFTRAGSVERARBEITERVERTRAG ist eine schriftliche oder elektronische Vereinbarung zwischen ADP und einem EXTERNEN UNTERAUFTRAGSVERARBEITER gemäß Artikel 7.1 des Privacy Codes für Kundendatenverarbeitungsdienste.
Verantwortliche Führungskraft	VERANTWORTLICHE FÜHRUNGSKRAFT bezieht sich auf den Geschäftsführer (Managing Director) einer KONZERNGESELLSCHAFT oder den Leiter eines Geschäftsbereichs oder eines Funktionsbereichs, der die primäre Verantwortung für das Budget der KONZERN-GESELLSCHAFT, des Geschäftsbereichs oder des Funktionsbereichs hat.
Verarbeitung	VERARBEITUNG bezeichnet alle Vorgänge, die mit PERSONENBEZOGENEN DATEN durchgeführt werden, unabhängig davon, ob sie automatisiert erfolgen oder nicht, wie z.B. die Erhebung, Aufzeichnung, Speicherung, Organisation, Änderung, Nutzung, Offenlegung (einschließlich der Gewährung von remote Zugriffen), Übertragung oder Löschung von PERSONENBEZOGENEN DATEN.
Vertragsschließende ADP Konzerngesellschaft	VERTRAGSSCHLIESSENDE ADP KONZERN-GESELLSCHAFT bezieht sich auf die KONZERNGE-SELLSCHAFT, die einen nach den CODES erforderlichen Vertrag, wie z.B. einen SERVICEVERTRAG, einen UNTERAUFTRAGSVERARBEITERVERTRAG oder eine Datenübermittlungsvereinbarung abgeschlossen hat.

Veräußertes Unternehmen	VERÄUSSERTES UNTERNEHMEN ist eine KONZERN-GESELLSCHAFT, die aufgrund eines Verkaufs der Unternehmensanteile und/oder Wirtschaftsgüter oder einer anderen Ausgliederung nicht mehr im Eigentum von ADP steht, sodass dieses Unternehmen nicht mehr als KONZERNGESELLSCHAFT gilt.
Verbraucher	VERBRAUCHER bedeutet eine EINZELPERSON, die in persönlichen Eigenschaft direkt mit ADP im Kontakt steht. Verbraucher sind beispielsweise Privatpersonen, die an Einzelpersonalentwicklungsprogrammen teilnehmen oder Produkte und Services von ADP für ihren persönlichen Gebrauch nutzen (d.h. außerhalb eines Anstellungs-verhältnisses mit ADP oder einem KUNDEN von ADP).
Vorübergehend Beschäftigter	Ein VORÜBERGEHEND BESCHÄFTIGTER ist eine EINZELPERSON, die Services für ADP auf einer vorläufigen oder nicht dauerhaften Basis erbringt (und dabei der direkten Aufsicht von ADP untersteht), wie beispielsweise Zeitarbeiter, Vertragsarbeitnehmer, selbständige Unternehmer oder Berater.
Zulieferer	ZULIEFERER steht für einen DRITTEN, der Waren oder Services an ADP liefert bzw. bereitstellt (z.B. als Dienstanbieter, Vermittler, Auftragsverarbeiter, Berater oder Verkäufer).
Zwingende Auflagen	ZWINGENDE AUFLAGEN sind die Pflichten gemäß einem ANWENDBAREN AUFTRAGSVERARBEITER-RECHT, die die VERARBEITUNG von PERSONENBEZOGENEN DATEN erfordern aus Gründen (i) der nationalen Sicherheit oder Verteidigung; (ii) der öffentlichen Sicherheit; (iii) der Verhütung, Untersuchung, Aufdeckung und Verfolgung von Straftaten oder von Verstößen gegen Ethikgrundsätze für regulierte Berufe; oder (iv) des Schutzes einer EINZELPERSON, oder der Rechte und Freiheiten von EINZELPERSONEN.

ANNEX 2 – Sicherheitsmaßnahmen

Vorgelegt von:	**ADP – Global Security Organization**
Version:	**2.0**
Freigabe:	**September 2019**

Inhalt

Begriffsbestimmungen

Im gesamten Dokument können folgende Begriffe vorkommen:

Verwendeter Begriff oder verwendetes Akronym	Definition
GETS	Global Enterprise Technology & Solutions (ADPs Technik / IT)
GSO	Global Security Organization (ADPs globale Sicherheitsorganisation)
CAB	Change Advisory Board
DRP	Disaster Recovery Plan (Notfallplan)
CIRC	GSO's Critical Incident Response Center
SIEM	Security Information and Event Management
IDS	Intrusion Detection System
DNS	Domain Name System
NTP	Network Time Protocol
SOC	Service Organization Controls
TPSI	Trusted Platform Security Infrastructure

Überblick

ADP betreibt ein förmliches Informationssicherheitsprogramm, das administrative, technische und physische Schutzmaßnahmen enthält, um die Sicherheit, Vertraulichkeit und Integrität von Kundeninformationen zu schützen. Dieses Programm ist sinnvoll konzipiert, um (i) die Sicherheit und Vertraulichkeit von Kundeninformationen zu schützen, (ii) Schutz vor jeglichen Gefahren im Hinblick auf die Sicherheit oder Integrität der Informationen sowie (iii) Schutz vor unautorisiertem Zugriff auf Informationen oder deren Nutzung zu gewährleisten.

Dieses Dokument enthält einen Überblick über ADPs Maßnahmen und Vorgehensweisen zur Gewährleistung der Informationssicherheit, die ab dem Freigabedatum gültig sind und für die ADP sich Änderungen vorbehält. Diese Anforderungen und Vorgehensweisen sind vereinbar mit den ISO/IEC 27001:2013 Informationssicherheits-standards. ADP untersucht seine Sicherheitsrichtlinien und -standards regelmäßig. Unser Ziel ist es sicherzustellen, dass das Sicherheitsprogramm effektiv und effizient arbeitet, um all die Informationen, die unsere Kunden und deren Angestellte uns anvertraut haben, zu schützen.

