Codice di riservatezza di ADP relativo ai servizi di trattamento dei dati dei clienti

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Codice di riservatezza di ADP quanto ai servizi di trattamento dei dati dei clienti

Introduzione

ADP offre ai propri clienti una vasta gamma di servizi di gestione delle risorse umane. ADP si impegna a proteggere i dati personali nel **codice di condotta ed etica aziendale di ADP.**

Il presente codice di riservatezza di ADP relativo ai servizi di trattamento dei dati dei clienti, indica in che modo questo impegno viene applicato al trattamento dei dati personali relativi ai dipendenti del cliente da parte di ADP, nell'ambito della fornitura di servizi ai clienti e delle attività di assistenza clienti. In questo contesto, i dati dei clienti vengono trattati da ADP, in qualità di responsabile del trattamento dei dati per conto dei propri clienti.

Per le regole applicabili al trattamento dei dati personali da parte di ADP in qualità di titolare del trattamento dei dati relativi agli individui con cui ADP ha una relazione commerciale (per esempio individui che rappresentano clienti, fornitori e partner commerciali di ADP, altri professionisti e consumatori) e ad altri individui i cui dati personali vengono trattati da ADP nel contesto delle sue attività commerciali, sempre in qualità di titolare del trattamento, fare riferimento al ***codice di riservatezza di ADP sui dati aziendali.***

Articolo 1 – Campo di applicazione, applicabilità e implementazione

Campo di applicazione – Applicabilità ai dati nell'SEE

1.1 Il presente codice disciplina il trattamento dei dati personali dei dipendenti del cliente da parte di ADP nel suo ruolo di responsabile del trattamento dei dati per i clienti nel corso della fornitura dei servizi ai clienti, laddove tali dati personali siano (a) soggetti alla legge applicabile dell'SEE (o erano soggetti alla legge applicabile dell'SEE precedentemente al trasferimento di tali dati personali a una società del Gruppo esternamente all'SEE in un Paese in cui le istituzioni competenti dell'SEE ritengono che non venga fornito un livello adeguato di protezione dei dati); e (b) trattati in conformità ad un contratto di servizi che preveda specificatamente che il presente codice venga applicato a tali dati personali.

In caso di domande sull'applicabilità del presente codice, il sorvegliante della riservatezza pertinente dovrà chiedere il parere del team globale di riservatezza e governance dei dati prima che il trattamento abbia inizio.

Elaborazione elettronica e su supporto cartaceo

1.2 Il presente codice si applica al trattamento dei dati del cliente con mezzi elettronici e in sistemi di archiviazione cartacei sistematicamente accessibili.

Applicabilità della legge locale

1.3 Nessuna delle disposizioni contenute nel presente codice deve essere interpretata in modo da escludere qualsiasi diritto o rimedio che i dipendenti del

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

cliente potrebbero vantare ai sensi della legge applicabile. Laddove la legge applicabile fornisca una protezione maggiore rispetto al presente codice, si applicano le disposizioni pertinenti nell'ambito della legge applicabile. Laddove il presente codice fornisca una protezione maggiore rispetto alla legge applicabile o laddove fornisca garanzie, diritti o rimedi aggiuntivi per gli individui, si applicherà il presente codice.

Politiche e linee guida **1.4** ADP può integrare il presente codice attraverso politiche, standard, linee guida e istruzioni coerenti con il codice stesso.

Responsabilità **1.5** Il presente codice è vincolante per ADP. I dirigenti responsabili avranno la responsabilità di garantire il rispetto del presente codice da parte delle rispettive organizzazioni aziendali. Il personale di ADP deve rispettare il presente codice.

Data di entrata in vigore **1.6** Il presente codice è stato approvato dal Consiglio generale, dietro presentazione da parte del responsabile globale della protezione della riservatezza ed è stato adottato dal comitato esecutivo di ADP. Il codice entrerà in vigore a partire dall'11 aprile 2018 (**data di entrata in vigore**). Il codice (incluso un elenco delle società del Gruppo coinvolte nell'elaborazione dei dati del cliente) sarà pubblicato sul sito www.adp.com. Sarà inoltre messo a disposizione degli individui che ne faranno richiesta.

Il presente codice sarà implementato dal Gruppo ADP in base alle tempistiche specificate nell'articolo 16.

Politiche precedenti **1.7** Il presente codice integra le politiche sulla riservatezza di ADP e sostituisce le precedenti disposizioni, nella misura in cui quest'ultime sono in contraddizione con il presente codice.

Ruolo dell'entità delegata di ADP **1.8** Automatic Data Processing, Inc. ha affidato a ADP Nederland B.V., con sede legale all'indirizzo Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Paesi Bassi, in qualità di entità delegata ADP, il compito di far rispettare il presente codice all'interno del Gruppo ADP e ADP Nederland, B.V. ha accettato il suddetto incarico.

Articolo 2 - Contratto di servizi

Contratto di servizi, subincaricati **2.1** ADP tratterà i dati del cliente unicamente sulla base di un contratto di servizio che incorpora i requisiti contrattuali obbligatori per il responsabile del trattamento dei dati ai sensi della legge applicabile al responsabile del trattamento dei dati e per gli scopi legittimi specificati nell'articolo 4.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

L'entità contraente di ADP utilizza nella regolare fornitura dei servizi ai clienti i subincaricati, sia subincaricati di ADP sia Terzi subincaricati. I contratti di servizi di ADP autorizzano l'uso di tali subincaricati, a condizione che l'entità contraente di ADP continui a essere responsabile nei confronti del cliente delle prestazioni dei subincaricati in conformità con i termini del contratto di servizio. Le disposizioni dell'articolo 7 disciplinano l'uso dei subincaricati.

Risoluzione del contratto di servizio

2.2 Al momento della cessazione dei servizi ai clienti, ADP deve adempiere ai propri obblighi nei confronti del cliente ai sensi del contratto di servizio con riferimento alla restituzione dei dati del cliente stesso, fornendogli i dati necessari per la continuità delle attività (sempre se i dati non sono stati precedentemente forniti o resi accessibili al cliente tramite le funzionalità del prodotto pertinente, come la possibilità di scaricare i dati del cliente).

Nel momento in cui gli obblighi di ADP ai sensi del contratto di servizio sono stati rispettati, ADP dovrà distruggere in modo sicuro le copie rimanenti dei dati del cliente e (su richiesta del cliente) certificare al cliente che ha proceduto alla distruzione. ADP può conservare una copia dei dati del cliente nella misura richiesta dalla legge applicabile, in base alle autorizzazioni del cliente o secondo necessità ai fini della risoluzione delle controversie. ADP non tratterà più i dati del cliente, salvo nella misura richiesta per gli scopi di cui sopra. Gli obblighi di riservatezza di ADP ai sensi del relativo contratto di servizi permarranno fino a quando ADP conserverà una copia di tali dati del cliente.

Verifica delle misure di risoluzione dei servizi

2.3 Entro 30 giorni dalla risoluzione del contratto di servizio (salvo se non diversamente richiesto da un'autorità di protezione dei dati competente), ADP, su richiesta del cliente o dell'autorità di protezione dei dati competente, accetterà che le sue strutture di trattamento siano sottoposte a verifica conformemente all'articolo 11.2 o 11.3 (a seconda dei casi) per verificare che ADP rispetti gli obblighi relativi alla risoluzione di cui all'articolo 2.2.

Articolo 3 - Obblighi di conformità

Istruzioni del cliente

3.1 ADP tratterà i dati del cliente per conto del cliente, solo in conformità con il contratto di servizio, nel rispetto di qualsiasi istruzione documentata ricevuta dal cliente o secondo necessità per conformarsi alla legge applicabile.

Conformità con la legge applicabile

3.2 ADP tratterà i dati del cliente in conformità con la legge applicabile al responsabile del trattamento dei dati.

ADP risponderà tempestivamente e in modo appropriato alle richieste di assistenza da parte del cliente, come richiesto dalla legge, per consentire al

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

cliente di adempiere ai propri obblighi ai sensi della legge applicabile al titolare del trattamento dei dati, in conformità con il contratto di servizio.

Non conformità, effetto negativo sostanziale

3.3 Se una società del gruppo viene a conoscenza del fatto che la legge applicabile al responsabile del trattamento dei dati di un Paese non SEE o qualsiasi modifica della legge applicabile al responsabile del trattamento dei dati di un Paese non SEE, o un'istruzione del cliente potrebbe avere un sostanziale effetto negativo sulla capacità di ADP di adempiere ai propri obblighi di cui all'articolo 3.1, 3.2 o 11.3, tale società del Gruppo dovrà tempestivamente informare l'entità delegata di ADP e il cliente coinvolto, nel qual caso il cliente avrà il diritto, ai sensi del presente codice, di sospendere temporaneamente il trasferimento dei dati del cliente ad ADP fino al momento in cui il trattamento non sarà adeguato a correggere la non conformità. Nel caso in cui tale adeguamento non sia possibile, il cliente avrà il diritto di interrompere questa parte del trattamento da parte di ADP, in conformità con i termini del contratto di servizio. Questi diritti e obblighi non si applicano quando le circostanze o l'eventuale modifica della legge applicabile al responsabile del trattamento dei dati deriva da requisiti obbligatori.

Richiesta di divulgazione dei dati del cliente

3.4 Se ADP riceve una richiesta di divulgazione dei dati del cliente da un'autorità giudiziaria o da un ente di sicurezza statale di un Paese non SEE (autorità), prima di tutto valuterà caso per caso se questa richiesta è legalmente valida e vincolante per ADP. Qualsiasi richiesta che non è legalmente valida e vincolante per ADP verrà respinta in conformità con la legge applicabile.

Fatto salvo il seguente paragrafo, ADP informerà tempestivamente il cliente, la principale autorità di protezione dei dati (DPA) e l'autorità di protezione dei dati (DPA) competente per il cliente ai sensi dell'articolo 11.3 circa le eventuali richieste dell'autorità legalmente valide e vincolanti per ADP e richiederà all'autorità di sospendere tali richieste per un periodo ragionevole al fine di consentire alla principale autorità di protezione dei dati (DPA) di emettere un parere sulla validità della divulgazione richiesta.

Se la sospensione dell'esecuzione e/o della notifica alla principale autorità di protezione dei dati (DPA) di una richiesta di divulgazione legalmente valida e vincolante è vietata, per esempio, ai sensi del diritto penale per preservare la riservatezza di un'indagine giudiziaria, ADP chiederà all'autorità di rinunciare a questo divieto e documenterà la presentazione di questa richiesta. ADP fornirà annualmente informazioni generali sul numero e sul tipo di richieste di divulgazione ricevute nel precedente periodo di 12 mesi dalle autorità alla principale autorità di protezione dei dati (DPA).

Il presente articolo non si applica alle richieste ricevute da ADP da parte delle autorità nel normale svolgimento delle sue attività come fornitore di servizi di gestione delle risorse umane (come decisioni giudiziarie per il pignoramento

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

delle retribuzioni), che ADP può continuare a fornire in conformità con la legge applicabile, il contratto di servizio e le istruzioni dei clienti.

Richieste da parte del cliente **3.5** ADP risponderà tempestivamente e in modo appropriato alle richieste dei clienti relative al trattamento dei dati del cliente in conformità con i termini del contratto di servizio.

Articolo 4 – Scopi del trattamento dei dati

Scopi commerciali legittimi **4.1** ADP tratterà i dati personali (comprese le categorie speciali di dati) relativi ai dipendenti del cliente secondo necessità: per fornire servizi ai clienti, per attività di assistenza clienti e per i seguenti scopi aggiuntivi:

(a) detenzione, archiviazione e altri processi necessari per garantire la business continuity e il disaster recovery, compreso il backup e l'archiviazione di copie dei dati personali;

(b) amministrazione e sicurezza del sistema e della rete, inclusi monitoraggio dell'infrastruttura, gestione delle identità e delle credenziali, verifica, autenticazione e controllo degli accessi;

(c) monitoraggio e altri controlli necessari per salvaguardare la sicurezza e l'integrità delle transazioni (per esempio transazioni finanziarie e attività di movimentazione di denaro), anche per "due diligence" (come la verifica dell'identità dell'individuo e dell'idoneità dell'individuo a ricevere prodotti o servizi, come la verifica dello stato occupazionale o dello stato dei conti);

(d) esecuzione di contratti e protezione di ADP, dei suoi associati e clienti, dei dipendenti dei clienti e del pubblico da furto, responsabilità legale, frode o abuso, incluse le seguenti azioni: (i) rilevare, indagare, prevenire e mitigare il danno da frodi finanziarie effettive o tentate, frodi relative all'identità e altre minacce contro beni finanziari e fisici, credenziali di accesso e sistemi di informazione; (ii) partecipare a iniziative di sicurezza informatica, antifrode e antiriciclaggio esterne e (iii) attività necessarie a tutelare gli interessi vitali degli individui, per esempio, informandoli di una minaccia alla sicurezza che è stata rilevata;

(e) esecuzione e gestione di processi aziendali interni di ADP che portano al trattamento accidentale dei dati del cliente per:

(1) revisione interna e rendicontazione consolidata;

(2) conformità legale, come archiviazioni, utilizzi e informazioni richiesti obbligatoriamente dalla legge applicabile;

(3) anonimizzazione dei dati e aggregazione di dati anonimizzati per la minimizzazione dei dati e l'analisi dei servizi;

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

(4) utilizzo di dati anonimizzati e aggregati, nella misura consentita dai clienti, per favorire l'analisi, la continuità e il miglioramento dei prodotti e dei servizi di ADP;

(5) agevolazione della governance aziendale, incluse fusioni, acquisizioni, cessioni e joint venture.

