ADP Privacy Code für Kundendatenverarbeitungsdienste

Einleitung 2
Artikel 1 – Umfang, Anwendbarkeit und Umsetzung 2
Artikel 2 – Servicevertrag 3
Artikel 3 – Verpflichtungen zur Einhaltung von Vorgaben 4
Artikel 4 – Zwecke für die Verarbeitung Personenbezogener Daten 6
Artikel 5 – Sicherheitsanforderungen 7
Artikel 6 – Transparenz gegenüber Beschäftigten des Kunden 7
Artikel 7 – Unterauftragsverarbeiter 8
Artikel 8 – Aufsicht und Einhaltung von Vorgaben 9
Artikel 9 – Richtlinien und Verfahren 13
Artikel 10 – Schulungen 13
Artikel 11 – Compliance Überwachung und Überprüfung 13
Artikel 12 – Rechtsfragen 16
Artikel 13 – Sanktionen für Non-Compliance 19
Artikel 14 – Widersprüche zwischen diesem Code und Anwendbarem Auftragsverarbeiter-Recht 19
Artikel 15 – Änderungen zu diesem Code 20
Artikel 16 – Implementierung und Übergangszeiten 21
ANNEX 1 – BCR Definitionen 23
ANNEX 2 – Sicherheitsmaßnahmen 32
ANNEX 3 – Liste der Konzerngesellschaften, für die dieser Code verbindlich ist 63

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 Datenschutzmanagement 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 Unterauftragsverarbeitern 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.

Beschwerde-verfahren **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 Geschäfts-einheit 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 Konzern-gesellschaften

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 Ersatz-dokumenten, 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, LLC.
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 Ent-scheidung 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, wie z.B. dem Privacy Shield.
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. Nach einer Entscheidung des General Counsel – die auf **www.adp.com** veröffentlicht wird – kann dies auch andere Länder mit Datenschutzgesetzen 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, LLC. ist, wenn entweder Automatic Data Processing, Inc. oder ADP, LLC. 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:	**1.8**
Freigabe:	**Oktober 2018**

Inhalt

1. Informationssicherheitsrichtlinie 36
   - A. Management der Informationssicherheit 36
   - B. Unabhängigkeit der Informationssicherheitsfunktion 36
   - C. Formale Definition einer Informationssicherheitsrichtlinie 36
   - D. Überprüfung der Informationssicherheitsrichtlinie 37
2. Organisation der Informationssicherheit 38
   - A. Rollen und Pflichten im Rahmen der Informationssicherheit 38
   - B. Richtlinie mobile Computernutzung und Telearbeit 38
3. Sicherheit im Personalwesen 39
   - A. Hintergrundprüfungen 39
   - B. Vertraulichkeitsvereinbarungen mit Mitarbeitern und Auftragnehmern 39
   - C. Schulungsprogramm zur Informationssicherheit 39
   - D. Sensibilisierung der Mitarbeiter und Auftragnehmer für das Thema Sicherheit 39
   - E. Mitarbeiterpflichten und Disziplinarwesen 39
   - F. Pflichten bei Beendigung des Arbeitsverhältnisses 40
4. Geräteverwaltung 41
   - A. Zulässige Nutzung von Geräten 41
   - B. Klassifizierung von Informationen 41
   - C. Entsorgung von Geräten und Medien 41
   - D. Transport physischer Medien 42
5. Zugangskontrolle 43
   - A. Fachliche Anforderungen der Zugangskontrolle 43
   - B. Zugang zu Infrastruktur – Zugangskontrollmanagement 43
   - C. Passwort Richtlinie 44
   - D. Zeitüberschreitung bei einer Sitzung 45
6. Kryptographie 46
   - A. Kryptographische Sicherheitsmaßnahmen 46
   - B. Schlüsselmanagement 46
7. Physische und umgebungsbezogene Sicherheit 47
   - A. Physische Sicherheit 47
   - B. Maßnahmen für die physische Zugangskontrolle 47
   - C. Prüfung des Zugangs zu sensiblen Bereichen 47
   - D. Kennzeichnung von ADP Personal 48

E. Physische und umgebungsgebundene Sicherheitsmaßnahmen in Datenzentren 48
8. Betriebliche Sicherheitsmaßnahmen 49
A. Formalisierung der IT-Betriebsverfahren 49
B. Change Management für die Infrastruktur 49
C. Systemkapazitätsplanung und -zulassung 49
D. Schutz vor bösartigem Code 49
E. Richtlinie zum Sicherungsmanagement 49
F. Sicherheitsprotokollierung und -überwachung 50
G. Infrastruktursysteme und Überwachung 51
H. Technisches Schwachstellenmanagement 51
9. Kommunikationssicherheit 52
A. Management der Netzwerksicherheit 52
B. Austausch von Informationen 52
C. Verwendung eines Nachrichtensystems 52
10. Systembeschaffung, -entwicklung und -wartung 52
A. Sicherheit bei Entwicklungs- und Supportprozessen 52
B. Sicherheit in der Entwicklungsumgebung 54
C. Testdaten 54
11. Lieferantenbeziehungen 55
A. Ermittlung von Risiken im Zusammenhang mit externen Parteien 55
B. Informationssicherheitsvereinbarungen mit externen Parteien 55
12. Information Security Incident Management 56
A. Management von Security Incidents und Verbesserungen 56
13. Informationssicherheitsaspekte des betrieblichen Resilienz Managements 57
A. ADPs Programm zur betrieblichen Resilienz 57
B. Umsetzung der betrieblichen Resilienz 58
C. Verfügbarkeit von Einrichtungen für Disaster Revocery 59
14. Konformität 60
A. Einhaltung gesetzlicher Bestimmungen 60
B. Compliance mit Sicherheitsrichtlinien und -normen 60
C. Technische Compliance 60
D. Aufbewahrung von Daten 61
15. Anhang 62
A. Logisches Netzwerkdiagramm 62

Begriffsbestimmungen

Im gesamten Dokument können folgende Begriffe vorkommen:

Verwendeter Begriff oder Akronym	Definition
PTSS	**GSO's Preventative Technical Security Solutions**
GETS	**Global Enterprise Technology & Solutions**
GSO	**Global Security Organization**
CAB	**Change Advisory Board**
DRP	**Disaster Recovery**
CIRC	**GSO's Critical Incident Response Center**
SIEM	**Security Information and Event Management**
IDS	**Intrusion Detection System**
DNS	**Domain Name System**
LDAP	**Lightweight Directory Access Protocol**
NTP	**Network Time Protocol**
SOC	**Service Organization Controls**
TPSI	**Trusted Platform Security Infrastructure**

Dokumentenhistorie

Version	Freigabedatum	Autor / Sponsor	Zusammenfassung Änderungen
1.0	Aug. 2013	ADP Global Security Organization	Originalausgabe
1.1	Jan. 2014	ADP Global Security Organization	Kleinere Aktualisierungen
1.2	Dez. 2014	ADP Global Security Organization	Aktualisierung LLC
1.3	Feb. 2015	Client Security Management Office	Überarbeitung nach ISO 27001:2013 zur Angleichung an EMEA
1.4	Januar 2016	ADP Global Security Organization / ADP Rechtsabteilung	Überarbeitung zur Angleichung an GES EMEA und MNC im gleichen Dokument
1.5	Juni 2017	Client Security Management Office	Kleinere Updates
1.6	September 2017	Client Security Management Office	DSGVO Updates Globalisierung des Dokuments
1.61	September 2017	Client Security Management Office	Kleinere Updates
1.7	März 2018	Client Security Management Office	Kleinere Updates
1.8	Oktober 2018	Client Security Management Office	Kleinere Updates

Überblick

ADP unterhält ein förmliches Informationssicherheitsprogramm mit administrativen, technischen und physischen Sicherheitsmaßnahmen, um die Sicherheit, Vertraulichkeit und Vollständigkeit von Kundendaten zu schützen. Dieses Programm ist sinnvoll konzipiert, um (i) die Sicherheit und Vertraulichkeit der Kundendaten zu schützen, (ii) Schutz vor erwarteten Bedrohungen oder Gefahren für die Sicherheit und Integrität der Daten zu bieten und (iii) gegen unbefugten Zugang zu oder unbefugte Nutzung von Informationen zu schützen.

Diese Unterlage enthält einen Überblick über die Informationssicherheitsmaßnahmen und -praktiken von ADP zum Zeitpunkt der Freigabe, für die sich ADP Änderungen vorbehält. Diese Anforderungen und Praktiken sind so angelegt, dass sie den Vorgaben der Datensicherheitsnormen der ISO/IEC 27001:2013 entsprechen. In jedem Abschnitt sind Bezugnahmen auf die entsprechenden Absätze der ISO 27001 in [*Kursivschrift*] enthalten.

