ACADEMIA ROMANA
INSTITUTUL DE CHIMIE MACROMOLECULARA "PETRU PONI"
Aleea Grigore Ghica Voda, nr. 41A, 700487 IASI, ROMANIA
Tel. +40.232.217454; Fax: +40.232.211299

Nr. ICMPP/ 5586 /2 VIII 2018

ACADEMIA ROMÂNĂ INSTITUTUL DE CHIMIE MACROMOLECULARĂ "PETRU PONI" IAŞI

APROBAT,
DIRECTOR
.....
DR. ANTON AIR[redacted]

POLITICA INTERNĂ DE PROTECŢIE A DATELOR CU CARACTER PERSONAL

1. Documente de referinţă

1.1. Regulamentul (UE) 679/2016 al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (RGPD), publicat în J. Of. nr. 119L/4.05.2016, care a intrat în vigoare la data de 25.05.2018;

1.2. Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), publicată în M. Of. nr. 651/26.07.2018;

1.3. Legea nr. 752/2001 privind organizarea şi funcţionarea Academiei Române;

1.4. Statutul Academiei Române;

1.5. Regulamentul de organizare şi funcţionare al Institutului de Chimie Macromoleculară "Petru Poni" - Iaşi;

1.6. Regulamente şi proceduri interne;

1.7. Legea nr. 53/2003 (Codul muncii), cu modificările şi completările ulterioare;

1.8. Legea nr. 319/2003 privind statutul personalului de cercetare – dezvoltare, cu modificările şi completările ulterioare;

1.9. H.G. nr. 286 din 23 martie 2011 pentru aprobarea Regulamentului-cadru privind stabilirea principiilor generale de ocupare a unui post vacant sau temporar vacant corespunzător funcţiilor contractuale şi a criteriilor de promovare în grade sau trepte profesionale imediat superioare a personalului contractual din sectorul bugetar plătit din fonduri publice, cu modificările şi completările ulterioare;

1.10. Legea-Cadru nr. 153 din 28 iunie 2017 privind salarizarea personalului plătit din fonduri publice, cu modificările şi completările ulterioare.

2. Scop

Scopul politicii interne de protecţie a datelor cu caracter personal (denumită în continuare „Politica") este de a garanta şi proteja drepturile şi libertăţile fundamentale ale persoanelor fizice, în special a dreptului la viaţa intimă, familială şi privată, cu privire la prelucrarea datelor cu caracter personal.

Această politică stabileşte:

2.1. Măsuri tehnice şi organizatorice pentru îndeplinirea obligaţiilor referitoare la securitatea şi controlul sistemelor informatice, în vederea asigurării confidenţialităţii datelor şi informaţiilor precum şi pentru păstrarea în siguranţă a acestora, în cadrul activităţii curente executate de angajaţii Institutului de Chimie Macromoleculară "Petru Poni" - Iaşi (ICMPP sau „Operator").

2.2. Responsabilităţile ICMPP în calitate de Operator de date personale, ale angajaţilor, colaboratorilor săi şi ale persoanelor împuternicite cu privire la respectarea prevederilor RGPD. Această politică, politicile, procedurile şi formularele asociate acesteia vor forma cadrul în care personalul trebuie să opereze pentru a asigura conformitatea cu legislaţia privind protecţia datelor.

3. Domeniu de aplicare

3.1. Prezenta Politică se aplica tuturor angajaţilor şi colaboratorilor ICMPP, persoanelor împuternicite de ICMPP şi operatorilor asociaţi ICMPP.