Articolo 5 - Requisiti di sicurezza

Sicurezza dei dati **5.1** ADP adotterà misure tecniche, fisiche e organizzative commercialmente ragionevoli e appropriate per proteggere i dati del cliente da uso improprio o distruzione, perdita, alterazione, divulgazione, acquisizione, accesso accidentale, illecito o non autorizzato durante il trattamento, che soddisfino i requisiti della legge applicabile dell'SEE o qualsiasi altro requisito più severo, come previsto dal contratto di servizi. ADP dovrà, in ogni caso, adottare le misure specificate nell'Allegato 2 del presente codice, le quali possono essere modificate da ADP, a condizione che tali modifiche non riducano in maniera sostanziale il livello di sicurezza fornito ai dati del cliente secondo l'Allegato 2.

Accesso ai dati e riservatezza **5.2** Il personale è autorizzato ad accedere ai dati del cliente solo nella misura necessaria per raggiungere gli scopi del trattamento dei dati applicabili ai sensi dell'articolo 4. ADP imporrà obblighi di riservatezza al personale che ha accesso ai dati del cliente.

Notifica di violazioni della sicurezza dei dati **5.3** ADP informerà il cliente circa una potenziale violazione della sicurezza dei dati senza indebito ritardo, in seguito all'accertamento di tale violazione, salvo che un funzionario giudiziario o un'autorità di vigilanza non ritenga che la notifica possa impedire un'indagine penale, pregiudicare la sicurezza nazionale o determinare una violazione di fiducia nel settore industriale pertinente. In questo caso, la notifica deve essere ritardata secondo le istruzioni di tale funzionario giudiziario o autorità di controllo. ADP risponderà tempestivamente alle richieste dei clienti relative a detta violazione della sicurezza dei dati.

Articolo 6 – Trasparenza nei confronti dei dipendenti del cliente

Altre richieste dei dipendenti del cliente **6.1** ADP informerà tempestivamente il cliente in merito a richieste o reclami pertinenti al trattamento da parte di ADP di dati personali che siano ricevuti direttamente dai dipendenti del cliente, senza rispondere a tali richieste o reclami, salvo diversamente previsto nel contratto di servizi o dalle istruzioni del cliente.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Se incaricata dal cliente di rispondere alle richieste e ai reclami dei dipendenti del cliente nel contratto di servizi, ADP garantisce che ai dipendenti del cliente siano fornite tutte le informazioni ragionevolmente richieste (come il punto di contatto e la procedura) affinché il dipendente del cliente sia in grado di presentare effettivamente la richiesta o il reclamo.

Le disposizioni del presente Articolo 6.1 non si applicano alle richieste che vengono gestite da ADP nel normale corso della fornitura di servizi ai clienti e delle attività di assistenza clienti.

Articolo 7 – Subincaricati

Contratti dei Terzi subincaricati del trattamento **7.1** I Terzi subincaricati del trattamento possono elaborare i dati del cliente unicamente in base a un contratto di subappalto. Il contratto di subappalto impone analoghi termini di trattamento, relativamente alla protezione dei dati in capo al Terzo subincaricato del trattamento, che non saranno meno protettivi di quelli imposti all'entità contraente di ADP dal contratto di servizi e dal presente codice.

Pubblicazione del riepilogo dei subincaricati **7.2** ADP pubblicherà un riepilogo delle categorie di subincaricati coinvolti nella fornitura dei servizi ai clienti pertinenti sul sito web ADP appropriato. Questo riepilogo deve essere tempestivamente aggiornato in caso di modifiche.

Notifica ai nuovi subincaricati e diritto di obiezione **7.3** ADP comunicherà al cliente qualsiasi nuovo subincaricato ingaggiato da ADP per l'effettuazione dei servizi ai clienti. Entro 30 giorni dalla ricezione di tale notifica, il cliente può opporsi al subincaricato inviando una comunicazione scritta ad ADP, specificando una serie di motivi oggettivi che giustifichino l'asserita incapacità di tale subincaricato di proteggere i dati del cliente in conformità con gli obblighi pertinenti previsti dal contratto del subincaricato, come indicato nell'Articolo 7.1. Nel caso in cui le parti non riescano a raggiungere una soluzione reciprocamente accettabile, ADP dovrà, a sua discrezione, astenersi dal consentire al subincaricato di accedere ai dati del cliente, o consentire al cliente di interrompere i servizi pertinenti in conformità con i termini del contratto di servizi.

Eccezione **7.4** Le disposizioni della presente Sezione 7 non si applicano nella misura in cui il cliente chieda ad ADP di consentire ad una propria terza parte di elaborare i suoi dati in base a un contratto che il cliente ha stipulato direttamente con la terza parte (per esempio un fornitore di prestazioni esterno).

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Articolo 8 – Supervisione e conformità

Responsabile globale della protezione della riservatezza

8.1 Il Gruppo ADP disporrà di un responsabile globale della protezione della riservatezza, che ha la responsabilità di:

(a) coordinare il consiglio per la leadership della riservatezza;

(b) supervisionare la conformità con il presente codice;

(c) supervisionare, coordinare, contattare e consultare i membri rilevanti della Network della riservatezza in materia di riservatezza e protezione dei dati;

(d) fornire al comitato esecutivo di ADP relazioni annuali sulla riservatezza pertinenti ai rischi di protezione dei dati e ai problemi di conformità;

(e) coordinare indagini o inchieste ufficiali sul trattamento dei dati del cliente da parte di un'autorità governativa, in collaborazione con i membri rilevanti del Network della riservatezza e l'ufficio legale di ADP;

(f) gestire i conflitti tra il presente codice e la legge applicabile;

(g) monitorare il processo attraverso cui vengono condotte le valutazioni dell'impatto sulla protezione dei dati (PIA) e riesaminare tali valutazioni in modo appropriato;

(h) monitorare la documentazione, notifica e comunicazione delle violazioni della sicurezza dei dati;

(i) offrire consulenza sui processi, i sistemi e gli strumenti di gestione dei dati per implementare il quadro normativo per la gestione della riservatezza e la protezione dei dati come stabilito dal consiglio per la leadership della riservatezza, tra cui:

(1) manutenere, aggiornare e pubblicare il presente codice nonché le politiche e gli standard pertinenti;

(2) offrire consulenza sugli strumenti per raccogliere, mantenere e aggiornare gli inventari contenenti informazioni sulla struttura e sul funzionamento di tutti i sistemi che elaborano i dati del cliente;

(3) fornire consulenza, assistenza o raccomandazioni sulla formazione in materia di riservatezza al personale, in modo che quest'ultimo comprenda e rispetti le proprie responsabilità ai sensi del presente codice;

(4) coordinarsi con il dipartimento di verifica interno di ADP e altri dipartimenti per sviluppare e mantenere un programma di garanzia appropriato per monitorare, verificare e dichiarare la conformità con il presente codice e per consentire ad ADP di verificare e certificare tale conformità secondo necessità;

(5) implementare le procedure necessarie per gestire richieste, dubbi e reclami sulla riservatezza e sulla protezione dei dati e

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

(6) offrire consulenza in merito a sanzioni appropriate per le violazioni del presente codice (per esempio norme disciplinari).

Rete della riservatezza

8.2 ADP deve istituire un network della riservatezza sufficiente per coordinare la conformità con il presente codice all'interno dell'organizzazione globale di ADP.

Il network della riservatezza creerà e manterrà un quadro di riferimento per supportare il responsabile globale della protezione della riservatezza e per intraprendere il controllo di quei compiti di cui all'articolo 8.1 e di altri compiti che potrebbero essere appropriati per gestire e aggiornare il presente codice. I membri della rete della riservatezza devono eseguire, in base al loro ruolo nella zona o nell'organizzazione, i seguenti compiti aggiuntivi:

(a) supervisionare l'implementazione di processi, sistemi e strumenti di gestione dei dati che consentano alle società del Gruppo di aderire al presente codice nelle rispettive zone o organizzazioni;

(b) supportare e valutare la gestione complessiva della riservatezza e della protezione dei dati nonché la conformità delle società del Gruppo all'interno delle rispettive zone;

(c) informare regolarmente i sorveglianti della riservatezza e il responsabile globale della protezione della riservatezza in merito ai rischi per la riservatezza e i problemi di conformità a livello regionale o locale;

(d) verificare che vengano mantenuti inventari adeguati dei sistemi che trattano i dati del cliente;

(e) essere disponibili a rispondere alle richieste di approvazione o consulenza sulla riservatezza;

(f) fornire le informazioni necessarie al responsabile globale della protezione della riservatezza per completare la relazione annuale sulla riservatezza;

(g) assistere il responsabile globale della protezione della riservatezza in caso di indagini ufficiali o richieste di informazioni da parte delle autorità governative;

(h) sviluppare e pubblicare politiche e standard sulla riservatezza che siano appropriati per le loro regioni o organizzazioni;

(i) consigliare le società del Gruppo sulla conservazione e sulla distruzione dei dati;

(j) informare il responsabile della riservatezza globale dei reclami e fornire assistenza nella risoluzione di tali reclami e

(k) assistere il responsabile globale della protezione della riservatezza, altri membri della rete della riservatezza, i sorveglianti della riservatezza e altri soggetti secondo necessità, al fine di:

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

(1) consentire alle società o organizzazioni del Gruppo di rispettare il codice, utilizzando le istruzioni, gli strumenti e i corsi di formazione che sono stati sviluppati;

(2) condividere le migliori pratiche per la gestione della riservatezza e la protezione dei dati all'interno della regione;

(3) confermare che i requisiti relativi alla riservatezza e alla protezione dei dati vengono presi in considerazione ogni volta che vengono implementati nuovi prodotti e servizi nelle società o organizzazioni del Gruppo e

(4) assistere i sorveglianti della riservatezza, le società del Gruppo, le business unit, le aree funzionali e il personale addetto all'approvvigionamento con l'utilizzo di terze parti e di subincaricati.

Sorveglianti della riservatezza

8.3 I sorveglianti della riservatezza sono dirigenti di ADP che sono stati nominati da un dirigente responsabile e/o dalla direzione esecutiva di ADP per implementare e far rispettare il codice all'interno di una specifica business unit o area funzionale di ADP. I sorveglianti della riservatezza sono responsabili dell'effettiva attuazione del codice all'interno della business unit o dell'area funzionale pertinente. In particolare, i sorveglianti della riservatezza devono verificare che i controlli sulla gestione della riservatezza e della protezione dei dati siano integrati in tutte le procedure aziendali che hanno un impatto sui dati dei clienti e che siano disponibili risorse e budget adeguati per soddisfare gli obblighi previsti dal presente codice. I sorveglianti della riservatezza possono delegare compiti e allocare risorse adeguate, secondo necessità, per far fronte alle loro responsabilità e conseguire gli obiettivi di conformità.

Le responsabilità dei sorveglianti della riservatezza includono:

(a) monitorare la gestione della riservatezza, della protezione dei dati e la conformità all'interno della rispettiva società del Gruppo, business unit o area funzionale e verificare che tutti i processi, i sistemi e gli strumenti ideati dal team globale di riservatezza e governance dei dati siano stati implementati in modo efficace;

(b) confermare che la gestione della riservatezza e della protezione dei dati e le attività di conformità siano delegate in modo appropriato nel normale corso dell'attività, nonché durante e dopo la ristrutturazione organizzativa, l'esternalizzazione ed eventuali fusioni, acquisizioni e cessioni;

(c) collaborare con il responsabile globale della protezione della riservatezza e i membri competenti della rete della riservatezza per comprendere e soddisfare eventuali nuovi requisiti legali e verificare che i processi di gestione della riservatezza e della protezione dei dati vengano aggiornati per far fronte a circostanze mutevoli e ai requisiti legali e normativi;

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

(d) consultarsi con il responsabile globale della protezione della riservatezza e con i membri competenti della rete della riservatezza in tutti i casi in cui vi è un conflitto reale o potenziale tra la legge applicabile e il presente codice;

(e) monitorare i subincaricati utilizzati dalla società del Gruppo, dalla business unit o dall'area funzionale per confermare l'attuale conformità dei subincaricati con il presente codice e i contratti dei subincaricati;

(f) confermare che tutto il personale della società del Gruppo, della business unit o dell'area funzionale ha completato i corsi di formazione sulla riservatezza previsti e

(g) ordinare la cancellazione, la distruzione, la anonimizzazione o il trasferimento dei dati clienti detenuti, come richiesto dall'articolo 2.2.

Dirigenti responsabili

8.4 I dirigenti responsabili, in qualità di direttori delle business unit o delle aree funzionali sono responsabili di garantire l'implementazione di un'efficace gestione della riservatezza e della protezione dei dati nelle rispettive organizzazioni. Ciascun dirigente responsabile dovrà (a) nominare adeguati sorveglianti della riservatezza, (b) garantire la disponibilità di risorse e budget adeguati ai fini della conformità e (c) fornire supporto al sorvegliante della riservatezza secondo necessità per risolvere le lacune in materia di conformità e gestione dei rischi.

Consiglio per la leadership della riservatezza

8.5 Il responsabile globale della protezione della riservatezza dovrà presiedere un consiglio della leadership della riservatezza composto dai sorveglianti della riservatezza, dai membri della rete della riservatezza selezionati dal responsabile globale della protezione della riservatezza e da altri soggetti che possono essere necessari per coadiuvare la missione del Consiglio. Il consiglio della leadership della riservatezza creerà e manterrà un quadro di riferimento per supportare i compiti che potrebbero essere appropriati affinché le società del Gruppo, le business unit e le aree funzionali possano conformarsi al presente codice, per intraprendere i compiti qui stabiliti e per supportare il responsabile globale della protezione della riservatezza.