ADP überarbeitet seine Sicherheitsrichtlinien und -normen in regelmäßigen Abständen. Wir wollen sicherstellen, dass das Sicherheitsprogramm effektiv und effizient läuft, damit alle uns von unseren Kunden und deren Mitarbeitern anvertrauten Daten effektiv und effizient geschützt werden.

1. Informationssicherheitsrichtlinie

A. Management der Informationssicherheit

ADP gewährleistet, dass ADP Mitarbeiter und entsprechende Dritte die Datensicherheit ordnungsgemäß handhaben und dass die in diesem Dokument beschriebenen Maßnahmen umgesetzt und eingehalten werden.

B. Unabhängigkeit der Informationssicherheitsfunktion

ADP setzt einen Chief Security Officer ein, der die Global Security Organization (GSO) von ADP überwacht und dem Chief Financial Officer (CFO), anstatt dem Chief Information Officer berichtet, was der GSO die notwendige Unabhängigkeit von der IT gewährt. Die GSO ist ein geschäftsbereichsübergreifendes Sicherheitsteam, das einen multidisziplinären Ansatz für die Bereiche Cyber- und Datensicherheit, betriebliches Risikomanagement, Kunden-sicherheitsmanagement, Mitarbeiterschutz und betriebliche Resilienz erarbeitet. Der Führungsstab der GSO unter Leitung unseres Chief Security Officers ist für die Handhabung der Sicherheitsrichtlinien, -verfahren und -vorgaben verantwortlich.

C. Formale Definition einer Informationssicherheitsrichtlinie

[5.1.1] Richtlinien zur Informationssicherheit

ADP hat förmliche Informationssicherheitsrichtlinien entwickelt und dokumentiert, in denen der von ADP genutzte Ansatz zur Handhabung der Informationssicherheit ausgeführt wird.
Die in diesen Richtlinien abgehandelten speziellen Bereiche sind unter anderem:

- **Richtlinie Sicherheits-, Risiko- und Datenschutzmanagement –** Thematisiert die Pflichten der Global Security Organization (GSO), des Chief Security Officer (CSO) und des Global Chief Privacy Officer (GCPO).
- **Globale Datenschutzrichtlinie -** Thematisiert Erhebung, Zugriff, Richtigkeit und Offenlegung von persönlichen Daten sowie die Datenschutzerklärung für Kunden.
- **Richtlinie zu den Pflichten für Mitarbeiter und Führungskräfte zum Thema Informationssicherheit –** Umfasst die Informationssicherheitsverantwortlichkeiten und -regelungen für Einstellungsverfahren aus sicherheitsrelevanter Hinsicht.
- **Richtlinie zur zulässigen Nutzung elektronischer Kommunikation und Datenschutz** – Erörtert die zulässige Nutzung, verschiedene elektronischen Kommunikationswege, Verschlüsselung sowie das Schlüsselmanagement.
- **Richtlinie zur Handhabung und Klassifizierung von Informationen –** Nennt Anforderungen an die Klassifizierung von ADP Informationen und legt Schutzregelungen fest.
- **Richtlinie zur physischen Sicherheit –** Untersucht die Sicherheit von ADP Einrichtungen und im Weiteren ebenso die Sicherheit der dort tätigen Mitarbeiter und Besucher.
- **Richtlinie zur Handhabung der Sicherheitsmaßnahmen –** Nennt Mindestregelungen für die Anwendung von Systempatches, die effektive Behandlung der Bedrohung durch Malware und sorgt für Backups und Befugniskontrollen bei Datenbanken.
- **Richtlinie Überwachung der Sicherheit –** Nennt Schutzvorkehrungen für Intrusion Detection Systems (IDS), Aufzeichnungen und für Data Loss Prevention (DLP).
- **Richtlinie für Ermittlungen, elektronische Entdeckung und Incident Management –** Hier sind abgedeckt: Reaktion auf Incidents, EDILS, Schutz der Arbeitnehmer, Zugang zu elektronisch gespeicherten Mitarbeiterdaten.
- **Zugangs- und Authentifizierungsrichtlinie –** Deckt die Themen Authentifizierung (z.B. Benutzer-ID und Passwort), Fernzugriff und Drahtloszugriff ab.
- **Richtlinie zur Netzwerksicherheit –** Sicherheitsarchitektur für Router, Firewalls, AD, DNS, E-Mail-Server, DMZ, Cloud Services, Netzgeräte, Web Proxy und geschaltete Netzwerke.
- **Richtlinie globale Lieferantensicherung –** Sieht Mindestsicherheitsvorkehrungen für die Einsetzung Dritter vor, die ADP bei der Erreichung der Geschäftsziele unterstützen.

- **Richtlinie Anwendungsmanagement –** Setzt angemessene Sicherheitsvorkehrungen in jeder Phase des Systementwicklungszyklus ein.
- **Richtlinie zur betrieblichen Resilienz –** Stellt den Schutz und die Integrität von ADP durch Anlegen von Mindestanforderungen für Dokumentation, Umsetzung, Unterhalt und fortlaufende Verbesserung von Programmen zur betrieblichen Resilienz sicher.
- **Richtlinie betriebliches Risikomanagement –** Identifizierung, Überwachung, Reaktion, Analyse, Lenkung und neue Geschäftsinitiativen.

Die Richtlinien werden im Mitarbeiterportal veröffentlicht und sind allen Mitarbeitern sowie Vertragsnehmern innerhalb des ADP Netzwerks zugänglich.

D. Überprüfung der Informationssicherheitsrichtlinie

[5.1.2] Überprüfung der Richtlinien zur Informationssicherheit

ADP überprüft seine Informationssicherheitsrichtlinie mindestens einmal jährlich oder wenn erhebliche Änderungen mit Auswirkungen auf die Funktionalität der ADP Informationssysteme erfolgt sind.

2. Organisation der Informationssicherheit

A. Rollen und Pflichten im Rahmen der Informationssicherheit

[6.1.1] Rollen und Pflichten im Rahmen der Informationssicherheit

Die GSO von ADP besteht aus geschäftsbereichsübergreifenden Sicherheitsteams, die einen multidisziplinären Ansatz für die Einhaltung der Normen im Bereich Cyber- und Datensicherheit, betriebliches Risikomanagement, Kundensicherheitsmanagement, Arbeitnehmerschutz und betrieblichen Resilienz nutzen. Die Rollen und Pflichten wurden förmlich und in Schriftform für alle Mitglieder der globalen Sicherheitsorganisation von ADP definiert. Die GSO ist beauftragt mit der Erstellung, Implementierung und Kontrolle unseres Informationssicherheitsprogrammes basierend auf Unternehmens Richtlinien, Die Aktivitäten der GSO werden durch ein Sicherheitskomitee überwacht, bestehend aus: Chief Security Officer, Chief Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Human Resources Officer und dem General Counsel.

B. Richtlinie mobile Computernutzung und Telearbeit

[6.2.1] Richtlinie mobile Geräte
[6.2.2] 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. Antivirensoftware mit aktualisierten Virensignaturdateien und Zweifaktorauthentifizierung über VPN sind ebenfalls erforderlich, um aus der Ferne auf das Firmennetz zuzugreifen. Alle Remotegeräte müssen passwortgeschützt sein.

ADP-Mitarbeiter müssen verlorene oder gestohlene Remotegeräte umgehend über einen Meldeprozess für sicherheitsrelevante Zwischenfälle melden.

Als Bedingung für eine Anstellung/Zusammenarbeit mit ADP müssen alle Mitarbeiter und Auftragnehmer die Richtlinien von ADP für die zulässige Nutzung und andere relevante Richtlinien einhalten.

3. Sicherheit im Personalwesen

A. Hintergrundprüfungen

[7.1.1] Screening

Im Einklang mit den im individuellen Jurisdiktionsbereich geltenden gesetzlichen Vorgaben führt ADP angemessene Hintergrundprüfungen aus, welche im Verhältnis zu den Pflichten und Verantwortlichkeiten des Mitarbeiters, Auftragnehmers und/oder Dritter stehen, um deren Eignung zur Handhabung von Kundendaten vor einer Einstellung oder Beauftragung zu prüfen.

Zur Hintergrundprüfung können folgende Punkte gehören:

a) Prüfung der Identität/Arbeitserlaubnis
b) Beschäftigungshistorie
c) Bildungshistorie und berufliche Qualifikationen
d) Strafregisterauszug (wo gesetzlich zulässig und je nach örtlichen Landesbestimmungen)

B. Vertraulichkeitsvereinbarungen mit Mitarbeitern und Auftragnehmern

[7.1.2] Arbeits- und Beschäftigungsbedingungen

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 Auftragnehmer von ADP sind zur Wahrung der Vertraulichkeit verpflichtet.

C. Schulungsprogramm zur Informationssicherheit

[7.2.2] Sensibilisierung für die Informationssicherheit, Schulung

ADP gewährleistet, dass sämtliches Personal mit Zugriff auf und/oder bei der Verarbeitung von Kundendaten von ADP, eine Sensibilisierungsschulung zum Thema Sicherheit und Datenschutz durchläuft, um so effektive Datenschutz- und Sicherheitspraktiken zu fördern.

