GDPR Prezentare Generală

Ghidul GDPR pentru cluburile de fitness

UPFIT CLOUD

v1

ATENȚIONARE

Autorii acestui manual nu sunt avocați. Aceste articole nu trebuie să fie luate ca o consultație juridică asupra legislației UE sau asupra modului în care firma ta ar trebui să aplice regulile GDPR. UPfit nu își asumă responsabilitatea pentru interpretarea greșită a acestor informații de către cititor.

În schimb, acest manual încearcă să ofere informații care să te ajute să înțelegi mai bine cum a reușit UPfit să pună în practică anumite reglementări. Aceste informații nu sunt o consultație juridică, în care un avocat aplică legea la circumstanțele specifice companiei tale. De aceea, insistăm să consulți un avocat pentru a obține sfaturi specifice referitoare la GDPR sau orice alt act normativ.

GENERAL DATA PROTECTION REGULATION

CUPRINS

GHIDUL GDPR
PENTRU CLUBURILE DE FITNESS

GDPR sau Regulamentul (UE) 679/2016 intră în vigoare la 25 mai 2018, fiind considerat cea mai restrictivă lege pentru protecția datelor din lume.

Clubul tău de fitness este pregătit pentru GDPR? Iată tot ce trebuie să știi despre Regulamentul General pentru Protecția Datelor!

CE ÎNSEAMNĂ GDPR?

GDPR sau Regulamentul General pentru Protecția Datelor este un nou regulament al Uniunii Europene care va înlocui Directiva 1995/46/CE referitoare la protecția datelor cu caracter personal. GDPR este menit să sporească protejarea datelor cu caracter personal ale cetățenilor UE. Ca urmare, companiile sau organizațiile care colectează ori procesează date personale au acum mai multe obligații.

Regulamentul intră în vigoare în 25 mai 2018 și include o serie de norme care vor consolida drepturile persoanelor. GDPR aduce și penalități aspre în cazul abaterilor grave.

Textul complet al Regulamentului General pentru Protecția Datelor aplicabil în România îl poți consulta aici: www.senat.ro/legis/PDF/2018/18b094FG.pdf

CUM AU FUNCȚIONAT LUCRURILE ÎNAINTE DE GDPR?

Cu siguranță ai auzit de ceva vreme despre GDPR, dar știai că Uniunea Europeană avea deja o legislație în acest sens? Deși Directiva 1995/46/CE este înlocuită cu GDPR, vechiul regulament a fost cel care a stabilit cele opt principii pentru protejarea datelor cu caracter personal.

Până în mai 2018 acea directivă a ghidat modul în care companiile au administrat datele personale pe teritoriul Uniunii Europene. Din moment ce noul Regulament este bazat pe directivele vechi, ar fi bine să te familiarizezi și cu prevederile acesteia.

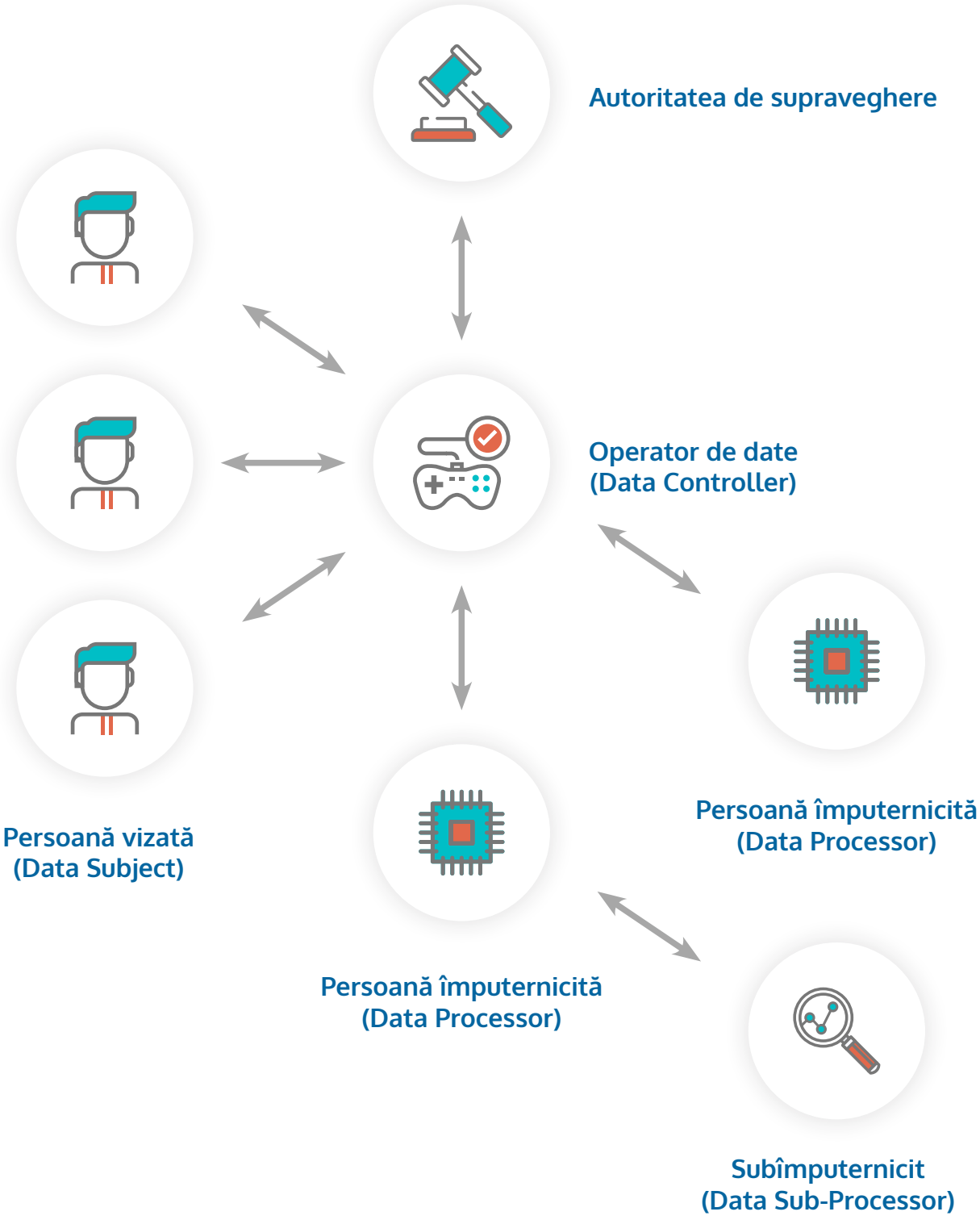
PE MINE MĂ AFECTEAZĂ GDPR?