Membri della rete della riservatezza e sorveglianti della riservatezza predefiniti

8.6 Se in qualsiasi momento non risultasse nominato un responsabile globale della protezione della riservatezza, oppure quest'ultimo non fosse in grado di svolgere le funzioni assegnate al ruolo, il Consiglio generale nominerà una persona che agirà in qualità di responsabile globale della protezione della riservatezza *ad interim*. Se in qualsiasi momento non vi fosse alcun membro del Network della riservatezza designato per una particolare regione o organizzazione, il responsabile globale della protezione della riservatezza si impegnerà a svolgere i compiti di tale membro della rete della riservatezza, come stabilito nell'articolo 8.2.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Se in qualsiasi momento non vi fosse alcun responsabile della riservatezza designato per una società del Gruppo, una business unit o un'area funzionale, il dirigente responsabile dovrà nominare una persona adeguata per svolgere i compiti di cui all'articolo 8.3.

Posizioni stabilite per legge **8.7** Laddove i membri del Network della riservatezza, per esempio, i responsabili della protezione dei dati ai sensi della legge applicabile dell'SEE mantengano le loro posizioni in conformità con la legge, dovranno adempiere alle proprie responsabilità lavorative nella misura in cui queste ultime non sono in conflitto con le loro posizioni stabilite per legge.

Articolo 9 – Politiche e procedure

Politiche e procedure **9.1** ADP svilupperà e implementerà politiche, standard, linee guida e procedure per conformarsi al presente codice.

Informazioni di sistema **9.2** ADP dovrà mantenere prontamente disponibili tutte le informazioni riguardanti la struttura e il funzionamento di tutti i sistemi e processi per il trattamento dei dati dei clienti, come gli inventari dei sistemi e dei processi che hanno un impatto sui dati dei clienti, insieme alle informazioni generate nel corso delle valutazioni dell'impatto sulla protezione dei dati. Una copia di queste informazioni sarà fornita alla principale autorità di protezione dei dati (DPA) o a un'autorità di protezione dei dati (DPA) competente per il cliente ai sensi dell'articolo 11.3, dietro specifica richiesta.

Articolo 10 – Formazione

Formazione **10.1** ADP deve fornire formazione sugli obblighi e principi stabiliti nel presente codice e altri obblighi in materia di riservatezza e sicurezza dei dati a tutto il personale che ha accesso ai dati clienti o responsabilità connesse al trattamento dei dati dei clienti.

Articolo 11 – Monitoraggio e verifica della conformità

Verifiche interne **11.1** ADP deve verificare regolarmente i processi e le procedure aziendali che contemplano il trattamento dei dati dei clienti per garantire la conformità al presente codice. In particolare:

(a) le verifiche possono essere eseguite nel corso delle normali attività di verifica interna di ADP (anche attraverso l'uso di terze parti indipendenti), di altri team interni impegnati in funzioni di garanzia e, su base ad hoc , su richiesta del responsabile globale della protezione della riservatezza;

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

(b) il responsabile globale della protezione della riservatezza può anche richiedere che una specifica verifica venga eseguita da un revisore esterno e informerà il dirigente responsabile della business unit e/o del comitato esecutivo di ADP, a seconda dei casi;

(c) durante la procedura di verifica, devono essere osservati gli standard professionali applicabili in materia di indipendenza, integrità e riservatezza;

(d) il responsabile globale della protezione della riservatezza e il membro competente della rete della riservatezza dovranno essere informati circa i risultati delle verifiche;

(e) nella misura in cui la verifica rivela la non conformità con il presente codice, tali risultati saranno trasmessi ai sorveglianti della riservatezza e ai dirigenti responsabili competenti. I sorveglianti della riservatezza collaboreranno con il team globale di riservatezza e governance dei dati per sviluppare ed attuare un piano di correzione appropriato.

(f) Una copia dei risultati della verifica relativa alla conformità sarà fornita alla principale autorità di protezione dei dati (DPA) o a un'autorità di protezione dei dati (DPA) competente ai sensi dell'articolo 11.3, dietro specifica richiesta.

Verifica su richiesta del cliente

11.2 ADP risponderà alle richieste di verifica avanzate dai clienti come descritto nel presente articolo 11.2. ADP risponderà alle domande poste dal cliente in merito al trattamento dei dati dei clienti da parte di ADP. Nel caso in cui il cliente ritenga ragionevolmente che le risposte fornite da ADP giustifichino ulteriori analisi, ADP, in accordo con il cliente, dovrà:

(a) mettere a disposizione le strutture che utilizza per il trattamento dei dati dei clienti per una verifica eseguita da un revisore indipendente qualificato esterno, ragionevolmente accettabile per ADP, vincolato da obblighi di riservatezza soddisfacenti per ADP e assunto dal cliente. Il cliente fornirà una copia del report di verifica al responsabile globale della protezione della riservatezza, che sarà trattato come materiale riservato da parte di ADP. Le verifiche devono essere effettuate non più di una volta all'anno, per ogni cliente, durante il periodo del contratto di servizio e durante il normale orario di lavoro e sono soggette a (i) una richiesta scritta presentata ad ADP almeno 45 giorni prima della data proposta per la verifica; (ii) a un dettagliato piano di audit scritto, revisionato e approvato dall'organizzazione della sicurezza di ADP e (iii) alle politiche di sicurezza in loco di ADP. Tali verifiche avranno luogo solo in presenza di un rappresentante dell'ufficio globale di sicurezza di ADP, del team globale di riservatezza e governance dei dati di ADP o della persona designata dal rappresentante competente. Le verifiche dovranno essere gestite in modo da non interrompere le attività di trattamento dati da parte di ADP o

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

da non compromettere la sicurezza e la riservatezza dei dati personali relativi ad altri clienti di ADP o

(b) ADP fornirà una dichiarazione al cliente, rilasciata da un revisore indipendente qualificato esterno, in cui si certifica che i processi aziendali e le procedure di ADP che comportano il trattamento dei dati dei clienti sono conformi al presente codice.

ADP può addebitare ai clienti una tariffa ragionevole per l'esecuzione di tale verifica.

Il presente articolo 11.2 integra o chiarisce i diritti di verifica che i clienti possono vantare ai sensi della legge applicabile e del contratto di servizio. In caso di contraddittorietà, prevarranno le disposizioni della legge applicabile e dei contratti di servizi.

Verifiche da parte delle autorità di protezione dei dati (DPA)

11.3 Qualsiasi autorità di protezione dei dati (DPA) di un Paese dell'SEE che ha la competenza di sottoporre a verifica un cliente di ADP sarà autorizzata a verificare il trasferimento dei dati rilevanti per garantire la conformità al presente codice, alle stesse condizioni applicabili a una verifica da parte di tale DPA sul cliente stesso ai sensi della legge applicabile sul titolare del trattamento dei dati.

Per agevolare queste verifiche:

(a) ADP e il cliente collaboreranno in buona fede per tentare di risolvere la richiesta, fornendo informazioni alla DPA, come i report di verifica di ADP e agevoleranno le discussioni tra la DPA e gli esperti in materia del cliente e di ADP, i quali possono riesaminare la sicurezza, la riservatezza e i controlli operativi in atto. Il cliente avrà accesso ai dati dei clienti in conformità con il contratto di servizio e potrà delegare tale accesso ai rappresentanti della DPA;

(b) Se le informazioni disponibili attraverso questi meccanismi sono insufficienti per conseguire gli obiettivi dichiarati dalla DPA, ADP fornirà alla DPA l'opportunità di comunicare con il revisore di ADP;

(c) Se ciò è ritenuto insufficiente, ADP fornirà alla DPA il diritto diretto di esaminare le strutture di trattamento dei dati di ADP utilizzate per trattare i dati dei clienti, con ragionevole preavviso, durante l'orario di lavoro e nel pieno rispetto della riservatezza delle informazioni ottenute e dei segreti commerciali di ADP. La DPA può accedere unicamente ai dati dei clienti appartenenti al cliente.

Il presente articolo 11.3 integra o chiarisce i diritti di verifica che le DPA possono vantare ai sensi della legge applicabile e dei contratti di servizi. In caso di contraddittorietà, prevarranno le disposizioni della legge applicabile.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Relazione annuale **11.4** Il responsabile globale della protezione della riservatezza redigerà una relazione annuale per il comitato esecutivo di ADP in merito alla conformità con il presente codice, ai requisiti di riservatezza, ai rischi di protezione dei dati e ad altre questioni pertinenti. Questa relazione rifletterà le informazioni fornite dalla rete della riservatezza e altre informazioni sugli sviluppi locali e su questioni specifiche all'interno delle società del Gruppo.

Attenuazione **11.5** ADP adotterà tutte le misure appropriate per affrontare eventuali casi di non conformità con il presente codice identificati durante le verifiche di conformità.

Articolo 12 – Questioni legali

Diritti dei dipendenti del cliente **12.1** Se ADP viola il codice in relazione ai dati personali di un dipendente del cliente coperti dal presente codice, tale dipendente del cliente può, in qualità di beneficiario terzo, applicare gli articoli 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 e 14.3 del presente codice applicabile ai responsabili del trattamento nei confronti dell'entità contraente di ADP.

Nella misura in cui il dipendente del cliente può far valere tali diritti nei confronti dell'entità contraente di ADP, quest'ultima non può rivendicare una violazione dei suoi obblighi da parte di un subincaricato per evitare la propria responsabilità, salvo nella misura in cui la difesa di un subincaricato non costituisca anche una difesa di ADP. Tuttavia, ADP può rivendicare qualsiasi difesa o diritto che sarebbe stato disponibile al cliente. ADP può anche rivendicare eventuali difese che ADP avrebbe potuto far valere nei confronti del cliente (per esempio una negligenza contributiva), nel difendersi contro la richiesta dell'individuo interessato.

Procedura di reclamo **12.2** I dipendenti del cliente possono presentare un reclamo scritto in relazione a qualsiasi rivendicazione che potrebbero vantare ai sensi dell'articolo 12.1, contattando il team globale di riservatezza e governance dei dati tramite posta o e-mail all'indirizzo indicato alla fine del presente codice. Il dipendente del cliente può anche presentare un reclamo o un ricorso alle autorità o ai tribunali in conformità con l'articolo 12.3 del presente codice.

Il team globale di riservatezza e governance dei dati è responsabile della gestione dei reclami. Ogni reclamo verrà assegnato a un membro del personale competente (all'interno del team globale di riservatezza e governance dei dati o all'interno dell'unità aziendale o dell'area funzionale pertinente). Il personale competente procederà a:

(a) confermare immediatamente la ricezione del reclamo;

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

(b) analizzare il reclamo e, se necessario, avviare un'indagine;

(c) se il reclamo è fondato, informare il sorvegliante della riservatezza competente e il membro competente della rete della riservatezza, in modo che possa essere messo a punto e seguito un piano correttivo e

(d) conservare i registri di tutti i reclami ricevuti, le risposte fornite e le azioni correttive adottate da ADP.

ADP farà tutto il possibile per risolvere tempestivamente i reclami, per fornire una risposta al dipendente del cliente entro quattro settimane dalla data in cui è stato presentato il reclamo. La risposta fornita sarà in forma scritta e sarà inviata al dipendente del cliente tramite i mezzi originariamente utilizzati da quest'ultimo per contattare ADP (per esempio tramite posta ordinaria o posta elettronica). La risposta delineerà le misure che ADP ha adottato per indagare sul reclamo e indicherà la decisione di ADP in merito a quali misure (se del caso) verranno prese in seguito al reclamo.

Nel caso in cui ADP non possa ragionevolmente completare l'indagine e la risposta entro quattro settimane, dovrà informare il dipendente del cliente entro quattro settimane dall'avvio dell'indagine e dovrà fornire una risposta entro le successive otto settimane.

Se la risposta al reclamo fornita da ADP non è soddisfacente per il dipendente del cliente (per esempio quando la richiesta viene respinta) o ADP non osserva le condizioni della procedura di reclamo definite nel presente articolo 12.2, il dipendente del cliente può presentare un reclamo o un ricorso alle autorità o ai tribunali conformemente all'articolo 12.3.

Giurisdizione per i reclami presentati dai dipendenti del cliente

12.3 I dipendenti del cliente sono incoraggiati a seguire innanzitutto la procedura di reclamo di cui all'articolo 12.2 del presente codice prima di presentare reclami o ricorsi alle autorità o ai tribunali competenti.

I dipendenti del cliente possono, a loro discrezione, presentare ricorso ai sensi dell'articolo 12.1 presentando un reclamo:
(i) alla DPA competente nel Paese della loro residenza abituale, nel luogo di lavoro o nel luogo in cui si è verificata la violazione, nei confronti dell'entità contraente di ADP o dell'entità delegata di ADP o
(ii) alla principale autorità di protezione dei dati (DPA) o ai tribunali dei Paesi Bassi, tuttavia, in tal caso, unicamente nei confronti dell'entità delegata di ADP.

I dipendenti del cliente possono, a loro discrezione, presentare ricorso ai sensi dell'articolo 12.1 presentando un reclamo:
(i) ai tribunali nel Paese di residenza abituale o nel Paese in cui ha avuto origine il trasferimento dei dati ai sensi del presente codice, nei confronti dell'entità contraente di ADP o dell'entità delegata di ADP o

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

(ii) alla principale autorità di protezione dei dati (DPA) o ai tribunali dei Paesi Bassi, tuttavia, in tal caso, unicamente nei confronti dell'entità delegata di ADP.

