Declarație de securitate și confidențialitate a Edenred Romania

1. Notă introductivă

Edenred România are angajamentul de a proteja securitatea și confidențialitatea tuturor informațiilor cu privire la clienți, consumatori și angajați.

Programul nostru de Securitate și Confidențialitate a Informației are la bază standardul ISO 27001 de securitate a informațiilor și cadrul de confidențialitate ISO 29100 și urmează o abordare bazată pe riscuri care cuprinde oameni, procese și tehnologii.

Echipa de Securitatea Informației (SI) din cadrul Edenred Franța este dedicată protecției informațiilor din rețeaua internațională Edenred. Echipa SI raportează direct nivelului superior de conducere și beneficiază de o rețea de specialiști în confidențialitate și securitate de pe glob, focalizați pe protecția continuă a informațiilor noastre.

Strategia noastră pentru livrarea de produse securizate este fundamentată pe cinci piloni, si anumeLeadership, Conștientizare, Managementul riscurilor, Securitatea Operațiunilor si Tehnologiilor și Conformitatea.

Leadership - ne construim programul și strategia de securitate și confidențialitate în jurul bunelor practici din industrie, standardelor de securitatea informației și a celor mai recente reglementări în materie de confidențialitate. Utilizăm un set de procese, tehnologii și resurse umane documentate și implementate astfel încât să atingem obiectivele de securitatea și confidențialitatea informațiilor.

Conștientizare - securitatea informațiilor începe cu securitatea oamenilor noștri și a resurselor manipulate de aceștia. Avem coduri etice dedicate, politici de securitate și confidențialitatea informațiilor care stabilesc regulile pentru protecția și confidențialitatea informațiilor și necesitatea interzicerii divulgării neautorizate a acestora.

Managementul riscurilor – utilizăm o abordare bazată pe riscuri pentru a identifica riscurile legate de securitatea și confidențialitatea informațiilor în cadrul proceselor comerciale. Cultivăm înțelegerea și managementul riscurilor la nivel comercial și oferim suport continuu în vederea aplicării celor mai bune opțiuni de remediere.

Securitatea Operațiunilor si Tehnologiilor – o provocare curenta pentru noi o reprezintă livrarea celor mai bune produse pe piață cu cele mai noi tehnologii ținând cont de confidențialitate și securitate. Ne asigurăm că cerințele de securitate și de confidențialitate sunt îndeplinite de orice nou sistem IT, că setul nostru de controale de securitate IT pentru managementul utilizatorilor, monitorizarea securității, consolidării sistemelor și protecția datelor sunt implementate și monitorizate. Testele de vulnerabilitate și evaluările de securitate ale sistemelor cheie asigură eficiența controalelor și confirmă bunele practici pentru dezvoltare pe care le utilizăm. Sistemele noastre informatice sunt protejate de controale de securitate precum firewall, sistem de

securitatea informației și managementul evenimentelor, tehnologie antivirus pe niveluri, securitate la nivel de e-mail și sisteme de prevenție a intruziunii.

Conformitate – echipa noastră de Audit intern efectuează periodic audituri independente și verificări pentru evaluarea conformității cu cadrul de securitate internă și legislația aplicabilă cu privire la protecția datelor. În coordonare cu Departamentele Juridic și Conformitate, revizuim și furnizăm periodic recomandări privind securitatea informațiilor pentru cadrul nostru contractual.

2. Măsuri de securitatea informațiilor pentru protecția datelor personale

Vă aducem la cunoștință în continuare declarațiile noastre pentru securitate și confidențialitate cu privire la controalele aplicabile.

Politici pentru securitatea informațiilor - un set de politici pentru securitatea informațiilor este definit, aprobat de conducere, publicat și comunicat angajaților și părților externe relevante.

Revizuirea politicilor de securitatea informațiilor – pentru a asigura caracterul potrivit, adecvat și eficacitatea, revizuim politicile noastre de securitatea informațiilor la intervale stabilite sau atunci când au loc schimbări importante.

Roluri și responsabilități cu privire la securitatea informațiilor – stabilim și alocăm responsabilități specifice cu privire la securitatea informațiilor către toți angajații și părțile interesate.