DA! Deoarece clubul tău de fitness este o firmă înregistrată în România, iar majoritatea membrilor tăi sunt rezidenți ai Uniunii Europene.

În cazul cluburilor de fitness, deoarece au o bază de date cu informațiile personale ale membrilor, inclusiv numele, adresa fizică, adresa de e-mail, numărul de telefon sau orice altă informație similară, sunt afectate de regulile GDPR.

Dacă vechea directivă făcea referire doar la teritoriul Uniunii Europene, GDPR se aplică și companiilor din afara UE, care monitorizează comportamentul rezidenților Uniunii. Astfel, chiar dacă o companie are sediul în afara UE, atâta timp cât administrează date cu caracter personal ale cetățenilor UE, este obligată să respecte GDPR.

RESPONSABILITĂŢI IMPUSE DE GDPR



DREPTURILE INDIVIDUALE

DREPTUL DE A FI INFORMAT

Trebuie să pui la dispoziția membrilor tăi informații despre modul în care le administrezi datele personale. Acest lucru trebuie făcut gratuit, într-un limbaj simplu și ușor de înțeles.

DREPTUL LA ACCES

Trebuie să le oferi membrilor acces la datele lor personale, în mod gratuit, într-un format utilizat în mod curent (ex. PDF, Word etc).

DREPTUL LA MODIFICARE

Membrii pot să-ți ceară să le modifici sau să le completezi datele lor personale pe care le deții; tu trebuie să onorezi această cerere în maxim 30 de zile calendaristice.

DREPTUL LA ȘTERGERE SAU DREPTUL DE A FI UITAT

Membrii au dreptul să-ți ceară să le ștergi datele cu caracter personal din baza ta de date, dacă este posibil.

DREPTUL LA RESTRICȚIONAREA PROCESĂRII

Un membru are dreptul de a restricționa sau de a bloca modul în care folosești datele lui cu caracter personal.

DREPTUL LA PORTABILITATEA DATELOR

O persoană are dreptul de a obține și de a refolosi pentru alte servicii informațiile sale personale pe care tu le ai în baza ta de date.

DREPTUL DE OPOZIȚIE

Membrul are dreptul să obiecteze împotriva folosirii datelor sale personale în scopuri de marketing, cercetare sau statistici.

DREPTUL DE A NU FI SUPUS DECIZIILOR AUTOMATE

Membrii tăi au dreptul ca datele lor personale să nu fie procesate în mod automat și să ceară ca o persoană să fie implicată în acest proces.

PROCEDURI INTERNE

PROTECȚIA DATELOR IMPLICITĂ (PRIVACY BY DESIGN)

Există mai multe reguli noi pentru companiile care administrează datele cu caracter personal. Una dintre ele este obligația de a asigura protecția datelor personale în mod implicit, atunci când dezvoltă sisteme noi.

De asemenea, aceste firme sunt obligate să facă o Evaluare a impactului asupra protecției datelor personale atunci când folosesc tehnologii noi. Asta înseamnă că firmele trebuie să verifice, în mod constant, impactul pe care îl poate avea un proiect sau o inițiativă nouă asupra protecției datelor.

