Reguli adoptate de către Asociația Real Sports pentru implementarea GDPR și asigurarea cerințelor minime de securitate

1. Scop

Prezentul document prezinta masurile minime de securitate a datelor pe care Asociația Real Sports le-a adoptat in scopul asigurarii confidentialitatii, disponibilitatii, accesibilitatii si a caracterului de non-repudiere aferent tuturor activitatilor de procesare a datelor cu caracter personal asa cum sunt ele definite de reglementarile in rigoare.

Masurile adoptate includ metode adecvate riscurilor la adresa securitatii informatiei in acord cu amenintarile si vulnerabilitatile specifice. Intrucat aceste riscuri, amenintari, vulnerabilitati sunt in continua schimbare metodele vor fi adoptate in permanenta.

Totodata, aceste cerinte vor fi revizuite, amendate si actualizate in contextul cerintelor legale, a reglementarilor in vigoare si a standardelor de securitate aplicabile.

2. Domeniul de aplicare a acestor cerințe

Măsurile de securitate necesare pentru procesarea Datelor cu Caracter Personal trebuie să garanteze un nivel de securitate indiferent de modul de realizare al procesarii informatiei si datelor, daca aceasta e realizata de Asociația Real Sports sau de Subcontractori, folosind metode de acces local sau la distanta, prin mijloace electronice sau fizice. Prezentele reguli se aplică angajaților si membrilor Asociația Real Sports precum și subcontractorilor, colaboratorilor, etc. ce prestează servicii pentru Asociația Real Sports.

Cerintele de securitate sunt descrise in cele ce urmeaza, avand in vedere masurile de organizare, cele tehnice si de personal.

3. Inventarul activelor informaționale

Asociația Real Sports folosește în activitatea curentă următoarele componente IT:

- desktop-uri;
- laptop-uri;
- stick-uri;
- CD-uri;
- hard disk-uri externe.

4. Prelucrarea datelor cu caracter personal se realizează în următoarele condiții:

Întocmirea, primirea, păstrarea, accesarea, transmiterea, transportul, utilizarea și predarea documentelor care conțin date cu caracter personal se fac exclusiv de către persoane instruite cu privire la regulile de protecție a datelor cu caracter personal.

Întocmirea, primirea, păstrarea, accesarea, transmiterea, transportul, utilizarea și predarea documentelor care conțin date cu caracter personal se fac cu respectarea strică a regulilor de protecție a datelor cu caracter personal.

Întocmirea, primirea, păstrarea, accesarea, transmiterea, transportul, utilizarea și predarea documentelor care conțin date cu caracter personal se fac exclusiv în scopul realizării atribuțiilor de serviciu sau îndeplinirii cerințelor legale.

Este interzisă orice divulgare a documentelor care conțin date cu caracter personal, precum și orice informație cu caracter personal cuprinsă în acestea.

Întocmirea. Documentele întocmite pentru salariați la nivelul serviciilor au regimul documentelor care conțin date personale și sunt supuse regulilor de protecție a datelor cu caracter personal.

Primirea. Primirea documentelor care conțin date cu caracter personal se face cu promptitudine și cu îndeplinirea imediată a procedurilor de păstrare sau utilizare.

Păstrarea. Documentele care conțin date cu caracter personal se păstrează în spațiu închis cu cheie, cu excepția situațiilor în care este necesară utilizarea lor firească, potrivit necesităților activității.

Accesarea. Accesarea documentelor care conțin date cu caracter personal se face doar în momentul și doar câtă vreme este necesară utilizarea lor. Accesarea documentelor cu character personal pentru buna desfășurare a activității, precum și pentru asigurarea realizării drepturilor și intereselor clientului/furnizorilor, cumpărătorilor etc., la nivelul fiecărui serviciu, prin solicitarea acestor date de la persoana/serviciul care răspunde de ele.

Utilizarea. Documentele care conțin date cu caracter personal părăsesc spațiul în care sunt păstrate doar în intervalul de timp necesar pentru utilizarea lor firească, potrivit necesităților activității.

Predarea. Predarea-primirea documentelor fizice care conțin date cu caracter personal se face doar în condițiile în care se respectă confidențialitatea datelor.