Le DPA e i tribunali applicheranno le proprie leggi sostanziali e procedurali alle controversie. La scelta fatta dal dipendente del cliente non pregiudicherà i diritti sostanziali o procedurali che le parti potrebbero vantare ai sensi della legge applicabile.

Diritti dei clienti

12.4 Il cliente può far valere il presente codice contro (i) l'entità contraente di ADP o (ii) l'entità delegata di ADP al cospetto della principale autorità di protezione dei dati (DPA) o dei tribunali dei Paesi Bassi, ma solo se l'entità contraente di ADP non è ubicata in un Paese dell'SEE. L'entità delegata di ADP dovrà garantire che vengano adottate misure adeguate per far gestire le violazioni del presente codice dall'entità contraente di ADP o da qualsiasi altra società del gruppo coinvolta.

L'entità contraente di ADP e l'entità delegata di ADP non possono rivendicare una violazione dei propri obblighi da parte di un'altra società del Gruppo o di un subincaricato per evitare le loro responsabilità, salvo nella misura in cui una difesa di tale società o subincaricato costituisca anche una difesa di ADP.

Rimedi disponibili, onere della prova per i dipendenti del cliente

12.5 Nel caso in cui un dipendente del cliente inoltri un reclamo ai sensi dell'articolo 12.1, il dipendente del cliente avrà diritto al risarcimento di eventuali danni nella misura prevista dalla legge applicabile dell'SEE.

Se i dipendenti del cliente richiedono un risarcimento dei danni ai sensi dell'articolo 12.1, spetterà ai dipendenti dei clienti dimostrare di aver subito un danno e di addurre prove fattuali a sostegno della plausibilità che il danno si è verificato a causa di una violazione del presente codice. Successivamente, l'entità contraente di ADP (o l'entità delegata di ADP, a seconda dei casi) avrà l'onere di dimostrare che i danni subiti dai dipendenti del cliente a causa di una violazione del presente codice non sono attribuibili alla società del Gruppo o al subincaricato interessato o di rivendicare altre forme di difesa applicabili.

Risarcimento del cliente

12.6 In caso di violazione del presente codice e in conformità con i termini del contratto di servizio, i clienti hanno diritto al risarcimento dei danni diretti in conformità alle disposizioni del contratto di servizi.

Assistenza reciproca

12.7 Tutte le società del Gruppo dovranno, secondo necessità, cooperare e offrire assistenza nella misura ragionevolmente possibile (a) nella gestione di una richiesta, un reclamo o un ricorso presentato da un cliente o da un dipendente del cliente o (b) nello svolgimento di un'indagine legale o di un'investigazione da parte di un'autorità governativa competente.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

La società del Gruppo che riceve una richiesta di informazioni ai sensi dell'articolo 6.1 o un reclamo o ricorso ai sensi dell'articolo 12.2 o 12.3, è responsabile della gestione di qualsiasi comunicazione con il cliente o con il dipendente del cliente in merito alla richiesta o al reclamo, salvo se non diversamente richiesto dalle circostanze o indicato dal team globale di riservatezza e governance dei dati.

Raccomandazioni e decisioni vincolanti della DPA

12.8 In buona fede, ADP collaborerà e farà tutto il possibile per seguire le raccomandazioni della principale autorità di protezione dei dati (DPA) e della DPA competente ai sensi dell'articolo 12.3 sull'interpretazione e sull'applicazione del presente codice. ADP si atterrà alle decisioni vincolanti delle DPA competenti.

Legge applicabile al presente codice

12.9 Il presente codice sarà disciplinato e dovrà essere interpretato in conformità alla legge olandese.

Articolo 13 – Sanzioni per non conformità

Non conformità

13.1 La mancata osservanza da parte del personale del presente codice può comportare l'adozione di misure disciplinari o contrattuali adeguate in conformità alla legge applicabile e alle politiche di ADP, fino alla risoluzione del rapporto di lavoro o del contratto.

Articolo 14 – Conflitti tra il presente codice e la legge applicabile al responsabile del trattamento dei dati

Conflitto tra il codice e la legge applicabile

14.1 Laddove esiste un conflitto tra la legge applicabile al responsabile del trattamento dei dati e il presente codice, il dirigente responsabile o il sorvegliante della riservatezza si consulteranno con il responsabile globale della protezione della riservatezza, i membri competenti della rete della riservatezza (a seconda dei casi) e l'ufficio legale della business unit per determinare come conformarsi al presente codice e come risolvere il conflitto nella misura ragionevolmente praticabile, tenendo conto dei requisiti legali applicabili ad ADP.

Nuovi requisiti legali in conflitto

14.2 I membri del dipartimento legale, i responsabili della sicurezza aziendale di ADP e i sorveglianti della riservatezza informeranno tempestivamente il team globale di riservatezza e governance dei dati di qualsiasi nuovo requisito legale di cui vengano a conoscenza che può interferire con la capacità di ADP di conformarsi al presente codice.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

I sorveglianti della riservatezza competenti, in consultazione con l'ufficio legale, informeranno tempestivamente i dirigenti responsabili di qualsiasi nuovo requisito legale che può interferire con la capacità di ADP di conformarsi al presente codice.

Segnalazione alla principale autorità di protezione dei dati (DPA)

14.3 Se ADP viene a conoscenza del fatto che la legge applicabile al responsabile del trattamento dei dati o qualsiasi modifica della legge applicabile al responsabile del trattamento dei dati può avere un sostanziale effetto negativo sulla capacità di ADP di rispettare gli obblighi di cui agli articoli 3.1, 3.2 o 11.3, lo segnalerà alla principale autorità di protezione dei dati (DPA).

Articolo 15 – Modifiche al presente codice

Approvazione delle modifiche

15.1 Qualsiasi modifica sostanziale al presente codice richiede la previa approvazione del responsabile globale della protezione della riservatezza e del Consiglio generale, nonché l'adozione da parte del comitato esecutivo di ADP, e dovrà essere successivamente comunicata alle società del Gruppo. Le modifiche immateriali al codice possono essere apportate previa approvazione del responsabile globale della protezione della riservatezza. L'entità delegata di ADP comunicherà alla principale autorità di protezione dei dati (DPA) le eventuali modifiche al presente codice su base annuale.

Laddove una modifica a il presente codice abbia un impatto significativo sulle condizioni di elaborazione dei servizi ai clienti, ADP informerà tempestivamente la principale autorità di protezione dei dati (DPA), includendo una breve spiegazione per motivare tale modifica e fornendo notifica di tale modifica al cliente. Entro 30 giorni dalla ricezione di tale comunicazione, il cliente può opporsi a tale modifica fornendo una comunicazione scritta ad ADP. Nel caso in cui le parti non riescano a raggiungere una soluzione reciprocamente accettabile, ADP dovrà adottare una soluzione alternativa per il trasferimento dei dati. Nel caso in cui non sia possibile implementare una soluzione di trasferimento dati alternativa, il cliente avrà il diritto, ai sensi del presente codice, di sospendere il trasferimento dei dati del cliente ad ADP. Nel caso in cui una sospensione dei trasferimenti di dati non sia possibile, ADP dovrà consentire al cliente di interrompere la fornitura dei servizi pertinenti in conformità ai termini del contratto di servizi.

Data di entrata in vigore delle modifiche

15.2 Qualsiasi modifica entrerà in vigore con effetto immediato in seguito alla sua approvazione conformemente all'articolo 15.1, alla sua pubblicazione sul sito www.adp.com e alla sua comunicazione ai clienti.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Versioni precedenti **15.3** Qualsiasi richiesta, reclamo o ricorso da parte di un dipendente del cliente che coinvolge il presente codice sarà giudicata rispetto alla versione del presente codice che è in vigore al momento in cui viene presentato la richiesta, il reclamo o il ricorso.

Articolo 16 – Periodi di implementazione e di transizione

Implementazione **16.1** L'implementazione del presente codice sarà supervisionata dai sorveglianti della riservatezza, con l'assistenza del team globale di riservatezza e governance dei dati. Fatte salve le eccezioni indicate di seguito, è previsto un periodo di transizione di diciotto mesi dalla data di entrata in vigore (come stabilito nell'articolo 1.6) per garantire la conformità al presente codice.

Di conseguenza, salvo se non diversamente specificato, entro un periodo di diciotto mesi dalla data di entrata in vigore, qualsiasi trattamento dei dati dei clienti sarà eseguito in conformità al presente codice e il codice sarà pienamente in vigore. Durante il periodo di transizione, il codice diventerà efficace per una società del Gruppo, non appena tale società del Gruppo avrà espletato i compiti necessari per la piena implementazione e tale società del Gruppo avrà fornito adeguata comunicazione al responsabile globale della protezione della riservatezza.

Nuove società del Gruppo **16.2** Qualsiasi entità che diventa una società del Gruppo dopo la data di entrata in vigore dovrà conformarsi al presente codice entro due anni da quando sarà diventata una società del Gruppo.

Entità cedute **16.3** Un'entità ceduta (o parti specifiche della stessa) può continuare a essere coperta dal presente codice in seguito alla cessione, per il periodo eventualmente richiesto da ADP per svincolarsi dal trattamento dei dati personali relativi a tale entità ceduta.

Periodo di transizione per gli accordi esistenti **16.4** Laddove esistano accordi con subincaricati o altre terze parti che siano condizionati dal presente codice, le disposizioni degli accordi in questione prevarranno fino a quando gli accordi non saranno rinnovati nel normale corso dell'attività, ma a condizione che tutti gli accordi esistenti vengano resi conformi al presente codice entro 18 mesi dalla data di entrata in vigore.

Recapiti

Team globale di riservatezza e governance dei dati di ADP:
privacy@adp.com

Entità delegata di ADP
ADP Nederland B.V.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Lylantse Baan 1, 2908
LG CAPELLE AAN DEN IJSSEL
PAESI BASSI

Interpretazioni

INTERPRETAZIONE DEL PRESENTE CODICE:

(i) Salvo se non diversamente richiesto dal contesto, tutti i riferimenti a un particolare articolo o allegato sono da considerarsi riferimenti a tale articolo o allegato del presente documento, così come modificato di volta in volta.

(ii) Le intestazioni sono incluse solo per praticità e non devono essere utilizzate per interpretare nessuna disposizione del presente codice.

(iii) Se viene fornita la definizione di una specifica parola o frase, tale definizione si applicherà anche alle varianti grammaticali della parola o frase.

(iv) Qualsiasi forma al maschile fa riferimento anche alla variante femminile.

(v) Le parole "include", "includono", "incluso", "inclusi" e tutte le parole successive devono essere interpretate, a titolo esemplificativo, in base alla generalità di qualsiasi parola o concetto precedente, e viceversa.

(vi) Il termine "scritto" fa riferimento a qualsiasi comunicazione documentata, atto scritto, contratto, registro elettronico, firma elettronica, copia facsimile o altro strumento giuridicamente valido e applicabile, indipendentemente dal formato.

(vii) Qualsiasi riferimento a un documento (incluso, a titolo esemplificativo, qualsiasi riferimento al presente codice) è un riferimento al documento in oggetto, così come modificato, rettificato, integrato o sostituito, salvo nella misura in cui sia proibito dal presente codice o dal documento di riferimento.

(viii) Gli eventuali riferimenti alla legge applicabile includono qualsiasi requisito normativo, raccomandazione settoriale e migliore pratica emessi dalle autorità di vigilanza nazionali o internazionali competenti o da altri organismi.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