3.2. Prezenta Politică se aplică prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate ale datelor cu caracter personal care fac parte sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

4. Definirea termenilor

În sensul definit de RGPD, termenii folosiţi în prezenta politică se definesc după cum urmează:

a) **operator** - orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autorităţile publice, instituţiile şi structurile teritoriale ale acestora, care stabileşte scopul şi mijloacele de prelucrare a datelor cu caracter personal; dacă scopul şi mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoana fizică sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza acelui act normativ;

b) **date cu caracter personal (dcp)** - orice informaţii referitoare la o persoană fizică identificată sau identificabilă; o persoană identificabilă este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un număr de identificare ori la unul sau la mai mulţi factori specifici identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

c) **prelucrarea datelor cu caracter personal** - orice operaţiune sau set de operaţiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terţi prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea;

d) **responsabil cu protecţia datelor (DPO)** - persoana care este responsabilă cu monitorizarea aplicării RGPD şi a altor legi aplicabile privind protecţia persoanelor vizate de prelucrarea dcp şi care exercită funcţiile care îi sunt atribuite de prezenta Politică şi de altă legislaţie aplicabilă, furnizează consultanţă cu privire la protecţia dcp operatorului, persoanelor împuternicite de operator şi angajaţilor care prelucrează date;

e) **persoana împuternicită de operator (PIO)** - persoana fizică sau juridică, autoritate publică, agenţie sau orice alt organism care prelucrează date cu caracter personal în numele operatorului. PIO realizează prelucrări conform indicaţiilor transmise de operator;

f) **operatori asociaţi** - operatori care stabilesc în comun scopurile şi mijloacele de prelucrare a dcp ale persoanelor vizate. Operatorii asociaţi trebuie să încheie un acord care să stabilească responsabilităţile fiecăruia în ceea ce îndeplineşte îndeplinirea normelor RGPD. Principalele aspecte ale acordului trebuie comunicate persoanelor vizate.

g) **persoana vizată** - persoana fizică ale cărei date cu caracter personal sunt prelucrate;

h) **consimţământ** - orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, că datele cu caracter personal care o privesc să fie prelucrate;

i) **sistem de evidenţă a datelor cu caracter personal** - orice structură organizată de date cu caracter personal, accesibilă potrivit unor criterii determinate, indiferent dacă această structură este organizată în mod centralizat ori descentralizat sau este repartizată după criterii funcţionale ori geografice;

j) **terţ** - orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autorităţile publice, instituţiile şi structurile teritoriale ale acestora, alta decât persoana vizată, operatorul ori persoana împuternicită sau persoanele care, sub autoritatea directă a operatorului sau a persoanei împuternicite, sunt autorizate să prelucreze date;

k) **destinatar** - orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autorităţile publice, instituţiile şi structurile teritoriale ale acestora, căreia îi sunt dezvăluite date, indiferent dacă este sau nu terţ; autorităţile publice cărora li se comunică date în cadrul unei competenţe speciale de anchetă nu vor fi considerate destinatari;

l) **încălcarea securităţii dcp** – o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizată a dcp transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea. Constatarea acestei stări de fapt reprezintă un "Incident de securitate".

5. Responsabilităţi

5.1. ICMPP, în calitate de operator, este responsabilă de respectarea legislaţiei aplicabile privind protecţia dcp şi se asigură că poate demonstra că prelucrarea este în conformitate cu RGPD.

ICMPP, în calitate de operator de date, este responsabilă de securitatea şi confidenţialitatea datelor cu

caracter personal pe care le prelucrează, chiar dacă aceste date sunt transmise ulterior unei alte organizații sau sunt stocate pe sisteme sau dispozitive deținute de alte organizații sau persoane fizice (inclusiv dispozitive personale deținute de angajați).

ICMPP se asigură că DPO:

- primește sprijin activ în îndeplinirea sarcinilor sale;
- are la dispoziție toate resursele necesare pentru îndeplinirea sarcinilor în mod eficient precum și accesul la dcp și la operațiunile de prelucrare din instituție, și pentru perfecționarea cunoștințelor sale de specialitate;
- este implicat, informat și consultat de la bun început în toate aspectele legate de protecția dcp;
- are autonomie și resurse suficiente pentru îndeplinirea sarcinilor.