În cazul în care un document fizic care conține date cu caracter personal nu este reglementat în Procedura privind protecția datelor cu caracter personal, va fi înștiințat de îndată reprezentantul legal al asociației.

În cazul în care o sursă de informații care conține sau este de natură să determine colectarea de date cu caracter personal nu este reglementată în Procedura privind protecția datelor cu character personal, va fi înștiințat de îndată reprezentantul legal al asociației.

5. Descrierea modului in care se realizeaza protectia acestora pentru asigurarea clasificariidatelor, a confidentialitatii si integritatii acestora.

Protecția datelor se realizează, în primul rând, prin introducerea prezentei proceduri de lucruprin care membrii, voluntarii și salariații asociației sunt instruiți cu privire la măsurile adoptate pentru asigurarea protecției datelor cu caracter personal.

Conectarea la activele informaționale se realizează de către personalul asociației în baza unui user și a unei parole unice generate de către reprezentant legalul site-ului web, devenind Utilizator autorizat. Fiecare persoană autorizată să gestioneze datele cu caracter personal trebuie să păstreze userul si parola secrete și să nu le încredințeze altui angajat sau terțe persoane. În situația în care userul și parola nu sunt utilizate mai mult de 6 luni sau când Utilizatorul autorizat încetează raportului de muncă, atunci reprezentant legalul site-ului va dezactiva și va sterge userul și parola.

Bazele de date transmise prin mijloace electronice vor fi parolate și parola va fi comunicată prin e-mail separat/telefonic/SMS.

6. Confidențialitatea datelor cu caracter personal :

a. Personalul asociației garantează seriozitatea personalului oricărei alte persoane similare subcontractate, care accesează Date cu Caracter Personal, și că personalul respectiv a beneficiat de o pregătire adecvată în domeniul protecției și manipulării Datelor cu Caracter Personal și a semnat clauze de confidențialitate cu privire la prelucrarea Datelor cu Caracter Personal.

b. Persoanlul asociației se obligă să nu dezvăluie datele cu caracter personal prelucrate, modul în care acestea au fost prelucrate, scopurile prelucrării, destinatarii datelor, perioada stocării datelor, procedurile de lucru în privința protecției datelor cu caracter personal, ștergerea datelor, plângerile și sesizările depuse la ANPDCP, cazurile de încălcare a securității datelor cu caracter personal, informații despre care a luat cunoştinţă pe durata executării contractului de muncă,

c. Sunt confidenţiale Datele cu Caracter Personal, astfel cum sunt definite de Regulamentul CE nr.2016/679: orice informaţii privind o persoană fizică identificată sau identificabilă; o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

d. Personalului asociației îi este interzis să divulge informațiile anterior menționate, să copieze, stocheze, modifice, intervină, fotografieze, salveze datele cu caracter personal ale persoanei vizate sau evidența prelucrărilor pe active informaționale proprii sau neautorizate, să nu utilizeze aceste informații în scop personal și indiferent de modul în care a luat la cunoștință despre aceste date.

e. Membrilor, voluntarilor și angajaților asociației le este interzis să permită persoanelor neautorizate, intenționat sau din culpă, să realizeze una dintre acțiunile anterior enumerate.

f. Personalului asociației va prelucra datele doar în condițiile în care s-a asigurat în prealabil că:

- activul informațional poate fi utilizat în siguranță;
- nu există pericolul unei dezvăluiri accidentale a datelor cu caracter personal;
- în proximitatea sa nu se află persoane care nu au dreptul să prelucreze datele cu caracter personal;
- persoanele din proximitate nu pot vedea și prelua user-ul și parola de acces;
- parola nu este afișată în mod clar în câmpul destinat.

g. Membrii, voluntarii și angajații asociației se obligă să:

- prelucreze datele cu caracter personal doar prin intermediul activelor informaționale autorizate de asociație și asupra cărora are autorizat accesul/activul informațional alpersonalului.
- păstreze în siguranță user-ul și parola de acces la activele informaționale ale asociației,