Unabhängigkeit der Informationssicherheitsfunktion

ADP setzt einen Chief Security Officer ein, der die Global Security Organization (GSO) von ADP überwacht und dem Chefsyndikus (Legal und Compliance), anstatt dem Chief Information Officer berichtet, was der GSO die notwendige Unabhängigkeit von der IT gewährt. Die GSO ist ein geschäftsbereichsübergreifendes, zusammengeführtes Sicherheitsteam, das eine multidisziplinäre Vorgehensweise in den Bereichen der Cyber- und Informationssicherheit und Compliance, der operativen Risikosteuerung, dem Kundensicherheitsmanagement, dem Arbeitnehmerschutz und der betrieblichen Resilienz verfolgt. Das Senior Management der GSO, unter unserem Chief Security Officer, ist für die Verwaltung von Sicherheitsrichtlinien, Sicherheitsmaßnahmen und -vorgaben verantwortlich.

Formale Definition einer Informationssicherheitsrichtlinie

ADP hat formale Informationssicherheitsrichtlinien, welche die Vorgehensweise bei der Verwaltung der Informationssicherheit darlegt, entwickelt und dokumentiert. Die spezifischen Bereiche, die von dieser Richtlinie abgedeckt werden, enthalten unter anderem:

- **Sicherheitsmanagementrichtlinie** – Beschreibt die Verantwortungsbereiche der GSO und des Chief Security Officers (CSO) einschließlich der Informationssicherheitsverantwortlichkeiten und -kontrollen des Einstellungsprozesses unter dem Aspekt der Sicherheit.
- **Globale Datenschutzrichtlinie –** Thematisiert Erhebung, Zugriff, Richtigkeit und Offenlegung von persönlichen Daten sowie die Datenschutzerklärung für Kunden.
- **Richtlinie zur zulässigen Nutzung für elektronische Kommunikation und Datenschutz –** Beschreibt die zulässige Benutzung, verschiedener elektronischer Kommunikationswege, Verschlüsselung und Schlüsselmanagement.
- **Informationsverarbeitungsrichtlinie –** Stellt Anforderungen für die Klassifizierung von Informationen von ADP zur Verfügung und schafft Schutzkontrollen.
- **Physische Sicherheitsrichtlinie –** Definiert die Sicherheitsanforderungen von ADPs Einrichtungen und im Weiteren, die unserer Mitarbeiter und Besucher, die dort tätig sind.
- **Verwaltungsrichtlinie für Sicherheitsoperationen –** Nennt Mindestregelungen für die Anwendung von Systempatches, die effektive Behandlung der Bedrohung durch Malware und sorgt für Backups und Befugniskontrollen bei Datenbanken.
- **Sicherheitsüberwachungsrichtlinie –** Nennt Schutzvorkehrungen für Intrusion Detection Systems (IDS), Aufzeichnungen und für Data Loss Prevention (DLP).
- **Untersuchungs- und Störfallverwaltungsrichtlinie –** Definiert Standards für Reaktionen auf Incidents, elektronische Beweissicherung, Arbeitnehmerschutz und Zugang zu den gespeicherten elektronischen Informationen der Mitarbeiter.
- **Zugangs- und Authentifizierungsrichtlinie –** Beschreibt Anforderungen für Authentifizierung (z.B. User-ID und Passwort), Remote-Zugriff und kabellosen Zugriff.
- **Netzwerksicherheitsrichtlinie –** Sicherheitsarchitektur von Routern, Firewalls, AD, DNS, E-Mail-Servern, DMZ, Cloud Services, Netzwerk-Geräten, Web Proxy und geswitchte Netzwerktechnologie.
- **Richtlinie für globale Risiken durch Dritte und M & A –** Definiert die Mindestsicherheitskontrollen für die Verpflichtung Dritter, um ADP bei der Erreichung seiner Geschäftsziele zu unterstützen.
- **Anwendungsverwaltungsrichtlinie –** Legt geeignete Sicherheitskontrollen in jeder Phase des Entwicklungszyklus des Systems fest.
- **Richtlinie zur betrieblichen Resilienz –** Regelt den Schutz, die Integrität und den Erhalt von ADP durch die Festlegung der Mindestanforderungen, um Business-Resilienz-Programme zu dokumentieren, zu implementieren, zu unterhalten und kontinuierlich zu verbessern.

- **Zusammengeführte Verwaltungsrichtlinie für Sicherheitsrisiken** – Identifizierung, Überwachung, Reaktion, Analyse, Steuerung und neue Unternehmensinitiativen.

Die Richtlinien werden im ADP-Intranet veröffentlicht und sind für alle Mitarbeiter und Auftragnehmer innerhalb des ADP-Netzwerks zugänglich.

Bewertung der Informationssicherheitsrichtlinie

ADP überprüft seine Informationssicherheitsrichtlinien mindestens einmal im Jahr oder immer dann, wenn wesentliche Änderungen die Funktion von ADPs Informationssystemen beeinträchtigen.

Organisation der Informationssicherheit

Funktionen und Verantwortlichkeiten in der Informationssicherheit

Die GSO besteht aus bereichsübergreifenden Sicherheitsteams, die eine multidisziplinäre Vorgehensweise für die Einhaltung von Cyber- und Informationssicherheitsstandards, operative Risikosteuerung, Kundensicherheitsmanagement, Arbeitnehmerschutz und betrieblichen Resilienz, unterstützen. Funktionen und Verantwortlichkeiten wurden formal für alle Mitglieder der GSO definiert. Die GSO ist mit dem Design, der Implementierung und der Kontrolle unseres Informationssicherheitsprogramms, das auf Unternehmensrichtlinien beruht, beauftragt. Die Aktivitäten der GSO werden vom Executive-Security-Komitee überwacht. Zu dessen Mitgliedern zählen: ADPs Chief Security Officer, Chief Executive Officer, Chief Financial Officer, Chief Strategy Officer, Chief Human Resources Officer und der General Counsel.