5.2. Șefii de/laboratoare/colective și șefii de birouri/departamente/compartimente din cadrul ICMPP au următoarele responsabilități:

- de a respecta și monitoriza implementarea prevederilor RGPD, ale prezentei Politici și ale procedurilor specifice protecției dcp la nivelul structurii pe care o conduc;
- de a informa DPO când apar activități noi de prelucrare a dcp;
- de a transmite DPO toate informațiile relevante în timp util pentru a permite ca acesta să ofere o consiliere corespunzătoare;
- de a solicita avizul DPO în toate aspectele legate de protecția dcp iar în caz în care nu sunt de acord cu acesta, să documenteze în scris motivele pentru care nu a fost urmat avizul DPO;
- de a raporta anual conducerii ICMPP gradul de conformare a structurii pe care o conduc la RGPD și acțiunile întreprinse în acest scop;
- de a informa/consulta DPO cu promptitudine imediat ce a avut loc o încălcare a securității datelor sau un alt incident.

5.3. Angajații care prelucrează dcp au următoarele responsabilități:

- de a cunoaște și de a aplica prevederile RGPD, ale prezentei Politici și ale procedurilor specifice protecției datelor cu caracter personal la nivelul ICMPP;
- de a informa persoana vizată atunci când dcp sunt colectate direct de la aceasta, în condițiile legii, cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute și consecințele refuzului de a le pune la dispoziție, drepturile prevăzute de lege, în special drepturile de acces, de intervenție asupra datelor și de opoziție, condițiile în care pot fi exercitate aceste drepturi;
- de a prelucra numai dcp necesare îndeplinirii atribuțiilor de serviciu și de a acorda sprijin conducătorului operatorului pentru realizarea activităților specifice ale acestuia;
- de a păstra confidențialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal;
- de a respecta măsurile de securitate, precum și celelalte reguli stabilite de ICMPP;
- de a informa de îndată șeful ierarhic și DPO despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situație în care au fost accesate/prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoștință;
- de a participa la ședințele de instruire cu privire la protecția dcp și de a solicita consiliere atunci când este necesar;
- de a se asigura că documentele trimise, în format fizic sau electronic, au ajuns la destinație;
- de a informa/consulta DPO, în scris, cu promptitudine, imediat ce a avut loc o încălcare a securității datelor sau un alt incident.

5.4. Responsabilul IT are următoarele răspunderi:

- de a elabora/actualiza proceduri specifice IT, care să asigure cerințele minime de protecție a datelor cu caracter personal la nivelul ICMPP, cum ar fi :

a) prevenirea accesului persoanelor neautorizate la sistemele dedicate prelucrării sau utilizării datelor cu caracter personal;

b) prevenirea utilizării sistemelor de prelucrare a datelor cu caracter personal fără autorizare;

c) garantarea faptului că persoanele autorizate să utilizeze sistemul de prelucrare a datelor cu caracter personal au acces exclusiv la acele date pentru care au obținut autorizarea și că datele cu caracter personal nu pot fi citite, copiate, modificate sau șterse fără autorizare pe durata prelucrării, utilizării și ulterior înregistrării;

d) garantarea faptului că datele personale nu pot fi citite, copiate, modificate sau șterse fără autorizare pe durata transferului electronic sau transportului sau pe durata înregistrării în dispozitivele de stocare a datelor;

e) garantarea posibilității de a verifica și evalua, retroactiv, dacă datele cu caracter personal au fost înregistrate, modificate sau șterse din sistemele de procesare date și, în cazul în care se constată acest lucru, identificarea persoanei responsabile;

f) garantarea faptului că datele cu caracter personal sunt protejate împotriva distrugerii sau pierderii accidentale şi există capacitatea de a le restabili disponibilitatea;

g) testarea, evaluarea şi aprecierea periodică a eficacităţii măsurilor tehnice şi organizatorice.

- de a instrui angajaţii în legătură cu utilizarea emailului, reţelelor wi-fi, aplicaţiilor etc.