- nu comunice sau să noteze user-ul și parola de acces pe foi, telefon, fișiere word sauexcel;
- nu părăsească activul informațional în momentul în care s-a logat cu user și parolă iar ecranul nu este blocat;
- nu acceseze activele informaționale ale altor angajați, cu excepția dispoziției date de personalul ierarhic superior, și, în condițiile respectării tuturor obligațiilor deconfidențialitate;
- acceseze informațiile din cloud sau cele stocate pe stick-urile / hard disk-urile asociației doar de pe activele informaționale pentru care asociația și-a dat acceptul;
- nu se logheze cu user și parolă prin intermediul altor active informaționale, cu excepția celor puse la dispoziție de asociație. În cazul în care primește permisiunea de a folosi alte mijloace active informaționale, atunci se va asigura în prealabil că acestea respectă toate condițiile tehnice de securitate impuse prin prezenta procedură precum și faptul că poate fi respectată întocmai obligația de confidențialitate;
- nu utilizeze la prelucrarea datelor stick-uri / hard disk-uri personale neautorizate de către angajtor;
- nu proceseze categorii speciale de date personale cu caracter personal în înțelesul art.9 din Regulamentul nr. 2016/679, cu excepția situației în care primește instrucțiuni exprese în acest sens;
- să notifice în termen de 24 de ore și să asigure suport nelimitat reprezentantului legal sau clientului său în condițiile apariției unui breșe de securitate, astfel cum este definită în continuare, și, că va urma procedura și va lua măsurile specifice în asemenea caz.
- să notifice reprezentantului legal atunci când nu poate respecta sau prefigurează că nu va putea respecta instrucțiunile de prelucrare și motivele și să înceteze prelucrarea până la noi instrucțiuni.

7. Breșă de securitate

Breșă de securitate reprezintă orice distrugere, pierdere, modificare, dezvăluire sau accesare a Datelor cu Caracter Personal accidentală, neautorizată sau ilegală, sau orice situație de încălcare proprie sau de către alte persoane a politicii și procedurilor privind securitatea datelor cu caracter personal de care a luat la cunoștință sau orice risc de apariție a unei Breșe de securitate.

Procedura în cazul unei Breșe de securitate este următoarea:

a) persoana trimite o Notificare către Reprezentant legal în care va menționa:

- detaliile Breșei de Securitate;
- tipul de date care au făcut obiectul Breșei de Securitate și
- identitatea fiecărei persoane afectate (sau, dacă nu este posibil,numărul aproximativ de persoane vizate și de înregistrări de Date cu CaracterPersonal vizate);
- descriere a consecințelor probabile ale Breșei de Securitate;

- descriere a măsurilor luate sau propuse a fi luate de către asociație pentru a soluționa Breșa de Securitate, inclusiv, dacă este cazul, măsuri de atenuare a posibilelor efecte negative ale acesteia;
- orice alte informații solicitate de reprezentantul legal în mod rezonabil, referitoare la Breșa de Securitate.

b. Personalul asociației va ajuta reprezentantul legal pentru a investiga Breșa de Securitate și pentru a identifica, preveni și a atenua cât mai mult posibil efectele acesteia, în conformitate cu obligațiile care îi revin conform contractelor încheiate cu clienții.

c. Personalul asociației nu va comunica altor angajați neautorizați, nu va emite sau publica nici o declarație, nici un anunț, comunicat de presă, sau raport privitor la Breșa de Securitate legată de Datele cu Caracter Personal („Anunțuri"). Acțiunile și măsurile descrise mai sus se vor lua pe cheltuiala persoanei în cauză, dacă se va stabili culpa acestuia.

d. Reprezentant legalul va forma o echipă desemnată să gestioneze și coordoneze reacția la incidente, formată din Reprezentant legal, persoana care a sesizat Breșa de securitate și responsabilul IT. În situația Breșei de securitate sesizată de către Persoana Împuternicită de Operator sau de către un Subcontractant, din echipă va face parte și persoana care a sesizat Breșa de Securitate precum și persoana desemnată să gestioneze astfel de situații din cadrul respectivelor companii.

e. Persoana care a identificat breșa va anunța și Operatorul despre Breșa de securitate, în situația în care Asociația Real Sports este Persoana Împuternicită de Operator.

f. Echipa astfel formată va colabora, dacă este cazul, cu reprezentanții responsabili cu securitatea din cadrul Operatorului, până la rezolvarea satisfăcătoare a incidentului sau a încălcării.