Alle Mitarbeiter durchlaufen in ihrem Einarbeitungsprogramm die Schulung zur Informationssicherheit. Zudem hält ADP jährlich Sicherheitsschulungen ab, um die Mitarbeiter für die Verantwortung im Arbeitsalltag zu sensibilisieren.

D. Sensibilisierung der Mitarbeiter und Auftragnehmer für das Thema Sicherheit

[7.2.2] Sensibilisierung für die Informationssicherheit, Schulung

Das Dokument zur ADP Informationssicherheitspolitik ist vom Management genehmigt, veröffentlicht und an alle Mitarbeiter und am Unternehmensstandort tätige Auftragnehmer und entsprechende Dritten kommuniziert.

Es ist erforderlich, dass ADP Mitarbeiter und am Unternehmensstandort tätige Auftragnehmer die Anforderungen der Informationssicherheit und zugehörige Richtlinien einhalten.

E. Mitarbeiterpflichten und Disziplinarwesen

[7.2.3] Disziplinarwesen

ADP hat eine Sicherheitspolitik veröffentlicht, die von allen ADP Mitarbeitern einzuhalten ist. Verstöße gegen Sicherheitsrichtlinien können zu dem Entzug von Zugangsrechten und/oder Disziplinarmaßnahmen bis hin zur Beendigung von Beraterverträgen oder Arbeitsverträgen führen.

F. Pflichten bei Beendigung des Arbeitsverhältnisses

[7.3.1] Pflichten bei Beendigung oder Änderung des Arbeitsverhältnisses
[8.1.4] Hardwarerückgabe
[9.2.6] Entzug oder Anpassung von Zugangsrechten

Die sich bei Beendigung des Arbeitsverhältnisses ergebenden Pflichten wurden förmlich dokumentiert und umfassen mindestens:

a) Die Rückgabe der noch beim jeweiligen Mitarbeiter befindlichen Geräte und aller ADP-Daten (unabhängig davon, auf welchem Medium diese gespeichert sind)
b) Entzug der Zugangsrechte zu ADP Einrichtungen, Daten und Systemen
c) Passwortänderung für weiter genutzte gemeinsame Benutzerkonten (sofern zutreffend)
d) Wissenstransfer (sofern zutreffend)

Die Zugriffsrechte aller ADP-Mitarbeiter und -Auftragnehmer auf Daten und Datenverarbeitungsanlagen werden bei Beendigung ihres Vertrages mit ADP entzogen.

4. Geräteverwaltung

A. Zulässige Nutzung von Assets

[8.1.3] Zulässige Nutzung von Assets

Die zulässige Nutzung von Assets wird in einer Reihe von Richtlinien ausgeführt. Sie betrifft ADP-Mitarbeiter und -Auftragnehmer und gewährleistet, dass Daten von ADP und seinen Kunden nicht durch die Verwendung dieser Assets gefährdet werden. Beispiele für in diesen Richtlinien genannte Bereiche sind: Einsatz der elektronischen Kommunikation, Nutzung elektronischer Geräte und Nutzung der Informationsressourcen.

B. Klassifizierung von Informationen

[8.2.1] Klassifizierung von Informationen

Die von oder im Namen von ADP erhobenen, erstellten oder verwalteten Daten werden wie jeweils angemessen in folgende Sicherheitsklassen eingestuft:

- Public
- ADP Internal Use Only
- ADP Confidential
- ADP Restricted

Die Anforderungen in Bezug auf die Handhabung der Daten stehen im direkten Zusammenhang mit der für die Daten geltenden Sicherheitseinstufung.

Personenbezogene Daten und sensible personenbezogene Daten werden in jedem Fall als ADP-Vertraulich eingestuft.

Die Mitarbeiter von ADP sind verantwortlich dafür, dass Informationswerte gemäß dem Grad der Sicherheitseinstufung geschützt und gehandhabt werden. Für jede dieser Klassifizierungsstufen ist festgelegt, wie die Datensicherheit und die Handhabung der Daten auf der jeweiligen Stufe zu erfolgen hat. Alle Kundendaten sind als vertrauliche Information eingestuft.

Die ADP-Vertraulichkeitseinstufung gilt für sämtliche gespeicherte, übermittelte oder durch Dritte gehandhabte Informationen.

C. Entsorgung von Geräten und Medien

[8.3.1] Verwaltung von Wechseldatenträgern
[8.3.2] Entsorgen von Medien

Werden bei ADP Geräte, Dokumente, Dateien und Medien entsorgt oder erneut verwendet, so werden geeignete Maßnahmen ergriffen, um eine Wiederherstellung der dort ursprünglich gespeicherten Kundendaten zu verhindern.

Unabhängig von der Sicherheitseinstufung werden alle auf Computern oder elektronischen Speichermedien enthaltene Daten überschrieben oder entmagnetisiert, außer das Medium wurde physisch zerstört bevor es außerhalb von ADP Einrichtungen gelangt.

Die Verfahren, mit denen sichergestellt wird, dass die auf Geräten, in Dokumenten, Dateien und Medien enthaltenen Daten sicher gelöscht/zerstört werden, sind formal dokumentiert.

D. Transport physischer Medien

[8.3.3] Transport physischer Medien

Es werden organisatorische Maßnahmen ergriffen, die gewährleisten, dass Ausdrucke mit Kundendaten nicht von unbefugten Personen eingesehen werden können.

Zudem werden Maßnahmen getroffen, die ausgedruckte Unterlagen mit Kundendaten vor Diebstahl, Verlust und/oder unbefugtem Zugriff / unbefugter Veränderung in folgenden Situationen schützen: (i) während des Transports durch z.B. versiegelten Umschlag, Behälter und persönlicher Übergabe an befugten Benutzer und (ii) während der Prüfung, Überarbeitung und bei anderen Verarbeitungsschritten, wenn die Unterlagen aus dem sicheren Speicher entfernt wurden.

5. Zugangskontrolle

A. Fachliche Anforderungen der Zugangskontrolle

[9.1.1] Richtlinie Zugangskontrolle

Die ADP Richtlinie zur Zugangskontrolle beruht auf den fachlich definierten Anforderungen. Die Richtlinien und Kontrollstandards werden in Zugangskontrollen umgesetzt, welche in allen Komponenten der bereitgestellten Services durchgesetzt werden. Sie basieren auf dem Konzept der geringsten Rechte und dem Prinzip des notwendigen Wissens (Least-Privilege und Need-to-Know).

B. Zugang zu Infrastruktur – Zugangskontrollmanagement

[9.2.1] Benutzerregistrierung und Löschung der Registrierung

[9.2.2] Bereitstellung des Benutzerzugangs

[9.2.5] Prüfung von Benutzerzugangsrechten

[9.4.3] Passwort-Verwaltungssystem

Zugangsanfragen für das Verschieben, Hinzufügen, Erstellen und Löschen von Daten werden protokolliert, genehmigt und regelmäßig geprüft.

Eine förmliche Prüfung erfolgt mindestens einmal pro Jahr, um sicherzustellen, dass einzelne Benutzer sich gemäß der entsprechenden Unternehmensrolle verhalten und der weitere Zugang nach einem Arbeitsplatzwechsel nicht mehr möglich ist. Dieser Prozess wird mithilfe eines Berichts entsprechend des Berichtsstandards SOC1[1] Typ II auditiert und dokumentiert.

Im Rahmen eines Identitätsmanagementsystems sorgt ein spezielles ADP-Team dafür, dass jeglicher Zugang zu Einrichtungen von ADP und seinen Informationssystemen entweder gewährt, verweigert, gelöscht, beendet, ausgesetzt oder deaktiviert wird.

Ein Administratorzugriff ist nur aus dem internen ADP-Netz oder einem gleichwertigen Netz über eine sichere Remote-VPN Verbindung mit Zweifaktorauthentifizierung möglich.

Für die UNIX-Domäne wird der Zugriff auf Konten, die nur mit Berechtigung zugänglich sind, nur auf dem Prinzip des notwendigen Wissens gewährt. Alle Zugangsanforderungen werden vom Sicherheitsteam validiert. Zudem wird ein Audit-Trail geführt.

Für die Windows-Domäne werden Benutzerkonten in einer zentralen Active Directory (AD) definiert. Die AD für Produktionsserver ist eine andere als die für Arbeitsplatzrechner verwendete.

ADP verwendet ein Tool für die zentrale Identitäts- und Zugangsverwaltung (IAM = identity and access management), das zentral von einem speziellen GETS Team verwaltet wird. Entsprechend der über das zentrale IAM-Tool angeforderten Zugangsrechte wird ein Workflow zur Validierung ausgelöst, bei dem ggf. der Vorgesetzte des Benutzers involviert wird. Der Zugang wird zeitlich begrenzt gewährt und die eingerichteten Workflows verhindern, dass solche Zugangsberechtigungen dauerhaft bestehen bleiben.