- de a informa în scris şeful ierarhic şi DPO imediat ce a avut loc o încălcare a securităţii datelor sau un alt incident.

- de a se consulta cu DPO privind consecinţele/cerinţele în planul măsurilor de protecţie a dcp care pot fi generate de achiziţionarea unor programe informatice noi ce urmează a realiza şi activităţi de prelucrare a datelor cu caracter personal, extinderea/restrângerea reţelei informatice, acordarea de drepturi pentru noi utilizatori etc.

5.5. Administratorii paginilor de internet create sub autoritatea ICMPP au următoarele responsabilităţi:

- asigura disponibilitatea, integritatea şi confidenţialitatea informaţiilor care sunt publicate pe site-urile web administrate;

- devoltă, administrează şi modernizează site-uri web complexe – cu conţinut în baze de date, acces utilizatori ierarhizat, zone private etc.;

- menţinerea la standardele unei bune funcţionări a site-urilor web administrate;

- utilizarea cu responsabilitate a serverelor, reţelei şi internetului la care are acces;

- păstrează confidenţialitatea rezultatelor obţinute şi a informaţiilor pe care le deţine legate de accesul la bazele de date, script-uri, cod sursă sau orice altă informaţie adiacentă activităţii depuse;

- informeaza semestrial şeful ierarhic sau persoana desemnată de acesta cu privire la rezultatele obţinute şi a informaţiilor pe care le deţine legate de accesul la bazele de date, script-uri, cod sursă sau orice altă informaţie adiacentă activităţii depuse;

- rezolvă sarcinile primite în termenul stabilit;

- asigură securitatea site-urilor web administrate şi previne / rezolvă prompt breşele de securitate, situaţiile de acces neautorizat pe servere, protejează informaţia şi raportează imediat orice incident de securitate şefului ierarhic şi DPO;

- asigură întreţinerea şi actualizarea bazelor de date create;

- îşi documentează activitatea de dezvoltare/modificare site-uri web;

- asigură publicarea conţinutului informaţional. Conţinutul informaţional este propus de responsabilul de conţinut informaţional numit prin decizie şi trebuie să aibă avizul scris al conducerii ICMPP, al institutului, departamentului sau structurii administrative;

- asigură asistenţă tehnică tuturor utilizatorilor bazei de date;

- asigură integritatea, securitatea, remedierea tehnică, corectarea, actualizarea şi modelarea bazei de date;

- menţine un contact permanent cu şefii departamentelor pentru completarea, ştergerea şi actualizarea structurii bazei de date, remedierea anumitor probleme de ordin logic apărute;

- realizează modificarea bazei de date în funcţie de schimbările apărute la nivelul datelor intrate în institut/departament;

- răspunde de rezolvarea promptă a tuturor reclamaţiilor din partea utilizatorilor bazei de date din ICMPP;

- răspunde de informarea imediată a persoanelor responsabile privind orice defecţiune în funcţionare a echipamentului cu care îţi desfăşoară activitatea;

- răspunde de menţinerea unei continue legături cu responsabilii din institute/birouri/departamente pentru completarea, ştergerea şi actualizarea structurii bazei de date;

- răspunde de elaborarea şi respectarea procedurilor de lucru şi a reglementarilor specifice utilizării bazei de date (politică de cookies; procedură privind gestionarea conţinutului informaţional al paginilor web aparţinând ICMPP; procedură privind utilizarea bazei de date; procedură denumire fişiere; etc.).

5.6. Consilierul juridic are următoarele responsabilităţi:

- asigură, la cerere, asistenţă juridică de specialitate şi sprijin DPO în aria protecţiei dcp, cum ar fi:

a) identificarea şi evaluarea temeiurilor legale ale prelucrărilor de dcp efectuate de ICMPP;

b) evaluarea consecinţelor şi a nivelului riscurilor ce pot fi generate de prelucrările de date realizate de ICMPP (ori în situaţia producerii unor incidente), în planul drepturilor şi libertăţilor persoanelor fizice vizate;

c) analiza temeiniciei cererilor de exercitare a drepturilor, adresate operatorului de către persoane fizice vizate.