g. De asemenea, echipa de securitate va analiza situația, va adopta măsurile cele mai bune de limitare pe moment a efectelor Breșei de securitate, de înlăturare a acestora și va adopta și implementa măsurile necesare pentru a evita în viitor apariția unui caz asemănător.

h. Fiecare persoană din cadrul asociației va ține un jurnal cu evidența incidentelor și a acțiunilor luate, în care se va consemna momentul producerii incidentului, persoana care a raportat incidentul, persoana căreia i s-a raportat incidentul și efectele acestuia.

i. Prezenta procedură va fi urmată și de către Persoana Împuternicită de Operator sau Subcontractanților, în cazul unor Breșe de securitate.

j. Personalul asociației va răspunde pentru prejudiciul cauzat asociației și clienților săi, rezultat din sau în legătură cu orice nerespectare a dispozițiilor prezentului Regulament sau ale Legii aplicabile privind protecția datelor.

Personalul asociației se obligă să nu stocheze pe niciun tip de suport (stick, hard disk extern, CD, etc.) orice date cu caracter personal fără acordul expres dat în prealabil de către Asociația Real Sports Dacă i se dă acest accept, atunci suporturile pe care sunt stocate baze de date nu vor fi depozitate în afara incintei asociației și a locurilor special desemnate, astfel încât să nu existe riscul să fie accesate de către persoane neautorizate.

Toate suporturile electronice și înscrisurile pe care se afla inregistrate/consemnate/stocate informatii cu caracter confidential, userul și parola de acces la activele informatice ale Asociației

Real Sports sunt și rămân proprietatea asociației sau dupa caz a Clienților acestuia, personalul având obligaţia de a le preda imediat la solicitarea reprezentantului legal sau o data cu încetarea contractului de prestari servicii, în caz de refuz urmând a suporta prejudiciul creat. Daca utilizarea dispozitivelor sau suporturilor de orice fel pe care se afla inregistrate/consemnate/stocate informatiile cu caracter confidential este necesara pentru desfasurarea serviciilor contractate, personalul raspunde direct si nemijlocit de siguranta respectivelor informatii si pentru consecintele produse de dezvaluirea acestora din neglijenta sa.

8 Personalul asociației va aduce, de urgență, la cunoștința reprezentantului legal orice solicitare de a divulga orice informaţii ce privesc datele cu caracter personal, indiferent de modul în care au fost făcute propunerile respective, contra cost sau nu.

9. Personalul asociației recunoaşte dreptul de proprietate exclusivă a asociațieii asupra tuturor datelor cu caracter personal, astfel cum sunt acestea definite în prezentele reguli.

10. Personalul asociației recunoaste importanta exceptionala pe care o are pentru asociație respectarea clauzelor referitoare la obligatia de confidentialitate, si avand in vedere aceasta, recunoaste ca nerespectarea acestor clauze constituie o grava abatere disciplinara care poate fi sanctionata de reprezentantul legal al asociației.

11. Asociația îşi rezervă dreptul de a cere daune-interese pentru acoperirea eventualelor prejudicii pe care le-ar suferi în urma divulgării intenţionate, neglijenţei, pierderii ori folosirii greşite a datelor cu caracter personal, încălcării prezentelor reguli și a instrucțiunilor primite de la asociație sau de la clienții acesteia.

12. În cazul în care mai multe persoane, membri, voluntar sau angajați, folosesc pentru a accesa o bază de date, concomitent sau alternativ, același user și aceeași parolă, fiecare persoană este obligată să respecte prezentele reguli de securitate și în ceea ce privește acest user și parolă.

