MINISTERUL EDUCAȚIEI
UNIVERSITATEA „OVIDIUS" DIN CONSTANȚA
Bd. Mamaia nr. 124, 900527 Constanța, România
Tel./Fax: +4 0241 606.407, +4 0241 606.467
E-mail: rectorat@univ-ovidius.ro
Web page: www.univ-ovidius.ro

REGULAMENTUL

UNIVERSITĂȚII "OVIDIUS" DIN CONSTANȚA

PRIVIND PROTECȚIA

DATELOR CU CARACTER PERSONAL

EDITIA	Nume, prenume, funcţia		Număr Art. şi alin modificat /adăugat	Avizat	Aviz de legalitate nr.	Aprobat prin HS	REVIZIA
	Elaborat	Verificat					
1	Roşoiu Radu Dumitru	Dan Loredana Maximiliana		HCA nr. 1195	AVIZ nr. 195/ 31.10.2019	HS nr. 798/ 31.10.2019	0
2	Roşoiu Radu Dumitru	C.J. Dan Loredana Maximiliana		HCA nr. 415/ 22.04.2021	Aviz nr. 103/ 27.04.2021	HS nr. 244/ 29.04.2021	1

APROBAT ÎN ŞEDINŢA SENATULUI UOC
DIN DATA DE:
29 APR 2021
Președinte SENAT

Preambul

Universitatea „Ovidius" din Constanţa este instituţie publică de învăţământ superior, cu personalitate juridică, parte componentă a sistemului de învăţământ de stat din România, autonomă, cu caracter deschis. În cadrul activităților sale specifice, Universitatea prelucrează date cu caracter personal, având în consecință calitate de operator de astfel de date conform prevederilor **Regulamentului (UE) 679/2016** privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, numit în continuare **RGPD**.

Luând în considerare importanța deosebită a garantării dreptului la viață intimă, familială și privată prevăzut la art. 26 din Constituția României, necesitatea protejării acestui drept fundamental, precum şi prevederile specifice incluse în cadrul **Regulamentului (UE) 679/2016** privind activitățile de prelucrare a datelor cu caracter personal, se impune cu necesitate adoptarea unei politici a Universității „Ovidius" din Constanţa privind asigurarea confidențialității datelor cu caracter personal în cadrul instituției.

Capitolul I. Dispoziții generale

Art. 1 – Scopul și domeniul de aplicabilitate

(1) Prezenta Politică are ca scop stabilirea unor principii de bază și norme de conduită în vederea asigurării unui nivel adecvat de protecție a datelor cu caracter personal prelucrate de către personalul didactic, didactic auxiliar și nedidactic al Universității „Ovidius" din Constanţa care accesează, introduce în evidență în orice fel, modifică, stochează sau transmite în orice mod date cu caracter personal.

(2) Respectarea confidențialității datelor cu caracter personal reprezintă o obligație a Universității „Ovidius" din Constanţa, în calitate de operator de astfel de date, și a angajaților săi, având în vedere sensibilitatea datelor cu caracter personal prelucrate, dreptul la protecția datelor personale și dreptul la viață privată ale persoanelor fizice.

(3) Normele de conduită stabilite prin prezenta Politică sunt obligatorii pentru toți angajații Universității „Ovidius" din Constanţa și definesc cadrul general în care are loc exercitarea drepturilor și obligațiilor ce revin respectivilor angajați în domeniul protecției persoanelor fizice în privința prelucrării datelor cu caracter personal în cadrul activităților interne, în cadrul relațiilor Universității cu persoanele vizate(în calitate de beneficiari ai serviciilor educaționale, de colaboratori, de salariați ai instituției etc.), în cadrul relațiilor acesteia cu alți operatori de date cu caracter personal, precum și cu alte persoane fizice și juridice.

(4) Prezenta Politică se aplică tuturor prelucrărilor de date cu caracter personal, indiferent de operațiunile particulare prin care angajații Universității realizează acest lucru.

(5) Prevederile cuprinse în prezenta Politică nu se substituie și nu aduc atingere altor obligații legale imperative sau deontologice care revin Universității „Ovidius" din Constanţa și angajaților săi.

(6) Angajații Universității au obligația de a avea reprezentarea deplină a faptului că încălcarea confidențialității datelor personale poate conduce la prejudicii fizice, materiale sau morale persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanelor fizice în cauză.

(7) În cazul în care se constată existența anumitor aspecte legate de confidențialitate pentru care prezenta Politică nu oferă directive corespunzătoare, angajații trebuie să solicite imediat consiliere din partea responsabilului cu protecția datelor cu caracter personal la nivelul Universității (DPO) și/sau a personalului din cadrul Direcției Juridice și Contencios.

Art. 2 – Definirea termenilor

(1) Termenii folosiți în cadrul prezentei Politici au următorul sens:

a) - *„date cu caracter personal"* - orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi

APROBAT ÎN ȘEDINȚA SENATULUI DIN DATA DE: 29 APR 2021 Președinte SENAT

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 identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

b) - ***„date anonime"*** - reprezintă orice date ale căror origine sau în baza cărora au fost efectuate prelucrări, însă acestea nu pot fi asociate cu nicio persoană vizată identificată sau identificabilă.

c) - ***„pseudonimizare"*** - înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

d) - ***„prelucrare"*** - înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

e) - ***„operator de date cu caracter personal"*** - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

f) - ***„persoană împuternicită de operator"*** - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

g) - ***„destinatar"*** - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării.

h) - ***„parte terță"*** - înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

i) - ***„consimțământ"*** - al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

j) - ***„încălcarea securității datelor cu caracter personal"*** - înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

k) - ***„reprezentant"*** - înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul RGPD.

l) - ***„autoritate de supraveghere"*** - înseamnă o autoritate publică independentă instituită de un stat membru.

m) - ***„DPO"*** - responsabilul cu protecția datelor (în limba engleză, data protection officer).

n) - ***„DPIA"*** - evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment, DPIA).

o) - ***„transmitere"*** - înseamnă transmiterea în orice formă a datelor cu caracter personal spre a fi cunoscute și consultate de una sau mai multe părți.

p) - ***„persoana vizată"*** - înseamnă persoana fizică la care fac referire datele cu caracter personal.

