Politica privind Protecția datelor
a
Sphera Franchise Group SA
și a Filialelor

Prezenta Politică acoperă procedurile aferente Societăţii şi Personalului, necesare pentru respectarea legilor aplicabile privind protecţia datelor, incluzând RGPD, din perspectiva activităţii zilnice.

Cuprins

Politici conexe
Prezenta Politică este completată de următoarele documente suplimentare:

- Politica de securitate a prelucrării datelor cu caracter personal
- Politica de retenție a datelor
- Procedura de Clasificare a Informației

Scop
Descrierea proceselor şi procedurilor pe care Societatea le-a implementat pentru a fi în conformitate cu legislaţia europeană privind protecţia datelor. Referinţele din prezenta politică cu privire la Societate, „noi", „pe noi" înseamnă societatea **Sphera Franchise Group SA**, împreună cu subsidiarele acesteia, respectiv societățile: **US Food Network SA**, **American Restaurant System SA**, **California Fresh Flavors SRL**, dacă nu se specifică altfel.

Prezenta Politică se bazează pe următoarele principii: **Legalitatea, Echitatea şi Transparenţa, Limitarea Scopului, Minimizarea Datelor, Corectitudinea Datelor, Păstrarea Datelor, Securitatea, Transferurile Internaţionale, Drepturile Persoanelor Fizice şi Responsabilitatea.**

Domeniul de aplicare
Prezentul document acoperă toate categoriile de Date cu caracter personal prelucrate de Societate, în variantă electronica sau în fişiere de hârtie structurate, în special în calitatea sa de Operator de date.

Se aplică tuturor reprezentantilor legali, directorilor *i.e. executivi si ne-executivi*, administratorilor, responsabililor şi angajaţilor Societatii (care, în scopul prezentei, include şi angajaţii temporari, personalul in sistem de leasing de personal şi contractanţii) (numiţi colectiv, „**Personal**" sau „**Personalul**"). Personalul trebuie să citească, să înţeleagă şi să adere la prezenta Politică şi la legislaţia aplicabilă.

Toţi directorii, responsabilii şi administratorii Societatii au responsabilitatea de a aplica prezenta Politică şi de a se asigura că angajaţii, persoanele şi entităţile pentru care sunt răspunzători sunt informaţi cu privire la, înţeleg şi aderă la cerinţele prezentei Politici. Orice încălcare a prezentei Politici trebuie raportată Ofiterului privind protectia datelor.

Nerespectarea intenţionată sau din neglijenţă de către Personal a legislaţiei europene privind protecţia datelor sau a prezentei Politici reprezintă o abatere disciplinară care poate fi considerată, în unele cazuri, abatere gravă, fiind tratată conformitate cu procedurile disciplinare ale Societatii.

Nerespectarea prezentei Politici poate implica şi faptul că Personalul este direct răspunzător pentru sancţiunile prevăzute de legislaţia europeană privind protecţia datelor. În particular, folosirea neautorizată de către o persoană fizică a datelor cu caracter personal obţinute ca urmare a faptului că este angajat al Societatii reprezintă o infracţiune.

Prezenta Politică nu înlocuieşte legile, regulamentele şi codurile de conduită aplicabile la nivel naţional în materie de protecţie a datelor şi de confidenţialitate, dar a fost elaborată în conformitate cu interpretarea prevederilor Regulamentului General privind Protecţia Datelor protecţia („RGPD"). Legile locale trebuie respectate în orice moment şi vor avea prioritate în faţa prezentei Politici în cazul în care acestea prevăd standarde mai stricte privind confidenţialitatea şi protecţia datelor. Orice variaţie va fi stabilită într-o Anexă la prezenta Politică. Se pot emite, ocazional, îndrumări suplimentare pentru echipe specifice.

Consultaţi-vă cu Ofiterul privind protectia datelor sau cu echipa Departamentului Juridic dacă aveţi nevoie de orice sfat, ajutor sau asistenţă privind orice temă acoperită de prezenta Politică.

Societatea a ales să desemneze în mod oficial un Responsabil cu protecţia datelor („DPO").

Ofiterul privind protectia datelor („DPO")

Date de contract:

- protectiadatelor@spheragroup.com
- protectiadatelor@kfc.ro
- protectiadatelor@pizzahut.ro
- protectiadatelor@pizzahutdelivery.ro
- protectiadatelor@taco-bell.ro

Definiţii cheie

Operatorul de date este o persoană sau un organism care (singur sau în comun) determină scopurile şi mijloacele de prelucrare a datelor cu caracter personal. În sensul prezentei Politici, Societatea este considerat a fi Operator de date.