13. Integritatea datelor:

a) Pentru a asigura integritatea datelor, asociația realizează periodic back-up-ul datelor stocate pe activele informatice folosite de membri, voluntari sau asociați.

b) Activele informaționale și bazele de date folosite de personalul asociației sunt parolate și pot fi accesate doar cu un user și o parolă unic atribuite fiecărei persoane.

c) Personalul asociației trebuie să respecte următoarea procedură cu privire la prelucrarea datelor cu character personal:

- Persoana va copia, dacă a primit instrucțiuni în acest sens, întreaga bază de date și nu doar anumite coloane sau rânduri din bazele de date;
- Dacă a primit instrucțiuni exprese de la persoane autorizate să încalce regula de la lit. a) atunci nu va aplica filtre în mod separat pe fiecare rând sau coloană astfel încât să existe riscul ca, după aplicarea filtrelor, să nu mai existe o corelare între toate rândurile și coloanele bazei de date;

- Personalul nu va modifica sau șterge baza de date, cu excepția situației în care a primit instrucțiuni exprese în acest sens și a urmat procedura prevăzută pentru acest tip de activitate;
- Personalul nu va procesa în același timp două baze de date ale unor clienți diferiți. Înainte de a accesa o nouă bază de date, Personalul se va deconecta de la baza de date anterioară;
- Bazele de date vor fi transferate doar prin intermediul e-mailului de serviciu și doar pe adresele de corespondență comunicate de către clienți;
- În cazul în care, în mod excepțional, transferul bazelor de date este necesar să se realizeze prin aplicații specializate (we transfer), acestea vor fi obligatoriu parolate și parola se va comunica doar telefonic și nu prin email / sms.

14. Metodele de securizare a activelor informationale.

a) Toate informațiile și bazele de date sunt salvate pe server. Există back-up salvat tot pe server.

b) Copiile de siguranță salvate pe suporturi electronice vor fi păstrate în încăperi distincte de cele în care se află cele originale, încăperi la care au acces doar Utilizatori autorizați să prelucreze respectivele informații.

c) Prelucrarea datelor se realizează de fiecare persoană conectându-se la activele informaționale doar în baza unui user și a unei parole.

d) Aplicația folosită de personal salvează mai multe date atunci când sunt modificate datele: persoana care a făcut modificările, modificările realizate.

e) Activele informaționale sunt protejate anti-malware.

15. Plan de restabillire in siguranta a activitatilor in caz de intrerupere urmare a unui eveniment major (precum catastorfa naturala, atac cibernetic, indisponibiltate a sistemelor suport sau alte incidente perturbatoare).

a) În cazul întreruperii activităților ca urmare a unui eveniment major (catastrofă naturală, atac cibernetic, indisponibilitate a sistemelor suport sau alte incidente perturbatoare) persoanalul asociației sunt obligate să aducă la cunoștința Reprezentant legalului acest aspect.

b) După verificarea situației, Reprezentant legalul va aviza personalul IT să:

- întrerupă conexiunea celorlalte active informaționale astfel încât să nu fie afectate;
- reinstaleze programele și a bazele de date;
- recuperează datele cu ajutorul back-up-ului.

c) Prevederile procedurilor vor fi revizuite atunci când intervin modificări și cunoașterea lor de către membri, voluntari și angajați va fi verificată anual de către Reprezentant legal în urma verificării prin sondaj.

d) Termenul de păstrare al documentului de securitate, evidențelor și documentațiilor aferente este de 5 ani de la închiderea prelucrării sau până la solicitarea de ștergere a datelor.

e) Activele informatice care conțin date cu caracter personal sunt conectate la UPS-uri care le asigură funcționarea și în caz de întrerupere a alimentării.

16. Masuri tehnice

a) Asociația aplică măsuri tehnice de securitate preventivă împotriva riscurilor de securitate a informatiei aferente activitatilor sale, cum ar fi:

- -parolarea laptopurilor și desktopurilor, parolele având minim 8 caractere;
- -salvarea datelor pe server;
- -back-up periodic;
- -instalarea programelor antivirus;
- -dezactivarea automată a activului informativ după o perioadă de inactivitate de 10 minute;
- -cripatarea datelor.

b) Pentru fiecare risc identificat masurile tehnice vor fi compensate cu un alt mecanism de protectie din sfera roganizatorica sau de personal.