APROBAT ÎN ȘEDINȚA SENATULUI UOC
DIN DATA DE:
29 APR 2021
Președinte SENAT

q) - *„difuzare/divulgare”* - înseamnă aducerea la cunoștința uneia sau mai multor părți a datelor cu caracter personal, în orice formă, și de asemenea, punerea acestora la dispoziție spre a fi consultate.

r) - *„restricționarea prelucrării”* - înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora.

s) - *„creare de profiluri”* - înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia.

t) – ***„nivel de protecție și de securitate adecvat al prelucrărilor de date cu caracter personal”*** – nivelul de securitate proporțional cu riscul pe care îl comportă prelucrarea față de datele cu caracter personal respective și față de drepturile și libertățile persoanelor fizice și conform cu cerințele minime de securitate a prelucrărilor de date cu caracter personal, elaborate de către autoritatea națională de supraveghere și actualizate corespunzător stadiului dezvoltării tehnologice și costurilor implementării acestor măsuri.

u) - *„autoritate de supraveghere”* - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

Capitolul II. Principiile generale ale prelucrărilor de date cu caracter personal efectuate în cadrul Universității “Ovidius” din Constanța

Art. 3 – Soluții de organizare

Universitatea “Ovidius” din Constanța, în calitate de operator de date cu caracter personal, a adoptat următoarele soluții de organizare în ceea ce privește confidențialitatea respectivelor date:

(1) Aspectele tehnice de securitate a datelor cu caracter personal stocate și prelucrate în format electronic intră în responsabilitatea Departamentului pentru IT&C și trebuie gestionate atât în baza liniilor directoare definite, a proceselor și procedurilor, cât și prin controale efectuate la nivelul sistemelor informatice.

(2) Responsabilitatea privind prelucrarea datelor cu caracter personal în acord cu prezenta Politică revine tuturor angajaților, Universitatea, în calitate de operator, asigurând măsurile organizatorice necesare implementării prevederilor Politicii privind confidențialitatea respectivelor date astfel încât prelucrările de date cu caracter personal să fie efectuate în conformitate cu prevederile **Regulamentului (UE) 679/2016.**

(3) Responsabilul cu protecția datelor cu caracter personal la nivelul Universității (DPO) va instrui și consilia angajații astfel încât aceștia să respecte confidențialitatea datelor cu caracter personal prelucrate și mecanismele de asigurare a acesteia.

(4) Fără prejudicierea celor de mai sus, Universitatea ca operator poate, la alegerea sa sau dacă acest lucru va fi prevăzut de legile în vigoare, să desemneze un angajat responsabil cu protecția datelor cu caracter personal la nivel de structură organizatorică distinctă din cadrul său care va superviza toate activitățile de prelucrare a datelor cu caracter personal la nivelul respectivei structuri și care va colabora cu DPO-ul. Această prevedere vizează cu precădere cazurile în care în activitatea structurii organizatorice sunt prezente operațiuni de prelucrare ce necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă și atunci când prelucrarea vizează categorii speciale de date(ex. date privind originea etnică, confesiunea religioasă, calitatea de membru de sindicat, date medicale etc.).

Art. 4 – Legalitatea și transparența prelucrărilor datelor cu caracter personal

(1) Universitatea “Ovidius” din Constanța, în calitate de operator de date cu caracter personal, și angajații ei recunosc și respectă dreptul la viață intimă, familială și privată al persoanelor fizice.

(2) Prelucrarea datelor cu caracter personal de către angajații Universității se desfășoară în conformitate cu prevederile legale în vigoare.

(3) Angajații sunt obligați să asigure transparența prelucrărilor de date cu caracter personal.

APROBAT ÎN ȘEDINȚA SENATULUI UOC
DIN DATA DE:
29 APR 2021
Președinte SENAT

Art. 5 – Responsabilitatea

(1) Angajații sunt responsabili pentru datele cu caracter personal aflate sub controlul lor, precum și pentru datele transferate către terți.

(2) Conducătorii structurilor organizatorice distincte din cadrul Universității stabilesc categoriile de date cu caracter personal pe care le prelucrează angajații aflați în subordinea acestora.

Art.6 – Legitimitatea scopului colectării și prelucrării datelor cu caracter personal

(1) Colectarea de date cu caracter personal prin mijloace frauduloase, neloiale sau ilegale este interzisă.

(2) Conducătorii structurilor organizatorice distincte din cadrul Universității definesc scopurile pentru care sunt colectate și prelucrate datele cu caracter personal **înainte** de momentul colectării acestora.

(3) Scopurile colectării și prelucrării datelor cu caracter personal sunt precis determinate, explicite și legitime, în conformitate cu prevederile legale în vigoare. Prelucrarea ulterioară a datelor în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice este permisă și nu este considerată a fi incompatibilă cu scopurile inițiale.

(4) Datele cu caracter personal colectate trebuie să fie adecvate, relevante si limitate la ceea ce este strict necesar în raport cu scopurile în care vor fi prelucrate.

(5) Comunicarea scopurilor colectării și prelucrării către persoanele vizate se realizează în scris sau în formă electronică într-un limbaj cât mai simplu și mai accesibil pentru persoanele vizate.

(6) Datele cu caracter personal nu pot fi prelucrate ulterior în alte scopuri incompatibile cu scopul inițial al colectării acestora.

(7) Angajații prelucrează datele cu caracter personal numai în scopurile pentru care au fost colectate inițial, excepție făcând doar cazurile în care prelucrările ulterioare au loc în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.

