Cod de conduită ADP privind serviciile de prelucrare a datelor clientului

Cod de conduită ADP privind serviciile de prelucrare a datelor clientului 2
Introducere 2
Articol 1 – Domeniu de aplicare și implementare 2
Articol 2 – Contract de prestări servicii 3
Articol 3 – Obligații de conformitate 4
Articol 4 – Scopurile prelucrării datelor 6
Articol 5 – Cerințe de securitate 7
Articol 6 – Transparență acordată angajaților clienților 7
Articol 7 – Subîmputerniciți 8
Articol 8 – Supraveghere și conformitate 9
Articol 9 – Politici și proceduri 13
Articol 10 – Instruire 13
Articol 11 – Monitorizare și audit pentru verificarea conformității 13
Articol 12 – Probleme legale 16
Articol 13 – Sancțiuni pentru neconformitate 19
Articol 20 – Conflicte între Cod și Legislație Aplicabilă 19
Articol 15 – Modificări aduse Codului 20
Articol 16 – Implementare și Perioade de Tranziție 20
ANEXA 1 – Definiții BCR 23
ANEXA 2 – Măsuri de securitate 32
ANEXĂ 3 – Lista companiilor grupului obligate să respecte codul de conduită privind împuternicitul operatorului de date 63

Copyright © 2019 ADP, LLC. All rights reserved.

Cod de conduită ADP privind serviciile de prelucrare a datelor clientului

Introducere

ADP furnizează clienților săi o gamă largă de servicii privind managementul capitalului uman. ADP și-a luat angajamentul de a proteja datele cu caracter personal conform **Codului de conduită și etică ADP.**

Codul de conduită ADP privind serviciile de prelucrare a datelor clientului indică modalitatea de implementare a angajamentului în vederea prelucrării datelor cu caracter personal aparținând angajaților clientului, în legătură cu furnizarea serviciilor pentru clienți și activităților de susținere a clienților. În acest cadru, datele clienților sunt prelucrate de către ADP în calitate de împuternicit al operatorului de date în numele clienților săi.

Pentru regulamentele aplicabile procesului ADP de prelucrare a datelor cu caracter personal aparținând persoanelor cu care ADP are o relație comercială (ex. persoane care reprezintă clienți, furnizori, parteneri comerciali, alți profesioniști și consumatori) și alte persoane a căror date cu caracter personal sunt prelucrate de către ADP în contextul propriilor activități comerciale în calitate de operator de date, vezi *Cod de conduită ADP privind confidențialitatea datelor comerciale*.

Articol 1 – Domeniu de aplicare și implementare

Domeniu de aplicare datelor SEE	1.1	Codul tratează prelucrarea datelor cu caracter personal aparținând angajaților clienților de către ADP în calitate de împuternicit al operatorului de date pe parcursul furnizării serviciilor pentru clienți, unde astfel de date cu caracter personal sunt (a) supuse Legislației aplicabile SEE (sau au fost supuse Legislației aplicabile SEE înainte de transferul unor astfel de date cu caracter personal către o Companie a Grupului din afara SEE, într-o țară care nu era considerată a furniza un nivel adecvat de protecție a datelor de către instituțiile competente SEE); și (b) prelucrate conform unui Contract de prestări servicii care prevede în mod special faptul că prezentul Cod se aplică unor astfel de date cu caracter personal. În cazul în care există întrebări cu privire la aplicabilitatea Codului, resoponsabilul cu procesul de prelucrare se consultă cu echipa responsabilă cu confidențialitatea și gestiunea datelor înainte de începerea procesului de prelucrare.
Prelucrare electronică și pe hârtie	1.2	Codul se aplică prelucrării datelor clienților prin intermediul mijloacelor electronice și în sisteme de evidență pe hârtie.
Aplicabilitatea legislației locale	1.3	Niciun aspect prevăzut în Cod nu se interpretează astfel încât să preia drepturile sau remediile pe care le au angajații clienților conform Legislației aplicabile. În cazul în care Legislația aplicabilă asigură mai multă protecție decât acest Cod, atunci se vor aplica prevederile relevante ale Legislației aplicabile. În cazul în care Codul asigură mai multă protecție decât

Copyright © 2019 ADP, LLC. All rights reserved.

Legislația aplicabilă, sau cazul în care asigură măsuri de protecție suplimentare, drepturi sau remedii pentru persoane, atunci se aplică Codul.

Politici și recomandări 1.4 ADP poate completa Codul cu politici, standarde, recomandări sau instrucțiuni în concordanță cu Codul.

Responsabilitate 1.5 Codul este obligatoriu pentru ADP. Directorii executivi responsabili sunt răspunzători pentru conformitatea organizațiilor comerciale cu acest Cod. Personalul ADP trebuie să respecte Codul.

Data intrării în vigoare 1.6 Codul a fost aprobat de consilierul general, la momentul prezentării de către directorul responsabil cu confidențialitatea datelor, și a fost adoptat de Comitetul executiv ADP. Codul va intra în vigoare începând cu 11 aprilie 2018 (**Data intrării în vigoare**). Codul (inclusiv o listă a Companiilor Grupului implicate în prelicrarea datelor clienților) este publicat pe site-ul www.adp.com. Va fi pus la dispoziția persoanelor la cerere.

Codul este implementat de către Grupul ADP pe baza termenelor prevăzute la Art. 16.

Politici precedente 1.7 Codul completează politicile de confidențialitate ADP și prevalează asupra acordurile anterioare în măsura în care acestea sunt în contradicție cu acest Cod.

Rolul Entității delegate ADP 1.8 Automatic Data Processing Inc. a numit ADP Nederland B.V., cu sediul social în Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Olanda, în calitate de entitate delegată ADP, responsabilă cu punerea în aplicare a Codului în cadrul ADP Group și ADP Nederland, B.V., a acceptat numirea.

Articol 2 – Contract de prestări servicii

Contract de prestări servicii, subîmputerniciți 2.1 ADP prelucrează datele cu caracter persoanl doar pe baza unui contract de prestări servicii care incorporează cerințele contractante obligatorii pentru împuternicitul operatorului de date în conformitate cu legislația aplicabilă împuternicitului operatorului de date și pentru scopurile legitime specificate la Art. 4.

Entitatea contractantă ADP utilizează subîmputerniciți – subîmputerniciți ADP și subîmputerniciți terți – în furnizarea regulată a serviciilor pentru clienți. Contractele de prestări servicii certifică utilizarea unor astfel de subîmputerniciți, cu condiția ca entitatea contractantă ADP să rămână răspunzătoare față de client pentru performanța subîmputerniciților, în conformitate cu termenii contractului de prestări servicii.

Dispozițiile Art. 7 reglementează în continuare utilizarea

Copyright © 2019 ADP, LLC. All rights reserved.

subîmputerniciților.

Rezilierea contractului de prestări servicii

2.2 La momentul încetării furnizării serviciilor pentru clienți, ADP își îndeplinește obligațiile față de client asumate în contractul de prestări servicii în ceea ce privește returnarea datelor clienților prin furnizarea clientului datele necesare pentru continuitatea activităților comerciale proprii (dacă datele nu au fost furnizate anterior sau puse la dispoziția clientului via funcționalitate relevantă a produsului, precum abilitatea de a descărca datele clienților).

Atunci când obligațiile ADP prevăzute în contractul de prestări servicii au fost îndeplinite, ADP distruge în siguranță exemplarele rămase ale datelor clienților și (la cererea clientului) certifică clientului faptul că a procedat astfel. ADP poate păstra un exemplar al datelor clienților în măsura în care este necesar conform Legislației aplicabile, astfel cum a fost aprobat de client sau astfel cum este necesar pentru soluționarea disputelor. ADP nu va mai prelucra datele clienților, exceptând cazul în care este necesar pentru scopurile menționate mai sus. Obligațiile de confidențialitate ADP în temeiul contractului de prestări servicii vor continua atât timp cât ADP păstrează un exemplar ale datelor clienților.

Auditul modalităților de reziliere

2.3 În termen de 30 de zile de la rezilierea contractului de prestări servicii (exceptând cazul în care se impune altfel de către o autoritate competentă responsabilă cu protecția datelor), ADP, la cererea clientului sau autorității responsabile cu protecția datelor, permite audierea facilităților de prelucrare, în conformitate cu Art. 11.2 sau 11.3 (după caz) pentru a se verifica dacă ADP respectă obligațiile de reziliere prevăzute la Art. 2.2.

Articol 3 – Obligații de conformitate

Instrucțiunile clientului

3.1 ADP prelucrează datele clienților în numele clientului doar în temeiul contractului de prestări servicii, în conformitate cu orice instrucțiune documentată primită de la client sau după cum este necesar în vederea respectării Legislației aplicabile.

Conformitate cu Legislația aplicabilă

3.2 ADP prelucrează datele clienților în conformitate cu Legislația aplicabilă împuternicitului operatorului de date.

ADP răspune imediat și corespunzător la cererile de asistență ale clienților, după cum este necesar în mod legal, pentru a permite acestora să-și îndeplinească obligațiile în temeiul Legislației aplicabile operatorului de date, în conformitate cu contractul de prestări servicii.

Neconformitate,

3.3 Dacă o Companie a Grupului constată că Legislația aplicabilă

Copyright © 2019 ADP, LLC. All rights reserved.

efect adevrs semnificativ

împuternicitului operatorului de date dintr-o țară non-SEE, orice modificare adusă Legislației sau o instrucțiune a clienților pot avea un efect adevrs asupra abilității ADP de a-și îndeplini obligațiile conform 3.1, 3.2 sau 11.3, o astfel de Companie a Grupului notifică imediat entitatea delegată ADP și clientul, caz în care clientul va avea dreptul, în temeiul prezentului Cod, să suspende temporar transferul relevant ale datelor clienților, până când prelucrarea este ajustată pentru remedierea neconformității. În cazul în care nu este posibilă o ajustare, clientul are dreptul de a rezilia partea relevantă a procesului de prelucrare, în conformitate cu termenii contractului de prestări servicii. Aceste drepturi și obligații nu se aplică atunci când circumstanțele sau modificările aduse Legislației rezultă din cerințele obligatorii.

Cerere pentru divulgarea datelor clienților

3.4 În cazul în care ADP primește o cerere pentru divulgarea datelor clienților de la o autoritate de aplicare a legii sau organism de asigurare a securității statului al unei țări non-SEE (Autoritate), evaluează, de la caz la caz, dacă această cerere este valabilă și obligatorie din punct de vedere legal pentru ADP. Orice cerere care nu este valabilă și obligatorie din punct de vedere legal pentru ADP va fi anulată în conformitate cu Legislația aplicabilă.

În temeiul paragrafului următor, ADP informează imediat clientul, conducerea DPA și persoana competentă DPA, în temeiul Art. 11.3, cu privire la orice cerere de divulgare valabilă și obligatorie din punct de vedere legal și solicită autorității suspendarea pentru o perioadă rezonabilă de timp pentru a permite conducerii DPA să emită o opinie cu privire la valabilitatea divulgării cerute.

Dacă suspendarea aplicării și/sau notificarea conducerii DPA a unei cereri de divulgare este interzisă, precum în cazul unei interziceri conform legislației penale pentru a păstra confidențialitatea investigației de aplicare a legii, ADP va solicita autorității să anuleze această interzicere și va documenta înaintarea solicitării. ADP va furniza conducerii DPA informații generale cu privire la numărul și tipul cererilor de divulgare primite în următoarele 12 luni, în măsura permisă de legislația aplicabilă.

Articolul nu se aplică cererilor primite de ADP de la autorități pe parcursul normal al activităților în calitate de furnizor de servicii HCM (precum ordine judecătorești pentru sporirea veniturilor), pe care ADP poate continua să le furnizeze în conformitate cu Legislația aplicabilă, contractul de prestări servicii și instrucțiunilor clientului.

Întrebări adresate de clienți

3.5 ADP răspunde imediat și corespunzător la întrebările adresate de clienți cu privire la prelucrarea datelor clienților, în temeiul condițiilor contractului de prestări servicii.

Copyright © 2019 ADP, LLC. All rights reserved.

Articol 4 – Scopurile prelucrării datelor

Scopuri profesionale legitime

4.1 ADP prelucrează date cu caracter personal (inclusiv categorii speciale de date) aparținând angajaților clienților, după cum este necesar pentru furnizarea serviciilor pentru clienți, activităților pentru sprijinirea clienților și în următoarele scopuri suplimentare:

(a) Păstrare, arhivare și alte procese de prelucrare necesare pentru continuitatea activității și recuperarea în caz de dezastru, inclusiv întocmirea unor exemplare de rezervă și copii ale datelor cu caracter personal;

(b) Administrare și securitate a sistemelor și rețelelor, inclusiv monitorizarea infrastructurii, managementul identității și procedurilor de acreditare, verificarea și autentificarea și controlul accesului;

(c) Monitorizare și alte controale necesare pentru protejarea securității și integrității tranzacțiilor (ex. tranzacții financiare și transfer al banilor) inclusiv pentru respectarea obligației de diligență (precum verificarea identității persoanei și eligibilitatea persoanei de a primi produse și servicii (precum verificarea contractului de muncă sau stării contului);

(d) Executarea contractelor și protejarea ADP, asociaților, clienților, angajaților clienților și publicului împotriva furtului, răspunderii legale, fraudei sau abuzului, inclusiv: (i) detectarea, investigarea, prevenirea și atenuarea prejudiciilor rezultate din încercări de fraudă financiară, de identitate și alte amenințări asupra activelor financiare și fizice, identificatorilor de acces și sistemelor de informare; (ii) participarea la securitatea cibernetică externă, inițiative anti-fraudă și anti-spălare de bani; și (iii) după cum este necesar pentru protejarea intereselor vitale ale persoanelor, precum prin alertarea persoanelor în legătură cu o amenințare constatată asupra securității;

(e) Executarea și managementul procesului comercial intern ADP conducând la prelucrarea accidentală a datelor clienților pentru:

(1) Audiere internă și raportare consolidată;

(2) Conformitate legală, inclusiv completări, utilizări și divulgări obligatorii ale informațiilor care sunt impuse de Legislația aplicabilă;

Copyright © 2019 ADP, LLC. All rights reserved.

(3) De-identificarea datelor și agregarea datelor de-identificate pentru minimalizarea datelor și analizarea serviciilor;

(4) Utilizarea datelor de-identificate și agregate, astfel cum se permite de clienți, pentru a facilita analizarea, continuitatea și îmbunătățirea produselor și serviciilor ADP; și

(5) Facilitarea guvernanței corporative, inclusiv fuziuni, achiziții, cesionări și asocieri în participație.