ALLEGATO 1 – Definizioni BCR

ADP (il Gruppo ADP)	ADP (il Gruppo ADP) indica collettivamente Automatic Data Processing, Inc. (la controllante) e le società del Gruppo, inclusa ADP, Inc.
Archivio	Per ARCHIVIO si intende una raccolta di dati personali che non sono più necessari per raggiungere le finalità per cui i dati sono stati originariamente acquisiti o che non vengono più utilizzati per attività commerciali generali, ma vengono potenzialmente utilizzati solo per scopi storici, scientifici o statistici, per la risoluzione di controversie, per indagini o per scopi generali di archiviazione. L'accesso a un archivio è limitato agli amministratori di sistema e ad altri soggetti il cui lavoro richiede specificamente l'accesso all'archivio.
Associato	Per ASSOCATO si intende un richiedente, un attuale dipendente di ADP o un ex dipendente di ADP, ad eccezione di un collaboratore. NOTA: il codice di riservatezza di ADP per quanto ai luoghi di lavoro non si applica, pertanto, al trattamento dei dati personali dei collaboratori
Attività di assistenza clienti	Per ATTIVITÀ DI ASSISTENZA CLIENTI si intendono le attività di trattamento svolte da ADP a supporto della fornitura dei propri prodotti e servizi. Le attività di assistenza clienti possono includere, ad esempio, la formazione dei professionisti, la risposta a domande sui servizi, l'apertura e la risoluzione dei ticket di assistenza, la fornitura di informazioni su prodotti e servizi (inclusi aggiornamenti e avvisi di conformità), il controllo e il monitoraggio della qualità e le attività correlate che facilitano l'uso efficace dei prodotti e dei servizi di ADP.
Automatic Data Processing, Inc.	AUTOMATIC DATA PROCESSING, INC. è la controllante del gruppo ADP ed è una società di Delaware (Stati Uniti d'America) con sede in One ADP Boulevard, Roseland, New Jersey, 07068-1728, Stati Uniti d'America.
Autorità di protezione dei dati o DPA	Per AUTORITÀ DI PROTEZIONE DEI DATI o DPA si intende qualsiasi autorità di regolamentazione o di controllo che vigila sulla protezione dei dati o sulla riservatezza in un Paese in cui ha sede una società del Gruppo.
Categorie speciali di dati	Per CATEGORIE SPECIALI DI DATI si intendono i dati personali che rivelano origine razziale o etnica, opinioni politiche o adesione a partiti politici od organizzazioni simili, convinzioni religiose o filosofiche, appartenenza a organizzazioni professionali o sindacali, salute fisica o mentale, compresi opinione, disabilità, patrimonio genetico, dipendenze, vita sessuale, reati, casellario giudiziale o procedimenti relativi a comportamenti illeciti o criminali.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Cliente	CLIENTE indica qualsiasi terza parte che utilizza uno o più prodotti o servizi di ADP nel corso della propria attività.
Codice	CODICE indica (a seconda dei casi) il codice di riservatezza di ADP sui dati aziendali, il codice di riservatezza di ADP quanto ai luoghi di lavoro (interno ad ADP) e il codice di riservatezza di ADP quanto ai servizi di trattamento dei dati dei clienti; collettivamente denominati i codici.
Collaboratore	COLLABORATORE indica un dipendente di un cliente statunitense che è co-dipendente di un'affiliata indiretta statunitense di Automatic Data Processing, Inc. nell'ambito dell'offerta di servizi dell'organizzazione professionale dei datori di lavoro negli Stati Uniti.
Comitato esecutivo di ADP	COMITATO ESECUTIVO DI ADP indica il comitato di funzionari composto da (i) amministratore delegato (AD) Automatic Data Processing, Inc. e (ii) altri funzionari che riferiscono direttamente all'AD e che, collettivamente, sono responsabili delle operazioni del Gruppo ADP.
Consiglio della leadership della riservatezza	CONSIGLIO DELLA LEADERSHIP DELLA RISERVATEZZA indica il Consiglio diretto dal responsabile globale di protezione della riservatezza e composto dai sorveglianti della riservatezza, dai membri della rete della riservatezza selezionati dal responsabile globale di protezione della riservatezza e da altri soggetti che possono essere necessari per coadiuvare la missione del Consiglio.
Consiglio generale	Per CONSIGLIO GENERALE si intende il Consiglio generale di Automatic Data Processing, Inc.
Consumatore	CONSUMATORE indica una persona che interagisce direttamente con ADP a titolo personale. Ad esempio, i consumatori includono individui che partecipano a programmi di sviluppo del talento o che utilizzano prodotti e servizi di ADP per uso personale (ossia esternamente a un rapporto di lavoro con ADP o con un cliente di ADP).
Contratto del responsabile del trattamento	CONTRATTO DEL RESPONSABILE DEL TRATTAMENTO indica qualsiasi contratto di trattamento dei dati personali sottoscritto da ADP e da un terzo responsabile del trattamento.
Contratto del subincaricato	CONTRATTO DEL SUBINCARICATO indica un accordo scritto o elettronico tra ADP e un Terzo subincaricato ai sensi dell'articolo 7.1 del codice di riservatezza sui servizi di trattamento dei dati dei clienti.
Contratto di servizio	CONTRATTO DI SERVIZIO indica qualsiasi contratto, accordo o termine in base al quale ADP fornisce servizi al cliente.
Data di entrata in	Per DATA DI ENTRATA IN VIGORE si intende la data in cui entrano in

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

vigore	vigore i codici, come indicato all'articolo 1.
Dati cliente	Per DATI CLIENTE si intendono i dati personali relativi ai dipendenti dei clienti (inclusi potenziali dipendenti, ex dipendenti e familiari dei dipendenti) trattati da ADP in relazione alla fornitura dei servizi al cliente.
Dati di contatto commerciali	Per DATI DI CONTATTO COMMERCIALI si intendono tutti i dati relativi a un professionista riportati, solitamente, su un biglietto da visita o all'interno di una firma e-mail.
Dati personali o dati	Per DATI PERSONALI o DATI si intende qualsiasi informazione relativa a un individuo identificato o identificabile. I dati personali possono anche essere indicati come informazioni personali nelle politiche e negli standard che implementano i codici.
Decisione di adeguatezza	DECISIONE DI ADEGUATEZZA indica qualsiasi decisione presa da un'autorità di protezione dei dati o da un altro organismo competente secondo la quale un Paese, una regione o un destinatario di un trasferimento di dati è considerato fornire un livello adeguato di protezione dei dati personali. I soggetti contemplati da una decisione di adeguatezza includono i destinatari situati in paesi che secondo la legge applicabile sono ritenuti fornire un adeguato livello di protezione dei dati, così come i destinatari che sono vincolati da un altro strumento (come un insieme di norme aziendali vincolanti) che sono stati approvati dall'autorità di protezione dei dati o da un altro organismo competente. Relativamente agli Stati Uniti d'America, le aziende che conseguono la certificazione secondo un quadro di riservatezza USA-SEE e/o USA-Svizzera saranno oggetto di una decisione di adeguatezza.
Dipendente del cliente	DIPENDENTE DEL CLIENTE indica qualsiasi persona i cui dati personali vengono trattati da ADP in qualità di responsabile del trattamento per un cliente in virtù di un contratto di servizi. Per chiarezza, DIPENDENTE DEL CLIENTE si riferisce a tutti gli individui i cui dati personali vengono trattati da ADP nella fornitura dei servizi al cliente (indipendentemente dalla natura giuridica del rapporto tra l'individuo e il cliente). Non sono inclusi i professionisti i cui dati personali vengono trattati da ADP in relazione al rapporto diretto di ADP con il cliente. Ad esempio, ADP può trattare i dati personali di un professionista delle Risorse Umane per stipulare un contratto con il cliente; tali dati sono soggetti al codice di riservatezza sui dati aziendali. Tuttavia, quando ADP fornisce servizi di elaborazione degli stipendi al cliente (ad esempio, emette buste paga, fornisce assistenza per l'utilizzo di un sistema di ADP), i dati dell'individuo vengono trattati come dati del cliente.
Dirigente	DIRIGENTE RESPONSABILE indica l'Amministratore Delegato di una

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

responsabile	società del Gruppo o il capo di una business unit o di un'area funzionale, che ha la proprietà primaria del bilancio della società del Gruppo, della business unit o dell'area funzionale.
Entità ceduta	Per ENTITÀ CEDUTA si intende una società del Gruppo non più posseduta da ADP a seguito di cessione di azioni e/o beni aziendali o di altra dismissione, tale da far venir meno la qualifica di società del Gruppo.
Entità contraente di ADP	ENTITÀ CONTRAENTE DI ADP indica la società del Gruppo che ha stipulato un contratto richiesto dai codici, come un contratto di servizio, un contratto di sub-incarico o un accordo di trasferimento dati.
Entità delegata di ADP	ENTITÀ DELEGATA DI ADP indica ADP Nederland, B.V., con sede legale in Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Paesi Bassi.
Familiare	FAMILIARE indica il coniuge, il partner, il figlio/la figlia o il beneficiario di un associato o il referente di emergenza di un associato o di un lavoratore temporaneo.
Fornitore	FORNITORE indica qualsiasi terza parte che fornisce beni o servizi ad ADP (ad esempio, in qualità di fornitore di servizi, agente, responsabile del trattamento dati, consulente o fornitore).
Individuo	INDIVIDUO indica qualsiasi persona fisica identificata o identificabile i cui dati personali vengono trattati da ADP in qualità di responsabile del trattamento dei dati o di titolare del trattamento, ad eccezione dei collaboratori. NOTA: il codice di riservatezza di ADP sui dati aziendali e il codice di riservatezza di ADP quanto ai luoghi di lavoro non si applicano, pertanto, al trattamento dei dati personali dei collaboratori.
Interesse prevalente	INTERESSE PREVALENTE indica gli interessi pressanti di cui all'articolo 13.1 del codice di riservatezza di ADP quanto ai luoghi di lavoro e del codice di riservatezza quanto ai dati aziendali, in base ai quali gli obblighi di ADP o i diritti degli individui di cui agli articoli 13.2 e 13.3 dei codici possono, in circostanze specifiche, essere superati se questo interesse pressante prevale sull'interesse dell'individuo.
Lavoratore temporaneo	LAVORATORE TEMPORANEO indica una persona che fornisce servizi ad ADP (e che è soggetta alla supervisione diretta di ADP) su base temporanea o non permanente, come lavoratori temporanei, lavoratori a contratto, appaltatori indipendenti o consulenti.
Legge applicabile	LEGGE APPLICABILE indica qualsiasi legge sulla riservatezza o sulla protezione dei dati applicabile a particolari attività di trattamento.
Legge applicabile al	Ai fini del codice di riservatezza sui servizi di trattamento dei dati dei

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

responsabile del trattamento dei dati	clienti, per LEGGE APPLICABILE AL RESPONSABILE DEL TRATTAMENTO DEI DATI si intende qualsiasi legge sulla riservatezza o sulla protezione dei dati che si applica ad ADP in qualità di responsabile del trattamento dei dati per conto di un cliente che è un titolare del trattamento dei dati.
Legge applicabile dell'SEE	Per LEGGE APPLICABILE DELL'SEE si intendono i requisiti previsti dalle leggi applicabili del SEE, che si applicano a qualsiasi dato personale originariamente acquisito nel contesto delle attività di una società del Gruppo stabilita nel SEE (anche dopo essere stato trasferito a un'altra società del Gruppo stabilita esternamente all'SEE).
Legge applicabile sul titolare del trattamento dei dati	Ai fini del codice di riservatezza sui servizi di trattamento dei dati dei clienti, per LEGGE APPLICABILE AL TITOLARE DEL TRATTAMENTO DEI DATI si intende qualsiasi legge sulla riservatezza o sulla protezione dei dati che si applica a un cliente di ADP in qualità di titolare del trattamento dei dati del cliente.
Limitazioni al trasferimento dei dati nell'SEE	Per LIMITAZIONI AL TRASFERIMENTO DEI DATI NEL SEE si intende qualsiasi limitazione riguardante i trasferimenti transfrontalieri di dati personali ai sensi della legislazione sulla protezione dei dati di un Paese del SEE.
Minori	Ai fini dell'acquisizione e della commercializzazione dei dati di ADP, per MINORI si intendono le persone di età inferiore a quella stabilita dalla legge applicabile come età legittima per prestare il consenso all'acquisizione e/o alla commercializzazione dei dati.
Norme aziendali vincolanti	Per NORME AZIENDALI VINCOLANTI si intende una politica sulla riservatezza di un gruppo di società collegate che si ritiene offrano un adeguato livello di protezione per il trasferimento dei dati personali all'interno di tale gruppo di società ai sensi della legge applicabile.
Partner commerciale	PARTNER COMMERCIALE indica qualsiasi terza parte, diversa da un cliente o da un fornitore, che intrattiene o ha intrattenuto un rapporto commerciale o un'alleanza strategica con ADP (ad esempio, un partner commerciale, una joint venture o un partner di sviluppo congiunto).
Personale	Per PERSONALE si intendono, collettivamente, gli associati di ADP attualmente impiegati e i lavoratori a tempo determinato che attualmente lavorano per ADP.
Principale autorità di protezione dei dati (DPA)	Per PRINCIPALE AUTORITÀ DI PROTEZIONE DEI DATI (DPA) si intende l'autorità olandese di protezione dei dati.
Professionista	PROFESSIONISTA indica qualsiasi individuo (diverso da un

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

	dipendente) che interagisce direttamente con ADP a titolo professionale o aziendale. Ad esempio, i professionisti comprendono il personale delle Risorse umane del cliente che intrattiene rapporti con ADP come utente di prodotti o servizi di ADP. I professionisti comprendono anche rappresentanti di account di clienti, fornitori e partner commerciali, contatti commerciali, contatti di associazioni di categoria, autorità di regolamentazione, contatti con i media e altri soggetti che interagiscono con ADP a titolo commerciale.
Requisiti obbligatori	REQUISITI OBBLIGATORI indica gli obblighi previsti dalla legge applicabile al responsabile del trattamento dei dati personali che richiedono il trattamento dei dati personali per (i) la sicurezza o la difesa nazionale; (ii) la sicurezza pubblica; (iii) la prevenzione, le indagini, l'accertamento o il perseguimento di reati o violazioni dell'etica per le professioni regolamentate o (iv) la protezione di qualsiasi individuo o dei diritti e delle libertà degli individui.
Responsabile del trattamento dei dati	RESPONSABILE DEL TRATTAMENTO DEI DATI indica l'entità o la persona fisica che tratta i dati personali per conto di un titolare del trattamento.
Responsabile globale della protezione della riservatezza	RESPONSABILE GLOBALE DELLA PROTEZIONE DELLA RISERVATEZZA indica l'associato di ADP titolare di questo titolo presso Automatic Data Processing, Inc.
Responsabile interno del trattamento	Per RESPONSABILE INTERNO DEL TRATTAMENTO si intende qualsiasi società del Gruppo che tratta i dati personali per conto di un'altra società del Gruppo titolare del trattamento.
Rete della riservatezza	RETE DELLA RISERVATEZZA indica i membri del team globale di riservatezza e governance dei dati e altri membri dell'Ufficio legale, inclusi i professionisti della conformità e i responsabili della protezione dei dati che sono responsabili della conformità alla riservatezza all'interno delle rispettive regioni, dei rispettivi paesi, delle rispettive business unit o delle rispettive aree funzionali.
Richiedente	RICHIEDENTE indica qualsiasi individuo che fornisce dati personali ad ADP nel contesto della richiesta di una posizione presso ADP in qualità di associato.
Scopo commerciale	SCOPO COMMERCIALE indica una finalità legittima del trattamento dei dati personali, come specificato negli articoli 2, 3 o 4 di qualsiasi codice di ADP o di trattamento di categorie speciali di dati, come specificato nell'articolo 4 di qualsiasi codice di ADP.
Scopo secondario	SCOPO SECONDARIO indica qualsiasi scopo diverso da quello