Art. 7 - Consimțământul

(1) Consimțământul persoanelor vizate este necesar pentru prelucrarea datelor cu caracter personal, în afara următoarelor cazuri conform art. 6 alin. (1) și art. 9 alin. (2) din **Regulamentul (UE) 679/2016**:

a) datele cu caracter personal sunt necesare pentru a îndeplini o obligație legală ce revine Universității;

b) datele cu caracter personal sunt necesare pentru a onora o obligație contractuală față de persoana vizată;

c) datele cu caracter personal sunt necesare pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

d) prelucrarea datelor cu caracter personal are scopul de a îndeplini o sarcină de interes public sau care rezultă din exercitarea autorității publice cu care este învestită Universitatea;

e) prelucrarea este necesară în scopul intereselor legitime urmărite de către Universitate în calitate de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

f) alte situații specifice care privesc categoriile speciale de date cu caracter personal, detaliate în cadrul art. 9 alin. (2) din **Regulamentul (UE) 679/2016.**

(2) Angajații vor folosi exclusiv mijloacele puse la dispoziție de către Universitatea "Ovidius" din Constanța pentru a informa persoanele vizate în legătură cu prelucrarea datelor cu caracter personal și pentru a solicita consimțământul acestora la momentul colectării respectivelor date.

(3) Persoana vizată își poate retrage consimțământul în orice moment, cu condiția avizării prealabile a Universității, ca operator. Universitatea, prin persoanele responsabile, va informa persoana vizată în legătura în legătură cu procedura și efectele retragerii consimțământului.

Art. 8 – Legitimitatea stocării și publicării datelor cu caracter personal

(1) Angajații sunt obligați să păstreze datele cu caracter personal exacte, complete și actualizate, în vederea realizării scopurilor pentru care sunt utilizate.

APROBAT ÎN ȘEDINȚA SENATULUI UOC
DIN DATA DE:
29 APR 2021
Președinte SENAT

(2) Datele cu caracter personal inexacte sau incomplete vor fi rectificate sau șterse fără întârziere la momentul constatării respectivei situații de către angajați sau la solicitarea persoanei vizate care semnalează existența caracterului lor inexact sau incomplet.
(3) Datele cu caracter personal se stochează într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care ele sunt prelucrate și, după caz, care se află în conformitate cu prevederile legale specifice care prevăd păstrarea și arhivarea lor. Datele respective pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.
(4) Conducătorii structurilor organizatorice distincte din cadrul Universității trebuie să argumenteze perioadele minime și maxime necesare pentru stocarea datelor colectate și prelucrate, având în vedere obligația de respectare a drepturilor persoanelor vizate prevăzute de către **Regulamentului (UE) 679/2016,** în special a dreptului de acces, a dreptului de intervenție asupra prelucrării datelor și a "dreptului de a fi uitat".
(5) În urma verificărilor periodice, datele cu caracter personal deținute de către Universitate și care nu mai servesc realizării scopurilor sau îndeplinirii unor obligații legale sau contractuale vor fi distruse, șterse sau transformate în date anonime într-un interval de timp rezonabil, potrivit prevederilor legale, sau, în lipsa unor astfel de dispoziții legale, în baza prevederilor interne.
(6) Publicarea pe website-ul Universității a datelor cu caracter personal aferente rezultatelor concursurilor de admitere la studii, rezultatelor examenelor de finalizare studii, precum și rezultatelor repartizării locurilor de cazare, va fi efectuată cu pseudonimizarea acestor tipuri de date, în conformitate cu cadrul legal în vigoare; excepție fac situațiile în care, prin dispoziții legale specifice, se instituie în mod expres obligația aducerii la cunoștință publică, fără pseudonimizare, a acestor tipuri de date.
(7) Termenul limită general de păstrare pe paginile web ale instituției a datelor menționate la alin. 6 este data de 15 octombrie a fiecărui an universitar, ulterior acestei date situațiile care conțin datele respective fiind excluse de la accesul on-line al publicului. Cu titlu de excepție, în cazul sesiunilor de examene de finalizare studii ce se derulează în alte perioade calendaristice decât cele din lunile iulie și septembrie, termenul maxim de păstrare pe website al situațiilor respective va fi de 30 de zile calendaristice.
(8) Datele personale publicate pe website trebuie să fie adecvate, relevante si limitate la ceea ce este strict necesar în raport cu prevederile legale care impun sau susțin publicarea lor, sau în raport cu scopurile în vederea cărora a fost obținut consimțământul persoanelor vizate în vederea publicării.
(9) Afișarea la avizierele Universității a situațiilor ce conțin date cu caracter personal va fi efectuată cu pseudonimizarea obligatorie a datelor cu caracter personal, dacă prin cadrul legal incident nu se prevede altfel, și nu va depăși durata de 30 de zile.

Art. 9 – Legitimitatea transferului datelor cu caracter personal

(1) Transferul de date cu caracter personal către alți operatori este permis în condițiile în care există consimțământul persoanelor vizate sau în cazurile care sunt echivalente consimțământului (obligații legale, obligații contractuale față de persoanele vizate, interes public major, interes legitim al Universității etc.).
(2) Persoanele vizate vor fi informate cu privire la transferurile efectuate (ex. prin intermediul declarațiilor RGPD completate la înscrierea la admitere, la încheierea contractelor de studii etc.).
(3) Garanțiile pentru asigurarea protecției datelor cu caracter personal în cadrul transferului de date către alți operatori vor fi prevăzute prin acorduri tehnice și procedurale încheiate cu aceștia, cu excepția cazurilor în care respectivele transferuri au caracter de obligativitate prevăzut prin lege (ex. transferuri de date către autorități publice, judecătorești, organe de cercetare penală etc.).

Art. 10 – Monitorizarea video

(1) Universitatea "Ovidius" din Constanța efectuează activități de monitorizare video în cadrul spațiilor și imobilelor din patrimoniul propriu urmărind următoarele scopuri:
   a) prevenirea și combaterea săvârșirii infracțiunilor;

APROBAT ÎN ȘEDINȚA SENATULUI UOC
DIN DATA DE:
29 APR 2021
Președinte SENAT

b) asigurarea pazei și protecției persoanelor, bunurilor și valorilor, a imobilelor și a instalațiilor de utilitate publică din patrimonial propriu, precum și a împrejmuirilor afectate acestora;
c) îndeplinirea unor măsuri de interes public;
d) realizarea unor interese legitime, cu condiția să nu se prejudicieze drepturile și libertățile fundamentale sau interesul persoanelor vizate.