Persoana împuternicită de operator înseamnă orice entitate juridică sau persoană fizică care prelucrează datele în numele Operatorului de date, spre exemplu, furnizorul IT extern al Societatii.

Date cu caracter personal înseamnă orice informaţii referitoare la o persoană fizică identificată sau identificabilă, cum ar fi clienţii noştri, partenerii de afaceri, angajaţii sau orice alte persoane. Exemple de date personale sunt numele, adresa, data naşterii, informaţii financiare şi bancare personale. O persoană identificabilă este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un identificator, cum ar fi numele, un număr de identificare, ori la unul sau mai mulţi factori specifici identităţii fizice, fiziologice, psihice, economice, culturale sau sociale ale respectivei persoane fizice. Datele cu caracter personal includ Date pseudonime, dar nu informaţii care sunt cu adevărat anonime. Poate include opinii şi fapte despre persoane, precum şi înregistrările video sau audio CCTV. **Faptul că informaţiile sunt disponibile public (de exemplu, pe LinkedIn) nu împiedică aplicarea legilor privind protecţia datelor.**

Încălcare a securităţii datelor cu caracter personal înseamnă o breşă în securitate ce duce la distrugerea accidentală sau ilegală, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau procesate in alt mod.

Date pseudonime înseamnă Date cu caracter personal care au fost prelucrate astfel încât acestea să nu mai poată fi atribuite unei anumite persoane fără utilizarea unor informaţii suplimentare.

Prelucrare este definit pe scară largă pentru a acoperi orice operaţiune sau set de operaţiuni care se efectuează asupra datelor cu caracter personal, incluzând colectarea, stocarea, utilizarea, divulgarea şi distrugerea acestora. Mai mult ca sigur, Personalul va prelucra anumite Informaţii cu caracter personal despre clienţii persoane fizice, precum şi despre alte contacte de Personal şi de afaceri.

Categoriile speciale de date sunt Datele cu caracter personal care beneficiază de o protecţie juridică specială în conformitate cu legislaţia aplicabilă. Acestea includ **originea rasială sau etnică, opiniile politice, convingerile religioase sau filosofice, calitatea de membru al sindicatelor, datele genetice, datele biometrice în scopul identificării unice a unei persoane, a stării de sănătate, vieţii sexuale sau orientării sexuale.** Prelucrarea datelor privind faptele penale şi a contravenţiilor („**Date privind fapte penale**”) este în plus interzisă sau restricţionată de legile aplicabile. De exemplu, informaţiile medicale şi alte informaţii privind sănătate despre Personal va reprezenta o categorie specială de date.

Declaraţia privind Politica de protecţie a datelor
Confidenţialitatea personalului, furnizorilor, partenerilor de operare, clienţilor şi a altor persoane despre care se prelucrează Date cu caracter personal în timpul furnizării serviciilor de gestionare a investiţiilor este extrem de importantă pentru Societate. Protejarea Datelor lor cu caracter personal şi folosirea acestora într-o manieră echitabilă şi demnă de încredere este esenţială pentru valorile de bază ale Societatii şi reprezintă un element important în menţinerea relaţiei şi reputaţiei sale cu clienţii săi.

Principiile europene privind protecţia datelor cu caracter personal
Societatea se angajează pe deplin să respecte obligaţiile care îi revin în temeiul legislaţiei europene privind protecţia datelor, ori de câte ori prelucrează date cu caracter personal. În acest scop, Societatea acceptă pe deplin principiile de protecţie a datelor, prezentate mai jos.

Principiul 1: Legalitatea
Putem prelucra doar acele Date cu caracter personal pentru care avem un temei legal, aşa cum este prevăzut în legislaţia privind protecţia datelor:

- în scopul interesului nostru comercial legitim (sau al unui terţ), cu condiţia ca acest interes să nu prejudicieze interesul sau drepturile persoanelor vizate (de exemplu, pentru a asigura gestionarea eficientă a Personalului nostru sau pentru a ne asigura că Personalul nostru oferă servicii bune pentru clienţi); sau

- pentru îndeplinirea unei obligaţii legale (e.g. în scopuri fiscale, sau de a raporta un incident autorităţilor de aplicare a legii).

Prelucrarea datelor cu caracter personal poate fi efectuată şi cu acordul persoanei vizate responsabile, cu respectarea cerinţelor pentru obţinerea consimţământului valid, în conformitate cu legislaţia privind protecţia datelor. Consimţământul ar putea fi necesar, spre exemplu, în scopuri de marketing şi de utilizare a cookies şi a tehnologiilor similare pe website-urile Societatii.