De exemplu, dacă adopți un soft de management nou în clubul tău de fitness, trebuie să te asiguri că respectă în totalitate normele GDPR.

RESPONSABILUL CU PROTECȚIA DATELOR (DPO)

GDPR cere ca majoritatea firmelor să aibă un Responsabil cu protecția datelor care să supravegheze modul în care firma respectă directivele regulamentului.

Printre organizațiile care vor fi nevoite să aibă un DPO se numără companii a căror activitate implică administrarea și monitorizarea în mod regulat a unui număr mare de date cu caracter personal.

Responsabilul cu protecția datelor trebuie să se asigure că și celelalte companii care au acces la baza de date a firmei respectă regulile GDPR.

CONTRACTE ȘI DOCUMENTE REFERITOARE LA PROTECȚIA DATELOR

Din moment ce scopul principal al GDPR este transparența și corectitudinea, Operatorii și Persoanele împuternicite trebuie să-și revizuiască Politica de confidențialitate și orice alte politici interne care au legătură cu datele cu caracter personal.

În cazul în care Operatorii lucrează cu alte companii pentru a procesa datele personale pe care le administrează (de exemplu, softuri de management pentru cluburi de fitness, cum este și UPfit), atunci ei trebuie să se asigure că toate contractele cu acei procesatori includ reglementările GDPR din Articolul 28. La rândul lor, procesatorii ar trebui să se asigure că fac modificările necesare la contractele cu clienții pentru a fi pregătiți de GDPR.

Deoarece UPfit este procesator de date, softul respectă în totalitate prevederile GDPR, iar clienții noștri au la dispoziție o serie de funcționalități care să-i ajute să implementeze mai ușor toate aceste reguli.

AUTORITĂȚILE DE SUPRAVEGHERE

O singură autoritate de supraveghere
Această reglementare GDPR este menită să ajute activitatea Responsabililor cu protecția datelor. Astfel, companiile au o singură autoritate de supraveghere, chiar și atunci când au birouri în mai multe țări din Uniunea Europeană. Astfel, nu se vor confrunta cu indicații contradictorii primite de la mai multe autorități de supraveghere.

În România autoritatea pentru GDPR este Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (www.dataprotection.ro).

Raportarea breșelor de securitate
Printre cerințele GDPR se numără și faptul că firmele care au rolul de controlori trebuie să anunțe autoritatea de supraveghere în cazul în care au o breșă de securitate ce afectează protecția datelor.

Astfel, companiile sunt obligate să raporteze în maxim 72 de ore din momentul în care află de respectiva breșă de securitate, în cazul în care datele afectate nu sunt anonime sau criptate. Asta înseamnă că majoritatea breșelor de securitate vor trebui raportate către ANSPDCP.

Breșele care pot afecta securitate individului - precum furtul de identitate sau încălcarea confidențialității - trebuie să fie raportate și către persoanele afectate.

ARIA DE ACOPERIRE, RESPONSABILITATE ȘI AMENZI

Aria de acoperire
Deși Directiva din 1995 guverna organizații din Uniunea Europeană, aria de acoperire a GDPR este mai mare. Astfel, noul regulament de protecție a datelor se aplică firmelor din afara UE, dacă acestea își vând produsele în țările din Uniune sau monitorizează comportamentul rezidenților UE. Cu alte cuvinte, chiar dacă ai sediul în afara Uniunii Europene, dacă procesezi sau controlezi date cu caracter personal al cetățenilor UE, trebuie să aplici GDPR.

Responsabilitate
Noul regulament prevede ca procesatorii și controlorii să poată demonstra oricând că respectă GDPR. Toate procedurile trebuie înregistrate, implementate și revizuite în mod regulat. Angajații trebuie să fie educați cu privire la regulile GDPR, iar companiile trebuie să implementeze măsuri organizaționale și tehnice pentru a se asigura că respectă GDPR și că pot demonstra acest lucru.

Amenzi severe
Importanța Regulamentului General de Protecția Datelor este subliniată și de penalizările impuse în cazul încălcării acestui act normativ. În funcție de gravitatea abaterii, controlorii și procesatorii care nu administrează datele cu caracter personal în concordanță cu GDPR sau încalcă drepturile cetățenilor UE în acest sens pot primi amenzi de până la 20 de milioane de euro sau 4% din profitul anual global, oricare sumă este mai mare.

ÎNTREBĂRI FRECVENTE

Este obligatorie confirmarea de două ori a consimțământului pentru trimiterea de e-mailuri în scop comercial (double opt-in)?
Confirmarea de două ori a consimțământului pentru notificări sau double opt-in este un mecanism în 2 pași prin care o persoană trebuie să-și confirme adresa de e-mail de două ori, după ce s-a abonat pentru un anumit serviciu. Deși GDPR nu obligă firmele să introducă acest procedeu, este bine să optezi pentru el, deoarece este o măsură adițională care te ajută să demonstrezi că ai obținut consimțământul necesar.