(2) Supravegherea video poate fi efectuată în locuri și spații deschise sau destinate publicului, inclusiv pe căile publice de acces de pe domeniul public sau privat, în condițiile prevăzute de lege. Montarea camerelor de supraveghere video este efectuată în locuri vizibile și este semnalată publicului prin intermediul unei pictograme sugestive care are vizibilitate suficientă, poziționată în apropierea locului de amplasare (pictograma conform Anexa).

(3) Este interzisă desfășurarea următoarelor tipuri de activități de monitorizare video:
a) utilizarea mijloacelor de supraveghere video ascunse, cu excepția situațiilor prevăzute de lege;
b) prelucrarea datelor cu caracter personal prin mijloace de supraveghere video în spații în care se impune asigurarea intimității persoanelor, cum ar fi: cabine de probă, vestiare, cabine de duș, toalete și alte locații similare;
c) prelucrarea datelor cu caracter personal prin mijloace de supraveghere video, exclusiv în legătură cu originea rasială sau etnică, convingerile politice, religioase ori filozofice, apartenența sindicală, starea de sănătate și viața sexuală, cu excepția cazurilor prevăzute expres de lege;

(4) Prelucrarea datelor cu caracter personal ale persoanelor care frecventează sau vizitează sediile și spațiile Universității prin mijloace de supraveghere video este realizată pentru îndeplinirea unor obligații legale exprese sau în temeiul unui interes legitim, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora prin intermediul anunțurilor/pictogramelor cu rol de avertizare.

(5) În situația în care nu este incidentă nicio obligație legală sau Universitatea "Ovidius" din Constanța, în calitate de operator, nu poate justifica un interes legitim, prelucrarea datelor cu caracter personal ale persoanelor vizate prin mijloace de supraveghere video nu se poate efectua decât pe baza consimțământului expres și liber exprimat al acestora, cu respectarea drepturilor persoanelor vizate, în special a informării prealabile a acestora într-o formă concise, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu.

(6) Imaginile înregistrate prin utilizarea mijloacelor de supraveghere video vor fi transmise de către Universitate către organelle de poliție și alte autorități cu atribuții privind apărarea drepturilor și libertăților fundamentale ale persoanei, a proprietății private și publice, prevenirea, descoperirea și sancționarea infracțiunilor, respectarea ordinii și liniștii publice, în condițiile legii. Imaginile astfel obținute nu pot fi transmise în străinătate.

(7) prelucrarea datelor cu caracter personal ale angajaților prin mijloace de supraveghere video în interiorul birourilor unde aceștia își desfășoară activitatea la locul de muncă, este permisă doar pentru îndeplinirea unor obligații legale exprese sau în temeiul unui interes legitim, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora. În situația în care nu este incidentă nicio obligație legală sau Universitatea nu poate justifica un interes legitim, prelucrarea datelor cu caracter personal ale angajaților prin mijloace de supraveghere video nu se poate efectua decât pe baza consimțământului expres și liber exprimat al acestora, cu respectarea drepturilor persoanelor angajate, în special a informării prealabile a acestora.

Art. 11– Colaborarea cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal(ANSPDCP)

(1) Ori de câte ori ANSPDCP va solicita, responsabilul cu protecția datelor cu caracter personal va prezenta autorității de supraveghere informații cu privire la sesizările/reclamațiile primite de către aceasta și la modul de soluționare a acestora, precum și orice alte informații solicitate privind prelucrările de date cu caracter personal.

(2) Responsabilul cu protecția datelor cu caracter personal are obligația de a notifica ANSPDCP cu privire la incidentele de securitate ce implică date cu caracter personal și care prezintă un grad de risc ridicat la adresa drepturilor și libertăților persoanelor vizate.

APROBAT ÎN ȘEDINȚA SENATULUI UOC
DIN DATA DE:
29 APR 2021
Președinte SENAT

(3) Termenul în care se face notificarea precum și conținutul acesteia se conformează prevederilor specifice ale Regulamentului (UE) 679/2016.

Art. 12 – Persoane împuternicite de operator

(1) Prin persoane imputernicite de operator sunt înțeleși partenerii contractuali/colaboratori ai Universității "Ovidius" din Constanța și ai entităților afiliate sau alte societăți sau instituții ce oferă servicii complementare serviciilor Universității, precum, dar fără a se limita la:
   a) entități care participă la negocierea, încheierea sau la aducerea la îndeplinire a contractelor (furnizori de bunuri, prestatori de servicii, operatori IT, avocați și alți consultanți etc.);
   b) entități care asigură buna funcționare a activităților Universității și a tuturor tranzacțiilor legate de activitățile acesteia;
   c) entități care asigură securitatea și alte tipuri de protecție sistemelor informatice ale Universității și ale entităților afiliate care funcționează în România;
   d) entități care cercetează nivelul calitativ pentru satisfacerea cerințelor studenților, angajaților sau altor persoane vizate sau care asigură sau mijlocesc oferta de servicii educaționale și culturale ale Universității;
   e) societăți care imprimă, administrează și/sau transmit facturi/deconturi/notificări;
   f) curieri;
   g) furnizori de servicii de contact/call-center;
   h) societăți de arhivare-stocare documente, dacă este cazul;
   i) consultanți, contabili, auditori;
   j) persoane către care au fost transferate drepturile și/sau obligațiile Universității;
   k) entități care asigură colectarea creanțelor și/sau recuperarea bunurilor.

(2) Datele cu caracter personal transmise persoanelor împuternicite vor fi adecvate, pertinente și neexcesive prin raportare la scopurile în care au fost colectate.