17. Controlul accesului:

a) Accesul la datele cu caracter personal se realizează de către personalul autorizat (Utilizatori autorizați) și în funcție de sarcinile de serviciu.

b) Persoanele care au acces la datele cu caracter personal sunt instruite și monitorizate în mod corespunzător.

c) Fiecare persoana desemnata sa realizeze operatiuni de procesare efectuează operațiunile cu ajutorul activului informatic ce i-a fost repartizat și la care se conectează în baza unui user și a unei parole.

d) Toate conturile programelor informatice utilizate de asociație sunt accesate în baza unui user și parolă alocate fiecărei persoane și sunt gestionate centralizat. Accesul la activele informatice (laptop-uri, desktop-uri) implicate in procesare vor fi autorizate in baza autentificarii fiecărei persoane cu un user și o parolă.

e) Parolele conțin cel puțin opt caractere iar dacă sistemul informatic nu permite acest lucru din punct de vedere tehnic, parola va consta din numărul maxim permis de caractere. Parolele sunt setate de către fiecare Utilizator autorizat, cu excepția parolelor pentru bazale de date primite de la clienți, și nu conțin niciun element care să poată fi ușor asociat cu Utilizatorul autorizat care răspunde de Prelucrare. Parolele și secvențele secrete sunt schimbate la intervale de 6 luni regulate.

f) Accesul la datele cu caracter personal, indiferent daca sunt stocate, transmise sau modificate este posibil doar pentru Utilizatorul autorizat.

g) Masurile de control la nivelul sistemului de operare, acces la baze de date si la stocarea datelor trebuie sa fie configurate conform cu nivelele minime de permisiuni. Numai personalul autorizat

prin documentul de securitate este îndreptățiți sa acorde, sa modifice sau sa retragă accesul utilizatorilor la sistemele informatice.

h) Asociația întocmește și păstrează jurnalele de acces la sistemele informatice pe perioada minimă prevăzută de lege sau, dacă legea nu prevede, pe o perioadă de 5 ani de la definitivarea prelucrării.

i) Pentru a asigura comunicarea în condiții de siguranță și reducerea riscurilor, accesul administrativ de la distanță la activele informationale esențiale se realizează în mod excepțional situație în care se utilizează soluții de autentificare puternica, monitorizarea indeaproape a accesului si prin utilizarea de protocoale sa nu permita interceptarea comunicatiilor, respectiv criptarea comunicațiilor.

18. Tipurile de date prelucrate de către membri, voluntari și salariați:

- numele și prenumele;
- data nasterii;
- sex;
- adresa de domiciliu;
- adresa de email;
- numărul de telefon;
- seria și numărul cărții de identitate;
- clubul sportiv din care face parte (optional).

Datele vor fi prelucrate atât în format digital cât și/sau in format tipărit.

19. Consimțământul prelucrării

a) Salariații își exprimă consimțământul ca asociația sa colecteze si sa prelucreze datele mele cu caracter personal: nume și prenume, adresă de domiciliu, adresă de email, număr de telefon, CNP, seria și numărului cărții de identitate, copia cărții de identitate, etc. in scopul incheierii si executarii contractului de munca cu Asociația Real Sports.

b) Mentionez ca sunt de acord in mod expres ca destinatarii datelor mele cu caracter personal sa fie angajatii societatii, departamentul de contabilitate, colaboratorii și clientii (in ceea ce priveste numele și prenumele, adresa de email si numarul de telefon), precum si autoritatile statului si ca sunt de acord cu stocarea acestor date in arhiva Asociația Real Sports.

c) Fiecare salariat se obligă să obțină acordul prealabil al persoanei vizate în vederea prelucrării datelor cu caracter personal.

20. Stocarea, copiere, imprimarea, transmiterea și ștergerea datelor

a) Datele cu caracter personal vor fi stocate pe suport fizic: hârtie, sau în format digital: stick, hdd, google drive, platforme digitale, etc.

b) Datele vor fi păstrate în arhiva, birourile și activele informatice ale asociației, precum și digital (mail gmail, mail server, whatsapp, facebook, email marketing, google contacts, google drive, cloud și alte platforme) și vor fi prelucrate de către angajații și colaboratorii asociației, clienții și serviciile suport.

c) Membrii, voluntarii și angajații vor avea asupra lor sau vor supraveghea, în permanență, activele informatice și suporturile fizice pe care sunt stocate Date cu Caracter Personal. Se va evita folosirea în preajma activelor informatice sau a suporturilor fizice a oricăror obiecte, proceduri, manevre care le-ar putea deteriora sau care ar putea duce la pierderea lor.