Der Zugang eines Mitarbeiters zu einer Einrichtung wird sofort nach dem letzten Tag des Beschäftigungsverhältnisses durch Deaktivieren der Zugangskarte (Mitarbeiterausweiskarte) ungültig gemacht. Die Benutzer-ID des Mitarbeiters wird sofort deaktiviert.

1 Im Falle bestimmter von ADP angebotener US-Dienste wird dies in einem SOC 2 Typ 2 Bericht geprüft.

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 Arbeitsplatzwechsel oder organisationsbezogenen Veränderungen werden Benutzerprofile oder Benutzerrechte umgehend durch die zuständige Leitung des jeweiligen Geschäftsbereichs und durch das IAM-Team geändert. Zudem wird alljährlich eine förmliche Prüfung der Zugangsrechte durchgeführt. Hier wird geprüft, ob die Rechte des einzelnen Benutzers auch seiner jeweiligen Rolle entsprechen und nach einem Wechsel des Aufgabengebiets keine Zugangsrechte verbleiben, die nicht mehr angemessen sind.

C. Passwort Richtlinie

[9.1.1] Richtlinie Zugangskontrolle

[9.4.2] Sichere Log-In Verfahren

[9.4.3] Passwort-Verwaltungssystem

Die ADP Passwort-Richtlinien werden in Servern, Datenbanken, Netzwerkgeräten und -anwendungen in dem von diesen Geräten/Anwendungen möglichen Maße umgesetzt. Die Komplexität des Passworts ergibt sich aus einer Risikobeurteilung für die geschützten Daten und Inhalte.
Die Richtlinien in Bezug auf die Sicherheit und Komplexität des Passworts entsprechen den vorherrschenden Branchennormen und sehen eine Mindestlänge von 8 Zeichen vor, wobei das Passwort aus einer Kombination von 1 oder mehr Zeichen aus mindestens 3 der folgenden 4 Klassen bestehen soll:

- Großbuchstaben (z.B. A, B, C ...Z)
- Kleinbuchstaben (z.B. a, b, c .... z)
- Ziffern (z.B. 0, 1, 2, ...9)
- Nicht alphanumerische Sonderzeichen (z.B., ?,!,%,$,#, usw.)

Zudem müssen Passwörter den folgenden Vorgaben entsprechen:

- Gemäß ADPs globaler Sicherheitsrichtlinien müssen Passwörter regelmäßig je nach der Sensibilität der Daten geändert werden, auf die sie über ihre zugehörigen Systeme Zugang gewähren.
- Passwörter werden mithilfe eines einmaligen Hashwerts unter Verwendung eines Salts gespeichert.
- Die Benutzer-ID darf nicht im Passwort enthalten sein
- Der Vor- und/oder Nachname des Benutzers darf nicht im Passwort verwendet werden
- Es dürfen maximal 4 gleiche Zeichen hintereinander im Passwort vorkommen
- Die letzten 4 Passwörter dürfen nicht verwendet werden
- Es gibt eine Liste verbotener Passwörter
- Passwörter können nur einmal pro Tag geändert werden
- Passwörter werden nach 90 Tagen ungültig
- Der Benutzer wird deaktiviert, wenn er 180 Tage lang nicht aktiv war
- Der Account wird nach 4 fehlgeschlagen Log-In-Versuchen gesperrt

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.

D. Zeitüberschreitung bei einer Sitzung

[A.9.4.1] Beschränkung des Informationszugangs

ADP setzt automatische Zeitüberschreitungen bei allen Servern, Arbeitsplatzrechnern, Anwendungen und VPN-Verbindungen durch.

- Server-Sitzung: Zeitüberschreitung nach 20 Minuten Inaktivität.
- Arbeitsplatzrechner-Sitzung: (Laptop, PC, Terminals usw.): Zeitüberschreitung nach 20 Minuten Inaktivität.
- Anwendungen: Bei allen Anwendungen gibt es eine Zeitüberschreitung nach einem Zeitraum der Inaktivität. Dieser variiert je nach Anwendung.
- VPN-Sitzung: Zeitüberschreitung nach 24 Stunden Nutzung.

Eine Wiederaufnahme der Sitzung erfolgt nur nach Eingabe eines gültigen Passworts durch den Benutzer.

6. Kryptographie

A. Kryptographische Sicherheitsmaßnahmen

[10.1.1] Richtlinie zur Nutzung kryptographischer Sicherheitsmaßnahmen

ADP fordert, dass sensible und zwischen ADP und Dritten ausgetauschte Daten verschlüsselt sein müssen (oder dass der Übermittlungskanal verschlüsselt sein muss). Hierbei sind branchenübliche Verschlüsselungstechniken und -stärken zu verwenden. Alternativ kann auch eine private Standleitung verwendet werden.

B. Schlüsselmanagement

[10.1.2] Schlüsselmanagement

Bei ADP gibt es einen internen Verschlüsselungs-Sicherheitsstandard, der ein klar definiertes Schlüsselmanagement und Schlüsselvereinbarungen umfasst, wobei das Management von symmetrischen als auch asymmetrischen Schlüsseln abgedeckt wird.

Die für ADP-Daten verwendeten kryptographischen Schlüssel sind immer als vertrauliche Information zu behandeln. Der Zugang zu solchen Schlüsseln ist strikt auf den Personenkreis begrenzt, der dieses Wissen benötigt und kryptographische Schlüssel werden - sofern keine Ausnahmegenehmigung erteilt wird - keinesfalls an Berater, Auftragnehmer, Mitarbeiter mit befristeten Arbeitsverträgen oder Dritte weitergegeben.

Für die Verschlüsselung werden Kopien der Serverzertifikate exportiert und gesichert. Zertifikate werden über einen VeriSign Global Server Account verwaltet.

7. Physische und umgebungsbezogene Sicherheit

A. Physische Sicherheit

[11.1.1] Physischer Sicherheitsumkreis

[11.1.3] Absicherung von Büros, Räumen und Einrichtungen

ADP stellt sicher, dass die für Lohn- und Gehaltsabrechnungen und Datenverarbeitung genutzten Einrichtungen physisch vom Rest der Einrichtung durch die Nutzung abgesicherter Zugangskontrollen und Wänden getrennt sind, welche vom Boden bis zur Decke reichen.

B. Maßnahmen für die physische Zugangskontrolle

[11.1.2] Physische Eingangskontrollen

ADP Einrichtungen

Für den Zugang zu Einrichtungen von ADP sind elektronische Sicherheitsausweise mit Karten-Schlüsselauthentifizierung erforderlich und es wird Protokoll über den physischen Zugang zu den Einrichtungen geführt.

Jeder Zugang einschließlich des Zugangs zu sensiblen Bereichen innerhalb der Einrichtungen von ADP wie z.B. Serverräume und Tape Libraries wird über elektronische Zutrittskontrollmechanismen (EAC) kontrolliert.

Datenzentren

Die Hosting Infrastrukturen von ADP befinden sich alle innerhalb physisch abgesicherter Umgebungen. Für den Zugang zu Hosting Zentren sind elektronische Sicherheitsausweise mit Karten-Schlüsselauthentifizierung und PIN oder biometrischer Authentifizierung erforderlich und es wird Protokoll über den physischen Zugang zu den Einrichtungen geführt.

C. Prüfung des Zugangs zu sensiblen Bereichen

[9.2.1] Benutzerregistrierung und Löschung der Registrierung

[11.1.2] Physische Eingangskontrollen

ADP Einrichtungen

Der Zugang zu Einrichtungen von ADP und zu sensiblen Bereichen ist auf ADP-Mitarbeiter und anderes befugtes Personal beschränkt. Der Zugang zu den Ressourcen der Einrichtung wird auf Grundlage der Arbeitspflichten einer jeden Person gewährt.
In allen Gebäuden und sensiblen Bereichen wird bei jedem Zugang und beim Verlassen ein Audit-Trail geführt. Audit-Trails werden geführt und angemessen überprüft.

Datenzentren

Der Sicherheitsbeauftragte des Datenzentrums und/oder Leiter der Einrichtung ist für die Handhabung der Zugangsrechte zu ADP Datenzentren verantwortlich. ADP ist für die Gewährung und Kontrolle des Zugangs zu ADP Bereichen nach einer vorab genehmigten Liste verantwortlich.

Bei jedem Zugang und Verlassen eines Datenzentrums wird ein Audit-Trail geführt. Die Audit-Trails werden monatlich von der Leitung des Hosting-Centers und dem Audit-Personal gepflegt und überprüft.

Um Zugang zu den Datenzentren zu erhalten, müssen sich alle Besucher vorher anmelden und nach Betreten der Einrichtung von autorisiertem Personal begleitet werden.