Articol 5 – Cerințe de securitate

Securitatea datelor

5.1 ADP ia măsuri tehnice și organizatorice corespunzătoare pentru a proteja datele clienților împotriva utilizării necorespunzătoare sau distrugerea, pierderea, alterarea, divulgarea, achiziția sau accesul accidental, ilegal sau neautorizat pe parcursul prelucrării, care vor fi în conformitate cu cerințele Legislației aplicabile SEE sau alte cerințe stricte, astfel cum sunt impuse în temeiul contractului de prestări servicii. ADP, în orice caz, ia măsurile specificate în anexa 2 atașată la prezentul Cod, măsuri care pot fi modificate de ADP, cu condiția ca astfel de modificări să nu diminueze din punct de vedere material nivelul de securitate asigurat datelor clienților conform anexei 2.

Acces la date și confidențialitate

5.2 Personalul este autorizat să acceseze datele clienților doar în măsura în care este necesar pentru a servi scopurilor aplicabile de prelucrare a datelor conform Art. 4. ADP impune obligații de confidențialitate personalului care are acces la datele clienților.

Notificarea Încălcării securității datelor

5.3 ADP notifică clientul cu privire la încălcarea securității datelor imediat după constatarea unei astfel de încălcări, exceptând cazul în care o forță de ordine sau autoritate de supraveghere stabilește faptul că notificarea ar împiedica investigația sau cauza daune asupra securității naționale sau un abuz de încredere în domeniul industrial relevant. În acest caz, notificarea este întârziată, astfel cum s-a stabilit de forța de ordine sau autoritatea de supraveghere. ADP răspunde imediat întrebărilor adresate de client cu privire la încălcarea securității datelor.

Articol 6 – Transparență acordată angajaților clienților

Alte cereri ale angajaților clienților

6.1 ADP notifică imediat clientul cu privire la cererile sau reclamațiile depuse în legătură cu prelucrarea datelor cu caracter personal de către ADP care sunt primite direct de la angajații clientului fără a răspunde la astfel de

Copyright © 2019 ADP, LLC. All rights reserved.

secundare

cereri sau reclamații, exceptând cazul în care se prevede altfel în contractul de prestări servicii sau s-a indicat de client.

Dacă a fost indicat astfel de către client pentru a răspunde la cererile și reclamațiile depuse de angajații clientului, ADP se asigură de faptul că angajații clientului primesc toate informațiile necesare (precum punctul și procedura de contact) pentru ca angajații clienților să poată depună cererea sau reclamația.

Dispozițiile Art. 6.1 nu se aplică cererilor care sunt gestionate de ADP pe parcursul furnizării serviciilor pentru clienți și activităților de sprijinire ale clienților.

Articol 7 – Subîmputerniciți

Contracte încheiate cu subîmputerniciți

7.1 Subîmputerniciții pot prelucra doar datele clienților în conformitate cu contractul încheiat în acest sens. Contractul încheiat cu un subîmputernicit impune condiții similare de prelucrare a datelor care nu vor avea un nivel mai scăzut de protecție față de cel impus entității contractante ADP de contractul de prestări servicii și prezentul Cod.

Publicarea prezentării generale a subîmputerniciților

7.2 ADP publică o prezentare generală a categoriilor subîmputerniciților implicați în furnizarea serviciilor pentru clienți pe site-ul ADP. Prezentarea generală este actualizată imediat în caz de modificări.

Notificarea noilor subîmputerniciți și dreptul de opoziție

7.3 ADP notifică clientul cu privire la noii împuterniciți angajați de ADP pentru furnizarea serviciilor pentru clienți. În termen de 30 de zile de la primirea unei astfel de notificări, clientul se poate opune angajării unor astfel de subîmputerniciți prin trimiterea unei notificări scrise către ADP invocând motivele obiective justificabile cu privire la inabilitatea subîmputerniciților de a proteja datele clienților în conformitate cu obligațiile prevăzute în contract, în temeiul Art. 7.1. În cazul în care părțile nu pot ajunge la o soluție comună, ADP, conform propriei opinii, va evita acordarea permisiunii subîmputerniciților de a accesa datele clienților sau de a permite clientului să încheie furnizarea serviciilor pentru clienți, în conformitate cu termenii contractului de prestări servicii.

Excepții

7.4 Dispozițiile secțiunii 7 nu se aplică în măsura în care clientul instruiește ADP să permită părților terțe să prelucreze datele clienților conform unui contract pe care clientul l-a încheiat direct cu o parte terță (ex. furnizor de beneficii terț).

Copyright © 2019 ADP, LLC. All rights reserved.

Articol 8 – Supraveghere și conformitate

Director responsabil cu protecția vieții private

8.1 Grupul ADP angajează un director responsabil cu protecția vieții private care este responsabil pentru:

(a) Prezidarea consiliului de conducere responsabil cu protecția vieții private;

(b) Supravegherea conformității cu acest Cod;

(c) Supravegherea, coordonarea, comunicarea și consultarea cu membrii relevanți din cadrul rețelei responsabile cu protecția vieții private în legătură cu aspectele protecției vieții private și datelor;

(d) Furnizarea rapoartelor anuale privind riscurile și problemele de conformitate ale protecției datelor Comitetului Executiv ADP;

(e) Coordonarea investigațiilor sau anchetelor oficiale privind prelucrarea datelor clienților de către o autoritate guvernamentală, împreună cu membrii relevanți ai Rețelei responsabile cu protecția vieții private și departamentului juridic ADP;

(f) Soluționarea conflictelor dintre Cod și Legislația Aplicabilă;

(g) Monitorizarea procesului prin care sunt realizate evaluările impactului asupra protecției datelor și revizuirea PIAs, după caz;

(h) Monitorizarea documentației, notificarea și comunicarea încălcărilor securității datelor;

(i) Consilierea cu privire la procese de gestiune a datelor, sisteme și programe pentru a implementa cadrul pentru gesiunea protecției vieții private și a datelor, astel cum s-a stabilit de consiliul responsabil cu protecția vieții private, inclusiv:

(1) Menținerea, actualizarea și publicarea Codului și politicilor și standardelor asociate;

(2) Consilierea cu privire la programele necesare pentru colectarea, menținerea și actualizarea arhivelor care conțin informații cu privire la structura și funcționarea tuturor sistemelor care prelucrează date ale clienților;

(3) Furnizarea, asistarea sau consilierea cu privire la instruirea pentru protecția vieții private acordată personalului, astfel încât să înțeleagă și să respecte responsabilitățile, în conformitate cu acest Cod;

(4) Colaborarea cu departamentul de audit intern și alte departamente pentru a elabora și menține un program de asigurare adecvat pentru a monitoriza, audia și raporta conformitatea cu acest Cod și

Copyright © 2019 ADP, LLC. All rights reserved.

pentru a permite ADP să verifice și să certifice o astfel de conformitate, după cum este necesar;

(5) Implementarea procedurilor, după caz, pentru a răspunde întrebărilor, preocupărilor și plângerilor care au în vedere protecția vieții private și a datelor; și

(6) Consilierea cu privire la sancțiunile adecvate pentru încălcarea Codului (*ex.*, standarde disciplinare);

Rețea responsabilă cu protecția vieții private

8.2 ADP stabilește o rețea responsabilă cu protecția vieții private pentru a asigura conformitatea cu acest Cod în cadrul organizației globale ADP.

Rețeaua responsabilă cu protecția vieții private elaborează și menține un cadru pentru a oferi asistență directorului responsabil cu protecția vieții private și pentru a supraveghea sarcinile prevăzute in Articolul 13.1 și alte sarcini considerate conrespunzătoare pentru a menține și actualiza acest Cod. Membrii rețelei responsabile cu protecția vieții private, conform rolului în cadrul regiunii sau organizației, îndeplinesc următoarele sarcini suplimentare:

(a) Țin sub supraveghere implementarea proceselor de gestiune a datelor, sistemele și programele care permit aderarea la Cod de către companiile din cadrul grupului în regiunile sau organizațiile respective;

(b) Susțin și evaluează gestiunea și comformitatea proceselor de gestiune a protecției vieții private și a datelor de către Companii în cadrul propriilor regiuni;

(c) Ofertă consultanță în mod regulat administratorilor și directorului responsabil cu respectarea vieții private în legătură cu riscurile regionale sau locale la adresa vieții private și problemele de conformitate;

(d) Verifică faptul că inventarele corespunzătoare ale sistemelor care prelucrează date cu caracter personal sunt menținute;

(e) Răspund cererilor de aprobare sau consultanță;

(f) Furnizează informațiile necesare de către directorul responsabil cu respectarea vieții private în vederea întocmiri raportului anual cu privire la respectarea vieții private;

(g) Însoțesc directorul responsabil cu protecția vieții private în caz de investigații sau dispute oficiale înaintate de autoritățile guvernamentale;

(h) Elaborează și publică politici și standarde corespunzătoare regiunilor și organizațiilor proprii;

(i) Oferă consultanță companiilor din cadrul grupului cu privire la reținere

Copyright © 2019 ADP, LLC. All rights reserved.

și distrugere;

(j) Notifică directorul responsabil cu protecția vieții private cu privire la plângeri și asistă la soluționarea plângerilor; și

(k) Însoțesc directorul, membrii și administratorii responsabili cu protecția vieții private și alte persoane, după cum este necesar pentru a:

(1) Permite Companiilor din cadrul Grupului sau altor organizații să respecte Codul, pe baza instrucțiunilor, programelor și training-urilor elaborate;

(2) Împărtășească cele mai bune practice în vederea gestiunii protecției vieții private și a datelor în cadrul regiunii;

(3) Confirma faptul că cerințele pentru protecția vieții private și a datelor sunt avute în vedere ori de câte ori este implementată o nouă tehnologie în cadrul Companiilor Grupului sau organizațiilor; și

(4) Însoțesc administratorii responsabili cu protecția vieții private, Companiile Grupului, unitățile comerciale, departamentele funcționale și personalul de achiziții în timpul utilizării subîmputerniciților.

Administratori responsabili cu protecția vieții private

8.3 Administratorii responsabili cu protecția vieții private sunt directorii executivi ADP numiți de către directorii executivi Responsabili și/sau Conducerea Executivă ADP pentru a implementa și pune în aplicare Codurile în cadrul unei unități operaționale sau departament funcțional ADP. Administratorii responsabili cu protecția vieții private sunt responsabili cu implementarea eficientă a Codurilor în cadrul unităților operaționale și depatamentelor funcționale relevante. În principal, Administratorii responsabili cu protecția vieții private trebuie să verifice dacă controalele de gestiune a protecției vieții private și datelor sunt implementate în toate practicile comerciale care au un impact asupra datelor cu caracter personal și dacă resursele și bugetul adecvat sunt puse la dispoziție în vederea respectării obligațiilor Codurilor. Administratorii responsabili cu protecția vieții private pot împărți sarcini și aloca resursele corespunzătoare, după caz, în vederea respectării responsabilităților și atinge scopurile de conformitate.

Responsabilitățile administratorilor includ:

(a) Monitorizarea gestiunii și conformității protecției vieții private și datelor în cadrul Companiei Grupului, unității operaționale sau departamentului functional și verificarea faptului că toate procesele, sistemele și programele elaborate de echipa responsabilă cu confidențialitatea și gestiunea datelor au fost implementate în mod eficient;

Copyright © 2019 ADP, LLC. All rights reserved.

(b) Confirmarea faptului că sarcinile de gestiune și conformitate a protecției vieții private și datelor sunt delegate corespunzător în cursul normal al activității și pe parcursul și după restructurarea organizațională, de externalizare, fuziune, achiziții și dezinvestiții;

(c) Colaborarea cu directorul responsabil cu protecția vieții private și membrii relevanți din cadrul rețelei pentru a înțelege și aduce în discuție noi cerințe legale și verificarea faptului că procesele de gestiune a vieții private și datelor sunt actualizate pentru a aborda schimbarea circumstanțelor și cerințelor legale și de reglementare;

(d) Consultarea cu directorul responsabil cu protecția vieții private și membrii relevanți ai rețelei în toate cazurile în care există in conflict actual sau potential între Legislația Aplicabilă și acest Cod;

(e) Monitorizarea subîmputerniciților utilizați de Compania Grupului, unitatea operațională sau departamentul functional pentru a confirma conformitatea continuă a subîmputerniciților cu acest Cod și contractele subîmputerniciților;

(f) Confirmarea faptului că întregul personal din cadrul Companiei Grupului, unității operaționale sau departamentului functional au finalizat cursurile de instruire cu privire la protecția vieții private; și

(g) Impunerea ștergerii, distrugerii, de-identificării sau transferării datelor cu caracter personal, astfel cum se prevede în Articolul 2.2.

Directori executivi responsabili

8.4 Directorii executivii responabili, în calitate de directori ai unităților operaționale sau departamentelor funcționale, sunt responsabili de a se asigura că gestiunea protecției vieții private și datelor este implementată în cadrul propriilor organizații. Fiecare director executiv responsabil (a) numește administratorii responsabili cu protecția vieții private, (b) se asigură de faptul că resursele și bugetul adecvat sunt puse la dispoziție în vederea verificării conformității, și (c) acordă asistență administratorului responsabil cu protecția vieții private în măsura necesară remedierii problemelor de conformitate și gestiunii riscului.

Consiliu de conducere responsabil cu protecția vieții private

8.5 Directorul responsabil cu protecția vieții private prezidează un Consiliu de Conducere format din administratori, membrii ai Rețelei aleși de acesta și alte persoane care ar fi necesar să participe la obiectivul Consiliului. Consiliul de conducere elaborează și menține un cadru pentru a susține activitățile în măsura necesară conformității unităților operaționale și departamentelor funcționale cu acest Cod, pentru a îndeplini sarcinile prevăzute în acest Cod și pentru a oferi asistență directorului responsabil cu protecția vieții private.

Membrii ai Rețelei și

8.6 Dacă, într-un moment, nu există un director numit sau în capacitatea de a îndeplini funcțiile atribuite rolului, atunci Consiliul General numește o

Copyright © 2019 ADP, LLC. All rights reserved.

Administratori responsabili cu protecția vieții private

persoană care va acționa în calitate de director interimar. Dacă, într-un moment, nu există un membru al Rețelei numit pentru o regiune sau organizație anume, Directorul îndeplinește sarcinile atribuite unui astfel de membru, astfel cum sunt prevăzute în Articolul 8.2.

Dacă, într-un moment, nu există un administrator responsabil cu protecția vieții private numit pentru o Companie a grupului, unitate operațională sau departament funcțional, directorul executiv responsabil numește o persoană corespunzătoare care să îndeplinească sarcinile prevăzute la Articolul 8.3.

Poziții obligatorii

8.7 În cazul în care membrii Rețelei, ex. responsabili cu protecția vieții private conform Legislației Aplicabile SEE, ocupă poziția în temeiul legii, atunci își vor îndeplini responsabilitățile postului în măsura în care nu contravin pozițiilor obligatorii.

Articol 9 – Politici și proceduri

Politici și proceduri

9.1 ADP elaborează și implementează politici, standarde, orientări și proceduri pentru a fi în conformitate cu acest Cod.