Segregarea atribuțiilor – segregăm domenii de responsabilitate pentru a reduce riscurile unor modificări neautorizare sau neintenționate, ori utilizarea neadecvată a activelor societății.

Contactul cu autoritățile – păstrăm contacte corespunzătoare cu autoritățile competente și organele de supraveghere.

Contactul cu grupuri de specialiști – păstrăm contacte corespunzătoare cu grupuri de specialiști și organizații profesionale din domeniul securității și confidențialității, specifici industriei relevante.

Securitatea informației în managementul proiectelor – abordăm securitatea informațiilor în managementul proiectelor, indiferent de tipul de proiect.

Politica dispozitivelor mobile – utilizăm o politică și măsuri aferente pentru a trata riscurile legate de utilizarea dispozitivelor mobile.

Teleworking – utilizăm o politică și măsuri aferente pentru a proteja informațiile accesate, prelucrate sau stocate în spațiile de teleworking.

Verificarea personalului înainte de angajare – verificăm istoricul tuturor candidaților pentru angajare, în conformitate cu legile, reglementările și etica aferentă, și proporțional cu cerințele activității, clasificarea informațiilor ce vor fi accesate și riscurile observate.

Termenii și condițiile angajării – acord contractual între noi și angajații noștri, care expun responsabilitățile ambelor părți cu privire la securitatea informației.

Responsabilitățile conducerii – conducerea solicită ca toți angajații și contractanții să aplice securitatea informațiilor în conformitate cu politicile și procedurile stabilite de societate.

Conștientizarea educarea și formarea cu privire la securitate – toți angajații societății beneficiază de educare și formare aferentă în mod regulat, în vederea conștientizării, cu privire la noutățile periodice legate de politicile și procedurile organizaționale, după cum este necesar pentru funcția pe care o dețin.

Încetarea sau modificarea responsabilităților angajaților – reponsabilitățile și atribuțiile cu privire la securitatea informațiilor vare rămân valabile după încetarea sau modificarea angajării sunt definite, comunicate angajatului sau contractantului și sunt aplicate.

Inventarierea și proprietatea activelor – identificam activele asociate cu informațiile, datele cu caracter personal și infrastructura pentru prelucrarea informațiilor și menținem la zi un inventar al acestor active. Definim de asemenea proprietatea asupra activelor.

Utilizarea acceptabilă a activelor – se definesc, se documentează și implementează reguli pentru utilizarea acceptabilă a informațiilor și activelor asociate informațiilor și infrastructura pentru prelucrarea informațiilor.

Returnarea activelor – angajații și utilizatorii externi returnează toate activele societății care se află în posesia lor, la încetarea calității de angajat, respectiv la încetarea contractului sau acordului de colaborare.

Clasificarea și etichetarea informațiilor – informațiile sunt clasificate utilizând schema internă de clasificare. Dezvoltăm si implementam o procedura adecvată pentru etichetarea informației în conformitate cu schema de clasificare a informațiilor pe care am adoptat-o.

Manipularea activelor – utilizăm proceduri pentru gestionarea activelor, definite în corelație cu schema de clasificare adoptata.

Managementul și eliminarea suporturilor mobile – utilizăm o procedură care implementează managementul suporturilor mobile conform schemei de clasificare adoptate. Atunci când nu mai sunt necesare, suporturile sunt eliminate în mod securizat.

Transferul pe suport fizic – suporturile care conțin informații sunt protejate împotriva accesului neautorizat, utilizării greșite sau alterării în timpul transportului.

Politica de control a accesului – utilizăm o politică de control a accesului care este revizuită pe baza cerințelor activității și securității informațiilor.

Accesul la rețele și servicii de rețea – utilizatorilor li se oferă acces numai la rețelele/serviciile de rețea pe care au fost autorizați să le utilizeze.

Înregistrarea și anularea înregistrării – implementăm un proces formal de înregistrare a utilizatorului și anulare a înregistrării pentru a permite alocarea de drepturi de acces.

Furnizarea accesului utilizatorilor – utilizăm un proces formal pentru furnizarea accesului utilizatorilor, în vederea alocării și revocării drepturilor de acces pentru toate tipurile de utilizatori către toate tipurile de sisteme și servicii.