Richtlinie für mobile Computernutzung und Telearbeit

ADP fordert, dass alle vertraulichen Informationen auf mobilen Geräten verschlüsselt sein müssen, damit es durch Diebstahl oder Verlust eines Rechners zu keinem Datenverlust kommt. Fortgeschrittener End-Point-Schutz und Zwei-Faktor-Authentifizierung via VPN wird ebenfalls benötigt, um remote auf die Firmennetzwerke zugreifen zu können. Alle Remote-Geräte müssen durch ein Passwort geschützt werden. Die Mitarbeiter von ADP sind verpflichtet, verlorene oder gestohlene Computer unverzüglich mittels des Security Incident Reporting Process zu melden.

Als Bedingung für die Beschäftigung bei ADP müssen alle Mitarbeiter und Auftragnehmer die Nutzungsbedingungen für elektronische Kommunikation, die Datenschutzrichtlinie sowie andere relevante Richtlinien einhalten.

Sicherheit des Personalwesens

Hintergrundüberprüfungen

In Übereinstimmung mit geltenden gesetzlichen Bestimmungen der individuellen Rechtsprechung führt ADP geeignete Hintergrundüberprüfungen entsprechend der Aufgaben und Verantwortlichkeiten seiner Mitarbeiter, Auftragsnehmer und Dritter durch. Diese Überprüfungen bestätigen die Eignung des Kandidaten, mit Kundeninformationen umzugehen bevor die Person eingesetzt oder angestellt wird.

Hintergrundüberprüfungen können die folgenden Komponenten beinhalten:

- Prüfung der Identität / der Arbeitserlaubnis
- Beruflicher Werdegang
- Bildungshistorie und berufliche Qalifikationen
- Vorstrafen (falls rechtmäßig befugt bzw. gesetzlich zulässig und abhängig von den lokalen Ländervorgaben)

Vertraulichkeitsvereinbarungen mit Mitarbeitern und Auftragsnehmern

Die in den Arbeitsverträgen von ADP und in seinen Verträgen mit Auftragnehmern enthaltenen Bedingungen enthalten eine Reihe von Verpflichtungen und Verantwortungen in Bezug auf die Kundeninformationen, zu denen die Vertragsparteien Zugang haben werden. Alle Mitarbeiter und Auftragsnehmer von ADP sind an die Verschwiegenheitspflichten gebunden.

Trainingsprogramm für Informationssicherheit

Alle Mitarbeiter sind verpflichtet, ein Informationssicherheitstraining als Teil ihres Onboardings zu absolvieren. Zusätzlich bietet ADP ein jährliches Sicherheitstraining an, um Mitarbeiter an ihre Verantwortlichkeiten bei der Erfüllung täglicher Aufgaben zu sensibilisieren.

Verantwortlichkeiten von Mitarbeitern und Disziplinarverfahren

ADP hat eine Sicherheitspolitik veröffentlicht, die alle Mitarbeiter befolgen müssen. Verstöße gegen die Sicherheitsrichtlinien können zur Widerrufung von Zugangsprivilegien und/oder Disziplinarmaßnahmen bis hin zur Beendigung der Beratungsverträge oder des Arbeitsverhältnisses führen.

Beendigung der beruflichen Tätigkeit

Verantwortlichkeiten bei der Beendigung des Arbeitsverhältnisses wurden formal dokumentiert und umfassen mindestens:

- Alle Geräte und Daten von ADP, die sich im Besitz des jeweiligen Mitarbeiters befinden, müssen zurückgegeben werden, ganz gleich auf welchem Medium sie aufbewahrt werden.
- Entzug der Zugangsrechte zu ADPs Einrichtungen, Informationen/Daten und Systemen.
- Passwortänderung für weiter genutzte gemeinsame Benutzerkonten (sofern zutreffend).
- Falls möglich Wissensstransfer.

Gerätemanagement

Zulässige Nutzung von Geräten

Die zulässige Nutzung von Geräten wird in mehreren Richtlinien ausgeführt. Sie betrifft ADP-Mitarbeiter und Auftragsnehmer und gewährleistet, dass Daten von ADP und seinen Kunden durch die Verwendung solcher Geräte nicht offengelegt werden. Beispiele für in diesen Richtlinien beschriebene Bereiche sind: Einsatz der elektronischen Kommunikation, Nutzung elektronischer Geräte und Nutzung der Informationsressourcen.

Klassifizierung von Informationen

Informationen, die von oder im Auftrag von ADP erworben, erzeugt oder unterhalten werden, wird eine der folgenden Sicherheitsklassifizierungen zugewiesen:

- Public-Beispiel: Marketingbroschüren, veröffentlichte Jahresberichte
- ADP Internal Use Only-Beispiel: Interoffice-Kommunikationen, Betriebsverfahren
- ADP Confidential-Beispiel: Persönliche und sensible personenbezogene Daten
- ADP Restricted-Beispiel: Finanzprognosen, Informationen zur strategischen Planung

Voraussetzungen für den Umgang mit Informationen stehen in direktem Zusammenhang mit der Informationssicherheitsklassifizierung. Persönliche und sensible personenbezogene Informationen werden immer als ADP Confidential betrachtet. Alle Kundeninformationen werden als vertraulich (ADP Confidential) klassifiziert.