Motivele suplimentare (şi mai restrictive) se aplică prelucrării categoriilor speciale de date cu caracter personal şi a datelor privind faptele penale. Acestea sunt foarte limitate sub incidenţa legislaţiei europene privind protecţia datelor şi în contextul datelor privind investiţiile, doar patru motive denotă relevanţă potenţială. Acestea includ prelucrarea care este (i) în interesul substanţial al publicului, în baza legislaţiei Uniunii sau a statului membru; (ii) datele care au fost făcute publice în mod evident de către persoana vizată; sau (iii) date care sunt prelucrate cu acordul explicit al persoanei vizate.

- Personalul trebuie să se asigure că există o bază legală pentru orice Prelucrare a Datelor cu caracter personal pentru care este responsabil. Personalul trebuie să solicite îndrumări din partea Ofiterului privind protectia datelor dacă doreşte să Prelucreze Date cu caracter personal pe bază de consimţământ.
- Dacă Personalul are nevoie să solicite Date cu Caracter personal suplimentare, sau dacă schimbă maniera în care Datele cu caracter personal sunt prelucrate, trebuie luat întotdeauna în considerare dacă respectivele Date cu caractere personal sau modificări au la bază un temei legal.

Principiul 2: Echitate şi transparenţă

Pentru a fi echitabili şi transparenţi, trebuie să informăm persoanele fizice despre modul în care Datele lor cu caracter personal sunt prelucrate de noi într-un mod concis, transparent, inteligibil şi uşor accesibil, folosind un limbaj clar şi simplu. Informarea ar trebui să includă ce date cu caracter personal prelucrăm, cum intenţionăm să le folosim, cu cine le partajăm, dacă intenţionăm să le transferăm în altă ţară din afara Spaţiului Economic European, precum şi modul în care persoanele ne pot contacta cu întrebări sau cu scopul de a-şi exercita drepturile.

Facem acest lucru pentru angajaţii noştri prin „Informare Salariați”, iar pentru vizitatorii site-ului nostru web în Politica privind confidenţialitatea şi cookies, precum si prin Politica privind prelucrarea datelor cu caracter personal disponibile pe web-site-ul Societății.

- Dacă Personalul trebuie să solicite mai multe Date cu caracter personal, ori să modifice maniera în care sunt Prelucrate Datele cu caracter personal, trebuie să aveţi întotdeauna în vedere faptul că informaţiile suplimentare trebuie transmise persoanelor fizice relevante. Personalul trebuie să investească o atenţie deosebită în furnizarea de informaţii despre orice utilizare a Datelor cu caracter personal la care persoana vizată nu s-ar aştepta.

Principiul 3: Restricţii

Datele cu caracter personal trebuie utilizate doar în scopurile pentru care au fost colectate. Personalul nu trebuie să utilizeze Datele cu caracter personal în niciun alt scop decât acela despre care au informat persoana fizică, sau care nu ar fi evident respectivei persoane (sau compatibil cu scopul iniţial). De exemplu:

- Personalul trebuie să dezvăluie Date cu caracter personal doar acelor persoane care, în virtutea poziţiei sau a activităţii comerciale, trebuie să cunoască respectivele informaţii pentru a-şi îndeplini funcţia în conformitate cu scopurile specificate;
- Pentru a determina dacă un nou scop al Prelucrării este compatibil cu scopul iniţial, Personalul va trebui să ia în considerare orice legătură între Scopuri, contextul în care au fost colectate Datele cu caracter personal şi relaţia dintre părţi, natura Datelor cu caracter personal, consecinţele posibile ale prelucrării viitoare şi orice garanţiilor propuse; şi
- Utilizarea Datelor cu caracter personal în scopuri noi poate, în anumite circumstanţe limitate, să necesite transmiterea de informări sau obţinerea unor autorizaţii de la autorităţile competente pentru Protecţia datelor. De asemenea, poate necesita consultarea cu reprezentanţii lucrătorilor. Personalul trebuie să se consulte cu Ofiterul de securitate în cazul în care există întrebări cu privire la dacă este permisă o anumită utilizare a Datelor cu caracter personal sau doresc să utilizeze Datele cu caracter personal pentru un scop nou.