Managementul drepturilor de acces privilegiate – alocarea și utilizarea drepturilor de acces privilegiate sunt restricționate și controlate.

Managementul informațiilor secrete de autentificare a utilizatorilor – utilizăm un proces pentru a controla alocarea informațiilor secrete de autentificare.

Revizuirea drepturilor de acces al utilizatorilor – deținătorii activelor revizuie drepturile de acces ale utilizatorilor la intervale regulate.

Revocarea și adaptarea drepturilor de acces – drepturile de acces ale tuturor angajaților și utilizatorilor externi la informații și la facilitățile de prelucrare sunt revocate la încetarea funcțiilor, contractului sau acordului sau sunt adaptate atunci când apar modificări.

Utilizarea informațiilor secrete de autentificare – utilizatorii respectă bunele noastre practici în utilizarea informațiilor secrete de autentificare.

Restricții de acces la informații – accesul la informații și la funcțiile sistemului de aplicații este restricționat în concordanță cu politica de control a accesului.

Proceduri de conectare securizată – accesul la sisteme și aplicații este controlat de o procedură de conectare securizată.

Sistemul de management al parolelor – utilizăm un sistem interactiv de management al parolelor, pentru a asigura calitatea acestora.

Utilizarea de programe utilitare privilegiate – restricționăm utilizarea programelor utilitare care ar putea să se suprapună controalelor sistemului și aplicațiilor.

Controlul accesului la codul sursă al programelor – restricționăm accesul la codul sursă al programelor.

Controale criptografice și managementul cheilor – implementăm o politică pentru pentru utilizarea controalelor criptografice pentru protecția informațiilor și utilizarea, protecția și durata de viață a cheilor criptografice.

Perimetre de securitate fizică și controale de acces – utilizăm perimetre de securitate pentru a proteja zonele care conțin fie informații sensibile sau critice și facilitățile de prelucrare a informațiilor. Zonele securizate sunt protejate cu controalele de intrare corespunzătoare pentru a asigura permiterea accesului numai angajaților autorizați.

Securizarea birourilor, încăperilor și facilităților – utilizăm controale de securitate fizică pentru a securiza mediul de lucru împotriva dezastrelor naturale, atacurilor răuvoitoare sau accidentelor. Definim și implementăm proceduri pentru securitatea la locul de muncă.

Zonele de livrare și de încărcare – punctele de acces precum zonele de livrare și de încărcare sunt controlate și când este posibil sunt izolate de facilitățile de prelucrare a informațiilor, pentru a evita accesul neautorizat.

Instalarea și protecția echipamentelor – echipamentele sunt instalate și protejate astfel incat sa reducem riscurile potentiale apărute din amenințări și pericole legate de mediu dar și posibilitatea accesului neautorizat.

Securitatea infrastructurii de cablare și a infrastructurii suport – echipamentele sunt protejate împotriva penelor de curent și alte întreruperi cauzate de pene în utilitățile de susținere. Cablurile electrice și de telecomunicații care transmit date sau susțin serviciile de informații sunt protejate împotriva intercepției, interferenței sau deteriorării.

Mentenanța echipamentului – echipamentele sunt întreținute corect pentru a asigura disponibilitatea și integritatea.

Mutarea activelor – echipamentele, informațiile sau programele nu sunt transferate în alte locații fără autorizație prealabilă.

Securitatea echipamentelor și activelor în afara spatiilor societatii – protejam activele noastre si în afara incintei, luând în considerare diferitele riscuri asociate muncii în afara incintelor societatiisocietatii.

Casarea și reutilizarea securizata a echipamentelor – echipamentele care conțin suporturi de stocare sunt verificate pentru a garanta eliminarea sau suprascrierea securizata a informațiile sensibile și programelor licentiateîn mod securizat.

Echipamentul neasistat al utilizatorului – echipamentul neasistat al utilizatorului folosește protecție adecvată.

Politica biroului curat și a ecranului curat – am adoptat o politică a biroului curat în ce privește hârtiile și suporturile de stocare mobile, precum și o politică a ecranului curat, pentru facilitatile de prelucrare a informațiilor.

Proceduri de operare documentate – folosim proceduri de operare și le-am pus la dispoziția tuturor utilizatorilor care au nevoie de ele.