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

	originale per il quale i dati personali vengono ulteriormente trattati.
SEE	Per SEE o SPAZIO ECONOMICO EUROPEO si intendono tutti gli Stati membri dell'Unione europea, più la Norvegia, l'Islanda e il Liechtenstein e, ai fini dei codici, la Svizzera e nel Regno Unito, dopo la sua uscita dall'Unione Europea. Per decisione del Consiglio generale, da pubblicare su www.adp.com, può includere altri paesi le cui leggi sulla protezione dei dati prevedono limitazioni al trasferimento dei dati simili a quelle dell'SEE.
Servizi ai clienti	Per SERVIZI AI CLIENTI si intendono i servizi di gestione delle risorse umane fornite da ADP ai clienti, quali servizi di reclutamento, buste paga e retribuzione, benefit dei dipendenti, gestione dei talenti, amministrazione delle risorse umane, consulenza e analisi e servizi pensionistici.
Società del Gruppo	Per SOCIETÀ DEL GRUPPO si intende qualsiasi entità giuridica affiliata di Automatic Data Processing, Inc. e/o ADP, Inc., se Automatic Data Processing, Inc. o ADP, Inc. detiene direttamente o indirettamente oltre il 50% del capitale azionario emesso, se detiene il 50% o più dei diritti di voto all'assemblea generale degli azionisti, se ha il potere di nominare la maggioranza degli amministratori o se dirige in altro modo le attività di tale entità giuridica.
Sorvegliante della riservatezza	SORVEGLIANTE DELLA RISERVATEZZA indica un dirigente di ADP che è stato nominato da un dirigente responsabile e/o da un quadro di ADP per implementare e far rispettare i codici di riservatezza all'interno di una business unit di ADP.
Subincaricati	SUBINCARICATI indica, collettivamente, i subincaricati ADP e i Terzi subincaricati del trattamento.
Subincaricato di ADP	Ai fini del codice di riservatezza sui servizi di trattamento dei dati dei clienti, per SUBINCARICATO DI ADP si intende qualsiasi società del Gruppo ingaggiata da un'altra società del Gruppo come subincaricato del trattamento dei dati dei clienti.
Team globale sulla riservatezza e governance dei dati	TEAM GLOBALE SULLA RISERVATEZZA E GOVERNANCE DEI DATI indica l'Ufficio di riservatezza e governance dei dati di ADP. L'Ufficio di riservatezza e governance dei dati è diretto dal responsabile globale della protezione della riservatezza ed è composto da funzionari della riservatezza, responsabili riservatezza e altro personale che presenta rapporti di segnalazione al responsabile globale della protezione della riservatezza o ai funzionari della riservatezza e ai responsabili della riservatezza.
Terza parte	TERZA PARTE indica qualsiasi persona, organizzazione privata o ente governativo che non è una società del Gruppo.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

TERZA PARTE Responsabile del trattamento	TERZA PARTE RESPONSABILE DEL TRATTAMENTO indica una terza parte che tratta i dati personali per conto di ADP che non è sotto la diretta autorità di ADP.
TERZA PARTE Titolare del trattamento	TERZA PARTE TITOLARE DEL TRATTAMENTO indica un terzo che tratta i dati personali e determina le finalità e le modalità del trattamento.
Terzo Subincaricato del trattamento	TERZO SUBINCARICATO DEL TRATTAMENTO indica qualsiasi terzo incaricato da ADP come subincaricato.
Titolare del trattamento dei dati	TITOLARE DEL TRATTAMENTO DEI DATI indica l'entità o la persona fisica che, autonomamente o assieme ad altre, determina le finalità e le modalità del trattamento dei dati personali.
Trattamento	TRATTAMENTO indica qualsiasi operazione eseguita sui dati personali, con o senza mezzi automatici, come l'acquisizione, la registrazione, l'archiviazione, l'organizzazione, la modifica, l'utilizzo, la divulgazione (inclusa la concessione dell'accesso remoto), la trasmissione o la cancellazione di dati personali.
Valutazione d'impatto sulla protezione dei dati (DPIA)	Per VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) si intende una procedura volta a condurre e documentare una valutazione preventiva dell'impatto che un determinato trattamento può avere sulla protezione dei dati personali, qualora tale trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone, in particolare, in caso di utilizzo di nuove tecnologie. Una DPIA deve contenere: (i) una descrizione di: (a) scopo e contesto del trattamento; (b) finalità per cui i dati personali vengono trattati; (c) specifiche finalità per cui vengono trattate le categorie speciali di dati; (d) categorie di destinatari di dati personali, inclusi destinatari non contemplati da una decisione di adeguatezza; (e) periodi di archiviazione dei dati personali; (ii) una valutazione di: (a) necessità e proporzionalità del trattamento; (b) rischi per i diritti di riservatezza degli individui; e misure volte ad attenuare tali rischi, comprese le misure di salvaguardia, le misure di sicurezza e altri meccanismi (quali

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

	riservatezza fin dalla progettazione) al fine di garantire la protezione dei dati personali.
Violazione della sicurezza dei dati	VIOLAZIONE DELLA SICUREZZA DEI DATI indica qualsiasi incidente che influenza la riservatezza, l'integrità o la disponibilità dei dati personali, come l'uso o la divulgazione non autorizzati dei dati personali o l'accesso non autorizzato ai dati personali, che compromette la riservatezza o la sicurezza dei dati personali.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Presentato da:	**ADP - Global Security Organization**
Versione:	**2.0**
Data di rilascio:	**Settembre 2019**

Indice

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Termini e definizioni

I termini seguenti possono comparire in tutto il documento:

Termini o Acronimi utilizzati	Definizione
GETS	**Global Enterprise Technology & Solutions**
GSO	**Global Security Organization**
CAB	**Change Advisory Board**
DRP	**Disaster Recovery Plan**
CIRC	**GSO's Critical Incident Response Center**
SIEM	**Security Information and Event Management**
IDS	**Intrusion Detection System**
DNS	**Domain Name System**
NTP	**Network Time Protocol**
SOC	**Service Organization Controls**
TPSI	**Trusted Platform Security Infrastructure**

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Overview

ADP mantiene un formale programma sulla sicurezza delle informazioni contenente garanzie amministrative, tecniche e fisiche per proteggere la sicurezza, la riservatezza e l'integrità delle informazioni dei clienti. Questo programma è ragionevolmente progettato per (i) salvaguardare la sicurezza e la riservatezza delle informazioni dei clienti, (ii) proteggere da minacce o rischi previsti per la sicurezza o l'integrità delle informazioni e (iii) proteggere dall' accesso non autorizzato o dall'uso delle informazioni .

Questo documento contiene una panoramica delle misure e delle pratiche della sicurezza delle informazioni di ADP, alla data di rilascio del documento e che sono soggette a modifiche da parte di ADP. Questi requisiti e pratiche sono progettati per essere coerenti con gli standard di sicurezza delle informazioni ISO / IEC 27001: 2013. ADP valuta periodicamente le proprie Policy e gli standard di sicurezza. Il nostro obiettivo è contribuire a garantire che il programma di sicurezza funzioni in modo efficace ed efficiente per proteggere tutte le informazioni a noi affidate dai nostri clienti e dai loro dipendenti.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Policy di Information Security

Autonomia delle Funzioni di Information Security

Il reponsabile della Sicurezza di ADP (Chief Security Officer) è responsabile della struttura Global Security Organization (GSO) e riporta al General Counsel (Legal e Compliance), invece che al Chief Information Officer; ciò conferisce a GSO la necessaria indipendenza dall'IT. GSO è un team di sicurezza trasversale e divisionale che ha un approccio multidisciplinare in materia di sicurezza informatica, gestione dei rischi operativi, gestione della sicurezza dei clienti, protezione dei dipendenti ADP e della resilienza aziendale. Il senior management di GSO, a riporto del Chief Security Officer, è responsabile della gestione delle Policy, delle procedure e delle linee guida di sicurezza.

Definizione Formale delle Policy di Information Security

ADP ha sviluppato e documentato le policy di Information Security che definiscono l'approccio di ADP alla gestione della sicurezza delle informazioni. Le aree specifiche coperte da queste policy includono, ma non sono limitate a:

- **Security Management Policy** – Definisce le responsabilità della Global Security Organization (GSO) e del Chief Security Officer (CSO), comprese le responsabilità sulla sicurezza delle informazioni e i controlli sul processo di assunzione dal punto di vista della sicurezza.
- **Global Privacy Policy –** Relativa alla raccolta di informazioni personali, l'accesso, l'accuratezza, la divulgazione e l'informativa sulla privacy ai clienti.
- **Utilizzo consentito da parte dei dipendenti delle comunicazioni elettroniche e Policy sulla protezione dei dati** – Descrive l'uso accettabile delle diverse comunicazioni elettroniche, la crittografia e la gestione delle chiavi.
- **Policy sulla gestione delle informazioni –** Fornisce requisiti per la classificazione delle informazioni ADP e stabilisce i controlli di protezione.
- **Policy sulla Sicurezza Fisica –** Definisce i requisiti di sicurezza delle strutture ADP per i visitatori e per i nostri dipendenti che vi lavorano.
- **Policy della gestione della Sicurezza Operativa –** Fornisce controlli minimi per la manutenzione delle patch di sistema, proteggersi efficacemente dalla minaccia dei malware, gestione dei backup e controlli di sicurezza dei database.
- **Policy sul Monitoraggio della Sicurezza –** Fornisce controlli per sistemi di rilevamento delle intrusioni (IDS), log e prevenzione della perdita di dati (DLP).
- **Policy sulle Investigazioni e gestione degli Incidenti –** Definisce gli standard per la risposta agli incidenti, le indagini forensi, la protezione della forza lavoro e l'accesso alle informazioni elettroniche archiviate dei dipendenti.
- **Policy di Accesso & Autenticazione –** Descrive i requisiti di autenticazione (ad es. ID utente e password), accesso remoto e accesso alle reti wireless.
- **Policy sulla Sicurezza della Rete –** Definisce l'architettura di sicurezza di router, firewall, AD, DNS, server di posta elettronica, DMZ, servizi cloud, dispositivi di rete, proxy Web e tecnologia di rete commutata.
- **Policy Globale sulle Terze Parti e Acquisizioni –** Definisce controlli minimi di sicurezza per coinvolgere terze parti per aiutare ADP a raggiungere i propri obiettivi aziendali.
- **Policy sulla Gestione delle Applicazioni –** Stabilisce adeguati controlli di sicurezza in ogni fase del ciclo di vita dello sviluppo del sistema.
- **Policy sulla Business Resiliency –** Gestisce la protezione, l'integrità e la conservazione del Business di ADP stabilendo i requisiti minimi per documentare, implementare, mantenere e migliorare continuamente i programmi di resilienza aziendale.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

- **Policy sulla Converged Security Risk Management–** Identificazione, monitoraggio, risposta, analisi, governance e nuove iniziative commerciali.

Le Policy sono pubblicate nella Intranet ADP e sono accessibili a tutti gli associate e i fornitori, all'interno della rete ADP.

Revisione delle Policy di Information Security

ADP rivede le sue Policy di sicurezza delle informazioni almeno una volta all'anno o ogni volta che ci sono cambiamenti importanti che incidono sul funzionamento dei sistemi di informazione di ADP.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Organizzazione dell' Information Security

Ruoli e Responsabilità dell'Information Security

Il GSO è costituito da diversi team di sicurezza strutturati che adottano un approccio multidisciplinare al rispetto degli standard di sicurezzainformatica, gestione dei rischi operativi, gestione della sicurezza dei clienti, protezione della forza lavoro e resilienza aziendale. I ruoli e le responsabilità sono stati definiti formalmente per tutti i membri del Team. Il GSO è incaricato della progettazione, dell'implementazione e della supervisione del nostro programma di sicurezza delle informazioni basato sulle Policy aziendali. Le attività di GSO sono supervisionate dall'Executive Security Committee, i cui membri includono Chief Security Officer, Chief Executive Officer, Chief Financial Officer, Chief Strategy Officer, Chief Human Resources Officer e il General Counsel di ADP.

Mobile Computing and Teleworking Policy

ADP richiede che tutte le informazioni riservate siano crittografate sui dispositivi mobili, per prevenire la perdita di dati, che potrebbe derivare dal furto o dalla perdita di un computer / dispositivo. Per accedere alle reti aziendali da remoto sono inoltre necessarie la protezione avanzata degli endpoint e l'autenticazione a due fattori tramite VPN. Tutti i dispositivi remoti devono essere protetti da password. I dipendenti ADP sono tenuti a segnalare immediatamente i dispositivi persi o rubati attraverso un processo di segnalazione di incidenti di sicurezza.

Tutti i dipendenti e i fornitori, come condizione per l'impiego presso ADP, devono rispettare la Policy sull'uso accettabile delle comunicazioni elettroniche e della protezione dei dati e altre Policy pertinenti.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Background Checks

Coerentemente con i requisiti legali applicabili nella giurisdizione della persona, ADP effettua adeguati controlli di base commisurati ai doveri e alle responsabilità dei suoi dipendenti, appaltatori e terze parti. Questi controlli confermano l'idoneità del candidato a gestire le informazioni dei clienti prima di ingaggiare o assumere tali soggetti.