Das ADP Management prüft die Richtigkeit und Angemessenheit der physischen Zugangsrechte zu den ADP Datenzentren monatlich und für andere ADP-Einrichtungen mindestens auf jährlicher Basis. Die Zugangsrechte werden entzogen, wenn ein Mitarbeiter ADP verlässt.

D. Kennzeichnung von ADP Personal

[11.1.5] Arbeit in sicheren Bereichen

ADP Einrichtungen

Innerhalb der ADP-Einrichtungen müssen alle Mitarbeiter von ADP stets ihre Mitarbeiterausweise gut sichtbar tragen. Besucher müssen sich im Besucherverzeichnis eintragen, einen Besucherausweis tragen und werden von ADP-Mitarbeitern begleitet.

Datenzentren

Alle Mitarbeiter, Kunden, Auftragnehmer und Besucher von ADP müssen innerhalb der Datenzentren stets die für die Datenzentren geltenden Ausweise tragen. Kunden, Auftragnehmer und Besucher müssen von autorisiertem Personal begleitet werden.

Praktiken des unbefugten Zugangs, wie das gleichzeitige Eintreten mit oder hinter einem autorisierten Ausweisinhaber oder der Versuch für einen Ausweisinhaber nicht freigegebene Bereiche zu betreten, sind verboten.

E. Physische und umgebungsgebundene Sicherheitsmaßnahmen in Datenzentren

[11.1.4] Schutz vor externen und umgebungsgebundenen Bedrohungen

Die ADP-Datenzentren werden mithilfe von umgebungsgebundenen Sicherheitsmaßnahmen, Überwachungskameras mit Bewegungsmelder und durch Wachschutzpersonal überwacht. Alle Einrichtungen verfügen über Alarmanlagen.

In den Datenzentren von ADP wurden physische und umgebungsgebundene Maßnahmen zum Schutz vor Standortbezogenen anzunehmenden Katastrophen wie Überschwemmungen und Brand ergriffen.

Die Datenzentren von ADP verfügen über einen Mindeststandard physischer und umgebungsgebundener Sicherheitsvorkehrungen:

a) Redundante HLK-Systeme (Heizung, Lüftung, Klimatechnik)
b) Temperatur-/Feuchteüberwachung
c) Lokale Alarme und Fernalarme (für Strom, Temperatur und Feuchtigkeit)
d) N+1 UPS
e) Redundante Stromversorgung
f) Automatisches Brandmeldesystem
g) Automatische Feuerlöscheinrichtung
h) Zusätzliche manuelle Feuerlöschvorrichtungen
i) Server befinden sich in geschützten Zonen

Kabel und Verdrahtungen zum oder von den Rechneranlagen und Endgeräten werden so geführt, dass Schäden möglichst gering ausfallen. Die Verkabelung für die Rechner wird in Kabelrinnen im Doppelboden oder in Kabelkanälen oberhalb der Hängedecke geführt. Zugang zu den Telefon-/Kabelschächten haben nur bestimmte Mitarbeiter des Hosting Zentrums sowie autorisiertes Support Personal. Die Anlagen werden ständig von Automatiksystemen überwacht. Alle Zwischenfälle werden täglich überwacht und Korrekturmaßnahmen wie Geräteaustausch erfolgen im Bedarfsfall. Für den Anlagentausch gelten ebenfalls angemessene Maßnahmen des Change Managements.

8. Betriebliche Sicherheitsmaßnahmen

A. Formalisierung der IT-Betriebsverfahren

[12.1.1] Dokumentierte Betriebsverfahren

GETS ist der ADP Bereich, der für IT Infrastrukturarbeiten und Wartung verantwortlich ist. GETS ist für die förmliche Führung und Dokumentierung der IT-Betriebsrichtlinien und -verfahren zuständig. Diese Verfahren beinhalten unter anderem:

a) Change Management
b) Sicherungsmanagement
c) Handhabung von Systemfehlern
d) System-Neustart und -wiederherstellung
e) Systemüberwachung
f) Aufgabenplanung und –überwachung

B. Change Management für die Infrastruktur

[12.1.2] Change Management

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.

C. Systemkapazitätsplanung und -zulassung

[12.1.3] Kapazitätsmanagement

Die Kapazitätsanforderungen werden fortlaufend überprüft und regelmäßig überarbeitet. Im Anschluss an diese Überarbeitungen werden die Systeme und Netzwerke je nach Erfordernis entweder erweitert oder verkleinert.

Sind erhebliche Änderungen aufgrund von Kapazitätsänderungen oder technischem Fortschritt notwendig, so kann das GETS Benchmarking Team Belastungsprüfungen der relevanten Anwendungen und/oder Systeme durchführen und so einen detaillierten Bericht zur Leistungsentwicklung durch Messung der Veränderungen bei den (i) Komponenten, (ii) der Systemkonfiguration oder -version oder (iii) der Middleware-Konfiguration oder -version erstellen.

D. Schutz vor bösartigem Code

[12.2.1] Maßnahmen gegen Malware

Auf sämtlichen mit dem ADP-Netzwerkverbundenen Computersystemen sind Antivirenprogramme installiert. Die Virensignaturen werden automatisch in gewissen Abständen je nach Aktualisierung durch den Herausgeber oder je nach Freigabeplan aktualisiert.

E. Richtlinie zum Sicherungsmanagement

[12.3.1] Datensicherung

Die geltenden ADP Richtlinien fordern, dass die Produktionsdaten aller produktionsbezogenen Hosting-Vorgänge gesichert werden müssen. Der Umfang und die Häufigkeit dieser Sicherungen richten sich nach den betrieblichen Anforderungen der jeweiligen ADP-Dienstleistungen, den Sicherheitsanforderungen der betroffenen Daten und der Kritikalität der Daten in Bezug auf Disaster Recovery.
Im Einklang mit diesen Vorgaben werden folgende Sicherungen durchgeführt:

a) Tägliche inkrementelle Datensicherung
b) Wöchentliche komplette Datensicherung
c) Monatliche komplette Datensicherung

Die Überwachung der turnusmäßigen Datensicherungen erfolgt durch GETS, um Probleme bei der Sicherung oder Ausnahmen zu identifizieren. Alle beobachteten Probleme oder abweichende Vorfälle lösen ein Ticket im Fallverwaltungssystem von ADP aus, welches dann bis zu seiner abschließenden Behebung nachverfolgt wird.

F. Sicherheitsprotokollierung und -überwachung

[12.4.1] Ereignisprotokollierung

[12.4.3] Administrator- und Bedienerprotokolle

ADP verfügt über eine zentrale Infrastruktur ausschließlich mit Lesezugriff (SIEM) und ein Protokoll-Korrelierungs- und Alarmierungssystem (TPSI). Protokollalarme werden zeitnah durch CIRC überwacht und bearbeitet.
Zu diesen Protokollen gehören, aber nicht limitiert auf:

- IDS
- Firewalls
- DNS
- LDAP
- Active Directory
- Betriebssystem
- Internet-Zugang
- SMTP Gateways

Diese Systeme sind über einen eindeutigen NTP-basierten Taktbezug synchronisiert.
Jedes einzelne Protokoll verfügt mindestens über:

- Zeitstempel
- Wer (nennt Bediener oder Administrator)
- Was (Angaben zum Vorfall)

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

- Befugter Zugang
- Privilegierte Aktivitäten
- Versuche unbefugten Zugangs
- Systemwarnungen oder -ausfall
- Änderungen an den Sicherheitseinstellungen des Systems, sofern das System eine derartige Protokollierung zulässt

Diese Protokolle sind nur befugtem Personal von ADP zugänglich und werden im Live-Modus gesendet, um eine Manipulation der Daten vor ihrer Speicherung in sicheren Protokollanwendungen zu verhindern.

G. Infrastruktursysteme und Überwachung

[12.4.1] Ereignisprotokollierung

ADP überwacht die Infrastruktur mithilfe entsprechender Maßnahmen 24 Stunden täglich, 7 Tage in der Woche. Störungswarnungen werden von verschiedenen Teams je nach Schweregrad und der zur Behebung erforderlichen Fähigkeiten gehandhabt.

Die ADP Hosting-Zentren nutzen Prüfanwendungen, die fortlaufend auf allen zugehörigen Datenverarbeitungssystemen und den Netzwerkgeräten laufen, damit das ADP Team proaktiv über aktuelle Probleme und Warnungen informiert wird. Diese Anwendungsfunktionen beinhalten unter anderem:

- Überwachung und Analyse des Webseitentraffics
- Überwachung von Netzwerkequipment
- Überwachung und Management der Internetleistung und -verfügbarkeit
- Überwachung der IDS Sensoren und Firewalls auf Eindringversuche

H. Technisches Schwachstellenmanagement

[12.6.1] Handhabung technischer Schwachstellen

Alle innerhalb der Hosting-Infrastruktur laufenden Rechner müssen über ein spezielles, sicherheitsverstärktes Betriebssystem (oder über einen sicheren Aufbau) verfügen. Gehostete Anwendungen nutzen für jeden Servertyp innerhalb unserer Infrastruktur eine sicherheitsverstärkte, genehmigte und genormte Bauart. Die vorkonfigurierte Installation von Betriebssystemen ist verboten, da es hierdurch zu Schwachstellen wie generische Systemkonten-Passwörtern kommen kann, die ein Infrastrukturrisiko ermöglichen würden. Diese Konfigurationen reduzieren die Exposition von gehosteten Computern, die unnötige Dienste ausführen, die Schwachstellen erzeugen könnten.