Informații despre sistem

9.2 ADP pune la dispoziție informații cu privire la structura și modalitățile de funcționare ale tuturor sistemelor și proceselor care prelucrează date cu caracter personal, precum inventare ale sistemelor și procese care au un impact asupra datelor cu caracter personal, împreună cu informații generate pe parcursul evaluărilor impactului asupra protecției datelor. O copie a acestor informații va fi furnizată Conducerii DPA sau unui competent DPA în vederea efectuării auditului, conform Articolului 11.3, la cerere.

Articol 10 – Instruire

Instruire

10.1 ADP asigură instruirea în legătură cu acest Cod și obligațiile de confidențialitate și securitate întregului personal care are acces la datele clienților sau responsabilitățile asociate cu prelucrarea datelor clienților.

Articol 11 – Monitorizare și audit pentru verificarea conformității

Audituri interne

11.1 ADP audiază procesele și procedurile operaționale care implică prelucrarea datelor clienților în vederea conformității cu acest Cod. În special:

(a) Auditurile pot fi efectuate pe parcursul activităților regulate ale auditului intern ADP (inclusiv prin utilizarea părților terțe independente), alte

Copyright © 2019 ADP, LLC. All rights reserved.

echipe interne implicate în funcțiile de asigurare și în mod ad-hoc la cererea directorului responsabil cu protecția vieții private;

(b) Directorul responsabil cu protecția vieții private poate solicita ca un audit să fie efectuat de către un auditor extern și informează directorul executiv responsabil al unității operaționale relevante și/sau Comitetul Executiv ADP, după caz;

(c) Standardele de independență, integritate și confidențialitate profesionale aplicabile vor fi ținute sub observație pe parcursul procesului de audit;

(d) Directorul responsabil cu protecția vieții private și membrii corespunzători ai Rețelei vor fi informați în legătură cu rezultatele auditurilor;

(e) În măsura în care auditul revelă cazuri de neresepctare a prezentului Cod, constatările în cauză vor fi raportate administratorilor și directorilor executivi responsabili. Administratorii vor coopera cu directorul pentru a elabora și pune în aplicare un plan de remediere corespunzător;

(f) O copie a rezultatelor auditului cu privire la respectarea prezentului Cod vor fi furnizate conducerii sau unei persoanei competente DPA, la cerere, conform Art. 11.3.

Audit solicitat de client

11.2 ADP va răspunde cererilor de audit înaintate de client, astfel cum se descrie la Art. 11.2. ADP va răspunde întrebărilor adresate de client în ceea ce privește prelucrarea datelor clienților de către ADP. În cazul în care clientul consideră în mod rezonabil faptul că răspunsurile acordate de către ADP necesită o analiză ulterioară, ADP, în acord cu clientul:

(a) Pune la dispoziție unităților pentru prelucrarea datelor clienților în vederea efecturării unui audit de către un evaluator terț independent, acceptat de ADP și care este supus unei obligații de confidențialitate, angajat de client. Clientul va furniza directorului responsabil o copie a raportului de audit care va fi tratată ca fiind o informație confidențială. Auditurile sunt efectuate o dată pe an/client, pe parcursul desfășurării contractului de prestări servicii și programului de lucru și este condiționat de (i) o cerere scrisă transmisă către ADP cu cel puțin 45 de zile înainte de data propusă pentru audit; (ii) un plan de audit scris și detaliat evaluat și aprobat de organizația de securitate ADP; și (iii) politicile de securitate la fața locului ADP. Astfel de audituri vor avea loc doar în prezența unui reprezentant al departamentului de securitate ADP, echipei responsabile cu confirdențialitatea și gestiunea datelor sau unei persoane desemnate de un reprezentant corespunzător. Auditurile nu sunt permise pentru a înterupe activitățile de prelucrare ADP sau compormite securitatea și confidențialitatea datelor cu caracter personal aparținând altor clienți ADP; sau

Copyright © 2019 ADP, LLC. All rights reserved.

(b) ADP furnizează clientului o declarație emisă de un evaluator terț independent calificat, certificând faptul că procesele și procedurile comerciale ADP care implică prelucrarea datelor clienților sunt în conformitate cu acest Cod.

ADP poate impune clienților o taxă pentru efectuarea unui astfel de audit.

Art. 11.2 înlocuiește sau clarifică drepturile de audit pe care clienții le pot avea în conformitate cu Legislația aplicabilă și contractele de prestare servicii. În caz de contradicții, dispozițiile Legislației aplicabile și contractele de prestare servicii prevalează.

Audituri efectuate de DPA

11.3 Orice DPA dintr-o țară SEE care este competentă să audieze un client ADP va fi autorizată să audieze transferul relevant de date pentru conformitatea cu acest Cod, în temeiul acelorași condiții care s-ar aplica unui audit efectuat de DPA clientului, conform legislației aplicabile operatorului de date.

Pentru facilitatea unui astfel de audit:

(a) ADP și clientul vor colabora cu bună-credință pentru a încerca să soluționeze cererile prin furnizarea informațiilor către DPA, precum rapoarte de audit, și să faciliteze discuțiile dintre DPA și experții clienților și ADP care pot evalua controalele de securitate, confidențialitate și operaționale în vigoare. Clientul va avea acces la datele clienților în conformitate cu contractul de prestări servicii și poate acorda accesul reprezentanților DPA;
(b) Dacă informațiile puse la dispoziție prin intermediul acestor mecanisme sunt insuficiente pentru a aborda obiectivele declarate, ADP va acorda DPA oportunitatea de a comunica cu auditorul ADP;
(c) Dacă acest lucru este considerat a fi insuficient, ADP va acorda DPA dreptul direct de a examina unitățile ADP de prelucrare a datelor utilizate pentru prelucrarea datelor clienților pe baza unei notificări prealabile adecvate, în timpul programului de lucru și respectând pe deplin confidențialitatea informațiilor obținute și secretelor comerciale ADP. DPA poate accesa datele clienților aparținând clientului.

Art. 11.3 înlocuiește sau clarifică drepturile de audit pe care DPA le poate avea în conformitate cu Legislația aplicabilă și contractele de prestare servicii. În caz de contradicție, dispozițiile Legislației aplicabile prevalează.

Raport anual

11.4 Directorul responsabil cu protecția vieții private întocmește un raport anual pentru Comitetul Executiv ADP cu privire la conformitatea cu acest Cod, riscurile protecției datelor și alte aspecte relevante. Acest raport va reflecta

Copyright © 2019 ADP, LLC. All rights reserved.

informațiile furnizate de Rețeaua responsabilă cu protecția vieții private și alte informații în legătură cu dezvoltările locale și aspectele specifice din cadrul Companiilor Grupului.

Remediere 11.5 ADP ia toate măsurile necesare pentru a remedia cazurile de neconformitate cu acest Cod identificate pe parcursul auditurilor pentru verificarea conformității.

Articol 12 – Probleme legale

Drepturile angajaților clienților 12.1 În cazul în care ADP încalcă Codul în legătură cu datele cu caracter personal ale unui angajat al clientului acoperit de acest Cod, angajatul clientului poate, în calitate de beneficiar terț, să pună în aplicare Art. 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, 12.8 și 14.3 împotriva entității contractante ADP.

În măsura în care angajatul clientului poate pune în aplicare astfel de drepturi împotriva entității contractante ADP, entitatea contractantă ADP nu se poate baza pe o încălcare a propriilor obligații de către un subîmputernicit pentru a evita răspunderea, exceptând cazul în care apărarea unui subîmputernicit ar reprezenta o apărare a ADP. ADP poate impune o apărare sau un drept pus la dispoziția clientului. ADP poate impune o apărare pe care ADP ar fi putut să o impună împotriva clientului (precum neglijență contributorie), în apărarea împotriva afirmației persoanei afectate.

Procedură privind reclamațiile 12.2 Angajații clienților pot depune reclamații scrise în legătură cu orice pretenție pe care o au în conformitate cu Art. 12.1 către echipa responsabilă cu confidențialitatea și gestiunea datelor via mail sau email la adresa indicată în închierea Codului. De asemenea, angajații clienților pot depune o reclamație sau cerere autorităților sau instanțelor, în conformitate cu Art. 12.3 al acestui Cod.

Echipa responsabilă cu confidențialitatea și gestiunea datelor va fi responsabile cu tratarea reclamațiilor. Fiecare reclamație va fi acordată unui membru din cadrul personalului (fie din cadrul echipei responsabile cu confidențialitatea și gestiunea datelor sau din cadrul unității operaționale sau departamentului funcțional aplicabil). Personalul va:

(a) Confirma imediat primirea reclamației;

(b) Analiza reclamația și, după caz, va porni o investigație;

(c) Dacă declarația se bazează pe motive întemeiate, înștiințează administratorul și membrul relevant din cadrul Rețelei, astfel încât să

Copyright © 2019 ADP, LLC. All rights reserved.

poată fi elaborat și executat un plan de remediere: și

(d) Păstra rapoarte ale reclamațiile primite, răspunsurilor acordate și acțiunilor de remediere luate de către ADP;

ADP va depune toate eforturile pentru a soluționa reclamațiile fără întârziere nejustificată, astfel încât un răspuns să fie acordat angajaților clienților în termen de patru săptămâni de la data la care a fost depusă reclamația. Răspunsul va fi în scris și trimis angajaților clienților prin mijloacele prin care angajații clienților au contactat ADP (ex., via mail sau email). Răspunsul va sublinia măsurile pe care ADP le-a luat în vederea investigării reclamației și va indica decizia ADP cu privire la măsurile (dacă există) pe care le va lua pentru a soluția reclamația.

În cazul în care ADP nu poate duce până la capăt investigația în termen de patru săptămâni, va angajații clienților în termen de patru săptămâni cu privire la faptul că investigația este în curs de desfășurare și un răspuns va fi acordat în următoarele opt săptămâni.

Dacă răspunsul la reclamație nu este satisfăcător pentru angajații clienților (ex. cererea este respinsă) sau ADP nu respectă condițiile procedurii privind reclamațiile prevăzute la Art. 12.2, angajații clienților pot depune o reclamație sau cerere către autorități sau instanțe de judecată, în conformitate cu Articolul 12.3.

Jurisdicție pentru reclamațiile depuse de angajații clienților

12.3 Angajații clienților sunt încurajați să urmeze mai întâi procedura privind reclamațiile prevăzută la Articolul 12.2 din acest Cod înainte de a depune o reclamație sau cerere către autorități sau instanțe de judecată.

Angajații clienților pot, la propria alegere, să depună o reclamație în temeiul Art. 12.1 către:

(i) DPA în țara în care își are reședință obișnuită, locul de muncă sau locul unde a survenit încălcarea, împotriva entității contractante ADP sau entității delegate ADP; sau

(ii) Conducerea ADP sau instanțele din Olanda, însă în acest caz doar împotriva entității delegate ADP.

Angajații clienților pot, la propria alegere, să depună o reclamație în temeiul Art. 12.1 către:

(iii) instanțele din țara în care își are reședință obișnuită sau țara de origine a transferului, în temeiul acestui Cod, împotriva entității contractante ADP sau entității delegate ADP; sau

(iv) Conducerea ADP sau instanțele din Olanda, însă în acest caz doar împotriva entității delegate ADP.

Copyright © 2019 ADP, LLC. All rights reserved.

DPA și instanțele de judecată vor aplica propriile legi substanțiale și procedurale asupra disputei. Orice alegere făcută de către angajații clienților nu vor prejudicia drepturile substanțiale sau procedurale pe care părțile le poate avea în temeiul Legislației aplicabile.

Drepturile clienților

12.4 Clientul poate pune în aplicare acest Cod împotriva (i) entității contractante ADP sau, (ii) entității delegate ADP înaintea conducerii DPA sau instanțelor din Olanda, însă doar dacă entitatea contractantă ADP nu este stabilită într-o țară SEE. Entitatea delegată ADP se asigură de faptul că sunt luate toate măsurile pentru a soluționarea încălcările acestui Cod de către entitatea contractantă ADP sau altă Companie implicată.

Entitatea contractantă și entitatea delegată ADP nu se pot baza pe o încălcare a propriilor obligații de către o altă companie a grupului sau un subîmputernicit pentru a evita răspunderea, exceptând cazul în care apărarea unei companii sau subîmputernicit ar reprezenta o apărare a ADP.

Remedii disponibile, sarcina probei pentru angajații clienților

12.5 În cazul în care un angajat al unui client are o pretenție în temeiul Art. 12.1, un astfel de angajat al clientului are dreptul la compensarea pagubelor în măsura prevăzută de legislația SEE aplicabilă.

În cazul în care angajații clientului depun o cerere de despăgubire în temeiul Articolului 12.1, este responsabilitatea angajaților clienților de a demonstra faptul că au a suferit pagube și de a stabili fapte care să indice că pagubele au survenit ca urmare a încălcării acestui Cod. Ulterior, este responsabilitatea entității contractante ADP (sau entității delegate ADP, după caz) să dovedească faptul că pagubele suferite de angajații clienților ca urmare a încălcării prezentului Cod nu pot fi atribuite companiei grupului sau unui subîmputernicit sau de a pretinde alte apărări aplicabile.

Despăgubirea clienților

12.6 În caz de încălcare a prezentului Cod și în temeiul condițiilor contractului de prestare servicii, clienții au dreptul la despăgubiri pentru daunele directe în conformitate cu dispozițiile contractului de prestare servicii.

Asistență reciprocă

12.7 Toate Companiile Grupului, după cum este necesar, cooperează și asistă în măsura posibilă la (a) gestiunea solicitărilor, reclamațiilor sau cererilor înaintate de un client sau angajați ai clienților sau (b) conformitatea cu o investigație sau anchetă ilegală de către o persoană competentă DPA sau autoritate guvernamentală.

Compania Grupului care primește o solicitare de informații în temeiul Art. 6.1, sau o reclamație sau cerere în temeiul Art. 12.2 sau 12.3, este responsabilă cu gestionarea comunicării cu clientul sau cu angajații clientului în legătură cu solicitarea sau cererea, exceptând cazul în care

Copyright © 2019 ADP, LLC. All rights reserved.

circumstanțele prevăd altfel sau astfel cum se indică de echipa responsabilă cu confidențialitatea și gestiunea datelor.

Recomandările DPA și decizii obligatorii 12.8 ADP, cu bună credință, cooperează cu și depune toate eforturile pentru a respecta recomandările oferite de conducerea DPA și persoana competentă DPA în temeiul Articolului 12.23 privind interpretarea și aplicarea acestui Cod. ADP se conformează deciziilor obligatorii DPA.

Legislația aplicabilă acestui Cod 12.9 Acest Cod este reglementat de și interpretat în conformitate cu legislația olandeză.

Articol 13 – Sancțiuni pentru neconformitate

Neconformitate 13.1 Neconformitatea personalului cu acest Cod poate avea ca rezultat aplicarea unor măsuri disciplinare corespunzătoare, în conformitate cu Legislația Aplicabilă și politicile ADP, până la și inclusiv rezilierea relației sau contractului de muncă.