Managementul schimbării – am implementat controale de securitatea informațiilor cu privire la eventualele modificări în organizație, procesele de activitate, facilitatile de prelucrare a informațiilor și sisteme.

Managementul capacității – monitorizăm și sincronizăm utilizarea resurselor și planificăm ajustări ale capacității atunci când volumul activității comerciale crește.

Separarea mediilor de dezvoltare, testare și productie – utilizăm medii separate pentru dezvoltare, testare și productie, pentru a reduce riscurile accesului neautorizat sau modificările în mediul de productie.

Controale împotriva atacurilor de tip malware – implementăm controale de detectie, prevenție și recuperare pentru a asigura protecția împotriva atacurilor de tip malware, la care adaugam siconștientizarea adecvată a utilizatorilor.

Copii de siguranță ale informațiilor – testăm în mod regulat copiile de siguranță ale informațiilor, programelor și imaginilor sistemului, conform politicii noastre cu privire la copiile de siguranță.

Jurnalizarea evenimentelor – generam, păstrăm și verificăm, în mod regulat, jurnalul de evenimente care înregistrează activitățile utilizatorilor, excepțiile, erorile și evenimentele legate de securitatea informațiilor.

Protecția informațiilor de jurnalizare – protejăm informațiile privind jurnalizarea și metodele de jurnalizare împotriva falsificării și accesului neautorizat.

Jurnalul administratorului și operatorilor – jurnalizăm atât activitățile administratorului, cât și ale operatorilor și protejăm și verificăm în mod regulat acele jurnale.

Sincronizarea ceasului – sincronizăm ceasurile pentru toate sistemele relevante de prelucrare a informațiilor la o singură sursă de timp de referință.

Instalarea de programe pe sistemele operaționale – am stabilit reguli care guvernează instalarea programelor pe sistemele operaționale, în special instalarea efectuată de utilizatori.

Managementul vulnerabilităților tehnice – vulnerabilitățile tehnice sunt gestionate prin obținerea lor în mod prompt, evaluarea expunerii societății și prin luarea măsurilor adecvate care adresează riscul asociat.

Controalele de audit al sistemelor informatice – cerințele de audit și activitățile care implică verificarea sistemelor operaționale sunt planificate și convenite înainte de a fi implementate, pentru a minimiza perturbările proceselor comerciale.

Controalele de rețea – gestionăm și controlam rețelele noastre pentru a asigura protecția informațiilor în sisteme și aplicații.

Securitatea serviciilor de rețea – în acordurile de servicii de rețea includem mecanismul de securitate, nivelurile de servicii și cerințele de management ale tuturor serviciilor de rețea.

Segregarea în rețele – separăm grupurile de servicii de informații, utilizatorii și sistemele informatice pe rețele.

Politici și proceduri privind transferul de informații – folosim politici, proceduri și controale oficiale de transfer pentru a asigura protecția informațiilor prin utilizarea tuturor tipurilor de metode de comunicare.

Acordurile privind transferul de informații – folosim clauze confidențiale în acordurile pentru a proteja transferul de informații comerciale între noi și terți.

Mesageria electronică – folosim mecanismul pentru a proteja informațiile transmise prin mesageria electronică.

Confidențialitatea sau acordurile de non-divulgare – clauzele de confidențialitate pe care le folosim în acordurile noastre sunt revizuite și documentate în mod regulat.

Analiza și specificațiile cerințelor de securitate a informațiilor – folosim cerințele de securitate a informației încă din stadiu incipient, atât pentru noile sisteme informatice, cât și pentru cele existente.

Securizarea serviciilor de aplicații pe rețele publice – protejăm informațiile implicate în serviciile de aplicații care trec prin rețelele publice împotriva activității frauduloase, litigiilor contractuale și dezvăluirea și modificarea neautorizată.

Protejarea tranzacțiilor serviciilor de aplicații – protejăm informațiile implicate în tranzacțiile cu serviciile de aplicații pentru a împiedica transmiterea incompletă, direcționarea greșită, modificarea neautorizată a mesajului, dezvăluirea neautorizată, duplicarea neautorizată a mesajului sau răspunsul.

Politica de dezvoltare securizată – utilizăm reguli privind dezvoltarea de software și sisteme.