PTSS ist für die Verwaltung des gesamten Bewertungs- und Fehlerbehebungsprozesses verantwortlich. PTSS ist unabhängig und seine Pflichten sind von denen der anderen Teams getrennt, welche für die Beteiligung an den Prozess- und Anforderungsdiensten und für die Fehlerbehebungsmaßnahmen zuständig sind.

ADP verfügt über eine dokumentierte Vorgehensweise bei der Durchführung von Freigabebewertungen und regelmäßig stattfindender Gefährdungsbeurteilungen sowie für die Durchführung von Compliance-Prüfungen der internetseitigen webgestützten Anwendungen und ihrer zugehörigen Infrastrukturkomponenten, die mindestens 15 Primärkategorien von Prüfungen umfasst.

Die Bewertungsmethode basiert sowohl auf internen als auch branchenweit genutzten, bewährten Verfahren, u.a. auch Open Web Application Security Project (OWASP), SANS Institute und Web Application Security Consortium (WASC).

9. Kommunikationssicherheit

A. Management der Netzwerksicherheit

[13.1.1] Netzwerkkontrollelemente

[13.1.2] Sicherheit der Netzwerkdienste

ADP nutzt ein netzwerkgestütztes Intrusion Detection System, das den Verkehr auf Netzwerk-Infrastrukturebene (24 Stunden am Tag, 7 Tage die Woche) überwacht und verdächtige Aktivitäten oder potentielle Angriffe identifiziert.
ADP erlaubt Modemnutzung nur unter bestimmten und entsprechend gerechtfertigten Umständen und diese Nutzung ist ausschließlich auf Dial-Out Funktionalität beschränkt. Drahtlosnetze und Zugangspunkte müssen sicherheitstechnisch genehmigt werden und sind nur dann zulässig, wenn sie mit sichereren Protokollen konfiguriert werden.
ADP hat eine Richtlinie für das Netzmanagement und die zugehörigen Sicherheitsmaßnahmen festgelegt:

a) *Dokumentation und Autorisierung von Änderungen der Sicherheitsparameter*: Anforderungen für Änderungen von Sicherheitsparametern (wie Regelungen für Firewalls) werden vom Netzkompetenzzentrum vor Anwendung in der Produktionsumgebung dokumentiert, qualifiziert und autorisiert.

b) Firewall-Einrichtungen und DMZ Schutz: Die Zugangspunkte zum ADP-Netz sind durch Firewall-Einrichtungen und Demilitarized Zones (DMZ) gesichert.

c) Trennung von Netzwerksegmenten: Produktionsnetzwerksegmente sind logisch vom Endnutzer-Netzwerk und von Umgebungen anderer Sicherheitsstufen getrennt.

d) Relay-Server: Der Zugriff auf Systeme (Netzwerkkomponenten, Anwendungs- und Datenbankserver) ist nur über autorisierte Relay-Server oder Authentifizierung in der DMZ zulässig.

e) Sicherheit bei der Datenübermittlung zwischen ADP Datenzentrum / Infrastruktur und den Kunden: Externe Datenübermittlungen zwischen den ADP Datenzentren und den Kunden von ADP sind über eine der folgenden Netze abgesichert: private Standleitung, IPSec VPN, MPLS-VPN. Zum Schutz der Daten, die Kunden an die ADP-Datenzentren übermitteln, nutzen Webanwendungen die von ADP genehmigten Verschlüsselungstechniken.

Zudem hat das GETS Netzwerkkompetenzzentrum ein Firewall-Compliance Tool eingesetzt. Firewall Ströme unterliegen vor ihrer Umsetzung ebenfalls dem Change Management Prozess.

B. Austausch von Informationen

[13.2.1] Richtlinien und Verfahren für die Informationsübermittlung

ADP setzt geeignete Schutzmaßnahmen ein, damit die Übermittlung von ADPs Kundendaten an Dritte nur zwischen autorisierten Informationssystemen und -ressourcen und nur mithilfe der sicheren und autorisierten Transfermechanismen von ADP erfolgt.

C. Verwendung eines Nachrichtensystems

[13.2.3] Elektronisches Nachrichtensystem

ADP verbietet die Nutzung von nicht gesicherten externen Nachrichtenanwendungen für die Übermittlung von Kundendaten.

10. Systembeschaffung, -entwicklung und -wartung

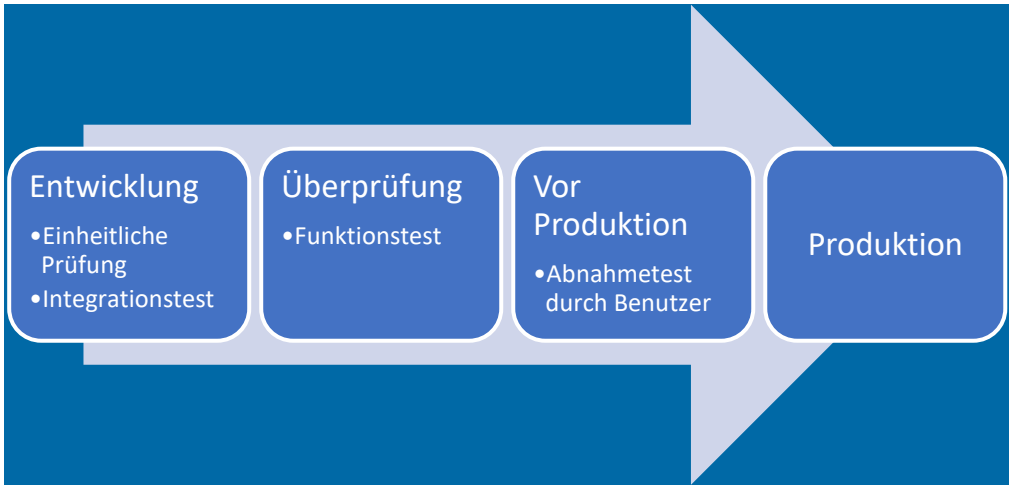
A. Sicherheit bei Entwicklungs- und Supportprozessen

[14.1.1] Analyse und Spezifikation der Anforderungen für die Informationssicherheit

[14.2.1] Richtlinie für die sichere Entwicklung

[14.2.2] Kontrollverfahren für Systemänderungen

Im Laufe des Entwicklungszyklus wird eine entsprechende Dokumentation angelegt und für die Prüfphase werden Prüfpläne erstellt. Für jede Umgebung werden unterschiedliche Phasen definiert mit entsprechender Freigabe in jeder dieser Phasen:



- Von der Prüfung bis hin zur Vorproduktionsumgebung ist die Freigabe durch das ADP Qualitätsteam erforderlich.
- Von der Vorproduktion bis zur Produktion ist die Freigabe der Abteilung IT Betrieb erforderlich.

Entwickler Teams sind dazu verpflichtet sichere Programmiermethoden zu verwenden. Die Anwendungsänderungen werden in den Entwicklungs- und Regressionsumgebungen getestet, bevor sie in den Produktionssystemen genutzt werden. Die Prüfungen werden durchgeführt und dokumentiert. Nach Freigabe werden die Änderungen dann in der Produktionsumgebung eingesetzt. Nach erheblichen Veränderungen werden Penetration Tests 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 IT Betriebsteam von ADP gibt die finale Freigabe vor jeder Hochstufung von Softwarepaketen in die Produktionsumgebung.

B. Sicherheit in der Entwicklungsumgebung

[14.2.6] Sichere Entwicklungsumgebung

Alle Umgebungen sind logisch voneinander getrennt und voneinander unabhängig. Es ist in jeder Phase des Entwicklungsprozesses möglich, auf Softwarepakete zuzugreifen, allerdings ist dies den in der jeweiligen Phase involvierten Teams vorbehalten.

C. Testdaten

[14.3.1] Schutz der Testdaten

Gemäß der globalen Sicherheitsrichtlinie von ADP ist die Verwendung realer oder nicht bereinigter Daten bei der Entwicklung oder beim Testen unzulässig, sofern der Kunde dies nicht ausdrücklich wünscht und dies genehmigt hat.

11. Lieferantenbeziehungen

A. Ermittlung von Risiken im Zusammenhang mit externen Parteien

[15.1.1] Informationssicherheitsrichtlinie für Lieferantenbeziehungen

In regelmäßigen Abständen werden für Dritte, die Zugriff auf die Daten von ADP und/oder Kunden benötigen, Risikobeurteilungen durchgeführt, um festzustellen, ob diesen 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.