ADP-Mitarbeiter sind verantwortlich dafür, Informationswerte /-bestände gemäß ihres Sicherheitsklassifikationslevels zu schützen und zu behandeln. Das Sicherheitsklassifikationslevel bestimmt den Informationsschutz und geeignete Handhabungsanforderungen für jedes Klassifikationslevel. ADPs Vertraulichkeitsklassifikation wird für alle gespeicherten und übermittelten Informationen verwendet sowie für jene, die von Dritten verarbeitet werden.

Equipment- und Medienentsorgung

Wenn Equipment, Dokumente, Dateien und Medien von ADP entsorgt oder wiederverwendet werden, werden angemessene Maßnahmen ergriffen, um einen späteren Abruf von Kundeninformationen, die ursprünglich darauf gespeichert waren, zu verhindern. Alle Informationen auf Computern oder elektronischen Speichermedien, unabhängig von ihrer Klassifikation, werden sicher entsorgt, sofern das Medium nicht physisch zerstört wird, bevor es die Einrichtungen von ADP verlässt oder umgerüstet wird. Die Abläufe für eine sichere Vernichtung/Löschung von ADPs Informationen, die sich auf Geräten, in Dokumenten, Dateien und Medien befinden, werden formal dokumentiert.

Transport physischer Medien

Organisatorische Schutzmaßnahmen wurden eingeführt, um Druckmaterial, das Kundeninformationen enthält gegen Diebstahl, Verlust und/oder unautorisierte/n Zugriff/Modifizierung (i) während des Transports, z.B. verschlossene Umschläge, Behälter und persönliche Zustellung an den autorisierten Nutzer; und (ii) während der Überprüfung, Überarbeitung oder anderweitiger Verarbeitung, bei der Druckmaterial aus sicherer Aufbewahrung entnommen wird, zu schützen.

Zugangskontrolle

Betriebliche Anforderungen der Zugangskontrolle

ADPs Richtlinie für Zugangskontrolle beruht auf geschäftlich definierten Anforderungen. Die Richtlinien und Kontrollstandards sind in Zugangskontrollen formuliert, die für alle Komponenten der erbrachten Leistung durchgesetzt werden und auf den Prinzipien „geringste Privilegien“ und „Kenntnis erforderlich“ (least-privilege and need to know) beruhen.

Zugang zur Infrastruktur – Zugangskontrollmanagement

Zugangsanfragen für das Bewegen, Hinzufügen, Erstellen und Löschen werden protokolliert, genehmigt und regelmäßig überprüft.

Eine formale Prüfung wird mindestens einmal jährlich durchgeführt, um zu bestätigen, dass individuelle Nutzer genau mit der relevanten Geschäftsfunktion übereinstimmen und nach einem Positionswechsel keinen fortgesetzten Zugang besitzen. Dieser Vorgang wird geprüft und in einem SOC11 Typ II Bericht dokumentiert. Innerhalb eines Identitätsmanagementsystems ist ein spezielles ADP-Team verantwortlich für die Gewährung, Ablehnung, Aufhebung, Beendigung und Stilllegung/Deaktivierung des Zugangs zu den ADP-Einrichtungen und deren Informationssystemen. ADP benutzt ein zentralisiertes Identitäts- und Zugangsverwaltungstool (IAM - identity and access management), das zentral von einem speziellen GETS-Team verwaltet wird. Gemäß der Zugangsrechte, die durch das IAM-Tool angefragt werden, wird ein Validierungs-Workflow ausgelöst, der den Vorgesetzen des Nutzers involviert. Der Zugang wird zeitlich begrenzt gewährt und die eingerichteten Workflows verhindern, dass solche Zugangsberechtigungen dauerhaft bestehen bleiben. Der Zugang eines Mitarbeiters zur Einrichtung wird unmittelbar nach dem letzten Arbeitstag durch die Deaktivierung der Zugangskarte (Mitarbeiterausweis) stillgelegt. Die Benutzer-IDs des Mitarbeiters wird sofort deaktiviert. Der zuständige direkte Vorgesetzte des Mitarbeiters prüft mithilfe der in der Configuration-Management-Database enthaltenen Hardwareliste, ob der Mitarbeiter sämtliche Geräte abgegeben hat. Nach einem Positionswechsel oder organisatorischen Änderungen müssen Nutzerprofile oder Nutzerzugangsrechte vom Management der zuständigen Geschäftseinheit und vom IAM-Team abgeändert werden. Zusätzlich wird jedes Jahr eine formale Überprüfung der Zugangsrechte durchgeführt, um zu verifizieren, dass die individuellen Nutzerrechte mit deren relevanten Geschäftsfunktionen übereinstimmen und dass nach einem Positionswechsel keine irrelevanten Zugangsrechten bestehen bleiben.

Passwortrichtlinie

Passwortrichtlinien für ADP-Mitarbeiter sind auf Servern, in Datenbanken sowie bei Netzwerkgeräten und -anwendungen in dem Maß zwingend, in dem es das Gerät/die Anwendung zulässt. Die Passwortkomplexität wird aus einer risikobasierten Analyse der geschützten Daten und Inhalte abgeleitet. Die Richtlinien entsprechen den geltenden Branchenstandards bezüglich Stärke und Komplexität, einschließlich, aber nicht beschränkt auf die Nutzung von Step-Up-Authentifizierung, Zwei-Faktor-Authentifizierung oder gegebenenfalls biometrischer Authentifizierung.

Anforderungen für die Authentifizierung in Kundenanwendungen variieren je nach Produkt und für spezielle ADP-Anwendungen stehen Verbunddienste (SAML 2.0) zur Verfügung, die mit einer durch GETS verwalteten Netzwerk- und Sicherheitsschicht arbeiten.

[1] Im Falle gewisser US-Dienstleistungen von ADP, wird dies in einem SOC 2 Typ II Bericht geprüft.