Cum va afecta GDPR drepturile individului?
Deja persoana fizică are o mulțime de drepturi menite să-i protejeze datele cu caracter personal. Cu toate astea, GDPR consolidează aceste drepturi, astfel încât persoanele fizice pot:

- să obțină detalii despre cum sunt procesate datele lor de către o organizație sau o companie
- să obțină copii ale datelor lor cu caracter personal care se află în baza de date a unei companii
- să li se corecteze informațiile personale care sunt incorecte sau incomplete
- să li se șteargă datele cu caracter personal dintr-o bază de date a unei companii sau a unei organizații, în cazurile în care respectiva companie nu are un motiv legitim pentru a le stoca
- să obțină datele lor personale de la o organizație sau companie și să le poată transmite unei alte organizații sau companii
- să obiecteze împotriva procesării datelor lor în anumite circumstanțe
- să nu fie supuși deciziilor automate (cu anumite excepții)

Este obligatoriu consimțământul individului pentru prelucrarea datelor sale personale?
Consimțământul individului este obligatoriu în majoritatea cazurilor în care i se procesează datele cu caracter personal. Totuși, există și anumite excepții în care informațiile personale pot fi procesate fără consimțământ specific:

- când sunt necesare pentru realizarea unui contract în care individul în cauză este unul dintre partenerii din contract
- când există o obligație legală de a procesa datele personale ale unui individ, de exemplu, trimiterea informațiilor unui angajat către ANAF
- uneori există interes legitim, precum obiective comerciale. Totuși, în aceste circumstanțe, interesul legitim trebuie să fie mai important, decât detrimentul confidențialității unei persoane

Când este consimțământul invalid?
Consimțământul este invalid în următoarele circumstanțe:

- când nu ești sigur că un individ și-a dat consimțământul necesar pentru a-i procesa datele cu caracter personal
- când individul nu își dă seama că și-a dat consimțământul
- când nu ai documente clare care să demonstreze faptul că persoanele și-au dat consimțământul
- când persoanele nu au avut de ales, nu și-au dat consimțământul în mod voit
- când individul ar putea fi penalizat dacă nu-și dă consimțământul
- când este o inegalitate de putere clară între firma ta și individ
- când consimțământul este o precondiție pentru un serviciu, dar prelucrarea datelor nu este necesară pentru acel serviciu
- când consimțământul a fost inclus în alți termeni și condiții
- când cerere de consimțământ a fost vagă sau neclară
- când folosești check-box-uri pre-selectate sau alte metode de consimțământ implicit
- când firma ta nu a fost menționată cu numele în cererea de consimțământ
- când nu le-ai spus persoanelor despre dreptul lor de a-și retrage consimțământul

- când oamenii nu își pot retrage într-un mod ușor consimțământul
- când scopul procesării datelor pe care le deții s-a schimbat

Cât timp este valabil consimțământul?
GDPR nu specifică o limită de timp exactă în care ai voie să păstrezi și să procesezi datele cu caracter personal. Cu toate astea, consimțământul poate să expire, în funcție de context, și trebuie să consideri scopul cu care a fost obținut acel consimțământ și care au fost așteptările individului în acest sens.

De exemplu, clubul tău de fitness face o campanie prin care ceri consimțământul membrilor tăi să primească e-mailuri cu sfaturi despre cum să fii în formă în vacanța de vară din acest an. Din moment ce cererea de consimțământ menționează o perioadă de timp exactă, așteptarea rezonabilă a membrilor care își dau consimțământul pentru această campanie este ca, la finalul vacanței de vară, să nu mai primească astfel de e-mailuri. Astfel, consimțământul expiră.

Dacă scopul pentru care ai colectat datele cu caracter personal s-a schimbat, consimțământul inițial nu mai este valabil.

De asemenea, în cazul minorilor, consimțământul părinților expiră în momentul în care copilul împlinește 16 ani. Atunci, respectiva persoană trebuie să-și dea singură consimțământul pentru prelucrarea datelor personale.

Regulile GDPR spun că trebuie să criptezi baza de date atunci când nu este folosită (encription at rest)?
GDPR nu impune măsuri anume pentru securitate în cazul folosirii sistemelor de tip CRM. În schimb, Regulamentul cere companiilor să ia toate măsurile tehnice și organizaționale necesare pentru a limita riscul de încălcare a confidențialității datelor. În anumite cazuri este recomandat să se folosească criptarea datelor când nu sunt folosite (encription at rest) sau folosirea pseudonimelor, dar acest lucru nu este obligatoriu.

Cetățenii din Uniunea Europeană au dreptul absolut să ceară ștergerea completă a datelor lor personale?
Dreptul de a cere ștergerea datelor cu caracter personal se numește și dreptul de a fi uitat. Acesta nu este un drept absolut, are anumite limitări. În cele mai multe cazuri, atunci când se consideră o cerere de ștergere a datelor, se ia în considerare mai mulți factori relevanți.