Principiul 4: Minimizarea datelor

Datele cu caracter personal pe care le colectăm trebuie să fie corespunzătoare, relevante şi limitate la ceea ce este necesar pentru scopurile pentru care sunt colectate. Nu trebuie să cerem mai multe Date cu caracter personal decât avem nevoie pentru baza legală pentru care le colectăm. Vom verifica periodic relevanţa Datelor cu caracter personal colectate de către Personal pentru a ne asigura că acestea sunt în continuare proporţionale cu scopul.

Următoarele tehnici de minimizare ar trebui luate în considerare ori de câte ori este fezabil:

- **Mai puţin este mai mult**: Întrebaţi-vă constant „avem nevoie să colectăm aceste informaţii pentru a ne atinge obiectivele?” Un exemplu de supra-colectare a Datelor cu caracter personal ar include trimiterea unui chestionar general solicitanţilor de locuri de muncă, care să includă întrebări specifice despre membrii familiei şi despre rude, aceasta reprezentând o colectare de informaţii care nu vor fi utilizate.
- **Anonimizare**: Dacă un set de date care include Date cu caracter personal poate fi anonimizat, atunci ar trebui să fie. Acest lucru reduce riscul de vătămare a persoanelor implicate şi elimină astfel de date din sfera de aplicare a prezentei politici (reţineţi că datele pot fi considerate cu adevărat anonime numai dacă nu este posibilă re-identificarea unei persoane din aceste date sau din alte date aflate în posesia noastră).
- **Pseudonimizarea:** Dacă anonimizarea nu este posibilă, luaţi în considerare dacă datele cu caracter personal pot face obiectul pseudonimiei, care este tehnica de prelucrare a informaţiilor personale, astfel încât nu mai pot fi atribuite unei anumite persoane fără utilizarea unor informaţii suplimentare, care trebuie păstrate separat şi sub rezerva unor măsuri tehnice şi organizatorice care să asigure neaplicarea.

Principiul 5: Corectitudinea datelor

Datele cu caracter personal trebuie să fie corecte şi actualizate. Vom încuraja persoanele fizice să ne informeze despre orice modificare survenită în datele lor cu caracter personal (şi să actualizeze, să rectifice sau să şteargă evidenţele, ca rezultat).

- Personalul nu ar trebui să utilizeze datele cu caracter personal despre care suspectează că ar putea să nu fie actualizate fără a confirma corectitudinea acestora.
- Personalul se asigură că Informaţiile personale sunt captate cu exactitate şi că sunt gestionate în conformitate cu regulile comerciale aplicabile fiecărui sistem. Informaţiile irelevante sau învechite ar trebui eliminate şi şterse în siguranţă, în conformitate cu Politica noastră privind păstrarea datelor.
- Oportunităţi recurente vor fi acordate Personalului pentru a verifica Datele cu caracter personal referitoare la ele pe care le deţinem şi trebuie să notifice prompt Superiorul direct despre orice modificare survenită în Datele lor cu caracter personal sau a circumstanţelor care pot afecta evidenţele păstrate despre ei (de exemplu adresa, informaţii bancare). Orice modificare va fi acţionată cu promptitudine.
- Dacă Personalul este informat despre o schimbare survenită în datele unui client sau a altei persoane, bazele de date relevante trebuie actualizate fără întârziere.

Principiul 6: Păstrarea datelor

Datele cu caracter personal nu trebuie păstrate mai mult decât este necesar pentru a îndeplini scopul legal pentru care au fost colectate. Ar trebui apoi să fie şterse în siguranţă. Această cerinţă este supusă altor legi şi obligaţii care ne obligă să păstrăm informaţii pentru anumite perioade.

Dacă Datele cu caracter personal nu pot fi şterse (sau anonimizate) deoarece, de exemplu, casetele arhivate sunt păstrate într-o locaţie de stocare terţă, principiul de mai sus va fi îndeplinit dacă astfel de informaţii au fost „depăşite", cu condiţia să:

- nu putem sau nu să încercăm să utilizăm Datele cu caracter personal pentru a informa orice decizie cu privire la orice persoană sau într-un mod care afectează în vreun fel persoana;
- nu conferim unei alte organizaţii acces la Datele cu caracter personal;
- înconjurăm Datele cu caracter personal cu metode de Securitate corespunzătoare din punct de vedere tehnic şi organizaţional; şi
- ne angajăm la să ştergem definitiv şi în siguranţă informaţiile dacă sau când va fi posibil.

Principiul 7: Siguranţa

Datele cu caracter personal trebuie păstrate şi utilizate în siguranţă. Trebuie să fie protejată împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, distrugerii sau deteriorării accidentale. Acest lucru se aplică sistemelor noastre informatice, site-urilor şi manipulării zilnice a Datelor cu caracter personal. Cel puţin, vom respecta orice măsuri de securitate şi organizare impuse de lege.