Session-Timeouts

ADP führt automatische Timeouts auf allen Servern, an allen Arbeitsplätzen, in allen Anwendungen und VPN-Verbindungen zwingend durch. Diese basieren auf einem risikobasierten Ansatz gemäß Branchenstandards. Sessions können erst wiederhergestellt werden, nachdem der Nutzer ein gültiges Passwort eingegeben hat.

Kryptographie

Kryptografische Kontrollen

ADP fordert, dass sensible Informationen, die zwischen ADP und Dritten von ADP ausgetauscht werden, durch die Nutzung branchenüblicher Verschlüsselungstechniken und - stärken verschlüsselt werden (oder der Transportkanal muss verschlüsselt werden). Alternativ kann auch eine private Standleitung verwendet werden.

Schlüssel-Management

ADP verfügt über einen internen Verschlüsselungssicherheitsstandard, der ein klar definiertes Schlüssel-Management und eine Vorgehensweise zur Schlüsselhinterlegung, einschließlich symmetrischem und asymmetrischem Schlüssel-Management enthält.

Kodierungsschlüssel, die für Informationen von ADP verwendet werden, werden immer als vertrauliche Informationen klassifiziert. Der Zugang zu solchen Schlüsseln ist strikt auf diejenigen beschränkt, die Wissensbedarf haben und, wenn eine Ausnahmegenehmigung vorliegt. Kodierungsschlüssel und Key-Lifecycle-Management folgen branchenüblichen Verfahren.

Physische Sicherheit und Umgebungssicherheit

ADPs Vorgehensweise für physische Sicherheit hat zwei Ziele – eine sichere Arbeitsumgebung für ADP-Mitarbeiter zu schaffen und persönliche Informationen, die in ADPs Rechenzentren und an anderen strategischen Standorten von ADP gespeichert sind, zu schützen.

Die Sicherheitsrichtlinie von ADP schreibt dem Management von ADP vor, diejenigen Bereiche zu identifizieren, die ein besonderes Maß an physischer Sicherheit benötigen. Zugang zu diesen Bereichen wird nur autorisierten Mitarbeitern für genehmigte Zwecke gewährt. Die Sicherheitsbereiche von ADP verwenden verschiedene physische Sicherheitsschutzmaßnahmen, einschließlich Videoüberwachungssystemen, der Nutzung von Sicherheitsausweisen (identitätsbasierter Zugang) und Sicherheitsbeauftragten, die an Ein- und Ausgängen postiert sind. Besuchern wird nur an autorisierten Stellen Zugang gewährt, und sie werden zu jeder Zeit überwacht.

Betriebssicherheit

Formalisierung von IT-Betriebsverfahren

Die GETS-Einheit von ADP ist für den IT-Infrastrukturbetrieb und deren Wartung verantwortlich. GETS unterhält und dokumentiert IT-Betriebsrichtlinien und -verfahren formal. Diese Verfahren enthalten unter anderem Folgendes:

- Change-Management
- Back-Up-Management
- Behandlung von Systemfehlern
- Systemneustart und -wiederherstellung
- Systemüberwachung
- Jobplanung und -überwachung

Change-Management der Infrastruktur

GETS beruft in regelmäßigen Abständen ein Change Advisory Board (CAB) samt Vertretern aus einer Reihe verschiedener ADP-Teams ein. Die CAB Meetings erfolgen zur Besprechung von Auswirkungen, zur Vereinbarung von Einsatzfenstern und zur Genehmigung der Hochstufung für die Produktion sowie zur Koordinierung jeglicher Änderungen in der Produktionsinfrastruktur.

Systemkapazitätsplanung und -akzeptanz

Kapazitätsanforderungen werden kontinuierlich überwacht und regelmäßig überprüft. Infolge dieser Überprüfungen werden Systeme und Netzwerke entsprechend aufgestockt oder zurückgefahren. Wenn aufgrund einer Kapazitätsänderung oder technischen Entwicklung wesentliche Änderungen vorgenommen werden müssen, kann das GETS-Benchmarking-Team Stresstests in der relevanten Anwendung und/oder im relevanten System durchführen. Beim Abschluss des Stresstests liefert das Team durch Messung der Änderungen von (i) Komponenten, (ii) Systemkonfiguration oder -version oder (iii) Middleware-Konfiguration oder Middleware-Version einen detaillierten Bericht zur Leistungsentwicklung.

Schutz vor schädlichem Code

Endpoint-Protection-Technologien werden nach Industriestandard eingesetzt, um ADPs Assets in Übereinstimmung mit den branchenüblichen Industriestandard zu schützen.

Back-Up-Management-Richtlinie

Die geltenden ADP Richtlinien fordern, dass die Produktionsdaten aller produktionsbezogenen Hosting-Vorgänge gesichert werden müssen. Der Umfang und die Häufigkeit von Sicherungen werden in Übereinstimmung mit den Geschäftsanforderungen relevanter ADP-Dienstleistungen, den Sicherheitsanforderungen der betreffenden Informationen und der Gefährlichkeit der Informationen in Hinblick auf Notfallwiederherstellung ausgeführt. Die Überwachung der turnusmäßigen Datensicherungen erfolgt durch GETS, um Probleme bei der Sicherung oder Ausnahmen zu identifizieren.

Sicherheitsprotokollierung und -überwachung

ADP verfügt über eine zentrale Infrastruktur ausschließlich mit Lesezugriff (SIEM) sowie ein Protokoll-Korrelierungs- und Alarmierungssystem (TPSI). Protokollalarme werden überwacht und rechtzeitig vom CIRC bearbeitet.

Diese Systeme sind über einen eindeutigen Network Time Protocol (NTP)-basierten Taktbezug synchronisiert.