De exemplu, acest drept nu se aplică atunci când o companie are obligații legale de a transmite datele personale ale unui individ autorităților. În schimb, o persoană are tot dreptul de a cere companiilor și organizațiilor să nu îi mai proceseze datele cu caracter personal în scopuri de marketing.

Este obligatoriu ca fiecare companie să aibă un Responsabil cu protecția datelor (DPO)?
Potrivit GDPR, este obligatoriu ca o organizație sau companie să aibă un DPO în următoarele circumstanțe:

- organizația este o instituție guvernamentală
- organizația procesează anumite date personale speciale, la scară largă (de exemplu, informații referitoare la sănătate sau religie), aceasta fiind activitatea sa principală
- organizația monitorizează în mod sistematic persoane (prin camere de supraveghere sau prin softuri care monitorizează comportamentul online), aceasta fiind activitatea sa principală

GDPR impune o evaluare a impactului asupra protecției datelor (DPIA) pentru toate activitățile de prelucrare a datelor persoanelor din UE?
Noul Regulament pentru Protecția Datelor impune o astfel de evaluare doar în circumstanțe cu un grad de risc ridicat, precum:

- prelucrarea datelor din categorii speciale la scară largă, precum date referitoare la sănătatea unei persoane
- atunci când o companie se bazează în mod regulat și extensiv pe decizii automate (inclusiv profiling - prelucrarea automată a datelor personale), iar rezultatul poate avea urmări legale (de exemplu, folosirea softurilor pentru detectarea fraudelor)
- monitorizarea sistematică și la scară largă a spațiului public (de exemplu, camerele de supraveghere)

Deciziile automate și profiling sunt interzise de GDPR?
Prelucrarea automată a datelor personale pentru a evalua, analiza sau a prezice orice caracteristică a persoanei în cauză (profiling) și deciziile automate ce implică datele cu caracter personal nu sunt interzise de GDPR.

Aceste activități pot fi supuse unor condiții. Mai ales când aceste decizii automate pot avea repercusiuni legale asupra indivizilor în cauză. În aceste circumstanțe, persoana trebuie să primească:

- informații ușor de înțeles referitoare la logica acestui proces și să îi fie aduse la cunoștință potențialele consecințe
- posibilitatea să ceară ca un om să fie implicat în acest proces (în anumite cazuri) sau să fie exclus cu totul din acest proces

RESURSE GDPR

Pentru mai multe informații despre ce înseamnă Regulamentul General pentru Protecția Datelor îți recomandăm următoarele resurse:

1. www.dataprotection.ro
2. www.eugdpr.org
3. www.gdpr-info.eu
4. www.edps.europa.eu

EXEMPLE DE DATE PERSONALE

Nume complet	Note / calificative	**Detalii loc de muncă** nume companie, adresă, colegi
Adresă de e-mail	Salariu	Membrii familiei
Adresă fizică	Profesie	Dependenți
Rasă / etnicitate	Poze	Soț / soție / partener (ă)
Sexul	Istoric educație și angajări	Prieteni
Serie și număr buletin / CNP	Viziuni și afilieri politice și religioase	Asociați
Număr pașaport	Viziuni asupra unor aspecte controversate	Username / pseudonime / alias-uri
Număr viză	Istoric	Parole
Număr permis de conducere	Numele de fată al mamei	Identități digitale
Numărul de înmatriculare al autovehiculului	Locul nașterii	**Date biometrice** retina, față, amprente, scrisul de mână
Informații despre dizabilități	Informații genetice	Token-uri de securitate
Informații despre locație	Detalii polițe de asigurare	Cookies
Ce faci într-un anume moment / status	Informații medicale	Informații sesiuni și token-uri
Participarea la evenimente	Cazier	Hash parole
Orientare sexuală	Istoric împrumuturi bancare	Site-uri pe care ești înregistrat

GLOSAR GDPR

Regulamentul General pentru Protecția Datelor a fost conceput și scris de avocați, așa că nu este surprinzător faptul că acest document cuprinde o mulțime de termeni greoi, care nu au niciun sens la prima vedere. Iată care sunt noțiunile cele mai importante din GDPR și ce înseamnă mai exact.

PERSOANĂ VIZATĂ (DATA SUBJECT)

Individul sau persoana a cărui date cu caracter personal sunt procesate.

DATE CU CARACTER PERSONAL (PERSONAL DATA)

Orice informație referitoare la o persoană care poate duce la identificarea acesteia (de exemplu, nume, numărul documentului de identitate, adresa fizică, adresa de IP, informații despre sănătate etc.)

OPERATOR DE DATE (DATA CONTROLLER)

O organizație sau o companie care colectează datele cu caracter personal și ia decizii referitoare la modul în care sunt administrate. Astfel, dacă sala ta de fitness colectează date personale și aceasta decide cum se procesează, clubul tău este Controlor de date și trebuie să respecte legislația GDPR referitoare la această entitate.