I controlli possono includere includere i seguenti componenti:

- Verifica dell'ammissibilità identità / impiego.
- Storico lavorativo precedent impieghi.
- Curriculum scolastico e qualifiche professionali
- Casellario giudiziale (ove legalmente autorizzato e in base alle normative locali)

Accordi di riservatezza con dipendenti e appaltatori

I contratti di lavoro e i contratti con gli appaltatori contengono termini che indicano gli obblighi e le responsabilità relative alle informazioni sui clienti a cui avranno accesso. Tutti i dipendenti e gli appaltatori di ADP sono vincolati da obblighi di riservatezza.

Programmi di Formazione sulla Sicurezza delle Informazioni

Tutti i dipendenti sono tenuti a completare la formazione sulla sicurezza delle informazioni come parte del loro piano di inserimento in azienda. Inoltre, ADP offre una formazione annuale sulla sicurezza per ricordare ai dipendenti le loro responsabilità quando svolgono le loro attività quotidiane..

Responsabilità degli associate e Processi Disciplinari

ADP ha pubblicato delle Policy di sicurezza che tutti i dipendenti ADP devono rispettare. Le violazioni delle Policy di sicurezza possono comportare la revoca dei privilegi di accesso e / o azioni disciplinari fino alla risoluzione dei contratti di consulenza o dell'impiego.

Cessazione delle responsabilità lavorative

Le responsabilità in caso di cessazione del rapporto di lavoro sono state formalmente documentate e comprendono :

- Restituire tutte le informazioni e le risorse ADP in possesso del rispettivo dipendente, su qualsiasi supporto sia memorizzato.
- Cessazione dei diritti di accesso a strutture, informazioni e sistemi ADP
- Modifica delle password per gli account condivisi attivi rimanenti, se applicabile
- Passaggio di consegne, se applicabile.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Gestione degli Asset

Utilizzo consentito dei dispositivi

L'uso accettabile delle risorse è spiegato in diverse Policy, applicabili a dipendenti e fornitori di ADP, per aiutare a garantire che le informazioni di ADP e dei clienti non siano esposte dall'uso di tali risorse. Esempi di aree descritte in queste Policy sono: l'uso di comunicazioni elettroniche, l'uso di apparecchiature elettroniche e l'uso di risorse informatiche.

Classificazione delle Informazioni

Le informazioni acquisite, create o gestite da o per conto di ADP ricevono, a seconda dei casi, una classificazione di sicurezza di:

- Public - Esempio: opuscoli di marketing, relazioni annuali pubblicate.
- ADP Internal Use Only - Esempio: comunicazioni tra uffici, procedure operative.
- ADP Confidential - Esempio: informazioni personali personali e sensibili.
- ADP Restricted - Esempio: previsioni finanziarie, informazioni sulla pianificazione strategica.

I requisiti per la gestione delle informazioni sono direttamente correlati alla classificazione della sicurezza delle informazioni. Le informazioni personali e le informazioni personali sensibili sono sempre considerate ADP Confidential. Tutte le informazioni del cliente sono classificate come riservate.

I dipendenti ADP sono responsabili della protezione e della gestione delle informazioni in conformità con il loro livello di classificazione di sicurezza, che fornisce il grado di protezione delle informazioni e requisiti di gestione applicabili per ciascun livello di classificazione. La classificazione di riservatezza ADP viene applicata a tutte le informazioni archiviate, trasmesse o gestite da terzi.

Smaltimento di Apparecchiature e Supporti

Quando apparecchiature, documenti, file e supporti di ADP vengono eliminati o riutilizzati, vengono prese le misure appropriate per impedire il successivo recupero delle informazioni del cliente originariamente memorizzate in essi. Tutte le informazioni su computer o supporti di archiviazione elettronici, indipendentemente dalla classificazione, vengono eliminate in modo sicuro, a meno che il supporto non venga distrutto fisicamente, prima di essere rilasciato al di fuori delle strutture ADP o riutilizzato. Le procedure per la distruzione / cancellazione sicura delle informazioni ADP contenute nelle apparecchiature, in documenti, file e supporti sono formalmente documentate.

Supporti fisici in transito

Sono state implementate misure organizzative per proteggere i materiali stampati contenenti le informazioni dei clienti contro furto, perdita e / o accesso / modifica non autorizzati (i) durante il transito, ad es. buste sigillate, contenitori e consegna a mano all'utente autorizzato; e (ii) durante la revisione, o altri trattamenti se rimossi dall'archiviazione sicura.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Controllo degli Accessi

Requisiti del Business sul Controllo Accessi

La Policy di controllo degli accessi di ADP si basa su requisiti definiti dall'azienda. Le Policy e gli standard di controllo sono articolati in controlli di accesso che vengono applicati in tutti i componenti del servizio fornito e si basano su un principio di "privilegio minimo" e "necessità di conoscere".

Accesso alle infrastrutture - Gestione del controllo degli accessi

Le richieste di accesso per lo spostamento, l'aggiunta, la creazione e l'eliminazione vengono registrate, approvate e riviste periodicamente.

Una revisione formale viene eseguita, almeno una volta all'anno, per confermare che i singoli utenti corrispondano esattamente al ruolo aziendale rilevante e che non avrebbero continuato l'accesso dopo un cambio di posizione. Questo processo è verificato e documentato in un rapporto SOC1[1] di tipo II. Dall'interno di un sistema di gestione dell'identità, un team ADP dedicato è responsabile della concessione, della negazione, dell'annullamento, della conclusione e della disattivazione / disattivazione dell'accesso alle strutture e ai sistemi di informazione ADP. ADP utilizza uno strumento di gestione centralizzata delle identità e degli accessi (IAM) gestito centralmente da un team GETS dedicato. In base ai diritti di accesso richiesti tramite lo strumento IAM centralizzato, verrà attivato un flusso di lavoro di convalida che potrebbe coinvolgere il supervisore degli utenti. L'accesso è fornito su base temporanea ed esistono flussi di lavoro per impedire che tale accesso rimanga permanente. L'accesso di un dipendente a una struttura viene disattivato immediatamente dopo l'ultimo giorno di assunzione disattivando la sua carta di accesso (badge del dipendente). Gli ID utente del dipendente vengono immediatamente disattivati. Tutte le risorse dei dipendenti vengono restituite e controllate dal responsabile di linea competente e confrontate con l'elenco delle risorse nella base dati di gestione della configurazione. A seguito di una modifica della posizione lavorativa o di modifiche organizzative, i profili utente o i diritti di accesso degli utenti devono essere modificati dalla direzione della business unit e dal team IAM. Inoltre, ogni anno viene eseguita una revisione formale dei diritti di accesso per verificare che i diritti dei singoli utenti corrispondano al loro ruolo commerciale rilevante e che non vi siano diritti di accesso irrilevanti rimanenti dopo un trasferimento di posizione.

Password Policy

I criteri password associati ADP vengono applicati ai server, database, dispositivi e applicazioni di rete, nella misura consentita dal dispositivo / applicazione. La complessità della password deriva da un'analisi basata sul rischio dei dati e dei contenuti protetti. Le Policy soddisfano gli standard di settore prevalenti in termini di robustezza e complessità, incluso ma non limitato all'uso dell'autenticazione step-up, a due fattori o biometrica laddove appropriato.

I requisiti di autenticazione delle applicazioni client variano in base al prodotto e i servizi federati (SAML 2.0) sono disponibili su applicazioni ADP specifiche utilizzando una rete unificata e un livello di sicurezza gestito da GETS.

Timeout delle Sessioni

ADP applica timeout automatici a tutti i server, workstation, applicazioni e connessioni VPN basati su un approccio basato sul rischio coerente con gli standard del settore. Il ripristino delle sessioni può avvenire solo dopo che l'utente ha fornito una password valida.

[1] Nel caso di alcuni servizi statunitensi offerti da ADP, è disponibile anche un report SOC 2 Type II.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Crittografia

Controlli Crittografici

ADP richiede che le informazioni sensibili scambiate tra ADP e terze parti ADP debbano essere crittografate (o che il canale di trasporto debba essere cifrato) utilizzando tecniche di crittografia accettati dagli Standard del settore. In alternativa, è possibile utilizzare una linea dedicata.

Gestione delle Chiavi di Cifratura

ADP ha uno standard interno di sicurezza della crittografia che include una gestione delle chiavi ben definita e procedure di deposito delle chiavi, compresa la gestione delle chiavi sia simmetrica che asimmetrica.

Le chiavi di crittografia utilizzate per le informazioni ADP sono sempre classificate come informazioni riservate. L'accesso a tali chiavi è strettamente limitato a coloro che hanno bisogno di sapere e, se viene fornita un'approvazione alle eccezioni. Le chiavi di crittografia e la gestione del ciclo di vita delle chiavi hanno seguito le pratiche standard del settore.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Sicurezza Fisica ed Ambientale

L'approccio di ADP alla sicurezza fisica ha due obiettivi: creare un ambiente di lavoro sicuro per i dipendenti ADP e proteggere le informazioni personali conservate nei data center ADP e in altri uffici strategici di ADP.

La Policy di sicurezza ADP richiede che la gestione ADP identifichi quelle aree che richiedono un livello specifico di sicurezza fisica. L'accesso a tali aree è fornito solo agli associati autorizzati per scopi autorizzati. Le aree protette dell'ADP adottano varie garanzie di sicurezza fisica, inclusi i sistemi di videosorveglianza, l'uso dei badge di sicurezza (accesso controllato dalle identità) e le guardie di sicurezza di stanza ai punti di entrata e di uscita. Ai visitatori può essere concesso l'accesso solo se autorizzati e sono accompagnati in ogni momento.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Sicurezza Operativa

Formalizzazione delle procedure operative IT

GETS è l'unità ADP responsabile delle operazioni e della manutenzione dell'infrastruttura IT. GETS mantiene e documenta formalmente le Policy e le procedure relative alle operazioni IT. Queste procedure includono, ma non sono limitate a quanto segue:

- Gestione degli aggiornamenti.
- Gestione del backup
- Gestione degli errori di sistema
- Riavvio e ripristino del sistema
- Monitoraggio del sistema
- Pianificazione e monitoraggio dei lavori

Gestione degli Aggiornamenti dell'Infrastruttura

Il Change Advisory Board (CAB), che comprende rappresentanti di una vasta gamma di Team ADP, è coordinato da GETS. Le riunioni CAB discutono dell'impatto, le finestre di distribuzione dei rilasci in produzione, nonché per coordinare qualsiasi altro cambiamento nell'infrastruttura di produzione.

Pianificazione dell'Approvigionamento dei Sistemi

I requisiti di capacità sono costantemente monitorati e rivisti periodicamente. A seguito di queste revisioni, i sistemi e le reti vengono dimensionati di conseguenza. Quando devono essere apportate modifiche significative a causa di una modifica della capacità o di un'evoluzione tecnologica, il team di benchmarking GETS può eseguire prove di stress per l'applicazione e / o il sistema pertinenti. Al termine delle prove di stress, il team fornisce un rapporto dettagliato sull'evoluzione delle prestazioni misurando le modifiche in (i) componenti, (ii) configurazione o versione del sistema o (iii) configurazione o versione del middleware.

Protezione contro Codice Malevolo

Le tecnologie di protezione degli endpoint vengono implementate per proteggere le risorse ADP in conformità con i migliori standard del settore.

Policy sulla Gestione dei Backup

ADP ha messo in atto delle Policy che richiedono che tutte le operazioni di hosting di produzione eseguano il backup delle informazioni. L'ambito e la frequenza dei backup vengono eseguiti in conformità con i requisiti aziendali dei servizi ADP pertinenti, i requisiti di sicurezza delle informazioni interessate e la criticità delle informazioni in relazione al ripristino di emergenza. Il monitoraggio dei backup pianificati viene eseguito da GETS per identificare problemi di backup o eventuali eccezioni.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Sicurezza dei Log e Monitoraggio

ADP ha implementato un'infrastruttura di registrazione centrale e di sola lettura (SIEM) e un sistema di correlazione dei log e avvisi di allarme (TPSI). Gli avvisi provenienti dai log sono monitorati e trattati in modo tempestivo dal CIRC.

Tutti questi sistemi sono sincronizzati utilizzando un unico riferimento basato su Network Time Protocol (NTP).

Ogni singolo log deve contenere almeno:

- Data e Ora
- Chi (identificazione dell'operatore o amministratore)
- Cosa (Informazioni sull'evento)

Gli audit trail e la registrazione del sistema per le applicazioni ADP sono progettati e configurati per tenere traccia delle seguenti informazioni:

- Accesso autorizzato
- Operazioni privilegiate
- Tentativi di accesso non autorizzati
- Avvisi o guasti dei sistemi
- Modifiche alle impostazioni di sicurezza del sistema, quando il sistema consente tale registrazione

Questi registri sono disponibili solo per il personale autorizzato ADP e vengono inviati in modalità live per impedire che i dati vengano manomessi prima di essere archiviati nelle apparecchiature di registrazione sicure.

Monitoraggio Systemi IT

ADP utilizza misure appropriate per il monitoraggio dell'infrastruttura 24 ore al giorno, 7 giorni alla settimana. Gli avvisi di sono gestiti da diversi team in base al livello di gravità e alle competenze necessarie per risolverli.

Le strutture del centro di hosting ADP utilizzano applicazioni di monitoraggio costantemente in esecuzione su tutti i sistemi di elaborazione correlati e sui componenti di rete per fornire allo staff ADP una notifica proattiva di problemi e avvisi in previsione di possibili problemi.