Jedes einzelne Protokoll enthält mindestens:

- Zeitstempel
- Wer (Identität des Operators oder Administrators)
- Was (Information über das Ereignis)

Zur Nachverfolgung der folgenden Informationen wurden Audit-Trails und Systemprotokolle für ADP-Anwendungen konzipiert und eingerichtet:

- Authorisierter Zugang
- Privilegierte Aktivitäten
- Unauthorisierte Zugangsversuche
- Systemwarnungen oder -ausfall
- Änderungen an den Systemsicherheitseinstellungen des Systems, sofern das System eine derartige Protokollierung zulässt

Diese Protokolle sind nur für autorisiertes Personal von ADP verfügbar und werden im Live-Modus gesendet, um zu verhindern, dass Daten manipuliert werden, bevor sie in sicheren Protokollierungsanwendungen gespeichert werden.

Infrastruktursysteme und -überwachung

ADP wendet angemessene Maßnahmen an, um eine Infrastrukturüberwachung 24 Stunden am Tag und 7 Tage die Woche zur Verfügung zu stellen. Störungswarnungen werden von verschiedenen Teams gemäß ihrem Schweregrad und den zur Lösung benötigten Fähigkeiten gehandhabt.

Hosting-Center-Einrichtungen von ADP verwenden Anwendungen zur Überwachung, die konstant auf allen verwandten Datenverarbeitungssystemen und auf den Netzwerkkomponenten laufen, damit den Mitarbeitern von ADP eine proaktive Benachrichtigung über Probleme und Warnungen in Erwartung möglicher Probleme ermöglicht wird.

Technisches Vulnerability Management

Alle Computer, die in der Hosting-Infrastruktur installiert sind, müssen der Installation eines spezialisierten sicherheitsgehärteten Betriebssystems (oder sicherem build process) nachkommen. Hosted operations verwenden eine gehärtete, genehmigte und standardisierte Bauart für jeden Servertyp, der innerhalb unserer Infrastruktur verwendet wird. Die Out-Of-The-Box-Installation von Betriebssystemen ist verboten, da diese Installationen Schwachstellen schaffen könnten, wie zum Beispiel generische Systemkontenpasswörter, welche ein Risiko für die Infrastruktur darstellen würden. Diese Konfigurationen reduzieren die Belastung von gehosteten Computern auf denen unnötige Dienste laufen, welche zu Schwachstellen führen können.

ADP verfügt über eine dokumentierte Methodik bei der Durchführung von Freigabewertungen sowie regelmäßig stattfindender Schwachstellenbewertung und Compliance Prüfungen von webbasierten Anwendungen im Internet und deren zugehörigen Infrastrukturkomponenten, welche mindestens 15 Testkategorien enthalten. Die Bewertungsmethode basiert sowohl auf internen als auch branchenweit genutzten, bewährten Verfahren, u.a. auch auf Open Web Application Security Project (OWASP), SANS Institute und Web Application Security Consortium (WASC).

Kommunikationssicherheit

Netzwerk-Sicherheits-Management

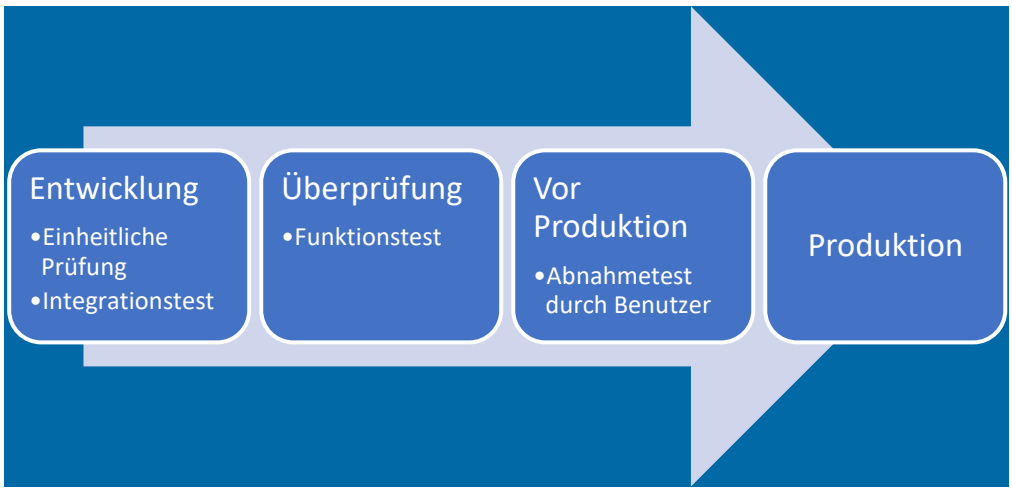
ADP verwendet eine netzwerkbasierte Einbruchmeldeanlage, die den Datenverkehr auf der Ebene der Netzwerkinfrastruktur überwacht (24 Stunden am Tag, 7 Tage die Woche) und die eine verdächtige Aktivität oder potenzielle Angriffe identifiziert.

Informationsaustausch

ADP implementiert geeignete Kontrollen, sodass Informationen von ADPs Kunden, die an Dritte gesendet werden, nur zwischen autorisierten Informationssystemen und -ressourcen übertragen und nur über die von ADP sicheren und autorisierten Transfermechanismen ausgetauscht werden.

Sicherheit in Entwicklungs- und Unterstützungsprozessen

Während des Entwicklungszyklus werden eine geeignete Dokumentation und Testpläne für die Testphase erstellt. Es werden verschiedene Stufen für jede Umgebung mit einer entsprechenden Genehmigung in jeder Phase definiert:



- Um von der Prüfungs- zur Vorproduktionsumgebung zu gelangen, wird die Genehmigung des ADP-Qualitätsteam benötigt.
- Um von der Vorproduktion zur Produktion zu gelangen, wird die Genehmigung des IT-Betriebs benötigt.