Procedurile de control al schimbărilor de sistem – utilizăm reguli în cazul modificării sistemelor pe parcursul ciclului de viață al dezvoltării.

Revizuirea tehnică a aplicațiilor după modificarea platformelor de operare – analizăm și testăm aplicațiile critice în cazul schimbării platformelor de operare, pentru a ne asigura că nu vor avea un impact negativ asupra operațiunilor sau securității societății.

Restricții privind modificările aduse pachetelor software – am stabilit reguli privind modificarea aplicațiilor software, limitând această acțiune la modificările necesare.

Gestionarea securizată a tehnologiilor – utilizam principii de gestionare securizată a sistemelor, pe care le documentăm, menținem și aplicăm oricăror eforturi de implementare a sistemului informațional.

Mediu de dezvoltare securizat – folosim medii de dezvoltare securizate pentru eforturile de dezvoltare și integrare a sistemelor, care acoperă întregul ciclu de viață al dezvoltării sistemului.

Dezvoltare externalizată – în cazul dezvoltării externalizate, supervizăm și monitorizăm această activitate.

Testarea securității sistemului – testăm funcționalitățile de securitate în timpul dezvoltării.

Testarea acceptantei sistemelor – pentru noile sisteme informatice, actualizări și versiuni noi, am stabilit programe de testare a acceptantei și criterii aferente.

Protecția datelor de testare – atunci când selectăm datele de testare, o facem cu precautie, într-un mod protejat și controlat.

Politica de securitate a informațiilor pentru relația cu furnizorii – analizăm, documentăm și convenim împreună cu furnizorii noștri asupra cerințelor de securitate a informațiilor pentru a atenua riscurile asociate accesului furnizorului la activele societății.

Abordarea securității în cadrul acordurilor cu furnizorii – analizăm, documentăm și convenim cu fiecare furnizor de componente informatice asupra cerințelor relevante de securitate a informațiilor.

Lanțul de aprovizionare al tehnologiei informației și comunicațiilor – includem în acordurile cu fiecare furnizor, cerințele care abordează riscurile legate de securitatea informațiilor asociate serviciilor de tehnologie a informației și comunicațiilor și lanțului de aprovizionare a produselor.

Monitorizarea și revizuirea serviciilor furnizorilor – monitorizăm, revizuim și auditățm în mod regulat livrările de servicii ale furnizorilor.

Gestionarea modificărilor serviciilor furnizorilor – gestionăm modificările aduse de furnizorii noștri luând în considerare caracterul esențial al informațiilor, sistemelor și proceselor comerciale implicate și reevaluarea riscurilor.

Responsabilități și proceduri – utilizăm proceduri și responsabilități pentru a asigura un răspuns rapid, eficient și metodic la incidentele de securitate a informațiilor.

Raportarea evenimentelor de securitate a informațiilor – atunci când raportăm evenimente de securitate informatică, o facem prin intermediul canalelor adecvate de management în mod prompt.

Raportarea punctelor slabe privind securitatea informațiilor – angajații și contractanții notează și raportează orice slabiciuni privind securitatea informatiilor observate sau suspectate în cadrul sistemelor sau serviciilor.

Evaluarea și luarea deciziilor privind evenimentele de securitate a informațiilor – evaluăm și clasificăm în consecință evenimentele privind securitatea informațiilor pe care le întâlnim.

Răspunsul la incidentele de securitate a informațiilor – răspundem în timp util și în conformitate cu procedurile noastre interne la incidentele de securitate a informațiilor.

Învățarea din incidentele legate de securitatea informațiilor – folosim cunoștințele pe care le dobândim atunci când analizăm și soluționăm incidentele de securitate a informațiilor pentru a reduce probabilitatea sau impactul incidentelor viitoare.

Colectarea dovezilor – avem un proces de identificare, colectare, culegere și păstrare a informațiilor care pot servi drept dovezi.

Planificarea continuității securității informațiilor – am definit politici pentru continuitatea comercială care conțin cerințe privind securitatea informațiilor și continuitatea gestionării securității informațiilor în situații nefavorabile, cum ar fi situatiile de criză sau dezastrele.