d) Mijloacele de stocare (CD-uri, stick-uri, hard disk-urilor) vor fi în posesia Utilizatorului autorizat sau vor fi păstrate în sertare cu cheie la care are/au acces doar Utilizatorii autorizați.

e) Accesul în incinta spațiuluiasociațieii se realizează doar de către salariați și partenerii contractuali.

f) Este interzisă abandonarea sau lăsarea nesupravegheată a înscrisurilor sau suporturilor de orice fel pe care sunt imprimate Date cu caracter personal pe birou sau în afara acestuia.

g) Dacă durata prelucrării se prelungește peste durata zilei de lucru atunci se va menționa motivul și locul unde au fost depozitate.

h) Operațiile de tipărire/ copiere trebuie controlate fizic de către Utilizatorii Autorizați, pentru a se asigura că niciun exemplar din documentul tipărit sau copiat, care conține date cu character personal, nu rămâne în echipamentele de copiere sau imprimare.

i) Suporturile care conțin date cu Caracter Personal sau copiile tipărite ale datelor cu Caracter Personal trebuie să poarte mențiunea Confidențial, iar documentele pe suport de hârtie, care conțin date cu caracter personal, trebuie transferate într-un container/plic sigilat sau în support închis, pe care se va menționa clar că documentul trebuie inmanat personal unui utilizator autorizat.

j) Anterior transmiterii datelor cu caracter personal, personalul asociației se va asigura că:

- subcontractorul are încheiat un contract prin care este desemnat persoană împuternicită, și acel contract este în termen de valabilitate,
- în contract este inserată o politică de confidențialitate cu privire la protecția datelor cu caracter personal în care sunt prevăzute obligații cel puțin la fel de oneroase ca cele la care Asociația Real Sports s-a angajat față de clientul său.

k) În cazul în care Datele cu Caracter Personal sunt transmise sau transferate printr-o rețea de comunicații electronice, ori sunt relocate temporar trebuie luate măsuri pentru a controla fluxul de date și pentru a înregistra momentul transmiterii sau al transferului, Datele cu Caracter Personal transmise sau transferate, destinația Datelor cu Caracter Personal transmise sau transferate și datele de identificare ale Utilizatorului autorizat care efectuează transmisia sau transferul.

l) Transmiterea documentelor se realizează fizic (înmânare personală, curier, etc.) sau digital prin email (mail gmail + mail server), email marketing, we transfer, share, google drive, google sheets, google maps, facebook, facebook tag, facebook ads, whatsapp,sociial media, linkedin, instagram, youtube, etc.

m) Transmiterea documentelor fizice care conțin date personale între salariații cu atribuții în gestionarea lor se face personal sau prin curier intern special.

n) Transmiterea și transportul pe dispozitive de stocare pe suport electronic (exemplu: stick USB, hard disk extern, etc.) a imaginilor și documentelor care conțin date cu caracter personal se fac respectând regulile transmiterii și transportului documentelor care conțin date cu character personal. Astfel de dispozitive sau documente se transportă în plicuri sigilate sau genți cu încuietoare, ce se vor afla în permanență, pe durata transportului, în posesia și sub atenția Utilizatorului autorizat. Acestea vor fi predate doar Utilizatorului autorizat care este necesar să intre în posesia lor. În situațiile în care este posibil, informațiile stocate pe suportul electronic vor fi criptate.

o) Transmiterea pe cale electronică a imaginilor și documentelor care conțin date cu character personal se face respectând regulile de securitate informatică ale companiei, descrise în prezentul document. Fișierul/documentul/corespondența va fi parolată de către Utilizatorul autorizat, înainte de transmitere. Parola va fi comunicată destinatarului într-o manieră securizată și separat de documentul/fișierul/corespondența în cauză.

p) Transmiterea oricăror informații în baza unor solicitări venite de la terțe părți sau autorități (inclusiv Autoritatea pentru Protecția Datelor) se va face după avizul acordat de Reprezentant legal. Orice înștiințare va fi înaintată Reprezentant legalului în cel mai scurt timp, maxim 24 de ore. După obținerea avizului Reprezentant legalului, transmiterea datelor se va realiza în conformitate cu procedura instituită prin prezentul act.

q) Ștergerea se va realiza în asemenea manieră încât să fie definitivă iar datele să nu poată fi recuperate. Personalul va verifica ștergerea datelor de către Subscontractanți, cerând de la aceștia dovezile necesare. După ștergerea datelor, personalul IT care a realizat ștergerea va completa în Registru data și ora ștergerii, datele șterse, locația datelor, dacă s-a solicitat și subcontractantului și, eventualele observații.