Entwicklungsteams müssen sichere Kodierungsverfahren verwenden. Anwendungsänderungen werden in Entwicklungs- und Regressionsumgebungen getestet bevor sie die Produktionssysteme erreichen. Die Tests werden durchgeführt und dokumentiert. Nach Freigabe werden die Änderungen dann in der Produktionsumgebung eingesetzt. Ein Penetrationstest wird nach wesentlichen Änderungen durchgeführt.

GETS beruft in regelmäßigen Abständen ein Change Advisory Board (CAB) samt Vertretern aus einer Reihe verschiedener ADP-Teams ein. Die CAB Meetings erfolgen zur Besprechung von Auswirkungen, zur Vereinbarung von Einsatzfenstern und zur Genehmigung der Hochstufung für die Produktion bzw. auch um über weitere Änderungen in der Produktionsinfrastruktur zu informieren.

Das ADP IT-Betriebs-Team gibt die endgültige Genehmigung vor einer Hochstufung von Softwarepaketen in die Produktionsumgebung.

Sicherheit in der Entwicklungsumgebung

Produktions- und Entwicklungsumgebungen sind getrennt und unabhängig voneinander. Es werden geeignete Zugangskontrollen verwendet, um eine ordnungsgemäße Aufgabentrennung durchzusetzen. Softwarepakete sind in jedem Stadium des Entwicklungsprozesses nur für die im jeweiligen Stadium involvierten Teams zugänglich.

Testdaten

Gemäß der Anwendungsmanagementrichtlinie von ADP ist die Benutzung von Echtdaten oder unbereinigten Daten in der Entwicklung und bei der Prüfung nicht erlaubt, es sei denn, sie ist explizit vom Kunden gewünscht und autorisiert.

Lieferantenbeziehungen

Identifizierung von Risiken verbunden mit externen Parteien

In regelmäßigen Abständen werden für Dritte, die Zugriff auf die Daten von ADP und/oder Kunden benötigen, Risikobeurteilungen durchgeführt, um festzustellen ob diese den ADP Sicherheitsanforderungen für Dritte entsprechen und ob die angewandten Sicherheitsvorkehrungen Schwachstellen aufweisen. Werden Schwachstellen festgestellt, so werden mit diesen externen Stellen neue Maßnahmen vereinbart.

Informationssicherheitsvereinbarungen mit externen Parteien

ADP schließt mit allen Dritten Vereinbarungen ab, welche angemessene Sicherheitsverpflichtungen gem. den Sicherheitsanforderungen von ADP enthalten.

Management von Sicherheitsvorfälle und Verbesserungen

ADP verfügt über eine dokumentierte Methodik, um rechtzeitig, konsistent und effektiv auf Sicherheitsvorfälle (Security Incident) zu reagieren.

Sollte sich ein Vorfall ereignen, aktiviert ein vorher festgelegtes Team bestehend aus ADP-Mitarbeitern einen formalen incident response plan, der sich unter anderem auf folgende Gebiete bezieht:

- Eskalationen basierend auf der Einstufung oder der Schwere des Incidents
- Kontaktliste für Incident-Bericht/-Eskalation
- Richtlinien für erste Reaktionen und Follow-Up mit betroffenen Kunden
- Übereinstimmung mit geltenden Gesetzen zur Meldepflicht für Sicherheitsverletzungen
- Untersuchungsprotokoll
- Systemwiederherstellung
- Problemlösung, -Bericht, und -Bewertung
- Grundlegende Ursachen und Behebung
- Gewonnene Erkenntnisse

ADPs Richtlinien definieren einen Sicherheitsvorfall, das Management von Sicherheitsvorfällen und die Verantwortlichkeiten aller Mitarbeiter hinsichtlich des Berichtens über einen Sicherheitsvorfall. Außerdem führt ADP regelmäßige Trainings für ADP-Mitarbeiter und Auftragnehmer durch, um die Aufmerksamkeit der Berichtspflichten sicherzustellen. Das Training wird nachverfolgt, um dessen Fertigstellung sicherzustellen.

ADPs Programm für betriebliche Resilienz

ADP verpflichtet sich dazu, weiterhin dafür zu sorgen, dass unsere Dienstleistungen und Arbeitsabläufe reibungslos ablaufen, so dass wir unseren Kunden den bestmöglichen Service anbieten können. Es ist unsere Priorität, die technologischen, umweltbedingten, prozessbezogenen und gesundheitlichen Risiken, die der Erfüllung unserer Unternehmensdienste im Weg stehen, zu identifizieren – und diese zu minimieren. ADP hat ein integriertes Rahmenwerk erstellt, das unsere Risikominderung-, Bereitschafts-, Reaktions- und Wiederherstellungsprozesse darlegt und schließt folgendes mit ein:

- Risikobewertung
- Risiko-/Gefahrenanalyse
- Business-Impact-Analyse
- Planentwicklung
- Geschäftskontinuitätsplanung
- Notfallwiederherstellungsplanung
- Gesundheits- und Sicherheitsplanung
- Real-World Reaktion
- Krisenmanagement
- Gefahrenabwehr
- Prüfung und Validierung
- Bewertung
- Überarbeitung
- Ausübung

Compliance

Einhaltung von Sicherheitsrichtlinien und -standards

ADP verwendet ein Verfahren, um intern regelmäßig Einhaltungsprüfungen durchzuführen. Zusätzlich führt ADP regelmäßig eine SOC1[2] vom Typ II durch. Diese Prüfungen werden von einer bekannten, dritten Prüfungsfirma durchgeführt. Die Prüfungsberichte sind für Kunden auf Nachfrage jährlich verfügbar (wenn zutreffend).

Technische Einhaltung

Um die technische Einhaltung von bewährten Praktiken durchzusetzen, führt ADP regelmäßig geplante Scans nach Netzwerksicherheitslücken durch. Die Scan-Ergebnisse werden dann von den Hosting-Teams und deren Management priorisiert und zu Korrekturplänen weiterentwickelt.