Articol 20 – Conflicte între Cod și Legislație Aplicabilă

Conflict între Cod și Legislație 14.1 În cazul în care există un conflict între Legislația Aplicabilă și acest Cod, directorul executiv responsabil sau administratorul responsabil cu protecția vieții private se consultă cu directorul responsabil cu protecția vieții private, membrul (membrii) relevant(ți) din cadrul Rețelei (după caz) și Departamentul Juridic al unității operaționale pentru a stabili modalitatea de conformitate cu prezentul Cod și soluționarea conflictului în măsura în care este posibil, luând în conisderare cerințele juridice aplicabile ADP.

Noi cerințe juridice contradictorii 14.2 Membrii Departamentului Juridic, responsabilii ADP cu securitatea datelor și administratorii responsabili cu protecția vieții private informează imediat echipa responsabilă cu confidențialitatea și gestiunea datelor cu privire la noile cerințe juridice identificate care pot interfera cu abilitatea ADP de a respecta acest Cod.

Administratorii relevanți responsabili cu protecția vieții private, după consultarea cu Departamentul Juridic, informează imediat directorii executivi responsabili cu privire la noile cerințe juridice identificate care pot interfera cu abilitatea ADP de a respecta acest Cod.

Raportare către Conducerea DPA 14.3 În cazul în care ADP constată faptul că legislația aplicabilă împuternicitului operatorului de date sau orice altă modificare a legislației poate avea un efect advers asupra abilității ADP de a-și respecta obligațiile în temeiul 3.1, 3.2 sau 11.3, ADP va raporta acest aspect Conducerii DPA.

Copyright © 2019 ADP, LLC. All rights reserved.

Articol 15 – Modificări aduse Codului

Aprobarea modificărilor

15.1 Orice schimbare materială adusă acestui Cod necesită aprobarea prealabilă a directorului și Consiliului General, precum și adoptarea de către Comitetul Executiv ADP și comunicată Companiilor Grupului. Modificările nemateriale aduse Codului pot fi efectuate în urma aprobării prealabile a directorului responsabil. Entitatea delegată ADP notifică anual conducerea DPA cu privire la modificările aduse Codului.

În cazul în care oricare dintre modificări are un impact semnificativ asupra condițiilor de prelucrare ale serviciilor pentru clienți, ADP va informa imediat conducerea DPA, inclusiv o prezentare generală a acestei modificări, precum și notificarea clientului cu privire la modificarea în cauză. În termen de 30 de zile de la primirea notificări, clientul poate obiecta împotriva unei astfel de modificări prin furnizarea unei notificări scrise către ADP. În cazul în care părțile nu pot ajunge la o soluție comună, ADP aplică o măsură alternativă pentru transferul datelor. În cazul în care nu poate fi pusă în aplicare nicio măsură alternativă, clientul va avea dreptul, conform acestui Cod, să suspende transferul relevant al datelor clienților către ADP. În cazul în care nu este posibilă suspendarea transferului datelor, ADP permite clientului să înceteze furnizarea serviciilor pentru clienți, îm temeiul contractului de prestare servicii.

Data de intrare în vigoare a modificărilor

15.2 Orice modificare intră în vigoare după ce a fost aprobată în conformitate cu Articolul 15.1 și publicată pe site-ul www.adp.com și comunicată clienților.

Versiuni prealabile

15.3 Orice solicitare, reclamație, cerere a unui angajat al clientului care implică acest Cod este evaluată în conformitate cu versiunea acestui Cod în vigoare la momentul depunerii solicitării, reclamației sau cererii.

Articol 16 – Implementare și Perioade de Tranziție

Implementare

16.1 Implementarea acestui Cod este efectuată sub supravegherea administratorilor, asistați de echipa responsabilă cu confidențialitatea și gestiunea datelor. Exceptând astfel cum se indică mai jos, va exista o perioadă de tranziție de optsprezece luni de la data intrării în vigoare (astfel cum se prevede la Articolul 1.6) pentru conformitatea cu acest Cod.

În acest sens, cu excepția cazului în care se indică altfel, în cadrul celor optseprezece luni de la data intrării în vigoare, prelucrarea datelor clienților este efectuată în conformitate cu acest Cod, iar Codul este pe deplin în

Copyright © 2019 ADP, LLC. All rights reserved.

vigoare. Pe parcursul perioadei de tranziție, Codul intră în vigoare pentru o Companie a Grupului imediat ce respectiva Companie finalizează sarcinile necesare pentru implementarea integrală și a notificat în mod corespunzător directorul responsabil cu protecția vieții private.

Companii noi

16.2 Orice entitate care devine o Companie a Grupului după data intrării în vigoare implementează acest Cod în doi ani de la numire.

Entități cesionate

16.3 O entitate cesionată va rămâne acoperite de acest Cod după cesionare pentru o perioadă impusă de ADP în vederea separării prelucrării datelor clienților referioare la o astfel de entitate cesionată.

Perioadă de tranziție pentru acordurile existente

16.4 Acolo unde există acorduri cu subîmputerniciți sau alte părți terțe afectate de acest Cod, prevederile acordurilor vor prevala până în momentul în care acestea vor fi reînnoite în cursul normal al activității, cu condiția ca toate acordurile existente să fie în conformitate cu acest Cod în termen de 18 luni de la data intrării în vigoare.

Detalii de contact

Echipa responsabilă cu confidențialitatea și gestiunea datelor:
privacy@adp.com

Entitate Delegată ADP
ADP Nederland B.V.
Lylantse Baan 1, 2908
LG CAPELLE AAN DEN IJSSEL
OLANDA

Interpretări

INTERPRETAREA PREZENTULUI COD:

(i) Exceptând cazul în care contextul impune altfel, toate trimiterile la un anumit Articol sau Anexă sunt trimiteri la acel Articol sau Anexă din sau la prezentul document, cu modificările ulterioare;
(ii) Titlurile sunt incluse exclusiv pentru simplificare și nu trebuie să fie utilizate în construirea niciunei prevederi a prezentului Cod;
(iii) Dacă un cuvânt sau o frază este definită, celelalte forme gramaticale au un sens corespunzător;
(iv) Genul masculin include genul feminin;
(v) Cuvintele „include”, „inclusiv” și alte cuvinte următoare sunt construite fără limitare la generalitatea oricărui cuvânt sau concept următor și invers;

Copyright © 2019 ADP, LLC. All rights reserved.

(vi) Cuvântul „scris” include orice comunicare documentată, scrisă, contract, raport electronic, semnătură electronică, copie fax sau alt instrument valabil din punct de vedere legal și aplicabil, indiferent de format;

(vii) O trimitere la un document (inclusiv, fără limitare, o trimitere la prezentul Cod) este reference to a document (including, without limitation, a reference to this Code) este la documentul modificat, variat, completat sau înlocuit, cu excepția cazului în care este interzis de prezentul Cod sau documentul la care se face trimitere; și

(viii) O trimitere la lege include orice cerință de reglementare, recomandare sectorială și cele mai bune practici emise de autoritățile relevante naționale și internațioanle de supraveghere sau alte organisme.

Copyright © 2019 ADP, LLC. All rights reserved.

ANEXA 1 – Definiții BCR

Decizie privind caracterul adecvat	DECIZIE PRIVIND CARACTERUL ADECVAT înseamnă orice decizie a autorității responsabile cu protecția datelor sau a altui organism competent cu privire la faptul că o țară, regiune sau destinatar al datelor transferate este obligat să asigure un nivel adecvat de protecție pentru datele cu caracter personal. Entitățile acoperite de o decizie privind caracterul adecvat includ destinatarii aflați în țările care, conform Legislației Aplicabile, sunt obligați să asigure un nivel adecvat de protecție a datelor, precum și destinatarii care sunt obligați de un alt program (precum setul Regulilor Corporatiste Obligatorii) care au fost autorizați de către autoritatea responsabilă cu protecția datelor sau alt organism competent. În ceea ce privește Statele Unite ale Americii, companiile care devin autorizate pentru cadrul SUA-SEE și/sau SUA-Elveția, precum Scutul de Confidențialitate, vor fi acoperite de o Decizie privind Caracterul Adecvat.
ADP (Grup ADP)	ADP (GRUPUL ADP) înseamnă, împreună, Automatic Data Processing, Inc. (Compania-mamă) și Companiile Grupului, inclusiv ADP, LLC.
Entitate contractantă ADP	ENTITATE CONTRACTANTĂ ADP înseamnă Compania Grupului care a încheiat un contract impus de Coduri, precum un Contract de prestare servicii, Contract încheiat cu un subîmputernicit sau acord pentru transferul datelor.
Entitate delegată ADP	ENTITATE DELEGATĂ ADP înseamnă ADP Nederland, B.V., cu sediul social în Lylantse Baan 1, 2908 LG CAPELLE AAN DEN IJSSEL, Olanda.
Comitet executiv ADP	COMITET EXECUTIV ADP înseamnă comitetul ofițerilor format din (i) directorul executiv Automatic Data Processing, Inc. (CEO) și (ii) alți ofițeri care raportează direct directorului executiv și care, împreună, sunt responsabili pentru operațiunile grupului ADP.
Subîmputernicit ADP	În temeiul Codului de Confidențialitate pentru Serviciile de Prelucrare a Datelor Clienților, un SUBÎMPUTERNICIT ADP înseamnă orice Companie a Grupului desemnată de o altă Companie a Grupului în calitate de subîmputernicit pentru prelucrarea datelor clientului.
Legislație aplicabilă operatorului de date	În temeiul Codului de Confidențialitate pentru serviciile de prelucrare a datelor clienților, LEGISLAȚIA APLICABILĂ OPERATORULUI DE DATE înseamă orice legislație de confidențialitate sau de protecție a datelor care se aplică unui client ADP în calitate de pperator de date a datelor unui client.
Legislație aplicabilă împuternicitului operatorului	În temeiul Codului de Confidențialitate pentru serviciile de prelucrare a datelor clienților, LEGISLAȚIA APLICABILĂ ÎMPUTERNICITULUI OPERATORULUI înseamă orice legislație de confidențialitate sau de

Copyright © 2019 ADP, LLC. All rights reserved.

	protecție a datelor care se aplică către ADP în calitate de operator de date, în numele unui client care este un operator de date.
Legislație aplicabilă	LEGISLAȚIE APLICABILĂ înseamnă orice legislație de confidențialitate sau de protecție a datelor care se aplică activităților de prelucrare.
Candidat	CANDIDAT înseamnă orice persoană care furnizează date cu caracter personal către ADP în contextul aplicării pentru o poziție cu ADP în calitate de asociat.
Arhivă	ARHIVĂ înseamnă o colecție de date cu caracter personal care nu mai sunt necesare pentru arhivarea scopurilor pentru care datele cu caracter personal erau colectate inițial sau care nu mai sunt folosite pentru activitățile comerciale generale, însă sunt folosite în scopuri istorice, științifice sau statistice, pentru soluționarea litigiilor, investigațiilor sau în scopuri generale de arhivare. Accesul la o arhivă este limitat la administratorii sistemului și la alte persoane a căror sarcini necesiră în mod specific accesul la arhivă.
Asociat	ASOCIAT înseamnă un candidat, un angajat actual ADP sau un fost angajat ADP, cu excepția persoanelor angajate independent. NOTĂ: Codul de confidențialitate la locul de muncă nu se aplică prelucrării datelor cu caracter personal a aersonelor angajate independent.
Automatic Data Processing, Inc.	AUTOMATIC DATA PROCESSING, INC. este compania-mamă a Grupului ADP și este o corporație înființată conform legislației Delaware (SUA) cu sediul social în One ADP Boulevard, Roseland, New Jersey, 07068-1728,SUA.
Reguli corporatiste obligatorii	REGULI CORPORATISTE OBLIGATORII înseamnă o politică de confidențialitate a unui grup din cadrul unor companii similare considerate a furniza un nivel adecvat de protecție pentru transferul Datelor cu Caracter Personal în cadrul grupului respectiv conform Legislației Aplicabile.
Date privind contacte de afaceri	DATE PRIVIND CONTACTE DE AFACERI înseamnă datele aparținând unui profesionist care se regăsesc în mod obișnuit pe o carte de vizită sau într-o semnătură digitală.
Partener comercial	PARTENER COMERCIAL înseamnă orice parte terță, alta decât un client sau furnizor care are sau a avut o relație de afacere sau alianță strategică cu ADP (*ex.*, partener comun de marketing, asociat în participație sau partener din domeniul dezvoltării comune).
Scop comercial	SCOP COMERCIAL înseamnă un scop legitim pentru prelucrarea datelor cu caracter personal, astfel cum se specifică la Art. 2, 3 sau 4 din orice Cod ADP sau pentru prelucrarea categoriilor speciale de date, astfel cum se specifică la Art. 4 din orice Cod ADP.

Copyright © 2019 ADP, LLC. All rights reserved.

Copii	În scopurile prevăzute colectării și marketingului datelor ADP, COPII înseamnă persoanele minore stabilite de legislația aplicabilă ca fiind capabile să își dea consimțământul pentru colectarea și/sau marketingul datelor.
Client	CLIENT înseamnă orice parte terță care utilizează unul sau mai multe dintre produsele sau serviciile ADP pe parcursul desfășurării propriei activități.
Date privind clientul	DATE PRIVIND CLIENTUL înseamnă datele cu caracter personal aparținând angajaților clientului (inclusiv posibili angajați, foști angajați și dependenți ai angajaților) prelucrate de ADP în legătură cu furnizarea serviciilor pentru clienți.
Angajatul clientului	ANGAJATUL CLIENTULUI înseamnă orice persoană a căror date cu caracter personal sunt prelucrate de ADP în calitate de operator de date pentru un client, în temeiul contractului de prestare servicii. În scopul asigurării clarității, ANGAJATUL CLIENTULUI se referă la toate persoanele a căror date cu caracter personal sunt prelucrate de ADP pentru furnizarea serviciilor pentru clienți (indiferent de natura legală a relației dintre persoană și client). Nu include profesioniștii a căror date cu caracter personal sunt prelucrate de ADP în legătură cu relația directă dintre ADP și client. De exemplu, ADP poate prelucra datele cu caracter personal ale unui profesionist HR pentru a încheia un contract cu clientul – aceste date sunt reglementate de Codul de Confidențialitate pentru datele comerciale. Cu toate acestea, atunci când ADP furnizează Clientului plata pentru serviciile de prelucrare (ex., emite fluturașe de salariu, asigură asistență cu privire la utilizarea unui sistem ADP), datele persoanei ar fi prelucrare ca date aparținând clientului.
Servicii pentru clienți	SERVICII PENTRU CLIENȚI înseamnă serviciile privind capitalul uman furnizate de ADP Clienților, precum recrutare, servicii de plată și compensare, beneficii, gestionarea talentului, administrare HR, consultare și statistici și servicii de pensionare.
Activități pentru sprijinirea clientului	ACTIVITĂȚI PENTRU SPRIJINIREA CLIENTULUI înseamnă acele activități de Prelucrare efectuate de ADP în vederea sprijinirii furnizării produselor și serviciilor. Activitățile pentru sprijinirea clientului pot include, de exemplu, instruirea Profesioniștilor, răspunderea la întrebări cu privire la servicii, deschiderea și soluționarea biletelor, furnizarea informațiile cu privire la produs și servicii (inclusiv actualizări și alerte de conformitate), control și monitorizare a calității și activități similare care facilitează utilizarea eficientă a produselor și serviciilor ADP.
Cod	COD înseamnă (după caz) Codul de confidențialitate ADP pentru datele comerciale, Codul de confidențialitate ADP la locul de muncă (intern pentru ADP) și Codul de confidențialitate pentru serviciile de prelucrare a datelor clientului; împreună denumite Codurile.