- avizează şi contrasemnează pentru verificarea conformităţii cu prevederile legale în vigoare politica internă de protecţie a datelor, precum şi alte documente întocmite de DPO;

- asigură asistenţă, consultanţă şi reprezentarea juridică a ICMPP în cauzele aflate pe rolul instanţelor de judecată sau al altor organisme cu caracter jurisdicţional.

5.7. Sarcinile Responsabilului cu protecţia datelor (DPO):

- participă la şedinţele conducerii ICMPP în care se iau decizii cu implicaţii asupra protecţiei dcp;

- beneficiază de sprijin direct din partea conducerii ICMPP şi nu primeşte instrucţiuni din partea operatorului

în ceea ce privește îndeplinirea sarcinilor sale;

- se implică în mod corespunzător și în timp util în toate aspectele legate de protecția dcp la nivelul ICMPP.
- acordă asistență conducerii ICMPP pentru implementarea și monitorizarea conformității cu prevederile RGPD;
- colectează informații pentru a identifica operațiunile de prelucrare;
- analizează și verifică gradul de conformitate al operațiunilor de prelucrare;
- informează, consiliază și emite recomandări cu privire la soluțiile de implementare a RGPD;
- avizează procedurile privind protecția datelor, adoptate la nivelul operatorului sau în relația cu persoanele împuternicite;
- este informat în timp util și consultat de către conducerea operatorului atunci când se intenționează realizarea unei evaluări de impact;
- participă la toate grupurile de lucru relevante care se ocupă de activități de prelucrare a dcp din cadrul ICMPP;
- acordă consultanță în situația producerii unei încălcări a securității dcp ori a unui alt incident de acest gen;
- întocmește și prezintă conducerii ICMPP un raport anual de activitate care cuprinde și analiza stării de conformitate cu RGPD;
- cooperează cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (se consultă cu aceasta în situațiile când este necesar) și își asumă rolul de punct de contact cu Autoritatea și persoanele fizice vizate privind aspectele legate de prelucrările efectuate de ICMPP și dacă este cazul, consultarea cu privire la orice altă chestiune;
- întocmește, actualizează și păstrează Evidența activităților de prelucrare a datelor cu caracter personal;
- se preocupă (cu sprijinul conducerii ICMPP) de dezvoltarea profesională continuă în domeniul protecției dcp.

6. Principii de prelucrare a datelor cu caracter personal prevăzute de RGPD

Institutul de Chimie Macromoleculară „Petru Poni" - Iași este responsabil pentru aplicarea principiilor protecției datelor oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Cele șase principii definite în art. 5 din RGPD sunt:

a) Dcp vor fi prelucrate în mod legal, echitabil și transparent („legalitate, echitate și transparență").

b) Dcp trebuie colectate în scopuri specificate, explicite și legitime și nu trebuie prelucrate în alt mod, incompatibil cu aceste scopuri. Este permisă prelucrarea ulterioară pentru arhivare, cercetări științifice sau istorice ori în scopuri statistice („limitarea scopului").

c) Dcp trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopul pentru care sunt prelucrate („reducerea la minimum a datelor").

d) Dcp trebuie să fie corecte și, dacă este necesar, să fie actualizate („exactitate").

e) Dcp prelucrate trebuie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele („limitare de stocare").

f) Dcp vor fi prelucrate într-un mod care asigură securitatea adecvată, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luare de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate").

Respectarea RGPD și respectarea acestor principii este responsabilitatea tuturor angajaților ICMPP. Orice încălcare deliberată a acestei politici poate conduce la măsuri disciplinare.