B. Informationssicherheitsvereinbarungen mit externen Parteien

[15.1.2] Berücksichtigung von Sicherheitsaspekten in Vereinbarungen mit Lieferanten

Um den Sicherheitsanforderungen von ADP zu entsprechen, enthalten alle Vereinbarungen von ADP mit externen Stellen angemessene Sicherheitsverpflichtungen.

12. Information Security Incident Management

A. Management von Security Incidents und Verbesserungen

[16.1.1] Pflichten und Verfahren

[16.1.4] Beurteilung von und Entscheidung über Information Security Events

ADP verfügt über eine dokumentierte Vorgehensweise zur raschen, konsistenten und effizienten Reaktion auf sicherheitsrelevante Incidents.
Bei Auftreten eines Incidents aktiviert ein spezielles ADP-Mitarbeiterteam einen formalen Plan zur Reaktion auf den Incident mit Berücksichtigung z.B. folgender Bereiche:

- Eskalationen entsprechend der Einstufung oder der Schwere des Incidents
- Kontaktliste für die Zwischenfallmeldung/-eskalation
- Richtlinien für erste Reaktionen und Nachverfolgung bei den betroffenen Kunden
- Einhaltung der jeweils im Bereich der Meldepflicht für Sicherheitsverletzungen geltenden Bestimmungen.
- Untersuchungsprotokoll
- Systemwiederherstellung
- Behebung des Problems, Meldung und Überprüfung
- Gewonnene Erkenntnisse

Die ADP Richtlinien legen in Bezug auf die Meldung von Security Incidents fest, was ein Security Incident ist, wie das Incident Management beschaffen ist und welches die Pflichten der Mitarbeiter sind. Alle Mitarbeiter und Auftragnehmer von ADP sind zur Einhaltung dieser Richtlinien verpflichtet.
ADP führt in regelmäßigen Abständen Schulungen für seine Mitarbeiter und Auftragnehmer durch, um das Bewusstsein für die Anforderungen in Bezug auf die Meldepflicht zu schärfen.

13. Informationssicherheitsaspekte des betrieblichen Resilienz Managements

A. ADPs Programm zur betrieblichen Resilienz

[17.1.1] Planung der Informationssicherheitskontinuität

Eine von ADP´s Prioritäten ist das Einrichten, Durchführen und Testen von umfassenden Programmen für die Wiederaufnahme des Betriebs und zur Krisenplanung. Diese Programme sollen bei teilweisen oder vollständigem Ausfall die zeitnahe und effektive Wiederherstellung von betriebskritischen ADP-Geschäftsfunktionen ermöglichen und verhindern, dass es zu längeren Störungen in Geschäftsbereichen von ADP oder des Kunden kommt.
Die Unternehmensleitung von ADP schützt den Geschäftsbetrieb von ADP vor Störungen. Sie stellt Folgendes sicher:

- Verständnis für die Vorteile und Ziele des Programms zur betrieblichen Resilienz und Nutzung eines proaktiven Ansatzes hierbei,
- Einführung von förmlichen Verfahren für die Handhabung von betrieblichen Störungen,
- Einbeziehung und Umsetzung der Anforderungen an die betriebliche Resilienz in Geschäftsaktivitäten,
- Die Konzepte und Kontrollmaßnahmen zur betrieblichen Resilienz werden von den Mitarbeitern, die für die Reaktion auf Zwischenfälle und betriebliche Störungen zuständig sind, verstanden.
- Die für die Wiederaufnahme der Geschäftstätigkeit notwendigen Ressourcen einschließlich Personal, Einrichtungen, technische Infrastruktur, Daten, externe Dienstleistungen und Lieferanten werden eingeschätzt und die entsprechend notwendigen Ressourcen werden dem Programm zur betrieblichen Resilienz zugeordnet.

Die ADP Organisation für betriebliche Resilienz hat auf der Grundlage der Managementrichtlinien die sich aus der betrieblichen Resilienz ergebenden Pflichten dokumentiert. Eine der Pflichten der ADP Organisation für betriebliche Resilienz ist die Verantwortung für:

- Die Umsetzung der Richtlinie zur betrieblichen Resilienz, der Normen, Praktiken und Leitlinien für die Organisation einschließlich der regelmäßigen Prüfung der entsprechenden Unterlagen,
- Die Einrichtung gemeinsamer Systeme für die Planungsdokumentation und für Melde-/Eskalationsverfahren,
- Die Umsetzung eines Programms zur betrieblichen Resilienz, einschließlich regelmäßiger Überprüfungen, Audits und Aktualisierungen der Dokumentation und der zugehörigen Verfahren,
- Das Festlegen von Messgrößen zur Messung und zum Nachweis der Effizienz und Ausgereiftheit des Programms,

Das ADP Programm zur betrieblichen Resilienz besteht aus drei Hauptkomponenten:

- Incident Management - es handhabt gravierende Incidents und sorgt dafür, dass diese sich nicht zu einer Krise ausweiten,
- Business Continuity - hierfür werden Protokolle entwickelt, die eine Wiederaufnahme der betrieblichen Abläufe gewährleisten,
- Disaster Recovery - hier werden Betriebsverfahren für Wiederherstellungsprozesse für die wichtigsten ADP Systeme erstellt und gepflegt

B. Umsetzung der betrieblichen Resilienz

[17.1.2] Umsetzung der Informationssicherheitskontinuität

[17.1.3] Überprüfen und Bewerten der Informationssicherheitskontinuität

Die drei Komponenten des ADP-Programms zur betrieblichen Resilienz – Incident Management, Business Continuity und Disaster Recovery - werden in mehreren Phasen eingesetzt:

- **Risk Threat Analysis (RTA)**
  Die Risk Threat Analysis dient der Bewertung von Bedrohungen, denen Standorte von ADP weltweit unterliegen, sowie der Einstufung dieses Risikos, damit jeder Einrichtung ein bestimmtes Risikoniveau zugewiesen werden kann. Sie ist in regelmäßigen Abständen zu überprüfen oder dann, wenn sich ein gravierender Zwischenfall ereignet hat.

- **Business Impact Analysis (BIA)**
  Eine formale Business Impact Analysis wird durchgeführt und regelmäßig überprüft, um die kritischen Betriebsabläufe zu identifizieren, die nach einer Betriebsunterbrechung wiederhergestellt werden müssen. Die Business Impact Analysis muss regelmäßig überprüft werden. Falls sich ein gravierender Zwischenfall ereignet oder eine Änderung einer kritischen Betriebsfunktion eintritt, so muss sie auch schon zu einem früheren Zeitpunkt überarbeitet werden. Die Business Impact Analysis arbeitet Folgendes heraus:

  - Kritische Betriebsfunktionen und -abläufe,
  - IT-Anwendungen, die die festgestellten kritischen Betriebsfunktionen unterstützen,
  - Wechselbeziehungen zwischen Prozessen, Anlagen, Infrastruktur und Ressourcen,
  - Recovery Time Objectives (RTO's) und Recovery Point Objectives (RPO's) für Betriebsabläufe und Daten;
  - Geschätzte mögliche Verluste aufgrund einer Betriebsunterbrechung.

- **Entwicklung des Incident Managements und der Business Continuity Pläne**
  Nach erfolgter RTA und BIA erfolgt eine Zusammenfassung der gesamten Information mit anschließender Erstellung der Incident Management Pläne und Business Continuity Pläne.

  ADP hat diese ineinandergreifenden Pläne und Ressourcen zur Stärkung des ADP Programms zur betrieblichen Resilienz geschaffen. Sie sollen die nachteiligen Auswirkungen einer Betriebsunterbrechung auf die Bereitstellung der Leistungen von ADP für Kunden und Dritte minimieren.

- **Tests und Übungen**
  Die Pläne zur betrieblichen Resilienz werden regelmäßig mithilfe einer Simulationsübung im Kreise des Krisenkomitees überprüft. Diese Übung beschränkt sich auf ein Basis-Szenario und eine theoretische Besprechung, auf das Testen der Fähigkeiten und Reaktionsmöglichkeiten des Komitees für Zwischenfallmanagement.

- **Pflege**
  Das gesamte Programm zur betrieblichen Resilienz wird mindestens einmal jährlich überprüft und überarbeitet - jedoch bei Bedarf auch häufiger, wenn personelle Änderungen erfolgt oder andere Umstände eingetreten sind. Zudem können eine Reihe von Komponenten regelmäßig Prüfungen unterzogen werden.