PERSOANĂ ÎMPUTERNICITĂ (DATA PROCESSOR)

O companie sau o organizație care ajută Controlorul să proceseze datele, urmând instrucțiunile acestuia. Procesatorul de date nu decide cum se utilizează datele personale. De exemplu, UPfit este procesatorul de date prin care clubul tău de fitness colectează aceste informații. Noi nu controlăm ce faci cu datele, noi doar le procesăm pentru tine, în concordanță cu instrucțiunile tale.

PRELUCRAREA DATELOR

Orice operațiune sau set de operațiuni care se realizează cu date personale sau seturi de date personale, prin metode automate sau nu, precum colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau alterarea, consultarea, recuperarea, folosirea, divulgarea (prin transmitere, diseminare sau prin alte metode), combinarea, ștergerea sau distrugerea datelor.

RESPONSABILUL CU PROTECȚIA DATELOR (DATA PROTECTION OFFICER - DPO)

Un reprezentant al unei companii sau organizații care este Controlor sau Procesator de date. DPO trebuie să fie expert în protecția datelor personale și să se asigure că organizația sau compania pentru care lucrează respectă toate regulile GDPR care i se aplică.

EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR (DPIA)

O evaluarea bine documentată asupra unui anumit tip de prelucrare a datelor, referitoare la utilitatea acestor date, care sunt riscurile pentru acest tip de prelucrare și ce opțiuni ai pentru reducerea și rezolvarea acestor riscuri.

AUTORITATEA DE SUPRAVEGHERE (SUPERVISORY AUTHORITY)

Una sau mai multe agenții guvernamentale dintr-o țară membră a Uniunii Europene care verifică respectarea GDPR în țara respectivă. De exemplu, în România există o singură astfel de autoritate. Este vorba despre Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal. (www.dataprotection.ro)

CONSIMȚĂMÂNTUL DE PRELUCRARE A DATELOR (OPT-IN)

Procesul de a aduna informații personale, prin care persoana în cauză își dă consimțământul de bună voie, într-un mod deliberat, pentru prelucrarea datelor sale cu caracter personal.

DOUBLE OPT-IN

Procesul prin care o persoană trebuie să treacă printr-un mecanism în 2 pași pentru a-și da consimțământul de prelucrare a datelor sale cu caracter personal.

PASSIVE OPT-IN

Procesul de adunare a datelor cu caracter personal care se folosește de un opt-in implicit. De exemplu, un checkbox deja selectat, pe care un user ar trebui să-l de-selecteze în cazul în care nu vrea să-și dea consimțământul pentru prelucrarea datelor sale personale.

OPT-OUT

Procesul de a adăuga informații despre clienți la o listă de contact fără consimțământul acestora, după ce aceștia s-au abonat la un alt serviciu. Ulterior, respectivii clienți trebuie să se dezaboneze, dacă nu vor să mai fie pe acea listă.

PROFILING

Prelucrarea automată a datelor cu caracter personal pentru a evalua, analiza sau a prezice orice caracteristici ale individului în cauză. De exemplu, trimiterea de e-mailuri automate unui grup de membri care au adresa fizică într-un anumit oraș sau care au o anumită vârstă.

PRIVACY BY DESIGN

Privacy by design înseamnă că orice acțiuni ale unei companii care implică prelucrarea datelor cu caracter personal trebuie făcute plecând de la grija pentru protejarea informațiilor personale. Asta include proiecte interne, dezvoltări de produs, dezvoltări de software, sisteme IT și nu numai. De fapt, înseamnă că departamentul de IT sau orice alt departament care procesează informații personale, trebuie să se asigure că orice proiect nou are un sistem de protecție a datelor pe tot parcursul de creare și implementare. Din mai, adăugarea de funcționalități pentru protecția datelor la finalul unui proces lung de dezvoltare nu mai este legal.

PRIVACY BY DEFAULT

Privacy by default înseamnă că odată ce un produs sau un serviciu a fost lansat public, cele mai stricte setări pentru protecția datelor au fost deja implementate în mod implicit. Asta fără ca user-ul să fie nevoit să facă vreo operațiune sau să achiziționeze o funcționalitate în plus.

CHECKLIST GDPR PENTRU CLUBUL TĂU DE FITNESS

Din moment ce cluburile de fitness lucrează cu diverse tipuri de date personale, este important să te asiguri că afacerea ta respectă în totalitatea normele GDPR.

În primul rând, trebuie să determini ce date personale deții și cum sunt folosite, inclusiv modul în care folosești funcționalitățile UPfit de marketing și vânzări. De asemenea, este important să ceri sfaturi legale pentru a te asigura că întrunești toate condițiile pentru a procesa datele membrilor tăi.

Pentru a determina ce pași trebuie să parcurgi astfel încât sala ta de fitness să respecte GDPR, iată o listă cu subiectele pe care trebuie să le iei în considerare înainte de 25 mai 2018.