Gestione Tecnica delle Vulnerabilità

Tutti i server installati nell'infrastruttura di hosting devono essere conformi ai criteri per l'installazione di un sistema operativo sicuro (o processo di Hardening). Le operazioni ospitate utilizzano una versione approvata e standardizzata per ogni tipo di server utilizzato all'interno della nostra infrastruttura. L'installazione immediata di sistemi operativi è vietata poiché queste installazioni possono creare vulnerabilità, come password generiche di account di sistema, che potrebbero comportare rischi per l'infrastruttura. Queste configurazioni riducono l'esposizione dei computer che eseguono servizi non necessari che possono causare vulnerabilità.

ADP adotta una metodologia documentata per condurre rilasci e valutazioni periodiche delle vulnerabilità ,revisioni della conformità delle applicazioni basate su Internet e dei relativi componenti dell'infrastruttura, che includono almeno 15 categorie primarie di test. La metodologia di valutazione si basa sulle migliori pratiche interne e di settore, inclusi, a titolo esemplificativo, Open Web Application Security Project (OWASP), SANS Institute e Web Application Security Consortium (WASC)

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Sicurezza delle Comunicazioni

Gestione della Sicurezza della Rete

ADP utilizza un sistema di rilevamento delle intrusioni basato sulla rete che monitora il traffico a livello di infrastruttura di rete (24 ore al giorno, 7 giorni alla settimana) e identifica attività sospette o potenziali attacchi.

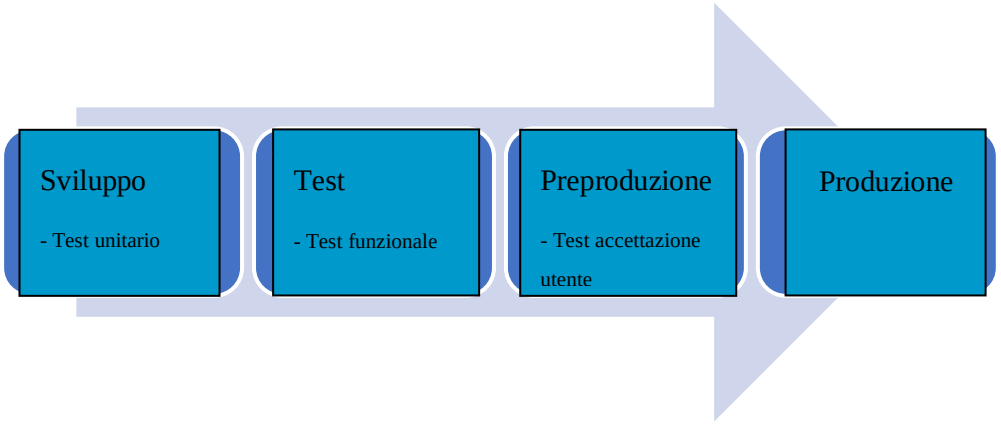
Scambio di Informazioni

ADP implementa controlli adeguati in modo che le informazioni dei clienti ADP inviate a terzi vengano trasferite solo tra i sistemi e le risorse di informazioni autorizzate e vengano scambiate solo attraverso i meccanismi di trasferimento sicuri e autorizzati di ADP.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Gestione dello Sviluppo e dei Processi di Supporto

Durante il ciclo di sviluppo, viene generata la documentazione applicabile e vengono creati piani di test per la fase di test. Sono definite diverse fasi per ciascun ambiente con l'approvazione pertinente in ciascuna fase:



- Per passare dall'ambiente di test all'ambiente di pre-produzione, è necessaria l'approvazione del team di qualità di ADP.
- Per passare dalla pre-produzione alla produzione, è necessaria l'approvazione delle operazioni IT.

I team di sviluppo sono tenuti ad utilizzare metodi di codifica sicuri. Le modifiche alle applicazioni vengono testate negli ambienti di sviluppo e regressione prima che raggiungano i sistemi di produzione. I test vengono eseguiti e documentati. Dopo l'approvazione, le modifiche vengono implementate nella produzione. Il test di penetrazione viene eseguito dopo cambiamenti significativi.

Un CAB periodico, che include rappresentanti di una vasta gamma di team ADP, è tenuto da GETS. Le riunioni CAB si svolgono su base regolare e hanno lo scopo di discutere gli impatti, concordare finestre di distribuzione e approvare la promozione di pacchetti software per la produzione, nonché per informare su eventuali altri cambiamenti nell'infrastruttura di produzione.

Il team operativo IT di ADP fornisce l'approvazione finale prima della promozione nell'ambiente di produzione dei pacchetti software.

Sicurezza negli Ambienti di Produzione

Gli ambienti di produzione e sviluppo sono separati e indipendenti l'uno dall'altro. Controlli di accesso adeguati sono impiegati per imporre una corretta separazione delle funzioni. I pacchetti software sono accessibili in ogni fase del processo di sviluppo e solo dai team coinvolti in quella fase.

Dati di Test

Secondo la Policy di gestione delle applicazioni di ADP, l'uso di dati reali o non anonimizzati in sviluppo e test non è consentito se non esplicitamente richiesto e autorizzato dal cliente.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Gestione dei Fornitori

Identificazione dei rischi relativi a terze parti esterne

Le valutazioni dei rischi di terzi che richiedono l'accesso ad ADP e / o informazioni sui clienti vengono periodicamente eseguite per determinare la loro conformità ai requisiti di sicurezza di ADP per i terzi e per identificare eventuali lacune nei controlli applicati. Se viene identificato un gap di sicurezza, vengono concordati nuovi controlli con tali soggetti esterni.

Accordi di sicurezza delle informazioni con parti esterne

ADP stipula accordi con tutte le terze parti che includono impegni di sicurezza adeguati per soddisfare i requisiti di sicurezza di ADP.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Gestione degli incidenti e dei miglioramenti della sicurezza delle informazioni

ADP ha una metodologia documentata per rispondere agli incidenti di sicurezza in modo tempestivo, coerente ed efficace.

In caso di incidente, un team predefinito di dipendenti ADP attiva un piano formale di risposta agli incidenti che affronta aree come:

- Escalation basate sulla classificazione della gravità dell'incidente
- Elenco contatti per la segnalazione / escalation di incidenti
- Linee guida per le risposte iniziali e follow-up con i clienti coinvolti
- Conformità alle leggi di notifica delle violazioni della sicurezza applicabili
- Registro delle indagini
- Ripristino del sistema
- Risoluzione dei problemi, rapporti e revisione
- Causa principale e rimedi
- Lesson Learned

Le Policy ADP definiscono un incidente di sicurezza, la gestione degli incidenti e tutte le responsabilità dei dipendenti in merito alla segnalazione di incidenti di sicurezza. ADP organizza regolarmente corsi di formazione per dipendenti e appaltatori di ADP per contribuire a garantire la consapevolezza dei requisiti di segnalazione. La formazione viene tracciata per garantire il completamento.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Aspetti di sicurezza delle informazioni della gestione della Resilienza del Business

ADP Business Resiliency Program

ADP è impegnata a mantenere i nostri servizi e le nostre operazioni in modo regolare, in modo da poter fornire ai nostri clienti il miglior servizio possibile. È la nostra priorità identificare - e mitigare - i rischi tecnologici, ambientali, di processo e sanitari che potrebbero ostacolare la fornitura dei nostri servizi aziendali. ADP ha creato un framework integrato che definisce i nostri processi di mitigazione, preparazione, risposta e recupero e include:

- Valutazione del rischio
- Analisi delle minacce al rischio
- Analisi dell'impatto sul business
- Pianificare lo sviluppo
- Pianificazione della continuità operativa
- Pianificazione del ripristino di emergenza
- Pianificazione della salute e della sicurezza
- Risposta nel mondo reale
- Gestione della crisi
- Risposta di emergenza
- Test e convalida
- Revisione
- Esercizio

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

Compliance

Compliance con le Policy di Sicurezza e gli Standard

ADP utilizza un processo per eseguire internamente revisioni della conformità su base periodica. Inoltre, ADP esegue un audit di tipo SOC1[2] tipo II su base periodica. Tali audit sono condotti da una nota società di revisione di terze parti e i rapporti di audit sono disponibili su base annuale per i clienti su richiesta, ove applicabile.

Compliance Tecnica

Per far rispettare la conformità tecnica con le migliori pratiche, ADP esegue scansioni di vulnerabilità della rete regolarmente pianificate. I risultati della scansione vengono quindi definiti in ordine di priorità e sviluppati in piani di azioni correttive con i team di hosting e la loro gestione.

Le scansioni delle vulnerabilità vengono eseguite su base regolare sia in ambienti interni che esterni. Inoltre, le scansioni del codice sorgente e i test di penetrazione vengono eseguiti in base al prodotto. Utilizzando strumenti specializzati di scansione delle applicazioni, le eventuali vulnerabilità a livello di applicazione vengono identificate, condivise con i team di gestione dello sviluppo del prodotto e incorporate nei processi di garanzia della qualità per azioni correttive. I risultati vengono analizzati e piani d'azione correttivi sviluppati e prioritari.

Retention dei Dati

La Policy di conservazione dei dati di ADP relativa alle informazioni sui clienti è progettata per conformarsi alle leggi applicabili. Alla fine di un contratto cliente, ADP rispetta i propri obblighi contrattuali relativi alle informazioni del cliente. ADP restituirà o consentirà al client di recuperare (mediante download di dati), tutte le informazioni del cliente richieste per la continuità delle attività commerciali del cliente (se non fornite in precedenza). Quindi, ADP distruggerà in modo sicuro le informazioni rimanenti sul cliente, tranne nella misura richiesta dalla legge applicabile, autorizzata dal cliente o necessaria ai fini della risoluzione delle controversie.

[2] Nel caso di alcuni servizi statunitensi offerti da ADP, è disponibile anche un report SOC 2 Type II.

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

ALLEGATO 3 – Elenco delle società del Gruppo vincolate dal codice applicabile ai responsabili del trattamento

ADP (Philippines), Inc	6/F Glorietta 2 Corporate Center, Palm Drive, Ayala Center, Makati City, Filippine, 1224
ADP (Suisse) SA	Lerzenstr. 10, 8953 Dietikon, Svizzera
ADP Canada Co.	3250 Bloor Street West, 16th Floor, Etobicoke, Ontario M8X 2X9, Canada
ADP Employer Services Belgium BVBA	Koningsstraat 97/4, 1000 Bruxelles, Belgio
ADP Employer Services Ceska Republika a.s.	Rohanske nabrezi 670/17, 18600 Praga 8, Repubblica Ceca
ADP Employer Services GmbH	Frankfurter Str. 227, 63263 Neu-Isenburg, Germania
ADP Employer Services Iberia, S.L.U.	Cami Antic de Valencia, 54 B, 08005 Barcellona, Spagna
ADP Employer Services Italia SPA	Viale G. Richard 5/A – 20143 Milano, Italia
ADP ES Tunisie SARL	MIRMAR Business City Lot B16 Centre Urbain Nord – 1003 Tunisi, Tunisia
ADP Europe, S.A.S.	31, avenue Jules Quentin, 92000 Nanterre, Francia
ADP France SAS	31, avenue Jules Quentin, 92000 Nanterre, Francia
ADP GlobalView B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Paesi Bassi
ADP GSI France SAS	31-41, avenue Jules Quentin, 92000 Nanterre, Francia
ADP HR and Payroll Services Ireland Limited	Unit 1, 42 Rosemount Park Dr, Rosemount Business Park, Dublin, D11 KC98, Ireland
ADP India Private Ltd.	Tamarai Tech Park, S.P. Plot No.16 to 20 & 20A, Thiru-Vi-Ka Industrial Estate, Inner Ring Road, Guindy, Chennai – 600 032 India
ADP International Services B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Paesi Bassi
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 Milano, Italia
ADP Payroll Services, Inc.	One ADP Boulevard, Roseland, NJ,USA 07068
ADP Polska Sp. zo.o.	Prosta 70, 00-838 Varsavia, Polonia
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, Londra, Inghilterra, WC2A 1LS

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.

ADP RPO, LLC	3401 Technology Drive, Findlay, OH 45840
ADP Screening and Selection Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Slovakia s.r.o.	Cernysevskeho 26, 851 01 Bratislava, Slovacchia
ADP Software Solutions Italia SRL	Via Oropa 28 – 10153 Torino, Italia
ADP, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
Automatic Data Processing (ADP) Romania SRL	4B Gara Herastrau St., 1st – 6th floor, District 2, Bucarest, Romania 020334
Automatic Data Processing Limited (Australia)	6 Nexus Court, Mulgrave, VIC 3170, Australia
Automatic Data Processing Limited (UK)	Syward Place, Pyrcroft Road, Chertsey, Surrey, KT16 9JT, England
Business Management Software Limited	2 Peterborough Business Park, Lynch Wood, Peterborough, Cambridgeshire, PE2 6FZ, England
Celergo Hungary kft	1093 Budapest, Kozraktar utca 30. 6. emelet., Cg. 01-090980824, Hungary
Celergo LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Celergo PTE. LTD.	62, Ubi Road 1, #11-07, Oxley Bizhub 2, Singapore 408734
Ridgenumber - Processamento de Dados LDA	Rua Brito e Cunha, 254 - 2º, 4450-082 Matosinhos, Portogallo
The Marcus Buckingham Company	8350 Wilshire Boulevard, #200, Beverly Hills, CA, USA 90211
VirtualEdge Corporation	One ADP Boulevard, Roseland, NJ, USA 07068

Copyright © 2021 ADP, Inc. Tutti i diritti riservati.