(3) Pentru îndeplinirea obligațiilor și angajamentelor ce îi revin din contractele încheiate cu studenții săi sau cu alte persoane vizate, precum și pentru a asigura o prelucrare eficientă și profesionistă, Universitatea "Ovidius" din Constanța poate prelucra datele cu caracter personal inclusiv prin terțe persoane, împuternicite în acest sens de către Universitate, cu care va încheia contracte scrise în condițiile **Regulamentului (UE) 679/2016**.

(4) Persoanele împuternicite sunt obligate să respecte cerințele Operatorului pentru siguranța prelucrării și să ia măsurile tehnice și organizatorice necesare pentru asigurarea protecției datelor cu caracter personal.

Capitolul III – Securitatea prelucrărilor datelor cu caracter personal

Art. 13 – Prevederi generale privind securitatea prelucrărilor de date cu caracter personal

(1) În cadrul operațiunilor de prelucrare a datelor cu caracter personal se asigură un nivel adecvat de protecție și securitate în vederea îndeplinirii următoarelor scopuri:
   (a) Limitarea accesului la documente și la bazele de date, acesta fiind permis numai în vederea îndeplinirii scopurilor specifice și legitime.
   (b) Interzicerea copierii datelor cu caracter personal în afara locurilor în care acestea sunt gestionate și stocate.
   (c) Prevenirea oricărei forme de circulație necontrolată a datelor cu caracter personal, în special a accesului neautorizat la respectivele date.

(2) În vederea aplicării prevederilor alin. (1), Departamentul pentru IT&C se consultă cu DPO-ul și apoi propune măsurile tehnice adecvate spre avizarea conducerii Universității.

(3) Tot în vederea aplicării prevederilor alin. (1), conducătorii structurilor organizatorice distincte din cadrul Universității se consultă cu DPO-ul și apoi propun conducerii instituției spre avizare măsurile organizatorice pe care le consideră necesare.

APROBAT ÎN ȘEDINȚA SENATULUI UOC
DIN DATA DE:
29 APR 2021
Președinte SENAT

(4) Accesul la datele cu caracter personal prelucrate va fi permis numai angajaților care au nevoie de acest acces în vederea îndeplinirii obligațiilor de serviciu, precum și altor angajați autorizați în mod expres de către conducerea Universității.

Art. 14 – Raportarea și tratarea incidentelor de securitate

(1) În situația în care un angajat intră în contact cu o informație care nu este destinată grupului de acces din care acesta face parte, acesta nefiind autorizat să o prelucreze, el este obligat să procedeze de îndată la informarea conducătorului structurii organizatorice distincte din care face parte, precum și a DPO-ului.

(2) Angajații nu vor da curs niciunei solicitări de transmitere/diseminare a unor date cu caracter personal către persoane fizice care nu sunt angajate în cadrul Universității "Ovidius" din Constanța, și nici către persoane juridice/autorități, cu excepția situațiilor prevăzute de lege (cereri ale organelor de cercetare penale, ale unor autorități publice sau judecătorești etc.) și a situațiilor în care persoanele juridice în cauză sunt persoane împuternicite de către Universitate sau sunt alți operatori de date cu caracter personal cu care Universitatea are încheiate protocoale sau alte forme legale de colaborare, caz în care va fi sesizată în prealabil Direcția Juridică și Contencios. În situația în care solicitarea este efectuată de către persoana vizată, angajatul care gestionează respectivele date personale va proceda la verificarea cererii transmise și la elaborarea răspunsului în conformitate cu normele și procedurile în vigoare privind drepturile persoanelor vizate stipulate în Regulamentul (UE) 679/2016, prin consultare cu persoana responsabilă cu protecția datelor de la nivelul structurii administrative de care aparține și, după caz, cu DPO.

(3) Angajații nu vor da curs niciunei solicitări de transmitere/diseminare a datelor cu caracter personal către un alt angajat, mai înainte de a se asigura că acesta face parte dintr-un grup de acces adecvat sau solicitarea acestuia este avizată de către conducătorul structurii organizatorice distincte din care face parte.

(4) Modalitatea concretă de notificare a ANSPDCP și de informare a persoanei vizate în cazul în care se produce o încălcare a securității datelor cu caracter personal, inclusiv activitățile ce trebuie desfășurate atunci când se produce un incident de securitate, vor fi prevăzute prin procedură specifică.

Art. 15 – Măsuri preventive de securitate

(1) Angajații sunt informați și consiliați de către DPO în colaborare cu Departamentul pentru IT&C privind pericolul reprezentat de către atacurile cibernetice și de către cele de tip social (social engineering), precum și repercusiunile pe care aceste atacuri le pot avea asupra Universității, asupra angajaților acesteia sau asupra persoanelor vizate.

(2) În vederea asigurării unui standard ridicat de securitate, Universitatea organizează instruiri cu privire la vulnerabilitățile datelor personale și măsurile preventive de securitate ce se adoptă în cazul atacurilor cibernetice.

(3) Angajații vor fi informați, într-o modalitate accesibilă pe măsura propriului nivel de înțelegere a domeniului, de către Departamentul pentru IT&C, privind particularitățile de ordin tehnic ale următoarelor tipuri de atacuri:

a) Phishing – atacuri prin intermediul cărora atacatorii utilizează e-mail-uri de tip spam pentru a direcționa victimele către site-uri web create de către ei astfel încât datele personale să fie introduse pe acele site-uri;

b) Atacuri de tip social engineering derulate prin folosirea comunicațiilor electronice – manipulări rău intenționate ale anumitor persoane prin care angajații pot fi convinși să disemineze date cu caracter personal;

c) Atacuri în cadrul cărora se utilizează diferite tipuri de programe malware.

(4) Pentru a fi prevenit accesul neautorizat, dispozitivele electronice pe care se află stocate date cu caracter personal trebuie să fie protejate prin utilizarea unui nume de utilizator și a unei parole.

(5) Pentru rezolvarea problemelor legate de dispozitivele electronice utilizate în vederea stocării și prelucrării datelor cu caracter personal (probleme de hardware, software, conectivitate etc.), angajații au obligația să contacteze Departamentul pentru IT&C.