Copyright © 2019 ADP, LLC. All rights reserved.

Persoană angajată individual	PERSOANĂ ANGAJATĂ INDIVIDUAL înseamnă un angajat al unui client SUA care este angajat individual de către un afiliat indirect SUA al Automatic Data Processing, Inc. ca parte din serviciile organizaționale profesionale oferite în SUA.
Client	CLIENT înseamnă o persoană care interacționează direct cu ADP în nume personal. De exemplu, consumatorii includ persoane care participă la programele de dezvolltare de talent sau utilizează produse și servicii de la ADP în scop personal (*ex.*, în afara unei relații de muncă cu ADP sau un client ADP).
Lucrător posibil	LUCRĂTOR POSIBIL înseamnă o persoană care furnizează servicii către ADP (și care sunt supravegheați direct de către ADP) în mod provizoriu sau nepermanent, precum lucrători temporari, ocazionali, independenți sau consultanți.
Operator de date	OPERATOR DE DATE înseamnă entitatea sau persoana fizică care, singură sau împreună cu alții, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.
Împuternicit al operatorului de date	ÎMPUTERNICIT AL OPERATORULUI DE DATE înseamnă entitatea sau persoana fizică care prelucrează date cu caracter personal în numele unui operator de date.
Autoritate responsabilă cu protecția datelor sau DPA	AUTORITATE RESPONSABILĂ CU PROTECȚIA DATELOR SAU DPA înseamnă orice persoană de reglementare sau supraveghere care verifică protecția sau confidențialitatea datelor într-o țară în care este înființată o Companie a unui Grup.
Evaluarea impactului asupra protecției datelor (DPIA)	EVALUREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR (DPIA) înseamnă a procedură de efectuare și documentare a evaluării prealabile a impactului pe care un anumit proces de prelucrare îl poate avea asupra protecției datelor cu caracter personal, unde un astfel de proces de prelucrare poate avea ca rezultat un nivel ridicat de risc pentru drepturile și libertățile Persoanelor, în special în cazul în care sunt utilzate tehnologii noi. O DPIA conține:

Copyright © 2019 ADP, LLC. All rights reserved.

	(i) o descriere a: (a) scopului și contextului procesului de prelucrare; (b) scopurilor comerciale pentru care datele cu caracter personal sunt prelucrate; (c) scopurile specifice pentru care categoriile speciale de date sunt prelucrate; (d) categoriilor datelor cu caracter personal ale destinatarilor, inclusiv destinatarii care nu sunt acoperiți de o decizie privind caracterul adecvat; (e) perioadelor de arhivare a datelor cu caracter personal; (ii) o evaluare a: (a) necesității și proporționalității procesului de prelucrare; (b) riscurilor asupra drepturilor de confidențialitate ale Persoanelor; și (c) măsurilor pentru a reduce acele riscuri, inclusiv măsuri de protecție, măsuri de securitate și alte mecanisme (precum confidențialitate prin design) pentru a asigura protecția datelor cu caracter personal.
Încălcarea securității datelor	ÎNCĂLCAREA SECURITĂȚII DATELOR înseamnă orice incident care are un impact asupra confidențialității, integrității sau disponibilității datelor cu caracter personal, precum utilizarea sau divulgarea neautorizată a datelor cu caracter personal sau accesul neautorizat la datele cu caracter personal care compromite confidențialitatea sau securitatea datelor cu caracter personal.
Dependent	DEPENDENT înseamnă soția/soțul, partenerul, copilul sau beneficiarul unui asociat sau contactul de urgență al unui asociat sau posibil lucrător.
Entitate cesionată	ENTITATE CESIONATĂ înseamnă o Companie a unui Grup care nu mai este deținută de ADP ca urmare a vânzării acțiunilor și/sau activelor companiei sau altă cesionare, astfel încât compania nu se mai califică ca o Companie a unui Grup.
SEE	SEE sau SPAȚIU ECONOMIC EUROPEAN înseamnă toți Membrii Statelor Uniunii Europene, plus Norvegia, Islanda și Liechtenstein și, în temeiul Codurilor, Elveția. Ca urmare a decizie Consilierului General – publicarea pe www.adp.com, poate include alte țări cu legi de protecție a datelor având restricții de transfer a datelor similare cu cele ale SEE.
Legislație aplicabilă SEE	LEGISLAȚIA APLICABILĂ SEE înseamnă cerințele conform Legislației Aplicabile SEE care se aplică datelor cu caracter personal și care sunt colectate inițial în contextul activitățiloe Companiei Grupului înființată în SEE (și după transferarea către o altă Companie a Grupului înființată în afara

Copyright © 2019 ADP, LLC. All rights reserved.

	SEE).
Restricție de transfer a datelor în SEE	RESTRICȚIE DE TRANSFER A DATELOR ÎN SEE înseamnă orice restricție cu privire la transferurile internaționale ale datelor cu caracter personal conform legislației de protecției a datelor dintr-o țară SEE.
Data intrării în vigoare	DATA INTRĂRII ÎN VIGOARE înseamă data la care Codurile intră în vigoare, astfel cum se prevede la Art. 1 din Coduri.
Consilier general	CONSILIER GENERAL înseamnă consilierul general al Automatic Data Processing, Inc.
Director responsabil cu protecția datelor	DIRECTOR RESPONSABIL CU PROTECȚIA DATELOR înseamnă asociatul ADP care deține acest titlu în cadrul Data Processing, Inc.
Compania grupului	COMPANIA GRUPULUI înseamnă orice entitate juridică care este un asociat Automatic Data Processing, Inc. și/sau ADP, LLC., dacă nici Automatic Data Processing, Inc. și nici ADP, LLC. nu deține direct sau indirect mai mult de 50% din capitalul subscris emis, deține 50% sau mai mult din puterea de vot în cadrul diferitelor întruniri ale acționarilor, are puterea de a numi în funcție directorii sau direcționează altfel activitățile unei astfel de entități juridice.
Persoană	PERSOANĂ înseamnă orice persoană fizică identificată sau identificabilă a căror date cu caracter persoanl sunt prelucrate de ADP, un operatorsau persoană împuternicită de un operator de date, cu excepția Persoanelor angajate individual. NOTĂ: Codul de confidențialitate ADP pentru datele comericale și Codul de confidențialitate ADP la locul de muncă nu se aplică prelucrării datelor cu caracter personal ale persoanelor angajate individual.
Împuternicit intern al operatorului	ÎMPUTERNICIT INTERN AL OPERATORULUI înseamnă orice Companie a Grupului care prelucrează datele cu caracter personal în numele altei Companii a Grupului în calitate de operator de date.
Conducere DPA	CONDUCERE DPA înseamnă autoritatea olandeză responsabilă cu protecția datelor.
Cerințe obligatorii	CERINȚE OBLIGATORII înseamnă acele obligații conform oricărei Legislații aplicabile unui persoane împuternicite de operator cu prelucrarea datelor care necesită prelucrarea datelor cu caracter persoanl pentru (i) securitate și apărare națională; (ii) siguranță publică; (iii) prevenirea, investigarea, detectarea sau urmărirea acuzațiilor penale sau încălcărilor eticii pentru profesioniștii de reglementare; sau (iv) protecția oricărei persoane sau drepturilor și libertăților persoanelor.
Echipa responsabilă cu	ECHIPA RESPONSABILĂ CU PROTECȚIA DATELOR înseamnă Biroul pentru protecția vieții private și de gestiune a datelor ADP. Biroul pentru

Copyright © 2019 ADP, LLC. All rights reserved.

protecția datelor și de gestiune	protecția vieții private și de gestiune a datelor este coordonată de Directorul responsabil cu confidențialitatea datelor și este format din administratori și manageri responsabili cu confidențialitatea datelor și alt personal responsabil cu informarea directorului, adminsitratorilor sau managerilor.
Interes superior	INTERES SUPERIOR înseamnă interesele presante prevăzute la Art. 13.1 din Codul de confidențialitate la locul de muncă și Codul de confidențialitate pentru datele comerciale pe baza cărora obligațiile ADP sau drepturile Persoanelor prevăzute la Art. 13.2 și 13.3 din Coduri pot, în circumstanțe specifice, să fie suprascrise dacă interesele presante depășesc interesele persoanei.
Date cu caracter personal sau date	DATE CU CARACTER PERSONAL sau DATE înseamnă orice informație cu privire la o persoană identificată sau identificabilă. Datele cu caracter personal pot face trimitere și la informațiile personale prevăzute în politici și standarde care implementează Codurile.
Consiliu de conducere responsabil cu confidențialitatea	CONSILIU DE CONDUCERE RESPONSABIL CU CONFIDENȚIALITATEA înseamnă consiliul condus de director și format din administratori responsabili cu confidențialitatea, membrii ai rețelei de confidențialitate aleși de director și alte persoane care pot fi necesare să participe la obiectivele Consilului.
Rețea de confidențialitate	REȚEA DE CONFIDENȚIALITATE înseamnă membrii Echipei responsabile cu confidențialitatea și gestiunea datelor și alți membrii ai Departamentului Juridic, inclusiv profesioniști cu asigurarea conformității și administratori responsabili cu protecția datelor care sunt răspunzători de conformitatea confidențialității din cadrul regiunilor, țărilor, unităților operaționale sau departamentelor funcționale respective.
Adminsitrator responsabil cu confidențialitatea	ADMINISTRATOR RESPONSABIL CU CONFIDENȚIALITATEA înseamnă un director executiv ADP numit de către un director executiv responsabil și/sau Conducere executivă ADP cu implementarea și punerea în aplicare a Codurilor de confidențialitate în cadrul Unității operaționale ADP.
Prelucrare	PRELUCRARE înseamnă orice operație efectuată asupra datelor cu caracter personal, prin mijloace automate sau nu, precum colectare, înregistrare, arhivare, organizare, alterare, utilizare, divulgare (inclusiv garantarea accesului de la distanță), transmitere sau ștergere a datelor cu caracter personal.
Contract încheiat cu un împuternicit al operatorului	CONTRACT ÎNCHEIAT CU UN ÎMPUTERNICIT AL OPERATORULUI înseamnă orice contract pentru prelucrarea Datelor cu caracter personal încheiat de ADP și un împuternicit terț al operatorului.

Copyright © 2019 ADP, LLC. All rights reserved.

Profesionist	PROFESIONIST înseamnă orice persoană (alta decât un angajat) care interacționează direct cu ADP în scopuri legate de activități profesioniste și comerciale. De exemplu, Profesioniștii includ personalul clientului HR care colaborează cu ADP în calitate de utilizatori ai produselor și serviciilor ADP. Profesioniștii includ și reprezentanții clientului, furnizorului și partenerului de afaceri, contacte de afaceri. contacte din organizații profesionale, contacte media și alte persoane care interacționează cu ADP în scopuri legate de activități comerciale.
Director executiv responsabil	DIRECTOR EXECUTIV RESPONSABIL înseamnă directorul general al companiei, sau directorul unei unități operaționale sau departament funcțional care are drept de proprietate asupra Companiei Grupului, unității operaționale sau departamentului funcțional.
Scop secundar	SCOP SECUNDAR înseamnă orice scop altul decât scopul original pentru care datele cu caracter personal sunt prelucrate.
Contract de prestare servicii	CONTRACT DE PRESTARE SERVICII înseamnă orice contract, acord sau termeni în temeiul cărora ADP furnizează servicii pentru clienți.
Categorii speciale de date	CATEGORII SPECIALE DE DATE înseamnă date cu caracter personal care semnifică originea etnică sau rasială, opiniile politice sau apartenența la partide politice sau organizații similare, opinii religioase sau filozofice, apartenența la o organizație sau uniune profesionistă sau comercială, starea de sănătate fizică și psihică, inclusiv orice opinie cu privire la acestea, incapacități, cod genetic, dependențe, viață sexuală, acuzații, caziere sau urmări cu privire la un comportament criminal sau ilegal.
Personal	PERSONAL înseamnă, împreună, asociații ADP angajați recent și posibilii lucrători care lucrează pentru ADP.
Contract încheiat cu un subîmputernicit al operatorului	CONTRACT ÎNCHEIAT CU UN SUBÎMPUTERNICIT AL OPERATORULUI înseamnă un acord scris sau electronic încheiat cu un subîmputernicit terț în temeiul Art. 7.1 din Codul de Confidențialitate pentru serviciile de prelucrare a datelor clientului.
Subîmputerniciți	SUBÎMPUTERNICIȚI înseamnă, împreună, subîmputerniciții ADP și subîmputerniciții terți.
Furnizor	FURNIZOR înseamnă orice parte terță care furnizează bunuri sau servicii (ex., în calitate de furnizor de serviciim agent, persoană împuternicită de operator cu prelucrarea datelor, consultant sau vânzător).
Parte terță	PARTE TERȚĂ înseamnă orice persoană, organizație privată sau organism guvernamental care nu este o Companie a Grupului.

Copyright © 2019 ADP, LLC. All rights reserved.

Operator terț	OPERATOR TERȚ înseamnă o parte terță care prelucrează datele cu caracter personal și stabilește scopurile și mijloacele de prelucrare.
Împuternicit terț al operatorului	ÎMPUTERNICIT TERȚ AL OPERATORULUI înseamnă o parte terță care prelucrează datele cu caracter personal în numele ADP și care nu se află sub conducerea directă ADP.
Subîmputernicit terț	SUBÎMPUTERNICIT TERȚ înseamnă orice parte terță numită de ADP ca subîmputernicit.

Copyright © 2019 ADP, LLC. All rights reserved.