1. EVALUAREA

- Ce date personale colectezi / stochezi?
- Le-ai obținut în mod corect? Ai consimțămintele necesare? Membrii tăi știu exact modul și scopul pentru care sunt utilizate informațiile lor? Ai fost suficient de clar atunci când le-ai explicat scopul cu care le procesezi datele și le-ai prezentat dreptul de a-și retrage consimțământul în orice moment?
- Ești sigur că nu stochezi date personale mai mult timp decât este necesar și că toate informațiile sunt la zi?
- Păstrezi datele cu caracter personal într-un sistem sigur, folosind un nivel de securitate suficient de ridicat? De exemplu, este necesar să folosești criptarea sau pseudonime pentru a proteja datele pe care le deții? Limitezi accesul la aceste date pentru a te asigura că sunt folosite doar în scopul în care au fost colectate?
- Colectezi sau procesezi date personale din categorii speciale, precum informații cu caracter personal despre copii, date genetice sau biometrice etc? Dacă faci asta, îndeplinești standardele necesare pentru a le colecta, procesa și stoca?
- Transferi date personale în afara Uniunii Europene? Dacă faci asta, ai un sistem sigur de transfer?

2. PLANUL GDPR

- Ai pus la punct un plan GDPR în clubul tău de fitness, pentru a te asigura că respecți regulamentul începând din 25 mai 2018?
- Ai stabilit un buget special pentru a pune în aplicare planul GDPR al clubului tău?
- Ai nevoie de o Evaluare a impactului asupra protecției datelor (DPIA)?
- Trebuie să angajezi un Responsabil cu protecția datelor (DPO)?
- Implementezi o politică de protecție a datelor personale implicită (privacy by design), prin care te asiguri că iei în considerare în mod regulat ce impact pot avea proiectele și măsurile noi pe care le implementezi în clubul tău asupra protecției datelor?
- Ai inclus în planul tău GDPR modul în care administrezi datele cu caracter personal al angajaților tăi?

3. PROCEDURI ȘI CONTROL

- Echipa sau compania care se ocupă de securizarea datelor știe care sunt obligațiile GDPR și au suficiente resurse să implementeze modificările și măsurile noi necesare?
- Ai proceduri puse la punct prin care să administrezi cererile membrilor sau ale LEAD-urile pentru modificarea, ștergerea sau accesul la datele lor personale?
- Ai pus la punct proceduri de notificare în cazul unor breșe de securitate, astfel încât să respecți toate obligațiile GDPR, inclusiv perioada de notificare asupra breșelor (72 de ore din momentul în care ai descoperit problema)?
- Ți-ai educat angajații vizavi de tot ce înseamnă GDPR și modul în care trebuie să administreze datele cu caracter personal la care au acces? Faci un audit în mod regulat al datelor cu caracter personal pe care le administrezi?

4. DOCUMENTAȚIE

- Ai deja o Politică de confidențialitate și dacă da, trebuie să o modifici pentru a fi în concordanță cu regulile GDPR?
- Ai o politică bine pusă la punct vizavi de perioada în care stochezi toate datele personale, de la membri, potențiali membri (LEADS) și furnizori, la angajați sau persoane care au aplicat pentru un job la clubul tău?
- Procedurile interne ale clubului tău au toată documentația necesară?
- Dacă ești Operator de date, ți-ai modificat contractele cu toți Controlorii pentru a te asigura că includ clauzele obligatorii specificate în Articolul 28 din Regulamentul General pentru Protecția Datelor?
- În cazurile în care alte companii procesează date pentru tine (third party), te-ai asigurat că toate contractele cu acestea includ aceleași clauze ca cele pentru Operatori?

CUM AFECTEAZĂ GDPR DEPARTAMENTUL DE MARKETING ŞI VÂNZĂRI AL CLUBULUI TĂU DE FITNESS

Dacă folosești strategii de e-mail / sms marketing în clubul tău de fitness, este foarte important să te pui la punct cu toate directivele GDPR. Cel mai important aspect pentru cei care se ocupă de marketing este noua definiție pentru consimțământ impusă de regulamentul european.

Consimțământul pentru a procesa datele cu caracter personal trebuie dat de bună voie, într-un mod deliberat. Cu alte cuvinte, individul este cel care trebuie să aleagă dacă vrea ca datele lui personale să fie procesate și în ce fel. În plus, companiile trebuie să demonstreze că o persoană și-a dat consimțământul în mod voit pentru prelucrarea datelor sale.

PROCEDURILE DE PASSIVE OPT-IN ȘI OPT-OUT SUNT INTERZISE DE GDPR

Potrivit Regulamentului pentru Protecția Datelor Personale, consimțământul de prelucrare a datelor (opt-in) este procesul prin care se adună informații personale, prin care individul în cauză își dă consimțământul de bună voie, într-un mod deliberat, pentru prelucrarea datelor sale.

Asta înseamnă că nu mai ai voie să folosești adresele de e-mail pe care le-ai adunat prin alte procedee, precum passive opt-in sau opt-out.