21. Securitatea sistemelor

a) Pentru menținerea securității prelucrării datelor cu caracter personal, asociația adoptă următoarele măsuri:

- interzicerea folosirii de către persoanele autorizate a programelor software care provin din surse externe sau dubioase,
- informarea periodică a persoanelor autorizate în privința pericolului privind virușii informatici,
- implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice,
- dezactivarea, pe cât posibil, a tastei ”Print screen”, atunci când sunt afișate pe monitor date cu caracter personal, interzicându-se scoaterea la imprimantă a acestora.

b) Asociația verifică în mod regulat ca programele software utilizate pentru procesarea datelor, inclusiv programele software ale salariaților, precum si că sistemele informatice suport sunt actualizate și ca patch-urile de securitate sunt aplicate. Totodata se asigură că s-au introdus mecanismele de verificare a integrității, programelor informatice, a firmware-ului și a datelor in sine.

c) Activele informationale (software, hardware, de comunicatii) utilizate în activitatile de procesare sunt verificate periodic, pentru a detecta și elimina vulnerabilitățile și deficiențele de natura a produce riscuri la adresa securitatii informationale, cel putin anual.

d) Sistemele informatice sunt prevazute cu pograme informatice, echipamente sau sisteme specializate care asigurăs protectia anti-malware si care resping atacurile informatice si tentativele de acces neautorizat la adresa acestora. Infrastructura de protectie si detectare sunt actualizate in permanenta, rulează fara intrerupere si vor fi configurate corespunzator cu cele mai noi tehnologii, recomandari si bune practici din industrie.

e) Implementarea de noi sisteme de procesare sau masuri de protectie care vizeaza datele cu caracter personal se realizează cu o testare prealabila, care sa asigure ca orice riscuri in functionare au fost eliminate sau controlate in mod adecvat.

f) Testarea înainte de implementarea sau modificarea sistemelor informatice de Prelucrare de Date cu Caracter Personal nu utilizează date reale sau live, decât dacă o astfel de utilizare este absolut necesară și nu există o alternativă rezonabilă. În cazul în care se utilizează date reale sau live, acestea se vor limita strict la datele absolut necesare în scopul efectuării testelor, iar nivelul de securitate corespunzător tipului de date cu Caracter Personal prelucrate trebuie obligatoriu garantat.

g) În unele situații, când se verifică funcționarea unei aplicații implementate, testarea se realizează folosind date reale.

22. Monitorizare, inregistrare si audit

a) Asociația are implementate măsuri de monitorizare continuă a funcțiilor aferente activităților de procesare, a sistemelor si activitatilor de suport și a activelor informaționale, pentru a depista activitățile anormale în ceea ce privește datele cu caracter personal. În cadrul monitorizării se asigură resurse corespunzătoare și eficiente pentru depistare breselor logice și fizice, precum și a încălcărilor confidențialității, ale integrității și ale disponibilității activelor informaționale utilizate în prestarea serviciilor.

b) Detaliile minime care trebuie înregistrate pentru fiecare acces la sistemele informatice sunt user-ul utilizatorului, data și ora accesului, fișierul sau datele accesate, scopul, și tipul prelucrării.

23. Masuri de personal

a) Asociația se asigură că personalul care îndeplinesc activitati de procesare a datelor sunt instruiți anual privind securitatea informațiilor vizate sau mai frecvent, dacă este cazul.

b) Asociația pune în aplicare periodic programe de conștientizare în domeniul securității, pentru a-și educa personalul și pentru a aborda riscurile aferente securității informațiilor in cadrul procesarii datelor cu caracter personal. Membrii, volunatarii și angajații asociației au obligația de a raporta orice incident sau activitate neobișnuită.

Asociația Real Sports

Președinte: Lazăr Gabriel