ANEXA 2 – Măsuri de securitate

Presented by:	**ADP - Global Security Organization**
Version:	**1.8**
Released:	**October 2018**

Contents

1. Information Security Policies....36
   - A. Information Security Management....36
   - B. Independence of Information Security Function....36
   - C. Formal Definition of an Information Security Policy....36
   - D. Information Security Policy Review....37
2. Organization of Information Security....38
   - A. Information Security Roles and Responsibilities....38
   - B. Mobile Computing and Teleworking Policy....38
3. Human Resource Security....39
   - A. Background Checks....39
   - B. Confidentiality Agreements with Employees and Contractors....39
   - C. Information Security Training Program....39
   - D. Security Awareness of Employee and Contractors....39
   - E. Employees Responsibilities and Disciplinary Processes....39
   - F. Termination of Employment Responsibilities....40
4. Asset Management....41
   - A. Acceptable Use of Assets....41
   - B. Classification of Information....41
   - C. Equipment and Media Disposal....41
   - D. Physical Media in Transit....42
5. Access Control....43
   - A. Business Requirements of Access Control....43
   - B. Access to Infrastructure - Access Control Management....43
   - C. Password policy....44
   - D. Session Timeouts....44
6. Cryptography....46
   - A. Cryptographic Controls....46
   - B. Key Management....46
7. Physical and Environmental Security....47
   - A. Physical Security....47
   - B. Physical Access Control Mechanisms....47
   - C. Review of Access to Sensitive Areas....47
   - D. Identification of ADP Personnel....48
   - E. Physical and Environmental Security Controls in Data Centers....48
8. Operations Security....49
   - A. Formalization of IT Operations Procedures....49
   - B. Infrastructure Change Management....49

Copyright © 2019 ADP, LLC. All rights reserved.

C. System Capacity Planning and Acceptance 49
D. Protection against Malicious Code 49
E. Back-Up Management Policy 49
F. Security Logging and Monitoring 50
G. Infrastructure Systems and Monitoring 50
H. Technical Vulnerability Management 51
9. Communications Security 52
A. Network Security Management 52
B. Exchange of Information 52
C. Use of Messaging Systems 52
10. System acquisition, development, and maintenance 53
A. Security in Development and Support Processes 53
B. Security in Development Environment 53
C. Test Data 54
11. Supplier relationships 55
A. Identification of Risks Related to External Parties 55
B. Information Security Agreements with External Parties 55
12. Information Security Incident Management 56
A. Management of Information Security Incidents and Improvements 56
13. Information Security Aspects of Business Resiliency Management 57
A. ADP Business Resiliency Program 57
B. Implementation of Business Resiliency 57
C. Availability of Disaster Recovery Facilities 58
14. Compliance 60
A. Compliance with Legal Requirements 60
B. Compliance with Security Policies and Standards 60
C. Technical Compliance 60
D. Retention of Data 61
15. Appendix 62
A. Logical Network Diagram 62

Copyright © 2019 ADP, LLC. All rights reserved.

Terms and Definitions

The following terms may appear throughout the document:

Term or Acronym used	Definition
PTSS	**GSO's Preventative Technical Security Services**
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**
LDAP	**Lightweight Directory Access Protocol**
NTP	**Network Time Protocol**
SOC	**Service Organization Controls**
TPSI	**Trusted Platform Security Infrastructure**

Document History

Version	Release date	Author/Sponsor	Revision Summary
1.0	Aug 2013	ADP Global Security Organization	Original Version
1.1	Jan 2014	ADP Global Security Organization	Minor updates
1.2	Dec 2014	ADP Global Security Organization	Update to LLC
1.3	Feb 2015	Client Security Management Office	Revised to ISO 27001:2013 to fit for EMEA
1.4	Jan 2016	ADP Global Security Organization / ADP Legal Department	Revised to fit GES EMEA and MNC in the same document
1.5	Jun 2017	Client Security Management Office	Minor updates
1.6	Sep 2017	Client Security Management Office	Document globalization
1.61	Sep 2017	Client Security Management Office	Minor update
1.7	Feb 2018	Client Security Management Office	Minor update
1.8	Oct 2018	Client Security Management Office	Minor updates

Copyright © 2019 ADP, LLC. All rights reserved.

Overview

ADP maintains a formal information security program containing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of client information. This program is reasonably designed to (i) safeguard the security and confidentiality of client information, (ii) protect against any anticipated threats or hazards to the security or integrity of the information, and (iii) protect against unauthorized access to or use of the information.

This document contains an overview of ADP's information security measures and practices, as of the release date and which are subject to change by ADP. These requirements and practices are designed to be consistent with the ISO/IEC 27001:2013 information security standards. References to the corresponding sections of ISO 27001 are included in each section in [italics].

ADP periodically assesses its security policies, standards. Our goal is to ensure that the security program effectively and efficiently operates to protect all of the information entrusted to us by our clients and their employees.

Copyright © 2019 ADP, LLC. All rights reserved.

1. Information Security Policies

A. Information Security Management

ADP is committed to ensuring that information security is properly managed and that the measures described in this document are implemented and appropriately adhered to by ADP staff and applicable third parties.

B. Independence of Information Security Function

ADP has a Chief Security Officer who oversees ADP's Global Security Organization (GSO) and reports to Chief Financial Officer, instead of to the Chief Information Officer, which gives GSO the necessary independence from IT. The GSO is a cross-divisional security team that creates a multi-disciplinary approach in the areas of cyber and information security and compliance, operational risk management, client security management, workforce protection, and business resilience. GSO senior management, under our Chief Security Officer are responsible for managing security policies, procedures and guidelines.

C. Formal Definition of an Information Security Policy

[5.1.1] Policies for information security

ADP has developed and documented formal information security policies that set out ADP's approach to managing information security.

Specific areas covered by this policy include, but are not limited to the following:

- **Security, Risk and Privacy Management Policy –** Reviews the responsibilities of the Global Security Organization ("GSO"), the Chief Security Officer ("CSO") and the Global Chief Privacy Officer ("GCPO").
- **Global Privacy Policy -** Discusses the collection of personal information, access to, accuracy, disclosures, and privacy statement to clients.
- **Information Security Responsibilities for Associates and Managers Policy –** Includes the Information Security Responsibilities and controls on hiring process from a security perspective.
- **Acceptable Use of Electronic Communications and Data Protection Policy** – Discusses acceptable use, different electronic communications, encryption, and key management.
- **Information Handling and Classification Policy –** Provides requirements for the classification of ADP information and establishes protection controls.
- **Physical Security Policy–** Examines the security of ADP facilities and subsequently our Associates and visitors who work there.
- **Security Operations Management Policy –** Provides minimum controls for maintaining system patches, effectively address the threat from malware, and maintain backups and database security controls.
- **Security Monitoring Policy –** Provides controls for intrusion detection systems (IDS), logs, and data loss prevention (DLP).
- **Investigations, Electronic Discovery and Incident Management Policy –** This covers: incident response, EDILS, workforce protection, access to associates electronic stored information.
- **Access & Authentication Policy –** Covers authentication (e.g. user ID and password), remote access and wireless access.
- **Network Security Policy –** Security architecture of routers, firewalls, AD, DNS, email servers, DMZ, cloud services, network devices, web proxy, and switched network technology.
- **Global Vendor Assurance Policy –** Sets minimum security controls for engaging any third party to assist ADP in achieving its business objectives.

Copyright © 2019 ADP, LLC. All rights reserved.

- **Application Management Policy –** Establishes appropriate security controls into each stage of the system development lifecycle.
- **Business Resiliency Policy –**Ensures the protection, integrity and preservation of ADP by establishing the minimum requirements to document, implement, maintain and continually improve Business Resiliency Programs
- **Operational Risk Management Policy –** Identification, monitoring, response, analysis, governance, and new business initiatives.

Policies are published in the Associate Portal and are accessible to all employees and contractors from within ADP network.

D. Information Security Policy Review

[5.1.2] Review of the policies for information security

ADP reviews its information security policy at least once a year or whenever there are major changes impacting the functioning of ADP's information systems.

Copyright © 2019 ADP, LLC. All rights reserved.

2. Organization of Information Security

A. Information Security Roles and Responsibilities

[6.1.1] Information security roles and responsibilities

The GSO consists of cross-divisional security teams leveraging a multi-disciplinary approach to compliance with cyber and information security standards, operational risk management, client security management, workforce protection and business resilience. Roles and responsibilities have been formally defined in writing for all members of the GSO. The GSO is charged with the design, implementation and oversight of our information security program based on corporate policies. The GSO's activities are overseen by the Executive Security Committee, composed of the Chief Security Officer, the Chief Executive Officer, the Chief Financial Officer, the Chief Information Officer, Chief Human Resources Officer and the General Counsel.

B. Mobile Computing and Teleworking Policy

[6.2.1] Mobile device policy

[6.2.2] Teleworking

ADP requires all confidential information to be encrypted on mobile devices, in order to prevent any data leakage resulting from a theft or a loss of a computer. Antivirus software, with updated virus signature files and two-factor authentication over VPN is also required to access the corporate networks remotely. All remote devices are required to be password protected.

ADP employees are required to report lost or stolen remote computing devices immediately through a Security Incident Reporting Process.

All employees and contractors, as a condition of employment with ADP, must comply with the ADP's acceptable use and other relevant Policies.

Copyright © 2019 ADP, LLC. All rights reserved.

3. Human Resource Security

A. Background Checks

[7.1.1] Screening

Consistent with applicable legal requirements in the individual's jurisdiction, ADP conducts appropriate background checks commensurate with the duties and responsibilities of its employees, contractors and/or third parties to ensure their suitability for handling clients' information prior to engaging or hiring such individuals.

Background screening may include the following components:

a) Identity/employment eligibility verification
b) Employment history
c) Educational history and professional qualifications
d) Criminal records (where legally authorized and depending on local country regulations)

B. Confidentiality Agreements with Employees and Contractors

[7.1.2] Terms and conditions of employment

ADP employment contracts and contracts with contractors contain terms setting out an appropriate catalogue of obligations and responsibilities concerning client information to which they will have access. All ADP employees and contractors are bound by confidentiality obligations.

C. Information Security Training Program

[7.2.2] Information security awareness, education and training

ADP ensures that all personnel scheduled to access and/or otherwise process ADP's clients' information, are provided with information security and privacy awareness training with the objective to promote effective privacy and security practices.

All employees receive information security training as part of their on boarding plan. In addition, ADP delivers annual security training in order to remind employees of their responsibilities when performing their day-to-day duties.

D. Security Awareness of Employee and Contractors

[7.2.2] Information security awareness, education and training

The ADP information security policy document is approved by management, published and communicated to all employees, onsite contractors and applicable third parties.

ADP employees and onsite contractors are required to comply with the Information Security Responsibilities and associated information security policies.

E. Employees Responsibilities and Disciplinary Processes

[7.2.3] Disciplinary process

ADP has published a security policy that all ADP associates need to comply with. Violations of security policies may lead to revocation of access privileges and/or disciplinary actions up to and including termination of consulting contracts or employment.

Copyright © 2019 ADP, LLC. All rights reserved.

F. Termination of Employment Responsibilities

[7.3.1] Termination or change of employment responsibilities

[8.1.4] Return of assets

[9.2.6] Removal or adjustment of access rights

Responsibilities upon termination of employment have been formally documented and include at least:

a) Return all ADP information and assets in the possession of the respective employee, on whatever medium it is stored
b) Termination of access rights to ADP facilities, information and systems
c) Change of passwords for remaining active shared accounts, if applicable
d) Transfer of knowledge, if applicable.

Access rights of all ADP employees and contractors to data and data processing facilities are removed upon termination of their contract with ADP.

Copyright © 2019 ADP, LLC. All rights reserved.

4. Asset Management

A. Acceptable Use of Assets

[8.1.3] Acceptable use of assets

Acceptable use of assets is articulated across several policies, applicable to ADP employees and contractors, in order to ensure that ADP's and clients' information are not exposed by use of such assets. Examples of areas described in these policies are: use of electronic communications, use of electronic equipment, and use of information assets.

B. Classification of Information

[8.2.1] Classification of information

Information acquired, created or maintained by or on behalf of ADP is assigned, as applicable, a security classification of:

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

Requirements for handling information are directly correlated to the information security classification.

Personal Information and Sensitive Personal Information are considered in all cases ADP Confidential.

ADP employees are accountable for protecting and handling information assets in accordance with their security classification level, which provides protection of information and applicable handling requirements for each classification level. All client information is classified as confidential.

The ADP confidentiality classification is applied to all information stored, transmitted or handled by third parties.

C. Equipment and Media Disposal

[8.3.1] Management of removable media

[8.3.2] Disposal of media

When ADP equipment, documents, files, and media are disposed of or reused, appropriate measures are taken to prevent subsequent retrieval of client's information originally stored in them.

All information on computers or electronic storage media regardless of classification is overwritten or degaussed, unless the media is physically destroyed before being released outside ADP facilities.

The procedures for ensuring the secure destruction/erasure of ADP information held on equipment, in documents, files, and media are formally documented.

Copyright © 2019 ADP, LLC. All rights reserved.

D. Physical Media in Transit

[8.3.3] Physical media transfer

Organizational measures are taken to ensure that printed materials containing clients' information cannot be viewed by unauthorized individuals.

Measures are also taken to protect printed materials containing clients' information against theft, loss, and/or unauthorized access/modification (i) during transit e.g. sealed envelopes, containers and hand delivery to authorized user; and (ii) during review, revision or other processing where removed from secure storage.

Copyright © 2019 ADP, LLC. All rights reserved.

5. Access Control

A. Business Requirements of Access Control

[9.1.1] Access control policy

ADP's Access control policy is based on business defined requirements. The policies and control standards are articulated into access controls enforced in all components of the provided service and are based on a "least-privilege" and "need to know" principle.

B. Access to Infrastructure - Access Control Management

[9.2.1] User registration and de-registration

[9.2.2] User access provisioning

[9.2.5] Review of user access rights

[9.4.3] Password management system

Access requests to move, add, create and delete are logged, approved and periodically reviewed.

A formal review is performed at least yearly to make sure individual users correspond correctly to the relevant business role and would not have continued access after a position change. This process is audited and documented in a SOC1[1] type II report.

From within an Identity Management System, a dedicated ADP team is responsible for granting, denying, cancelling, terminating and decommissioning/deactivating any access to ADP facilities and information systems.

Administrator access is only possible from ADP internal network or equivalent through a secure remote VPN access using two-factor authentication.

For the UNIX domain, access to privilege accounts is based on a "need to know" principle. All access requests are validated by the Security Team and an audit trail is maintained.

For the Windows domain, user accounts are defined in a central Active Directory (AD). The AD for servers in production is different from the AD used for workstations.

ADP uses a centralized identity and access management (IAM) tool that is managed centrally by a dedicated GETS team. According to the access rights requested through the centralized IAM tool, a validation workflow will be triggered that could involve the users' supervisor. Access is provided on a temporary basis and workflows exist to prevent such access from remaining permanent.

An employee's access to a facility is decommissioned immediately after the last day of employment by deactivating their access card (employee badge). The employee's user IDs are immediately deactivated.

Any employee's assets will be returned and checked by the competent line manager against the asset list present in the configuration management data base.

Following a job position change, or organizational changes, user profiles or user access rights are required to be modified by the applicable business unit management and the IAM Team. Additionally, a formal review of access rights is performed every year to verify

[1] In the case of certain US Services offered by ADP, this is audited in a SOC 2 Type 2 report.

Copyright © 2019 ADP, LLC. All rights reserved.

that individual users' rights correspond to their relevant business role and that there are no remaining irrelevant access rights after a position transfer.