Numirea Persoanelor împuternicite de Operator

Dacă Societatea (în calitate de operator de date) angajează o altă organizaţie care să prelucreze datele cu caracter personal în numele său, această organizaţie („Persoana împuternicită") trebuie să fi implementat „măsuri tehnice şi organizatorice adecvate" pentru a întruni cerinţele legislaţiei europene aplicabile privind protecţia datelor şi a

asigura protecţia drepturilor persoanelor fizice. În cadrul acestui proces, trebuie încheiat un contract scris cu Operatorul de date, care conţine obligaţii contractuale specifice.

În cazul în care Societatea acţionează ca Persoană împuternicită în numele Francizorului (*i.e. YUM! Restaurants International*) (Operatorul de date), acesta **nu poate angaja o altă persoană împuternicită fără acordul prealabil scris specific sau general al Operatorului de date.** În cazul unui acord general scris, Societatea va trebui să informeze Operatorul de date cu privire la orice modificări intenţionate privind adăugarea sau înlocuirea altor persoane împuternicite, oferind astfel Operatorului de date oportunitatea de a se opune unor astfel de modificări. De asemenea, va trebui să se asigure că acesta reduce fluxul obligaţiilor relevante către sub-procesatori.

- Orice membru al personalului responsabil cu desemnarea unui Operator de date trebuie să asigure că toate contractele conţin prevederi corespunzătoare şi că au efectuat un control al măsurilor de securitate ale Operatorului de date pentru a se asigura că respectă cerinţele Societatii.
- Societatea va efectua inspecţii şi audituri periodice ale sistemelor, înregistrărilor, incintelor, personalului şi oricăror altor materiale utilizate în furnizarea serviciilor relevante pentru a verifica dacă Operatorul de date (şi oricare sub-procesatori) întruneşte obligaţiile sale contractuale şi orice obligaţii aplicabile în temeiul legilor europene privind protecţia datelor. O dispoziţie privind auditul va fi inclusă în contractele scrise.

Principiul 8: Transferuri internaţionale

Normele europene de protecţie a datelor restricţionează transferurile de Date cu caracter personal în afara SEE (incluzând către alte societăţi din grup şi Operatori de date externi), cu excepţia cazului în care există o protecţie adecvată a Datelor cu caracter personal sau dacă au fost luate măsuri pentru a asigura protecţia Datelor cu caracter personal. Societatea poate face ocazional exporturi către alte părţi situate în afara SEE. Dacă procedăm astfel, vom face acest lucru în conformitate cu clauzele contractuale standard aprobate de Comisia Europeană pentru a reglementa transferurile anumitor Date cu caracter personal între noi şi alţi membri ai Grupului nostru.

Există un număr (limitat) de alte situaţii în care Datele cu caracter personal pot fi transferate în afara SEE, incluzând:

- cazul în care sunt trimise într-o ţară sau pe un teritoriu sau către o organizaţie internaţională recunoscută de Comisie ca oferind protecţie corespunzătoare (ar putea include şi organizaţiile SUA care sunt certificate prin Scutul de confidenţialitate UE-SUA);
- încrederea în regulile corporative obligatorii;
- cazul în care persoana fizică a fost de acord cu transferul în mod explicit;
- cazul în care sunt necesare pentru a executa un contract;
- cazul în care sunt necesare din motive de interes public important; sau
- cazul în care sunt necesare pentru stabilirea, exercitarea sau apărarea revendicărilor legale.

Solicitaţi sfatul Ofiterului privind protecția datelor dacă:

- o terţă parte va prelucra Datele cu caracter personal ale Societatii în afara SEE (nu numai în cazul în care terţa parte are sediul în afara SEE, ci şi dacă Datele cu caracter personal vor fi deţinute sau accesate de la distanţă de o terţă parte sau de subcontractanţii săi într-o locaţie în afara SEE); sau
- există întrebări cu privire la ce Date personale pot fi transferate în afara SEE.

Principiul 9: Drepturile persoanelor fizice

Noi întotdeauna vom respecta drepturile persoanelor fizice, în temeiul legislaţiei europene privind protecţia datelor cu caracter personal (în măsura aplicabilă):

- de a primi informaţii despre cum sunt Prelucrate Datele lor cu caracter personal (a se vedea Secţiunea despre Echitate şi Transparenţă de mai sus pentru mai multe detalii);
- de a accesa şi rectifica Datele cu caracter personal aferente;
- de a şterge sau restricţiona activitatea de Prelucrare;
- de a transfera Datele cu caracter personal către alt Operator de date;
- de a se opune anumitor modalităţi de prelucrare în situaţii speciale; şi
- de a nu se supune utilizării unor decizii complet automate (incluzând realizarea de profiluri) care produc efecte juridice sau afectează semnificativ persoanele fizice.