APROBAT ÎN ȘEDINȚA SENATULUI UOC
DIN DATA DE:
29 APR 2021
Președinte SENAT

(6) Angajații se vor asigura că atunci când o stație de lucru nu este utilizată sau un birou nu este ocupat o perioadă lungă de timp, informațiile privind datele cu caracter personal, fie ele pe hârtie, un dispozitiv electronic de stocare sau un dispozitiv hardware, sunt blocate sau încuiate în mod corespunzător:

(a) Toate documentele ce conțin date cu caracter personal, în mod particular cele cu caracter sensibil, trebuie să fie scoase de pe birou și plasate într-un sertar sau dulap de depozitare. Acest lucru este valabil atât pentru documentele tipărite pe hârtie cât și pentru CD-uri, DVD-uri și unități USB.

(b) Distrugerea hârtiilor ce conțin date personale (ex. ciorne ale unor documente) trebuie efectuată prin metode adecvate care să nu permită utilizarea lor de către persoane rău intenționate care le pot prelua din spațiile de colectare a deșeurilor.

(c) Stațiile de lucru pentru calculatoare trebuie să fie închise/blocate atunci când biroul este neocupat sau este închis complet la sfârșitul zilei.

(d) Laptopurile si alte dispozitive hardware mobile utilizate în interes de serviciu și lăsate în incinta spațiului de lucru trebuie, în măsura în care este posibil, sa fie scoase de pe birou și plasate într-un sertar sau dulap de depozitare.

(e) Cheile pentru accesarea sertarelor sau a dulapurilor de depozitare nu trebuie lăsate nesupravegheate.

(f) Orice lucrare de imprimare care conține date cu caracter personal trebuie recuperată imediat.

Capitolul IV. Drepturile persoanelor vizate și soluționarea sesizărilor/reclamațiilor care le vizează

Regulamentul (UE) 679/2016 conferă persoanelor fizice următoarele drepturi:

- Dreptul de a fi informat în privința datelor personale prelucrate de operator
- Dreptul de acces la datele personale
- Dreptul la rectificarea datelor personale
- Dreptul la ștergerea datelor personale
- Dreptul de a restricționa prelucrarea datelor personale
- Dreptul la portabilitatea datelor
- Dreptul de a se opune prelucrării datelor personale
- Dreptul de a nu fi supus/ă unei decizii bazată pe prelucrarea automatizată a datelor personale sau bazată pe crearea de profiluri

Art. 16– Dreptul la informare

(1) Înainte de colectarea datelor cu caracter personal, precum și la solicitarea persoanelor vizate, angajații sunt obligați să comunice informații în legătură cu datele cu caracter personal prelucrate, sursele din care sunt colectate datele cu caracter personal, scopurile prelucrării, terții cărora le sunt dezvăluite aceste date, cu excepția cazurilor în care legea nu interzice o astfel de informare;

(2) În cazul în care dezvăluirea datelor este impusă de către lege (ex. în vederea executării unei hotărâri judecătorești, pentru desfășurarea unei anchete/cercetări penale), angajații se vor asigura că terțul care solicită dezvăluirea acționează în conformitate cu dispozițiile legale aplicabile, iar cererea are ca obiect numai datele cu caracter personal neexcesive prin raportare la scopul dezvăluirii. Persoana vizată va fi informată în legătură cu dezvăluirea numai dacă legea permite acest lucru.

(3) Aducerea la cunoștință persoanelor vizate a drepturilor de care beneficiază se poate face prin materiale scrise sau prin mijloace electronice.

Art.17 – Dreptul de acces

(1) Angajații sunt obligați să permită accesul persoanelor vizate la datele cu caracter personal care le privesc, după ce acestea fac proba propriei identități și după consultarea DPO-ului, prin cele mai facile mijloace aflate la dispoziție, în mod rezonabil și numai dacă legea nu prevede altfel.

(2) Accesul persoanei vizate nu poate fi permis, cu excepția cazurilor prevăzute de lege sau stabilite de autoritatea de supraveghere, în situații precum solicitarea fără procură a datelor personale ale unei

alte persoane, în cazul în care dezvăluirea datelor personale ar putea afecta viața și siguranța altei persoane, în cazul în care sunt solicitate date care pot privi informații comerciale confidențiale, sau în cazul în care prin dezvăluirea datelor s-ar aduce atingere soluționării unui litigiu sau unui proces penal.

(3) Angajații sunt obligați să motiveze refuzul dea permite accesul la anumite date cu caracter personal.

(4) Angajații și DPO-ul vor păstra o evidență a solicitărilor privind exercitarea dreptului de acces.

Art. 18 – Dreptul la rectificare

(1) Persoanele vizate au dreptul de a solicita verificarea exactității și a caracterului complet al datelor cu caracter personal care le privesc, precum și de a solicita rectificarea datelor inexacte sau incomplete prin formularea unor contestații.

(2) Angajații și DPO-ul vor păstra o evidență a contestațiilor care nu au fost rezolvate privind caracterul exact sau complet al datelor, iar în cazul în care datele vor fi transferate către alți operatori de date cu caracter personal sau alți terți vor fi precizate datele care nu au fost rectificate sau în privința cărora există contestații nerezolvate.

(3) Actualizarea bazelor de date ale Universității ce conțin date cu caracter personal se face pe baza informațiilor transmise de persoanele vizate precum și a informațiilor furnizate de către orice sursă externă autorizată de lege.

Art. 19– Dreptul la ștergerea datelor personale ("Dreptul de a fi uitat")

(1) Prin exercitarea „dreptului de a fi uitat", persoana vizată este îndreptățită să solicite ștergerea datelor cu caracter personal care îi aparțin și care se află în evidențele și/sau în bazele de date gestionate de către angajații Universității „Ovidius" din Constanța, **atât timp cât acest lucru nu contravine obligațiilor legale sau contractuale ale Universității.**

(2) Persoanele vizate își pot exercita dreptul de a fi uitat în orice moment **ulterior scurgerii perioadei stabilite de lege** pentru păstrarea datelor cu caracter personal care se referă la:

a) salarizare;
b) achitarea contribuțiilor de asigurări sociale, contribuțiilor de asigurări de sănătate precum și a impozitelor reținute la nivelul angajatorului;
c) durata frecventării studiilor;
d) durata/perioadele calendaristice în care persoana vizată a fost înmatriculată la studii fiind finanțată de stat;
e) durata/perioadele calendaristice în care persoana vizată a beneficiat de burse sau alte forme de ajutor;
f) rezultatele școlarizării în temeiul cărora s-au emis diplome de licență, diplome de studii postuniversitare, doctorale sau postdoctorale;
g) rezultatele participării în cadrul concursurilor de admitere la studii universitare în cadrul Universității.