C. Password policy

[9.1.1] Access control policy

[9.4.2] Secure log-on procedures

[9.4.3] Password management system

ADP associate password policies are enforced in servers, databases and network devices and applications, to the extent the device/application allows it. The password complexity is derived from a risk based analysis of the protected data and content.

The policies meet prevailing industry standards for strength and complexity, and include a minimum password length of 8 characters, with password composition of 1 or more characters from at least 3 of the following 4 classes:

- English upper case letters (e.g., A, B, C, ...Z)
- English lower case letters (e.g., a, b, c, ...z)
- Digits (e.g., 0, 1, 2, ...9)
- Non-alphanumeric special characters (e.g., ?,!,%,$,#, etc.)

Additionally, ADP associate passwords must be compliant with the following rules:

- Passwords are changed at regular intervals according to the sensitivity of the information accessible through the systems to which they relate in accordance with ADP global security policies
- Passwords are stored using one-way hash with "salt"
- Passwords must not contain the user ID in the password
- Passwords must not contain the user's first and/or last name
- Maximum of 4 repeating characters in the password
- Previous 4 passwords cannot be reused
- There is a list of prohibited passwords
- Passwords can be changed only once per day
- Password expire after 90 days
- User is disabled after 180 days of inactivity
- Account is locked after 4 failed logon attempts

Client application authentication requirements vary by product, and federated services (SAML 2.0) is available on specific ADP applications using a unified network and security layer managed by GETS.

D. Session Timeouts

[A.9.4.1] Information access restriction

ADP enforces automatic timeouts to all servers, workstations, applications and VPN connections.

- Server session: timeout after 20 minutes of inactivity.
- Workstation session (laptops, PCs, terminals, etc.): timeout after 20 minutes of inactivity.
- Applications: all applications have a timeout after a period of inactivity, which will vary depending on the application.

Copyright © 2019 ADP, LLC. All rights reserved.

- VPN session: timeout after no longer than 24 hours of usage.

Re-establishment of sessions may take place only after the user has provided a valid password.

Copyright © 2019 ADP, LLC. All rights reserved.

6. Cryptography

A. Cryptographic Controls

[10.1.1] Policy on the use of cryptographic controls

ADP requires that sensitive information being exchanged between ADP and ADP third parties must be encrypted (or transport channel must be encrypted) using industry accepted encryption techniques and strengths. Alternatively, a private leased line must be used.

B. Key Management

[10.1.2] Key management

ADP has an internal Encryption Security Standard that includes well-defined key management and key escrow procedures, including both symmetric and asymmetric keys management.

Encryption keys used for ADP information are always classified as confidential information. Access to such keys is strictly limited to those who have a need to know and, unless an exception approval is provided, encryption keys are not revealed to consultants, contractors, temporary associates, or third parties.

For encryption, copies of server certificates are exported and secured. Certificates are managed via a VeriSign Global Server account.

Copyright © 2019 ADP, LLC. All rights reserved.

7. Physical and Environmental Security

A. Physical Security

[11.1.1] Physical security perimeter

[11.1.3] Securing offices, rooms and facilities

ADP ensures that designated workspaces for payroll processing and information processing facilities are physically isolated from the rest of the facility through the use of secured access controls and walls extending from floor to ceiling.

B. Physical Access Control Mechanisms

[11.1.2] Physical entry controls

ADP facilities

Access to ADP facilities requires electronic security badges using card key authentication and the maintenance of physical access logs to the premises.

Any access, including access to sensitive areas of ADP facilities, such as server rooms and tape libraries, is controlled by Electronic Access Control (EAC) mechanisms.

Data Centers

ADP hosting infrastructures are all contained within physically secured environments. Access to the hosting center requires electronic security badges using card key and pin or biometric authentication and the maintenance of a physical access logs to the premises.

C. Review of Access to Sensitive Areas

[9.2.1] User registration and de-registration

[11.1.2] Physical entry controls

ADP facilities

Access to ADP facilities and sensitive areas is restricted to ADP employees and other authorized persons. Access to facility resources is granted on the basis of each individual's work responsibilities.

Audit trails are kept of all admissions in and out of all buildings and sensitive areas. Audit trails are maintained and reviewed as appropriate.

Data Centers

The data center security officer and/or facilities manager is/are responsible for managing access rights to any ADP data center. ADP is responsible for maintaining and controlling access to ADP areas according to a pre-approved list.

Audit trails are kept of all admissions in and out of data centers. Audit trails are maintained and reviewed by hosting center management and audit personnel on a monthly basis.

In order to gain admittance into the data centers, all visitors must be announced in advance and accompanied by authorized personnel once in the facility.

ADP management reviews the accuracy and appropriateness of physical access rights to ADP data centers monthly and for other ADP facilities at least on an annual basis. Access is removed when an employee leaves ADP.

Copyright © 2019 ADP, LLC. All rights reserved.

D. Identification of ADP Personnel

[11.1.5] Working in secure areas

ADP facilities

All ADP personnel must wear and display their identification badges at all times within ADP facilities. Visitors are required to sign a visitors' log, wear a visitor badge and be escorted by ADP personnel.

Data Centers

All ADP personnel, clients, contractors, and visitors must wear and display data center's identification badge at all times within the data center. Clients, contractors, and visitors are required to be accompanied by authorized personnel.

Tailgating or any similar practices of allowing an unauthorized person to enter behind or along with an authorized cardholder, or attempting to enter where a cardholder has not been granted access, are prohibited.

E. Physical and Environmental Security Controls in Data Centers

[11.1.4] Protecting against external and environmental threats

ADP data center facilities are monitored using controls of environmental conditions, surveillance cameras, motion detection cameras and security guards. All facilities utilize entry alarms.

Physical and environmental controls against reasonably anticipated site specific disasters such as flood and fire have been applied to ADP data centers.

ADP data centers have a minimum of the following environmental and physical security controls:

a) Redundant HVAC (heating, ventilation, and air conditioning) systems
b) Temperature/humidity monitoring
c) Local and remote alarms (power, temperature, humidity)
d) N+1 UPS
e) Redundant power supply
f) Automatic fire detection alarm
g) Automatic fire suppression
h) Additional manual fire suppression mechanisms
i) Servers located in protected areas

Cables and wires connected to or coming from computing equipment and peripherals are routed to minimize damage. Power distribution cabling for the computer equipment is located in trays under a raised floor or in conduits routed above the suspended ceiling. Only dedicated staff from hosting center and authorized support personnel can access phone/cable closets. Equipment is continuously monitored by automatic systems. All incidents are reviewed on a daily basis and corrective actions, such as replacement of equipment, are taken, as necessary. Appropriate change management controls also apply to equipment replacement.

Copyright © 2019 ADP, LLC. All rights reserved.

8. Operations Security

A. Formalization of IT Operations Procedures

[12.1.1] Documented operating procedures

GETS is the ADP unit responsible for IT infrastructure operations and maintenance. GETS formally maintains and documents IT operations policies and procedures. These procedures include, but are not limited to the following:

a) Change management
b) Back-up management
c) System error handling
d) System restart and recovery
e) System monitoring
f) Jobs scheduling and monitoring

B. Infrastructure Change Management

[12.1.2] Change management

A periodic Change Advisory Board (CAB), including representatives from a wide variety of ADP teams, is held by GETS. CAB meetings take place to discuss impacts, to agree on deployment windows and to approve the promotions to production, as well as to coordinate any other change in the production infrastructure.

C. System Capacity Planning and Acceptance

[12.1.3] Capacity management

Capacity requirements are continuously monitored and regularly reviewed. Following these reviews, systems and networks are scaled up or down accordingly.

When significant changes have to be performed due to a change in capacity or a technological evolution, the GETS benchmarking team can perform stress tests to the relevant application and/or system, thus providing a detailed report of performance evolution by gauging the changes in (i) components, (ii) system configuration or version, or (iii) middleware configuration or version.

D. Protection against Malicious Code

[12.2.1] Controls against malware

Antivirus software is installed on all computer systems connected to an ADP network, and virus signatures are updated automatically and periodically as per vendor updates and release schedule.

E. Back-Up Management Policy

[12.3.1] Information backup

ADP has policies in place that require all production hosting operations to back-up production information. The scope and the frequency of back-ups are executed in accordance with the business requirements of relevant ADP services, the security requirements of the information involved, and the criticality of the information in respect of disaster recovery.

According to those requirements, the following back-ups are performed:

Copyright © 2019 ADP, LLC. All rights reserved.

a) Daily incremental back-ups
b) Weekly full back-ups
c) Monthly full back-ups

Monitoring of scheduled back-ups is performed by GETS, in order to identify back-up issues or exceptions. Any issue identified or abnormal event will trigger a ticket in ADP's case management system and will be tracked until resolution.

F. Security Logging and Monitoring

[12.4.1] Event logging

[12.4.3] Administrator and operator logs

ADP has implemented a central and read-only logging infrastructure (SIEM) and a log correlation and alerting system (TPSI). Log alerts are monitored and treated in a timely manner by the CIRC.

Such logs include, but are not limited to:

- IDS
- Firewalls
- DNS
- LDAP
- Active Directory
- Operating System
- Internet accesses
- SMTP Gateways

All of these systems are synchronized using a unique NTP based clock reference.

Every single log contains at a minimum:

- Timestamp
- Who (identity of the operator or administrator)
- What (information about the event)

Audit trails and System logging for ADP applications have been designed and set up in order to track the following information:

- Authorized access
- Privileged operations
- Unauthorized access attempts
- Systems alerts or failures
- Changes to systems security settings, when the system allows such logging

These logs are only available to ADP authorized personnel, and are sent in live mode to prevent data from being tampered with before being stored in the secure logging appliances.

G. Infrastructure Systems and Monitoring

[12.4.1] Event logging

ADP uses appropriate measures to provide infrastructure monitoring 24 hours per day, 7 days per week. Disruption alerts are managed by different teams according to their severity level and the skills required to resolve them.

Copyright © 2019 ADP, LLC. All rights reserved.

ADP hosting center facilities employ monitoring applications that are constantly running on all related processing systems and on the network components to provide ADP staff proactive notification of issues and warnings in anticipation of possible problems. These application functions include, but are not limited to, the following:

- Monitoring and analysis of web site traffic
- Monitoring network equipment
- Monitoring and management of Internet circuit performance and availability
- Monitoring IDS sensors and firewalls for intrusions

H. Technical Vulnerability Management

[12.6.1] Management of technical vulnerabilities

All computers installed in the hosting infrastructure must comply with the installation of a specialized security hardened operating system (or secure build process). Hosted operations employ a hardened, approved and standardized build for every type of server used within our infrastructure. Out-of-the-box installation of operating systems is prohibited since these installations may create vulnerabilities, such as generic system account passwords, that would introduce an infrastructure risk. These configurations reduce the exposure of hosted computers running unnecessary services that can lead to vulnerabilities.

PTSS is responsible for managing the entire assessment and remediation processes. PTSS is independent and maintains a separation of duties from other teams that are responsible for participating in the process, requesting services, and providing remediation efforts.

ADP has developed a documented methodology for conducting release and periodic vulnerability assessments and compliance reviews of Internet facing web-based applications and their corresponding infrastructure components, which include at least 15 primary categories of testing.

Assessment methodology is based on both internal and industry best practices, including, but not limited to, Open Web Application Security Project (OWASP), SANS Institute and Web Application Security Consortium (WASC).

Copyright © 2019 ADP, LLC. All rights reserved.

9. Communications Security

A. Network Security Management

[13.1.1] Network controls

[13.1.2] Security of network services

ADP employs a network-based intrusion detection system that monitors traffic at the network infrastructure level (24 hours a day, 7 days a week) and identifies suspicious activity or potential attacks.

ADP only permits modem usage under special, duly justified circumstances and that usage is limited to dial out. Wireless network and access points must be approved by security and are only permitted when configured using secure protocols.

ADP has defined a network management policy and related controls:

a) *Security parameter changes documentation and authorization*: Security parameter change requests (like firewall rule sets) are documented, qualified and authorized by the network competency center prior to being applied into the production environment.

b) *Firewalls facilities and DMZ protections*: ADP network access points are protected by firewalls facilities and Demilitarized Zones (DMZ).

c) *Segregation of network segments*: Production network segments are logically segregated from the end-user network and between environments with different security level.

d) *Relay servers*: Access to systems (network components, application and database servers) is only permitted from authorized relay servers or authentication DMZ.

e) *Data transmission security between ADP data center/infrastructure and its clients*: External data transmissions between ADP data center and its clients are secured via one of the following network means: private leased line, IPSec VPN, MPLS-VPN. Web applications use ADP-approved encryption technology to secure data transmitted by clients to ADP data centers.

Additionally, the GETS Network competency center has implemented a firewall compliance tool. Firewall flows are subjected to change management process before being implemented.

B. Exchange of Information

[13.2.1] Information transfer policies and procedures

ADP implements appropriate controls so that ADP clients' information sent to third parties is transferred between authorized information systems and resources only, and is only exchanged through ADP’s secure and authorized transfer mechanisms.

C. Use of Messaging Systems

[13.2.3] Electronic messaging

ADP prohibits the use of non-secured external instant messaging applications for transmission of client data.

Copyright © 2019 ADP, LLC. All rights reserved.

10. System acquisition, development, and maintenance

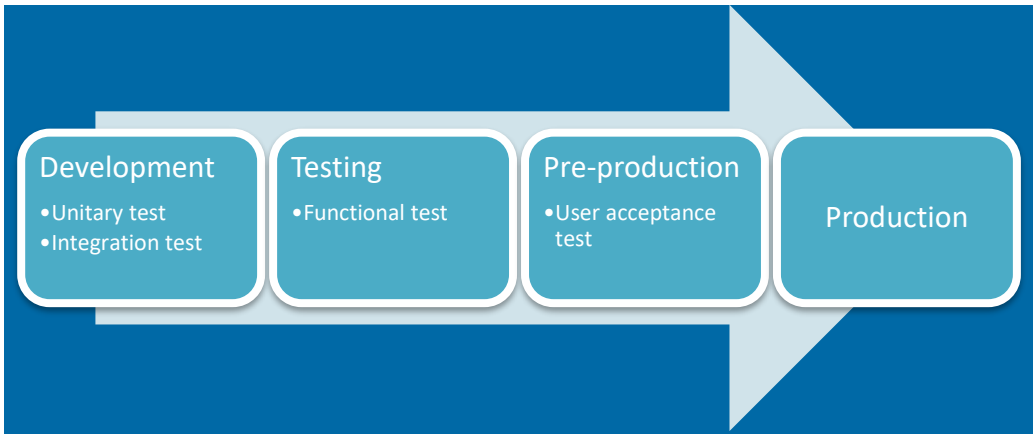
A. Security in Development and Support Processes

[14.1.1] Information security requirements analysis and specification

[14.2.1] Secure development policy

[14.2.2] System change control procedures

During the development cycle, applicable documentation is generated and testing plans are built for the testing phase. Different stages are defined for each environment with relevant approval at each phase:



- From testing to pre-production environment, approval from ADP's Quality team is needed.
- From pre-production to production, approval from IT Operations is required.