Implementarea continuității securității informațiilor – implementăm politici pentru continuitatea activității pentru a asigura nivelul necesar de continuitate pentru securitatea informațiilor în timpul unei situații nefavorabile.

Verificăm, revizuim și evaluăm continuitatea securității informațiilor – verificăm în mod regulat politicile de continuitate a activității, pentru a ne asigura că acestea sunt valabile și eficiente în situațiile nefavorabile.

Identificarea legislației aplicabile și a cerințelor contractuale – identificăm, documentăm și monitorizăm toate cerințele legale, reglementare și contractuale ale legislației relevante pentru fiecare sistem informatic și societate.

Drepturi de proprietate intelectuală – implementăm procedurile adecvate pentru a asigura conformitatea cu cerințele legislative, reglementare și contractuale cu privire la drepturile de proprietate intelectuală și utilizarea produselor software de proprietar.

Protecția înregistrărilor, confidențialitatea și protecția datelor cu caracter personal – protejăm înregistrările împotriva pierderii, distrugerii, falsificării, accesului neautorizat și divulgării neautorizate, în conformitate cu cerințele legislative, reglementare și contractuale comerciale.

Confidențialitatea și protecția datelor personale – confidențialitatea și protecția datelor personale sunt asigurate în conformitate cu legislația și regulamentele unde este cazul.

Reglementarea controalelor criptografice – utilizăm controale criptografice în conformitate cu toate acordurile relevante, legislația și reglementările, unde este cazul.

Revizuirea independentă a securității informațiilor – abordarea societății privind gestionarea securității informațiilor și implementarea acesteia este revizuită independent la intervale planificate sau atunci când apar modificări semnificative.

Respectarea politicilor și standardelor de securitate – conformitatea procedurilor și prelucrării informațiilor este revizuită în mod regulat de către fiecare manager din aria lor de responsabilitate.

Revizuirea conformității tehnice – sistemele informatice sunt verificate în mod regulat pentru a respecta politicile și standardele de securitate ale societății cu privire la informații.

3. Măsuri de confidențialitate pentru protecția informațiilor personale

Identificarea și documentarea scopului – identificăm și documentăm scopurile specifice pentru care se prelucrează datele cu caracter personal.

Identificarea bazei legale – determinăm, documentăm și respectăm baza legală pentru prelucrarea datelor cu caracter personal în scopurile identificate.

Determinarea momentului și a modului în care se va obține consimțământul – stabilim și documentăm un proces pentru demonstrarea momentului și modului în care se va obține consimțământul de la persoanele vizate.

Obținerea și înregistrarea consimțământului – obținem și înregistrăm consimțământul primit de la persoanele vizate, conform cerințelor documentate.

Evaluarea impactului asupra confidențialității – evaluăm necesitatea unei evaluări a impactului asupra confidențialității atunci când este planificată o nouă prelucrare a datelor cu caracter personal sau o modificare a datelor personale.

Contracte cu persoanele împuternicite pentru prelucrarea datelor cu caracter personal - ne asigurăm că contractele noastre cu persoanele împuternicite pentru prelucrarea datelor cu caracter personal abordează controalele corespunzătoare cu privire la acele persoane împuternicite pentru prelucrarea datelor cu caracter personal.

Înregistrări legate de prelucrarea datelor cu caracter personal – determinăm și păstrăm înregistrările necesare pentru a demonstra respectarea obligațiilor noastre privind prelucrarea datelor cu caracter personal.

Determinarea drepturilor persoanelor vizate și permiterea exercitării acestora – ne asigurăm că drepturile persoanelor vizate legate de prelucrarea datelor personale deținute de noi sunt respectate și că oferim mijloacele necesare pentru a le permite să își exercite drepturile.

Oferirea de informații persoanelor vizate – oferim persoanelor vizate informații clare și ușor accesibile cu privire la operatorul de date și prelucrarea datelor lor cu personale.

Asigurarea unui mecanism pentru modificarea sau retragerea consimțământului – oferim un mecanism pentru ca persoanele vizate să modifice sau să-și retragă consimțământul.

Asigurarea unui mecanism pentru a se opune prelucrării – oferim un mecanism care permite persoanelor vizate să se opună prelucrării datelor lor personale.