Noi vom răspunde oricăror solicitări fără întârzieri nejustificate şi, în general, în termen de o lună de la primirea solicitării.

- Solicitările Personalului de a-şi vedea înregistrările sau de a-şi exercita oricare dintre celelalte drepturi pe care le au în temeiul legilor privind protecţia datelor ar trebui să facă, în scris, Ofiterului pentru protectia datelor, care va lua măsurile adecvate pentru a răspunde cererii depuse.
- Personalul trebuie să aibă grijă atunci când înregistrează detalii în documente, deoarece cei cărora la care face referire textul (cum ar fi clienţii persoane fizice) pot vedea aceste informaţii la o dată ulterioară. Doar informaţiile corespunzătoare, proporţionale şi justificate trebuie introduse.
- Dacă Personalul primeşte orice solicitare de a vedea Datele cu caracter personal de la alte persoane (de exemplu, clienţi) sau oricare alte solicitări sau plângeri legate de modul în care Datele lor cu caracter personal sunt Prelucrate de către Societate, acestea trebuie imediat transmise imediat catre Ofiterul privind protectia datelor, care va coordona în mod corespunzător. Există adesea termene stricte pentru a se conforma unor astfel de solicitări, astfel că cererile trebuie transmise cât mai curând posibil după ce au fost primite.

Principiul 10: Răspunderea

Legislaţia europeană privind protecţia datelor ne obligă să implementăm o gamă largă de măsuri pentru a reduce riscul de încălcare a RGPD şi pentru a demonstra că luăm în serios gestionarea datelor. O descriere a unora dintre măsurile pe care le-am implementat pentru a întruni aceste cerinţe se regăseşte mai jos.

Evidenţa activităţii de prelucrare

Înainte de RGPD, autoritatea pentru protecţia datelor (Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal) a solicitat Operatorilor de date să notifice autoritatea relevantă pentru protecţia datelor cu privire la activităţile lor de Prelucrare. Aceste obligaţii sunt susceptibile să dispară sub incidenţa RGPD. Cu toate acestea, vom fi obligaţi să ţinem o evidenţă a activităţilor de prelucrare a datelor cu caracter personal pe care le prelucrăm. În consecinţă, Personalul relevant şi echipa lor trebuie să se asigure că pastreaza o evidenta a activitatilor de prelucrarea a bazelor de date ce contin date cu caracter personal. Această evidenţă trebuie pusă la dispoziţia unei autorităţi de supraveghere competente, la cerere.

Formare şi orientări

Toti membrii Personalului trebuie să citească prezenta politică si sa respecte condiţiile acesteia. Toţi membrii Personalului care prelucrează date cu caracter personal ca o parte semnificativă a funcţiei lor vor beneficia de o formare adecvată privind protecţia şi securitatea datelor ca parte a programului lor de introducere, iar membrii existenţi ai Personalului vor beneficia de formare continuă.

Noi sisteme şi procese

Legislaţia europeană privind protecţia datelor ne obligă să punem în aplicare măsuri tehnice şi organizatorice care să demonstreze că am luat în considerare şi că am integrat măsurile de respectare a datelor în activităţile noastre de prelucrare (cunoscut sub numele de „principiul protecţiei datelor începând cu momentul conceperii *(by design)* şi în mod implicit *(by default)*").

Ne angajăm să respectăm acest principiu prin:

- Identificarea riscurilor de confidenţialitate la începutul oricărui proiect sau înainte de implementarea unui nou produs, sistem sau serviciu şi planificarea acestora în mod corespunzător;
- Respectarea principiului minimizării datelor, asigurarea faptului că datele cu caracter personal sunt pseudonime, acolo unde este posibil;
- Încorporarea confidenţialităţii în tehnologiile, operaţiunile şi arhitecturile noastre de informaţii şi consultarea tuturor părţilor interesate relevante;
- Menţinerea integrităţii şi standardelor înalte ale produselor şi serviciilor noastre; şi
- Depunerea de eforturi pentru a fi transparenţi cu persoanele fizice privind măsurile luate pentru protejarea Datelor lor cu caracter personal.