Development teams are required to utilize secure coding methods. Application changes are tested in development and regression environments before they reach the production systems. Tests are performed and documented. Upon approval, changes are deployed into production. Penetration testing is performed after siginificant changes.

A periodic CAB, including representatives from a wide variety of ADP teams, is held by GETS. CAB meetings take place on a regular basis, and are meant to discuss impacts, to agree on deployment windows and to approve the promotion of software packages to production, as well as to inform about any other changes in production infrastructure.

ADP's IT Operations team provides the final approval before any promotion to production environment of the software packages.

B. Security in Development Environment

[14.2.6] Secure development environment

All environments are logically segregated and independent from each other. Software packages are accessible at each stage of the development process and only by the teams involved in that particular stage.

Copyright © 2019 ADP, LLC. All rights reserved.

C. Test Data

[14.3.1] Protection of test data

Use of real or unsanitized data in development and testing is not permitted as per ADP's global security policy unless explicitly requested and authorized by client.

Copyright © 2019 ADP, LLC. All rights reserved.

11. Supplier relationships

A. Identification of Risks Related to External Parties

[15.1.1] Information security policy for supplier relationships

Risk assessments of third parties who require access to ADP and/or client information are periodically performed with a view to determine their compliance with ADP security requirements for third parties, and to identify any gaps in the applied controls. If a security gap is identified, new controls are agreed upon with such external parties.

B. Information Security Agreements with External Parties

[15.1.2] Addressing security within supplier agreements

ADP enters into agreements with all third parties which include appropriate security commitments in order to meet ADP's security requirements.

Copyright © 2019 ADP, LLC. All rights reserved.

12. Information Security Incident Management

A. Management of Information Security Incidents and Improvements

[16.1.1] Responsibilities and procedures

[16.1.4] Assessment of and decision on information security events

ADP has developed a documented methodology for responding to security incidents quickly, consistently, and effectively.

Should an incident occur, a predefined team of ADP employees will activate a formal incident response plan that addresses areas such as:

- Escalations based on the classification of incident or incident severity
- Contact list for incident reporting/escalation
- Guidelines for initial responses and follow up with involved clients
- Compliance with applicable security breach notification laws
- Investigation log
- System recovery
- Issue resolution, reporting, and review
- Lessons learned

ADP policies define a security incident, incident management and all employees' responsibilities regarding the reporting of security incidents. All ADP employees and contractors must read and follow these policies.

ADP also schedules regular training for ADP employees and contractors to ensure awareness of reporting requirements.

Copyright © 2019 ADP, LLC. All rights reserved.

13. Information Security Aspects of Business Resiliency Management

A. ADP Business Resiliency Program

[17.1.1] Planning information security continuity

One of ADP's priorities is to establish, maintain and test comprehensive business resumption and contingency planning programs. These programs must allow for the timely and effective recovery of mission-critical ADP business functions in the event of a partial or total loss, preventing an extended period of disruption to any ADP client or ADP business unit.

ADP's Executive Management is committed to protecting ADP's business operations from disruption, ensuring that:

- An understanding of the benefits and goals of the Business Resiliency Program are defined and a proactive approach is taken to Business Resiliency;
- Formal procedures are established to manage business disruptions;
- Business Resiliency requirements are included and implemented in business operations;
- Business Resiliency concepts and controls are understood by associates responsible for responding to incidents and business disruptions;
- Resource requirements are estimated to resume business operations including staffing, facilities, technical infrastructure, information, external services and suppliers and proper resources are allocated to the Business Resiliency Program.

ADP Business Resiliency Organization has documented the Business Resiliency responsibilities of the organization based on Management directives. Among other responsibilities, the ADP Business Resiliency Organization is in charge of:

- Maintaining the Business Resiliency Policy, Standards, Practices and Guidelines for the organization, including the review of these documents on a periodic basis;
- Establishing common systems designated to be used for Plan documentation and notification/escalation processes;
- Maintaining the Business Resiliency Program, including regular reviews, audits, updates to documentation and related procedures;
- Establishing metrics for measuring and demonstrating program effectiveness and maturity;

ADP's Business Resiliency Program is composed of three main components:

- Incident Management, which is in charge of major incident management, and preventing them from escalating to a crisis;
- Business Continuity, to develop protocols that ensure the resumption of business operations;
- Disaster Recovery, where operating procedures to address restoration processes are created and maintained for ADP's critical systems;

B. Implementation of Business Resiliency

[17.1.2] Implementing information security continuity

[17.1.3] Verify, review and evaluate information security continuity

Copyright © 2019 ADP, LLC. All rights reserved.

The three components of ADP's Business Resiliency Program – Incident Management, Business Continuity, and Disaster Recovery – are deployed following the following phases:

- **Risk Threat Analysis (RTA)**
  The Risk Threat Analysis is used to evaluate threats against all ADP locations worldwide, and rate this risk in order to assign a risk level to each facility. It is required to be reviewed periodically or sooner if a significant event has occurred.

- **Business Impact Analysis (BIA)**
  A formal Business Impact Analysis has been conducted and is regularly reviewed to identify critical business processes that need to be recovered after a business disruption. The BIA is required to be reviewed and revised periodically or sooner if a significant event or a change in a critical business function has occurred. The Business Impact Analysis identifies:
  - Critical business functions and processes;
  - IT applications that support the identified critical business functions;
  - Interdependencies of processes, assets, infrastructure and resources;
  - Recovery Time Objectives (RTO's) and Recovery Point Objectives (RPO's) for processes and data;
  - Estimated potential losses from a business disruption.

- **Incident Management and Business Continuity Plans Development**
  Once the RTA and BIA are completed, all information is compiled and Incident Management Plans and Business Continuity Plans are created.

  ADP has defined this set of plans and capabilities that work together collectively to enhance the ADP Business Resiliency Program thereby minimizing the adverse impacts a disruption may have on ADP service delivery to clients and third parties.

- **Testing and Exercising**
  Business Resiliency Plans are tested periodically through a table-top exercise held with the Crisis Committee. This exercise is limited to a basic scenario and a theoretical discussion, testing the abilities and reaction capabilities of the Incident Management Committee.

- **Maintenance**
  The overall Business Resiliency Program is reviewed and revised at least once annually or more frequently as required due to changes in personnel or other circumstances. Additionally, various components may be subject to periodic reviews.

C. Availability of Disaster Recovery Facilities

[17.2.1] Availability of information Processing facilities

[10.5] Back-Up

In addition, a standard Disaster Recovery operating procedure contains detailed plans to address restoration processes for ADP's mission critical systems, based on the following scenarios:

- Critical equipment failure at the primary computing center
- Site disaster at the primary computing center

Copyright © 2019 ADP, LLC. All rights reserved.

ADP data is synchronized on an ongoing basis between the primary Data Center and the disaster recovery site. Local back-ups are also stored in the primary Data Center in order to keep a longer period and volume of data.

The IT department conducts an annual test of its ability to restore the IT platforms and communication capabilities, which support the critical business functions. Business units define and validate the DRP test scope together with GETS. Once the DRP scope is defined and validated, several teams from the IT department and business units are involved.

The Disaster Recovery test methodology covers the following areas:

- Disaster Recovery Plan Playbook: technical documentation to activate the DRP;
- Disaster Recovery testing: technical and functional test scripts to validate DRP activation;
- Disaster Recovery test results: executive report, including results of the DRP test as well as findings and lessons learned;
- Disaster Recovery improvement activities: post mortem review action items and plan.

Guidelines describing preparatory measures and communication plans in case of a severe incident are published and communicated to all employees and relevant external parties, in order to be prepared. These include:

- Internal and external communication guidelines;
- Preparatory guidelines and preventive measures for employees;
- Planned or unplanned building evacuation simulation, updated annually.

Copyright © 2019 ADP, LLC. All rights reserved.

14. Compliance

A. Compliance with Legal Requirements

[18.1.1] Identification of applicable legislation and contractual requirements

ADP privacy and security controls are designed to allow us to meet the obligations imposed on data processors by data protection laws in all of the countries where ADP offers its services, including those deriving from the Data Protection Directive 95/46/EC and EU's Global Data Protection Regulation (officially, Regulation (EU) 2016/679) on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

ADP reserves the right to use third party data processors and subcontractors including for processing, hosting and storage purposes. ADP remains responsible for the quality of the services and for these sub-processors' compliance with data protection / privacy law as it applies to data processors. ADP is committed to working with its clients to achieve an appropriate level of transparency around its use of sub-processors.

In order to protect its clients' personal data (client information) wherever they are processed, ADP has implemented a Global Privacy Policy that provides the foundation for the processing of client data worldwide. The Global Privacy Policy requires every ADP affiliate and every ADP associate to protect client personal data and to only use it for the purposes specified in our client contracts.

B. Compliance with Security Policies and Standards

[18.2.1] Independent review of information security

[18.2.3] Technical compliance review

To the extent indicated in the terms and conditions of the Agreement, ADP performs a SOC1[2] type II audit on a periodic basis. These audits are conducted by a well-known third-party audit firm and audit reports are available on a yearly basis for clients upon request, when applicable.

C. Technical Compliance

[18.2.2] Compliance with security policies and standards

In order to ensure technical compliance with best practices, ADP performs regularly scheduled network vulnerability scans. The scan results are then prioritized and developed into corrective action plans with the hosting teams and their management.

Vulnerability scans are performed on a product-by-product basis. Utilizing specialized application scanning tools, application level vulnerabilities, if any, are identified, shared with the product development management teams, and incorporated into the quality assurance processes for corrective action. The results are analyzed and corrective action plans developed and prioritized.

[2] In the case of certain US Services offered by ADP, there would be also SOC 2 Type II exec. reports

Copyright © 2019 ADP, LLC. All rights reserved.

D. Retention of Data

[18.1.3] Protection of records

ADP's data retention policy regarding client information is designed to comply with applicable laws.

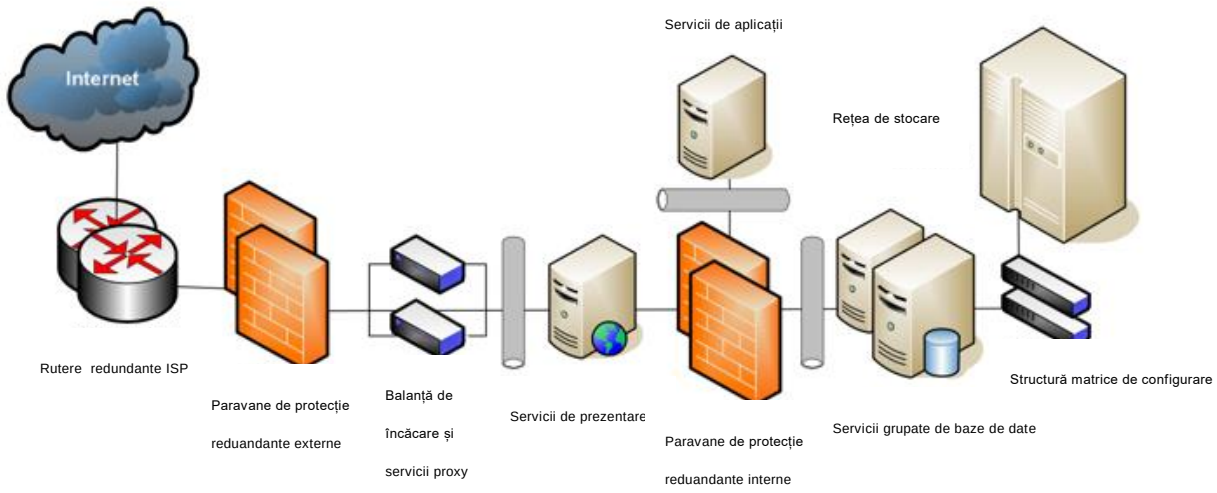
At the end of a client contract, ADP will comply with its contractual obligations relating to client's information, i.e. ADP will either return, or allow client to retrieve (e.g. by data download), all client information required for the continuity of client's business activities (if not previously provided). Then ADP will securely destroy remaining client information, except to the extent required under applicable law, authorized by the client or needed for dispute resolution purposes.

Copyright © 2019 ADP, LLC. All rights reserved.

15. Appendix

A. Logical Network Diagram

Imaginea de mai jos este o reprezentare logică a modalității de abordare:



Copyright © 2019 ADP, LLC. All rights reserved.

ANEXĂ 3 – Lista companiilor grupului obligate să respecte codul de conduită privind împuternicitul operatorului de date

ADP (Philippines), Inc	6/F Glorietta 2 Corporate Center, Palm Drive, Ayala Center, Makati City, Filipine, 1224
ADP (Suisse) SA	Lerzenstr. 10, 8953 Dietikon, Elveția
ADP Canada Co.	3250 Bloor Street West, 16th Floor, Etobicoke, Ontario M8X 2X9, Canada
ADP Employer Services Belgium BVBA	Koningsstraat 97/4, 1000 Bruxelles, Belgia
ADP Employer Services Ceska Republika a.s.	Rohanske nabrezi 670/17, 18600 Praga 8, Cehia
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 Barcelona, Spain
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 Tunis, Tunisia
ADP Europe, S.A.S.	31, avenue Jules Quentin, 92000 Nanterre, Franța
ADP France SAS	31, avenue Jules Quentin, 92000 Nanterre, Franța
ADP Gestion des Paiements SAS	31, avenue Jules Quentin, 92000 Nanterre, Franța
ADP GlobalView B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Olanda
ADP GSI France SAS	31-41, avenue Jules Quentin, 92000 Nanterre, Franța
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, Olanda
ADP Nederland B.V.	K.P. van der Mandelelaan 9-35, 3062 MB Rotterdam, Postbus 4065, 3006 AB Roterdam
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 Varșovia, 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, Anglia, WC2A 1LS
ADP RPO, LLC	3401 Technology Drive, Finlanda, OH, USA 45840
ADP Screening and Selection Services, Inc.	One ADP Boulevard, Roseland, NJ, USA 07068
ADP Slovakia s.r.o.	Cernysevskeho 26, 851 01 Bratislava, Slovacia
ADP Software Solutions Italia SRL	Via Oropa 28 – 10153 Torino, Italia
ADP, LLC	One ADP Boulevard, Roseland, NJ, USA 07068

Copyright © 2019 ADP, LLC. All rights reserved.

Automatic Data Processing (ADP) Romania SRL	4B Gara Herastrau St., 1st – 6th floor, District 2, București, România 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, St. Petersburg, 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
Ridgenumber - Processamento de Dados LDA	Rua Brito e Cunha, 254 - 2º, 4450-082 Matosinhos, Portugalia
The Marcus Buckingham Company	8350 Wilshire Boulevard, #200, Beverly Hills, CA, USA 90211
VirtualEdge Corporation	One ADP Boulevard, Roseland, NJ, USA 07068

Copyright © 2019 ADP, LLC. All rights reserved.