C. Verfügbarkeit von Einrichtungen für Disaster Revocery

[17.2.1] Verfügbarkeit von Datenverarbeitungseinrichtungen

[10.5] Datensicherung

Des Weiteren umfasst ein Standardbetriebsverfahren zur Disaster Recovery detaillierte Pläne (DRP) für die Wiederherstellung der betriebskritischen Systeme von ADP auf der Grundlage folgender Szenarien:

- Ausfall kritischer Anlagen im Hauptrechenzentrum
- Standortbezogener Notfall am Hauptrechenzentrum

Es erfolgt eine fortlaufende Synchronisierung der Daten von ADP zwischen dem Hauptrechenzentrum und dem Standort der Notfallwiederherstellung. Lokale Sicherungen werden ebenfalls im Hauptrechenzentrum aufbewahrt, um die Aufbewahrungsdauer und den Datenumfang zu steigern.
Die IT Abteilung prüft jährlich ihre Fähigkeit zur Wiederherstellung der IT-Plattformen und Kommunikationsmöglichkeiten, die zur Unterstützung der kritischen Betriebsfunktionen notwendig sind. Die Geschäftsbereiche definieren und validieren den DPR Testumfang in Zusammenarbeit mit GETS. Nach Festlegung und Validierung des DRP-Umfangs werden verschiedene Teams aus dem EDV-Bereich und den Geschäftsbereichen mit einbezogen.
Die Prüfverfahren für die Disaster Recovery decken die folgenden Bereiche ab:

- Dokument Disaster Revovery Plan: Technische Unterlage zur Aktivierung der DRP,
- Prüfen der Disaster Recovery: technische und funktionsbezogene Prüfunterlagen zur Validierung der DRP-Aktivierung,
- Testergebnisse der Disaster Recovery: Kurzbericht mit den Ergebnissen des DRP-Tests und den gewonnenen Erkenntnissen,
- Maßnahmen zur Verbesserung der Disaster Recovery: Post-Mortem-Analyse von Action Items und Plänen.

Die Leitlinien mit den vorbereitenden Maßnahmen und Kommunikationsplänen im Fall eines gravierende Zwischenfalls werden allen Mitarbeitern und relevanten externen Stellen zugänglich gemacht, damit eine Vorbereitung erfolgen kann. Dazu gehören:

- Interne und externe Kommunikationsleitlinien,
- Vorbereitungsrichtlinien und Vermeidungsmaßnahmen für Mitarbeiter,
- Simulation von geplanten und ungeplanten Gebäude-Evakuierungen - mit jährlicher Aktualisierung.

14. Konformität

A. Einhaltung gesetzlicher Bestimmungen

[18.1.1] Identifizierung der jeweils geltenden gesetzlichen Bestimmungen und Vertragsanforderungen

Die Datenschutz- und Sicherheitskontrollen sind so konzipiert, dass ADP als Auftragsverarbeiter die sich aus den Datenschutzgesetzen ergebenden Verpflichtungen in allen Ländern, in denen ADP seine Leistungen anbietet, einhalten können. Hierzu zählen auch die Verpflichtungen, die sich aus der Datenschutzrichtlinie 95/46/EK ergeben und der Europäischen Datenschutz Grundverordnung (DSGVO, Verordnung (EU) 2016/679) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

ADP behält sich das Recht vor, externe Datenverarbeiter und Unterauftragsnehmer für Verarbeitungs-, Hosting- und Speicherzwecke zu nutzen. ADP bleibt weiterhin verantwortlich für die Qualität der Leistungen und die Einhaltung der Bestimmungen des Datenschutz-/Datensicherheitsrechts durch Unterauftragsnehmer, sofern dieses auf Auftragsverarbeiter anwendbar ist. ADP ist verpflichtet mit seinen Kunden zusammen zu arbeiten, um ein angemessenes Transparenzlevel im Zusammenhang mit der Nutzung von Unterauftragsnehmern zu schaffen.

Um die personenbezogenen Daten seiner Kunden (Kundeninformationen) bei jeder Verarbeitung zu schützen, hat ADP eine Richtlinie für den globalen Datenschutz umgesetzt, die die Grundlage für die Verarbeitung der Kundendaten weltweit darstellt. Diese globale Datenschutzrichtlinie fordert von jeder ADP Tochtergesellschaft und von allen ADP Mitarbeitern den Schutz der personenbezogenen Daten des Kunden und die ausschließliche Nutzung für die mit dem Kunden vertraglich vereinbarten Zwecke.

B. Compliance mit Sicherheitsrichtlinien und -normen

[18.2.1] Unabhängige Prüfung der Datensicherheit

[18.2.3] Überprüfung der technischen Compliance

ADP führt regelmäßig ein SOC1[2] Typ II Audit in dem Umfang durch, welcher durch die Bedingungen der Vereinbarung bezeichnet ist. Diese Audits werden durch ein bekanntes, externes Auditunternehmen durchgeführt und die Auditberichte stehen den Kunden jährlich auf Anfrage zur Verfügung (sofern zutreffend).

C. Technische Compliance

[18.2.2] Einhaltung der Sicherheitsrichtlinien und –standards

Um zu gewährleisten, dass die technischen Vorgaben bewährte Verfahrensweisen berücksichtigen, führt ADP in regelmäßigen Abständen planmäßige Überprüfungen auf Schwachstellen im Netz durch. Die Ergebnisse der Überprüfungen werden dann mit den Hosting-Teams und ihren Führungsgremien priorisiert und in Korrekturpläne umgesetzt.

Überprüfungen auf Schwachstellen in den Anwendungen erfolgen auf produktbezogenen Basis. Mithilfe spezieller Prüf-Tools für Anwendungen werden vorhandene Schwachstellen auf Anwendungsebene, wenn vorhanden, erkannt, den Produktentwicklungsmanagementteams bekanntgegeben und für Korrekturmaßnahmen in die Qualitätssicherungsprozesse einbezogen. Die Ergebnisse werden analysiert und es werden entsprechende Korrekturpläne entwickelt und priorisiert.

[2] Im Falle bestimmter von ADP angebotener US-Dienste wird dies in einem SOC 2 Typ 2 Bericht geprüft.

D. Aufbewahrung von Daten

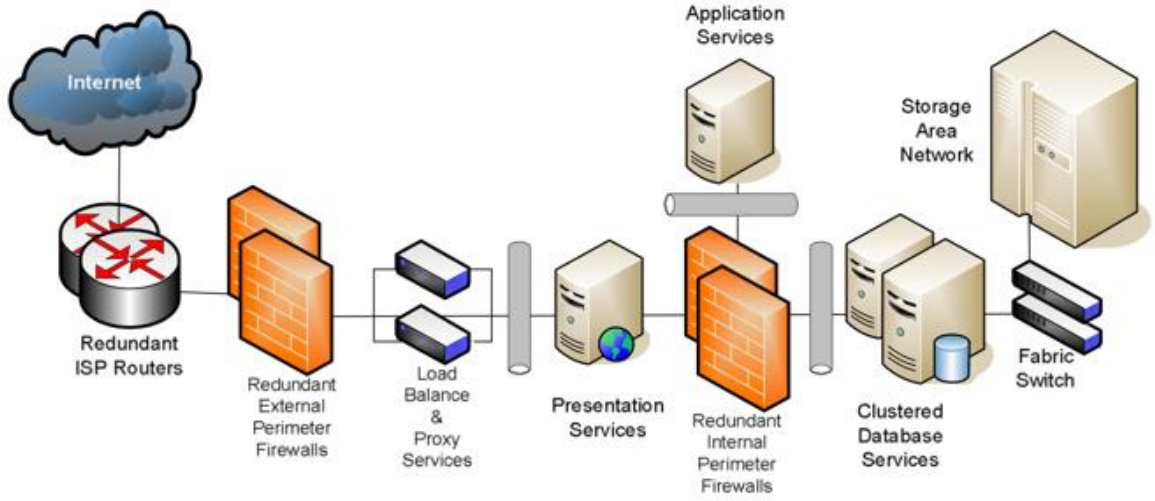
[18.1.3] Schutz der Datensätze

Die Richtlinien von ADP zur Aufbewahrung von Kundendaten entsprechen den geltenden gesetzlichen Bestimmungen.

Nach Ende des Kundenvertrages hält ADP seine vertraglichen Verpflichtungen in Bezug auf die Kundendaten ein, d.h. ADP wird sämtliche Kundendaten, die für die Fortführung der betrieblichen Aktivitäten des Kunden notwendig sind, entweder an den Kunden zurückgeben oder es dem Kunden ermöglichen, diese abzurufen (z.B. durch Datendownload), sofern dies nicht bereits zu einem früheren Zeitpunkt erfolgt ist. Anschließend zerstört ADP die verbleibenden Kundendaten auf sichere Art und Weise. Ausgenommen hiervon sind solche Datenumfänge, die vom Gesetz vorgegeben, vom Kunden genehmigt oder für die Beilegung von Streitigkeiten erforderlich sind.

15. Anhang

A. Logisches Netzwerkdiagramm



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 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 Gestion des Paiements 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 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, LLC	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
Business Management Software Limited	2 Peterborough Business Park, Lynch Wood, Peterborough, Cambridgeshire, PE2 6FZ
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