Evaluări de impact

În situaţia în care o activitate de prelucrare este identificată ca fiind de „risc ridicat", va fi necesară o evaluare mai detaliată (o „Evaluare de impact privind protecţia datelor") înainte de a fi iniţiată în temeiul RGPD.

O Evaluare de impact privind protecţia datelor va include o descriere a activităţilor de prelucrare, a riscurilor aferente şi a măsurilor adoptate pentru diminuarea respectivelor riscuri, şi în special a măsurilor de protecţie şi securitate luate pentru a proteja Datele cu caracter personal şi a fi în conformitate cu RGPD.

În circumstanţe limitate am putea fi obligaţi să ne consultăm cu persoanele fizice relevante sau cu autoritatea relevantă pentru protecţia datelor.

Audit

Pentru a demonstra conformitatea cu Principiile de Protecţie a Datelor şi cu alte cerinţe legale aplicabile, vom efectua, din când în când, audituri interne ale activităţilor noastre de prelucrare. Întregul Personal trebuie să colaboreze în procesul de auditare.

Anexă – Informaţii privind siguranţa

Siguranţa fizică

Securitatea fizică este de o importanţă capitală pentru noi şi este esenţială pentru a asigura siguranţa şi securitatea echipamentului nostru, precum şi a informaţiilor pe care Personalul nostru îl utilizează sau îl manipulează.

- La finalul fiecărei zile nu trebuie lăsat niciun document care conţine Date cu caracter personal pe birou;
- Datele cu caracter personal trebuie păstrate într-un dulap de depozitare, sertar sau seif încuiat. Dacă este computerizat, acesta trebuie codificat, criptat sau protejat prin parolă, atât pe hard disk-ul local, cât şi pe o unitate de reţea căreia îi sunt făcute regulat copii de rezervă. Dacă o copie este păstrată pe un suport de stocare amovibil, acel suport trebuie să fie păstrat într-un dulap de depozitare, sertar sau seif încuiat.
- Eliminaţi deşeurile de hârtie în condiţii de siguranţă.
- Blocarea accesului la calculator la parasirea locului de munca.

Descoperirea, catalogarea şi clasificarea datelor

Pe lângă cele de mai sus, am implementat controale pentru a ne asigura că datele cu caracter personal sunt tratate în mod adecvat în afara sistemelor noastre principale. Acestea includ protejarea şi asigurarea informaţiilor, precum:

- Copii ale bazelor de date de producţie care conţin date cu caracter personal luate în scopuri de testare, dezvoltare sau analiză;
- Foi de calcul şi alte surse de date populate prin exportul de informaţii privind datele de contact şi profilul clienţilor şi detalierea profilului pentru o îmbinare de corespondenţă (supusă aceluiaşi standard de securitate ca şi sistemele de bază);
- Arhive de e-mail care cel mai probabil conţin Date cu caracter personal care trebuie protejate în temeiul legislaţiei europene privind protecţia datelor.

Prevenirea pierderii de date

Controlăm pierderea datelor prin măsuri precum blocarea automată a e-mailurilor de ieşire, a altor mesaje şi a mişcărilor de fişiere care conţin date cu caracter personal care nu au fost protejate prin măsuri de protecţie adecvate, *de ex. criptarea datelor*.

În anumite situaţii, criptarea poate fi aplicată automat Datelor cu caracter personal când este clasificată sau identificată într-un mesaj e-mail sau într-un document ataşat, în timp ce în alte situaţii mesajele pot fi plasate în carantină pentru a permite un răspuns organizaţional.

Criptarea datelor şi a E-mail-ului

Criptarea este una dintre puţinele tehnologii specifice menţionate în textul RGPD, iar prezenţa sa mandatează, în esenţă, utilizarea sa de către organizaţii. Am implementat măsuri de criptare a datelor în timp de repaus şi atunci când sunt utilizate sau transmise. Acest lucru asigură că, dacă se produce o breşă în oricare sistem, informaţiile rămân confidenţiale şi nu declanşează penalităţile RGPD.

Identificarea unei încălcări a securităţii datelor şi blocarea

Legislaţia europeană privind protecţia datelor ne obligă să raportăm orice eveniment de Încălcare a securităţii datelor cu caracter personal autorităţii competente pentru protecţia datelor fără întârzieri nejustificate (şi acolo unde este posibil, în termen de 72 de ore), după ce am luat la cunoştinţă despre evenimentul de Încălcare a securităţii datelor cu caracter personal (cu excepţia cazului în care este puţin probabil ca acest lucru să ducă la un risc pentru drepturile şi libertăţile persoanei fizice). De asemenea, este posibil să fie necesar să informăm persoanele fizice în anumite circumstanţe şi trebuie să documentăm evenimentul de Încălcare a securităţii datelor cu caracter personal.