(3) Angajații și DPO-ul vor păstra o evidență a solicitărilor privind exercitarea dreptului de acces.

Art. 20 - Dreptul de a restricționa prelucrarea datelor personale

(1) Persoanele vizate au dreptul de a solicita restricționarea prelucrării în cazul în care se aplică unul dintre următoarele cazuri:

a) se contestă exactitatea datelor, pentru o perioadă care permite Universității ca operator să verifice exactitatea datelor în cauză;
b) prelucrarea este nelegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;
c) ca operator, Universitatea nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată le solicită pentru o acțiune în instanță;

APROBAT ÎN ȘEDINȚA SENATULUI UOC
DIN DATA DE
29 APR 2021
Președinte SENAT

d) persoana vizată s-a opus prelucrării (art. 21 alin. (1) din RGPD) pentru intervalul de timp în care se verifică dacă drepturile legitime ale Universității ca operator prevalează asupra celor ale persoanei vizate.

(2) Dacă prelucrarea a fost restricționată, astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță. În situația datelor cu caracter personal asupra cărora au fost instituite măsuri de restricție acestea pot fi în continuare stocate fără îndeplinirea altor formalități suplimentare.

(3) În situația în care se impune prelucrarea datelor cu caracter personal restricționate, aceasta poate opera cu respectarea următoarelor condiții prevăzute situațiilor ce impun necesitatea obținerii consimțământului, precum și:

a) prelucrarea să fie necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță;
b) prelucrarea să fie necesară pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Uniunii sau al unui stat membru;
c) în orice alte cazuri care ar necesita prelucrarea datelor în discuție este necesară obținerea consimțământului persoanei vizate.

(4) Angajații și DPO-ul vor păstra o evidență a solicitărilor privind restricționarea prelucrării datelor personale, iar în situația încetării/dispariției împrejurării care a determinat restricționarea prelucrării datelor cu caracter personal, Universitatea „Ovidius" din Constanța va notifica persoana vizată, înainte de ridicarea restricției de prelucrare cu privire la acest lucru.

Art. 21 - Dreptul la portabilitatea datelor

(1) Portabilitatea datelor constituie un drept al persoanei vizate de a primi un subset de date cu caracter personal prelucrate de către Universitate prin mijloace automate cu privire la aceasta, de a stoca datele respective pentru uz personal în viitor, precum și de a le transfera unui alt operator de date cu caracter personal.

(2) În situația primirii unei solicitări de portabilitate a datelor, se va verifica, în prealabil, acuratețea și corectitudinea datelor.

(3) În cazul exercitării dreptului la portabilitatea datelor de către persoanele vizate, Universitatea „Ovidius" din Constanța va lua măsurile de securitate necesare pentru a se asigura că datele cu caracter personal sunt transmise în condiții de siguranță la destinația corectă și pentru a proteja în continuare datele cu caracter personal care rămân în sistemele sale.

(4) Portabilitatea datelor garantează dreptul persoanei vizate de a primi date cu caracter personal și de a le prelucra conform intențiilor sale. În consecință, Universitatea „Ovidius" din Constanța nu poartă răspunderea pentru prelucrarea gestionată de către persoana vizată sau de către o altă instituție sau societate care primește de la persoana vizată respectivele date cu caracter personal.

(5) Angajații și DPO-ul vor păstra o evidență a solicitărilor privind exercitarea dreptului la portabilitatea prelucrării datelor personale.

Art. 22 - Dreptul de a se opune prelucrării datelor personale

(1) În anumite situații expres prevăzute de RGPD la art. 21, persoana vizată are dreptul, din motive legate de situația particulară în care se află, de a se opune prelucrării.

(2) Dacă scopul principal al procesării datelor personale este de natură legală sau în interesul legitim al Universității „Ovidius" din Constanța, în momentul primirii unei obiecții legate de natura acestor procesări, va fi încetată prelucrarea datelor respective numai dacă nu se va putea demonstra cu claritate că prelucrarea se face pentru stabilirea, exercitarea sau apărarea revendicărilor legale. Toate acestea trebuie explicate clar și concis persoanei vizate care a ridicat vreo obiecție.

(3) Dacă prelucrarea de date personale este efectuată în în scop de marketing direct(ex. în vederea promovării unor servicii educaționale oferite de Universitate), în momentul primirii unei obiecții legate de natura acestor procesări, va fi încetată prelucrarea datelor respective. Chiar dacă în anumite circumstanțe a existat un consimțământ inițial pentru prelucrarea datelor, ridicarea unei obiecții explicite pentru interzicerea prelucrării datelor personale în scopuri de marketing direct trebuie acceptată fără întârziere și comunicată persoanei vizate.

APROBAT ÎN ȘEDINȚA SENATULUI UOC
DIN DATA DE
29 APR 2021
Președinte SENAT

(4) În situația în care scopul prelucrării datelor este de cercetare științifică sau istorică, sau în scopuri statistice, persoanele fizice trebuie să aibă *„motive legate de situația lor particulară"* pentru a-și exercita dreptul de a se opune prelucrării în scopuri de cercetare. Dacă scopul principal al proiectului de cercetare este legat în mod direct de îndeplinirea unei sarcini de interes public, Universitatea „Ovidius" din Constanța nu este obligată să se conformeze unei obiecții față de prelucrarea datelor.
(5) Angajații și DPO-ul vor păstra o evidență a solicitărilor privind exercitarea dreptului de a se opune prelucrării datelor personale.