Împărtășirea exercitării drepturilor de principiu cu privire la datele cu caracter personal - luăm măsuri rezonabile pentru a informa terții cu care au fost împărtășite datele cu caracter personal, despre orice modificare, retragere sau obiecții care rezultă din exercitarea drepturilor persoanelor vizate.

Rectificarea sau ștergerea – implementăm un mecanism pentru a facilita exercitarea drepturilor persoanelor vizate să acceseze, să corecteze și/sau să șteargă datele lor cu caracter personal.

Oferirea une copii a datelor cu caracter personal prelucrate – putem oferi o copie a datelor cu caracter personal prelucrate, supusă politicii de reținere și ștergere, atunci când nis e solicită de către un responsabil cu datele cu caracter personal.

Managementul solicitărilor – avem mijloacele de a gestiona solicitările legale ale persoanelor vizate.

Luarea de decizii automatizate – identificăm și tratăm orice obligații, inclusiv legale, față de persoanele vizate, care rezultă din deciziile bazate numai pe prelucrarea automată a datelor cu caracter personal.

Limitarea colectării – limităm colectarea datelor personale la minimul relevant, proporțional și necesar pentru scopurile identificate.

Limitarea prelucrării – limităm prelucrarea datelor cu caracter personal la ceea ce este adecvat, relevant și necesar pentru scopurile identificate.

Definirea și documentarea obiectivelor de minimizare și de dezidentificare a datelor cu caracter personal - definim și documentăm necesitatea prelucrării datelor cu caracter personal fără o dezidentificare prealabilă pentru atingerea scopului identificat sau măsura în care sunt stabilite obiectivele de dezidentificare a datelor personale, într-un mod care să permită ca prelucrarea datelor cu caracter personal dezidentificate rezultate să fie suficientă pentru scopul identificat.

Respectarea obiectivelor de minimizare și de dezidentificare a datelor personale - identificăm și documentăm mecanismul prin care datele personale sunt prelucrate în timp util, astfel încât măsura în care datele personale pot fi identificate sau asociate cu persoanele vizate îndeplinește obiectivele de minimizare și de dezidentificare a datelor cu caracter personal.

Dezidentificarea și ștergerea datelor personale - fie ștergem datele cu caracter personal, fie le transpunem într-o formă care nu permite identificarea persoanelor vizate, de îndată ce datele personale inițiale nu mai sunt necesare pentru scopul identificat.

Fișiere temporare – ne asigurăm că fișierele temporare și documentele temporare create în urma prelucrării datelor cu caracter personal sunt eliminate, conform procedurilor documentate, într-un termen specificat documentat.

Reținerea – nu reținem date cu caracter personal mai mult decât este necesar în scopul pentru care s-au prelucrat datele cu caracter personal.

Eliminarea – avem un mecanism documentat pentru eliminarea datelor cu caracter personal.

Proceduri de colectare – ne asigurăm că datele personale sunt corecte, complete și actualizate, așa cum este necesar pentru scopurile pentru care urmează să fie prelucrate, pe tot parcursul ciclului de viață al datelor cu caracter personal.

Controalele de transmitere a datelor personale – supunem datele cu caracter personal transmise prin intermediul unei rețele de transmisii de date unor controale adecvate menite să asigure că datele ajung la destinația dorită.

Identificarea bazei pentru transferul datelor cu caracter personal – identificăm și documentăm baza relevantă pentru transferurile de date cu caracter personal.

Țările și organizațiile cărora le-ar putea fi transferate date cu caracter personal – specificăm și documentăm țările și organizațiile internaționale cărora le-ar putea fi transferate datele cu caracter personal.

Evidența transferului de date cu caracter personal – înregistrăm transferurile de date cu caracter personal către sau de la terți și asigurăm cooperarea cu acele părți pentru a susține exercitarea viitoarelor drepturi de acces persoanelor vizate.

Evidențele privind divulgarea datelor cu caracter personal către terți – înregistrăm divulgarea datelor cu caracter personal către terți, inclusiv ce date cu caracter personal au fost dezvăluite, cui și în ce moment.

Operatori comuni – stabilim rolurile și responsabilitățile respective pentru prelucrarea datelor cu caracter personal, cu orice operator comun de date cu caracter personal, inclusiv cerințele de securitate.