Prin urmare, am implementat măsuri pentru a observa într-o manieră proactivă evenimentele de încălcare a securităţii datelor, a audita dimensiunea evenimentului şi a crea un răspuns organizaţional adecvat.

- În cazul în care orice persoană fizică are informaţii despre un eveniment de Încălcare a securităţii datelor cu caracter personal, aceasta trebuie să informeze imediat Ofiterul privind protectia datelor şi să furnizeze cât mai multe informaţii (inclusiv natura şi consecinţele evenimentului de Încălcare a securităţii datelor cu caracter personal şi orice măsuri luate sau propuse pentru a atenua orice efecte adverse). Exemple de evenimente de Încălcare a securităţii datelor cu caracter personal includ trimiterea Datelor cu caracter personal unui destinatar greşit, accesarea fără autorizare a Datelor cu caracter personal, pierderea sau furtul documentelor sau calculatoarelor care conţin Date cu caracter personal.

Portabilitatea datelor

În conformitate cu art. 20 privind Drepturile persoanei vizate, persoanele fizice au dreptul de a solicita exportul datelor lor într-un format utilizabil care poate fi dat altui furnizor sau furnizor de servicii pentru a le importa în serviciul său în anumite circumstanţe.

Securitate de tip „endpoint” şi Gestionarea dispozitivelor mobile („MDM”)

RGPD cere ca dispozitivele informatice să fie protejate împotriva pierderilor sau furtului prin intermediul capabilităţilor de gestionare a dispozitivelor mobile, cum ar fi „wipe and kill” *(ştergerea şi eliminarea)* de la distanţă. Un dispozitiv pierdut ar putea reprezenta veriga slabă din lanţul de protecţie a datelor, ducând la o breşă de date bazată pe informaţiile stocate pe dispozitiv sau accesibile prin acreditările de utilizator încă active.

Stocare în cloud şi Servicii de partajare

Societatea desfăşoară o revizuire periodică a documentelor partajate în exterior pentru a minimiza gradul de partajare cu părţile externe. Utilizarea restricţiilor implicite (cum ar fi linkurile cu durată limitată) este, de asemenea, încurajată pentru a restricţiona partajarea în mod implicit fără a fi nevoie de intervenţia utilizatorului.

- Orice transfer de Date cu caracter personal trebuie efectuat în condiţii de siguranţă, fie extern, fie intern. Când trimiteţi prin e-mail sau postaţi, verificaţi de două ori că informaţiile sunt trimise destinatarului potrivit.
- Aveţi în vedere faptul că cei care caută informaţii apelează uneori la înşelăciune. Înainte de a trimite orice Date cu caracter personal unei terţe părţi, asiguraţi-vă de identitatea părţii respective. Acest lucru ar putea implica efectuarea de

verificări pentru a confirma identitatea părţii terţe, în special dacă transmiteţi informaţii prin telefon. Dacă aveţi îndoieli, contactaţi Ofiterul pentru protectia datelor.

Anti-Malware

În timp ce o infiltrare reuşită a programelor malware poate face calculatoarele inutilizabile, una din preocupările mai severe ridicate în temeiul RGPD este potenţialul programului malware de a recupera acreditările pentru conturile utilizatorilor şi administratorilor. Acreditările recuperate pot fi apoi utilizate pentru a accesa sursele de date din cadrul organizaţiei (atât în sediu, cât şi în serviciile cloud), incluzându-le pe cele care conţin date cu caracter personal şi sensibile.

Societatea lucrează îndeaproape cu furnizorul de servicii IT pentru a se asigura de aplicarea celui mai puternic nivel practic de securitate (în special prin utilizarea de software antivirus şi de detectare a intruziunilor).

Managementul identităţii şi accesului

Un sistem coerent de identitate şi de gestionare a accesului, care unifică cu uşurinţă identitatea angajaţilor între aplicaţii, este o cerinţă fundamentală pentru respectarea standardelor RGPD. Societatea utilizează cele mai recente protocoale de gestionare a identităţii, plus, identităţile utilizatorilor sunt conectate la furnizorii de software terţi care folosesc opţiunea Single-Sign-On, după caz. Acest lucru asigură că accesul poate fi controlat la nivel central (şi rapid) printr-o serie de aplicaţii, într-un mod uniform.

***