Așadar, nu ai voie să folosești liste cu adrese de e-mail, numere de telefon sau orice alte informații personale, dacă aceste date nu au fost primite de la membri sau LEAD-uri în mod voit. De asemenea, aceste date trebuie folosite doar în scopul pentru care ți s-a dat consimțământ și nu pentru altceva.

Odată cu intrarea în vigoare a noului regulament, va trebui să poți demonstra faptul că ai primit consimțământul voit de la membrii tăi pentru a le procesa informațiile. În multe cazuri, asta înseamnă ca va trebui să le ceri membrilor tăi sau LEAD-urilor din baza ta de date să îți reconfirme faptul că sunt de acord să le procesezi datele lor personale.

MEMBRII CLUBULUI TĂU TREBUIE SĂ ȘTIE DACĂ FOLOSEȘTI PROCEDEE DE PROFILING

Deși GDPR nu interzice procedeele de profilling, adică prelucrarea automată a datelor personale pentru evaluarea, analiza sau prezicerea unor caracteristici ale individului, Regulamentul obligă companiile care folosesc aceste tehnici să-și informeze clienții / membrii.

Acest aspect este cu atât mai important în domeniul marketingului.

Poți să folosești în continuare procedee automate, atâta timp cât îți informezi membrii și LEAD-urile despre acest procedeu și le oferi posibilitatea de a ieși din sistemul automat. De asemenea, aceștia îți pot solicita ca o persoană să fie implicată în prelucrarea automată a informațiilor lor.

CUM SĂ-ȚI PREGĂTEȘTI DEPARTAMENTUL DE MARKETING ȘI VÂNZĂRI PENTRU GDPR

Întreaga ta echipă trebuie să știe ce înseamnă GDPR și cum le va afecta activitatea din club odată ce regulamentul intră în vigoare la 25 mai 2018. Totuși, departamentul tău de marketing și vânzări are ceva mai mult de lucru.

Astfel, primul pas pentru a te asigura că sala ta de fitness respectă GDPR este să verifici dacă lista ta actuală de contacte are toate consimțămintele necesare (opt-in). Pentru asta trebuie să te întrebi:

- Membrii și LEAD-urile tale și-au dat consimțământul să primească e-mailuri de la clubul tău de fitness printr-un formular de opt-in?
- Consimțământul a fost dat pentru scopul specific cu care le folosești informațiile? De exemplu, dacă ei și-au dat consimțământul să primească e-mailuri referitoare la rezervările la clasele de Group Fitness, nu ai voie să le trimiți și e-mailuri de newsletter sau oferte.
- Ai un istoric precis și sigur al tuturor consimțămintelor primite?
- Potrivit legii, copiii sub 16 ani nu își pot da consimțământul pentru prelucrarea datelor lor personale, fără consimțământul părinților lor - dacă lista ta conține membrii sub 16 ani, ai toate opt-in-urile necesare?
- Politica ta de confidențialitate conține un limbaj simplu prin care li se explică membrilor care sunt drepturile lor cu privire la protecția datelor lor personale?
- Ai proceduri speciale prin care să le oferi posibilitatea membrilor tăi să-ți ceară o copie a datelor lor, să le modifici informațiile, să le ștergi sau să le exporți datele cu caracter personal pe care le ai în baza de date? Acest lucru se poate face printr-un formular special, în pagina de contact a site-ului sau printr-un link în newsletter.
- Ai stabilit un procedeu simplu prin care membrii sau LEAD-urile pot să refuze ca datele lor să fie procesate prin metode automate?

CE TREBUIE SĂ FACI ACUM

- **Să-ți informezi echipa despre regulile GDPR și să le explici cum le vor afecta activitatea în companie**
- **Să inventariezi toate datele cu caracter personal pe care le deții și să te asiguri că ai toate consimțămintele necesare**
- **Să identifici măsurile necesare pentru a implementa un plan GDPR**
- **Să înțelegi și să te documentezi despre bazele legale pentru fiecare tip de prelucrare a datelor personale**
- **Să te asiguri că toți controlorii și procesatorii de date cu care lucrezi respectă în totalitate regulile GDPR**
- **Să stabilești proceduri prin care să răspunzi la cereri, atunci când o persoană își exersează drepturile definite de GDPR**
- **Să cureți datele cu caracter personal vechi, pe care nu le mai folosești**
- **Să pui la punct Evaluări a impactului asupra protecției datelor personale în cazul operațiunilor cu risc ridicat**
- **Să stabilești proceduri în cazul breșelor de securitate**

CE DEPARTAMENTE TREBUIE IMPLICATE

- **Echipele de marketing** - trebuie să verifice că au toate consimțămintele necesare de la membri / clienți pentru a le procesa datele personale
- **Echipele de management și dezvoltare de produs** - să construiască funcționalități pentru protecția datelor. Să se asigure că procesează datele într-un mod sigur
- **Departamentele juridice** - să revizuiască toate contractele existente cu alte entități (third parties) și să monitorizeze faptul că firma respectă GDPR

UPFIT CLOUD

www.upfit.cloud