Scans nach Sicherheitslücken werden regelmäßig sowohl in internen und externen Umgebungen durchgeführt. Zusätzlich werden Quellcode-Scans und Penetrationstests je Produkt durchgeführt. Durch die Nutzung spezialisierter Tools für das Scannen von Anwendungen werden Sicherheitslücken auf Anwendungsebene, falls vorhanden identifiziert, mit den Produktentwicklungs-Managementteams geteilt und in die Qualitätssicherungsprozesse für Korrekturmaßnahmen aufgenommen. Die Ergebnisse werden analysiert und Korrekturpläne werden entwickelt und priorisiert.

Aufbewahrung von Daten

ADPs Richtlinie zur Datenspeicherung bezüglich Kundeninformationen ist gemäß geltenden Gesetzen gestaltet. Am Ende eines Kundenvertrags erfüllt ADP seine vertraglichen Verpflichtungen, die sich auf Kundeninformationen beziehen. ADP gibt alle Kundeninformationen, die für den Fortbestand der Geschäftsaktivitäten des Kunden benötigt werden, zurück (sofern nicht bereits geschehen) oder erlaubt dem Kunden diese (per Datendownload) zurückzuholen. Anschließend löscht ADP die verbleibenden Kundeninformationen sicher, ausgenommen in dem Umfang, der nach geltendem Recht vorgeschrieben ist, vom Kunden autorisiert ist oder zum Zwecke der Streitschlichtung benötigt wird.

[2] Im Falle gewisser US-Dienstleistungen von ADP, würden es ebenfalls SOC 2 Durchführungsberichte vom Typ II geben.

ANNEX 3 – Liste der Konzerngesellschaften, für die dieser Code verbindlich ist

ADP (Philippines), Inc	6/F Glorietta 2 Corporate Center, Palm Drive, Ayala Center, Makati City, Philippines, 1224
ADP (Suisse) SA	Lerzenstr. 10, 8953 Dietikon, Switzerland
ADP Brazil Ltda.	João Tibiriçá, 1112 - Vila Anastácio, São Paulo - SP, 05077-000, Brazil
ADP Canada Co.	3250 Bloor Street West, 16th Floor, Etobicoke, Ontario M8X 2X9, Canada
ADP Employer Services Belgium BVBA	Koningsstraat 97/4, 1000 Brussels, Belgium
ADP Employer Services Ceska Republika a.s.	Rohanske nabrezi 670/17, 18600 Praha 8, Czech Republic
ADP Employer Services GmbH	Frankfurter Str. 227, 63263 Neu-Isenburg, Germany
ADP Employer Services Iberia, S.L.U.	Cami Antic de Valencia, 54 B, 08005 Barcelona, Spain
ADP Employer Services Italia SPA	Viale G. Richard 5/A – 20143 Milan, Italy
ADP ES Tunisie SARL	MIRMAR Business City Lot B16 Centre Urbain Nord – 1003 Tunis, Tunisia
ADP Europe, S.A.S.	31, avenue Jules Quentin, 92000 Nanterre, France
ADP France SAS	31, avenue Jules Quentin, 92000 Nanterre, France
ADP GlobalView B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Netherlands
ADP GSI France SAS	31-41, avenue Jules Quentin, 92000 Nanterre, France
ADP HR and Payroll Services Ireland Limited	Unit 1, 42 Rosemount Park Dr, Rosemount Business Park, Dublin, D11 KC98, Ireland
ADP India Private Ltd.	Tamarai Tech Park, S.P. Plot No.16 to 20 & 20A, Thiru-Vi-Ka Industrial Estate, Inner Ring Road, Guindy, Chennai – 600 032 India
ADP International Services B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Netherlands
ADP Nederland B.V.	K.P. van der Mandelelaan 9-35, 3062 MB Rotterdam, Postbus 4065, 3006 AB Rotterdam

ADP Outsourcing Italia SRL	Viale G. Richard 5/A – 20143 Milan, Italy
ADP Payroll Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Polska Sp. zo.o.	Prosta 70, 00-838 Warsaw, Poland
ADP Private Limited	6-3-1091/C/1, Fortune 9, Raj Bhavan Road, Somajiguda, Hyderabad, Telangana, India – 500082
ADP RPO UK Limited	22 Chancery Lane, London, England, WC2A 1LS
ADP RPO, LLC	3401 Technology Drive, Findlay, OH, USA 45840
ADP Screening and Selection Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Slovakia s.r.o.	Cernysevskeho 26, 851 01 Bratislava, Slovakia
ADP Software Solutions Italia SRL	Via Oropa 28 – 10153 Turin, Italy
ADP Sverige AB	Östermalmstorg 1, 114 42 Stockholm, Schweden
ADP, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
Automatic Data Processing (ADP) Romania SRL	4B Gara Herastrau St., 1st – 6th floor, District 2, Bucharest, Romania 020334
Automatic Data Processing Limited (Australia)	6 Nexus Court, Mulgrave, VIC 3170, Australia
Automatic Data Processing Limited (UK)	Syward Place, Pyrcroft Road, Chertsey, Surrey, KT16 9JT, England
Business Management Software Limited	2 Peterborough Business Park, Lynch Wood, Peterborough, Cambridgeshire, PE2 6FZ, England
Celergo Hungary kft	1093 Budapest, Kozraktar utca 30. 6. emelet., Cg. 01-090980824, Hungary
Celergo LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Celergo PTE. LTD.	62, Ubi Road 1, #11-07, Oxley Bizhub 2, Singapur 408733
Ridgenumber - Processamento de Dados LDA	Rua Brito e Cunha, 254 - 2º, 4450-082 Matosinhos, Portugal
The Marcus Buckingham Company	8350 Wilshire Boulevard, #200, Beverly Hills, CA, USA 90211

VirtualEdge Corporation	One ADP Boulevard, Roseland, NJ, USA 07068