Art. 23 - Dreptul de a nu fi supus/ă unei decizii bazată pe prelucrarea automatizată a datelor personale sau bazată pe crearea de profiluri

(1) Persoanele fizice au dreptul de a nu face obiectul unei decizii atunci când aceasta se bazează pe prelucrarea automată și aceasta poate produce un efect juridic sau un efect semnificativ similar asupra individului.
(2) Acest drept nu se aplică tuturor deciziilor automate. Dreptul nu se aplică în cazul în care decizia:
   a) este necesară pentru încheierea sau executarea unui contract între instituție și persoana fizică;
   b) este autorizată prin lege (de exemplu, în scopuri de detectare sau prevenire a fraudelor sau prevenirea evaziunii fiscale);
   c) pe baza consimțământului explicit (art. 9 alin. (2) din Regulament);
   d) atunci când o decizie nu are un efect legal sau similar semnificativ asupra unei persoane.
(3) RGPD definește profilarea ca orice formă de procesare automată destinată să evalueze anumite aspecte personale ale unei persoane, în special pentru a le analiza sau a prezice: performanța școlară, performanța științifică, performanța la locul de muncă; situația economică; starea de sănătate; preferințele personale; fiabilitatea; comportamentul; locația; deplasările.
(4) La prelucrarea datelor cu caracter personal în scop de realizare a unui profil, dacă este cazul, Universitatea "Ovidius" din Constanța se va asigura că există garanții adecvate cu privire la următoarele aspecte:
   a) procesarea este corectă și transparentă prin furnizarea de informații semnificative despre logica implicată, precum și despre semnificația și consecințele avute în vedere;
   b) folosește procedurile matematice sau statistice adecvate pentru profilare;
   c) are implementate măsurilor tehnice și organizatorice adecvate care să vă permită remedierea erorilor și minimizarea riscului de eroare;
   d) asigură securitatea datelor personale într-o manieră proporțională cu riscul pentru interesele și drepturile individului și previne efectele discriminatorii.
(5) În urma unei solicitări din partea persoanei vizate cu privire dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, trebuie ca persoana vizată să fie informată într-o manieră specifică care să includă: existența unor procese decizionale automatizate în privința datelor sale, care se bazează exclusiv pe prelucrarea automată, scopurile acestora, efectele juridice care se pot produce în privința persoanei vizate, existența unor garanții corespunzătoare, măsura în care persoana vizată ar fi afectată, precum și dreptul acesteia de a obține intervenție umană, de a-și exprima punctul de vedere, de a primi o explicație privind decizia luată în urma unei astfel de evaluări, precum și dreptul de a contesta decizia.
(6) Angajații și DPO-ul vor păstra o evidență a solicitărilor privind exercitarea dreptului de a nu fi supus/ă unei decizii bazată pe prelucrarea automatizată a datelor personale sau bazată pe crearea de profiluri.

Art. 24 – Soluționarea sesizărilor/reclamațiilor/contestațiilor

(1) Procedura de primire, înregistrare și soluționare a plângerilor, sesizărilor, reclamațiilor și a celorlalte cereri ale persoanelor vizate va fi conformă cu prevederile interne și practicile interne ale Universității „Ovidius" din Constanța.

APROBAT ÎN ȘEDINȚA SENATULUI UOC
DATA DE:
28 APR 2021
Președinte SENAT

(2) Responsabilul cu protecția datelor cu caracter personal(DPO) are obligația de a organiza, coordona, monitoriza și comunica soluționarea plângerilor, reclamațiilor și a celorlalte tipuri de cereri adresate Universității „Ovidius" din Constanța legate de prelucrarea datelor cu caracter personal, în termenele și condițiile prevăzute de lege.
(3) Pentru realizarea scopului mai sus menționat, DPO-ul va colabora cu toate structurile organizatorice din cadrul Universității „Ovidius" din Constanța, conform prevederilor Regulamentului de Organizare și Funcționare și ale Regulamentului Intern al instituției.
(4) Angajații și conducerea instituției vor lua măsuri pentru asigurarea unui nivel rezonabil al cheltuielilor ocazionate de exercitarea de către persoanele vizate a drepturilor privind datele cu caracter personal, cheltuieli care sunt în sarcina persoanelor vizate numai în acele cazuri specifice în care respectivele drepturi nu pot fi exercitate în mod gratuit.

Art 25 – Sancțiuni

(1) Încălcarea cu vinovăție a normelor din prezenta Politică de către angajații Universității „Ovidius" din Constanța constituie abatere disciplinară ce va atrage răspunderea disciplinară a respectivilor angajați în condițiile prevăzute de către Regulamentul Intern al instituției.
(2) În cazul în care faptele săvârșite constituie infracțiuni potrivit legii penale, vor fi sesizate organele abilitate în domeniu. Răspunderea penală nu exclude răspunderea disciplinară pentru fapta comisă.
(3) Dacă în conținutul unei sesizări/reclamații, în formă scrisă sau electronică, ce privește datele cu caracter personal sunt descrise fapte ale unui sau mai multor angajați ai Universității „Ovidius" din Constanța de natură să contravină prevederilor din prezentul regulament, va fi sesizat de îndată responsabilul cu protecția datelor cu caracter personal.
(4) Responsabilul cu protecția datelor cu caracter personal va informa conducătorul structurii organizatorice distincte din care face parte angajatul ale cărui fapte au fost reclamate, urmându-se ca situația de fapt și de drept să fie analizată pentru a se stabili dacă faptele semnalate se încadrează în prevederile alineatelor (1) și (2) de mai sus.
(5) Stabilirea abaterilor disciplinare și sancțiunile disciplinare aplicabile angajaților este realizată în conformitate cu dispozițiile Regulamentului Intern al Universității „Ovidius" din Constanța, în condițiile legii.

Prezentul regulament a fost aprobat în ședința Consiliului de Administrație din data de 27.04.2021 și validat în ședința Senatului din data de 29.04.2021.