7. Securitatea datelor

Protecția datelor cu caracter personal implică două aspecte:

7.1. Securitatea fizică și IT a datelor cu caracter personal (prelucrate, stocate și transmise)

a) Securitatea fizică a dcp se va asigura prin păstrarea tuturor documentelor care conțin dcp în dulapuri/sertare închise cu cheie la care are acces doar personalul care are prevăzut în fișa postului atribuții referitoare la prelucrarea acelor documente. În cazul în care nu este posibilă încuierea dulapului/sertarului se va proceda la sigilarea dulapului/sertarului. Birourile nu vor fi lăsate nesupravegheate. Documentele care conțin dcp nu vor fi lăsate pe birou nesupravegheate pentru a preîntâmpina accesul/divulgarea către alți utilizatori care nu au atribuții de prelucrare referitoare la documentele respective. Imediat ce prelucrarea s-a încheiat, documentele vor fi depozitate în dulapuri închise. Transportul documentelor fizice în afara instituției este responsabilitatea angajatului care are sarcini în acest sens prevăzute în fișa postului.

Angajații ICMPP care au acces la dcp au dreptul să prelucreze numai acele date de care au nevoie pentru a-și îndeplini responsabilitățile specifice de muncă legate de oricare dintre temeiurile menționate la art. 9.

Documentele care conțin dcp sunt stocate în departamentele structurale ale ICMPP ai căror angajați au acces

la dcp legat de îndeplinirea atribuţiilor lor oficiale şi sunt responsabili de interacţiunea cu datele relevante ale persoanei vizate.

O persoană care prelucrează dcp în numele ICMPP respectă principiile şi regulile de prelucrare a dcp stabilite prin prezenta Politica. Dacă ICMPP autorizează o altă persoană cu prelucrarea dcp, ICMPP este responsabilă faţă de persoana vizată de prelucrarea dcp pentru faptele sau omisiunile acelei persoane. O persoană care prelucrează dcp în numele ICMPP este responsabilă faţă de ICMPP.

b) Securitatea IT a dcp se va asigura de către responsabilul IT şi administratorii site-urilor create sub autoritatea ICMPP prin:

- monitorizarea activităţilor în sistemul informatic, conform Politicii de monitorizare a activităţilor în sistemul informatic;
- constituirea şi gestionarea drepturilor şi a nivelurilor de acces ale angajaţilor;
- metodologia de evaluare şi tratare a riscurilor la adresa datelor cu caracter personal;
- proceduri specifice, conform Anexei nr. 1, nelimitându-se la ele.

c) Măsurile tehnice şi organizatorice necesare pentru a asigura confidenţialitatea şi securitatea datelor cu caracter personal sunt următoarele: Autentificare; Criptare; Pseudonimizare; Anonimizare; Drepturi de acces; Politica interna de protecţia datelor cu caracter personal; Regulament intern; Fişe de post; Proceduri de lucru; Clauze de confidenţialitate în contracte; Acces controlat în baze de date; Politica de securitate; Plan de securitate; Planul de răspuns la incidente; Controlul procesării interne; Utilizarea mecanismelor de semnare electronică; Firewall - dispozitiv prin care este controlat traficul dintre reţeaua ICMPP şi reţelele externe acestuia; Sistem antivirus; Întreţinerea sistemului, incluzând realizarea copiilor de siguranţă, întreţinerea jurnalelor de operare, menţinerea înregistrărilor cu erori de execuţie; Managementul reţelei, necesar asigurării reţelelor de calculatoare; Manipularea şi securitatea mediilor de stocare fizice, pentru a preveni întreruperea activităţii; Obţinerea unei analize a riscului de antiefracţie (este obligatorie prin lege); Pregătirea personalului în vederea utilizării sistemului informatic; Consilierea din partea unui specialist în securitatea informaţiei; Securitatea accesului terţilor; Evaluări de impact asupra DCP; alte măsuri juridice.

ICMPP va elabora şi implementa proceduri de lucru pentru măsurile enumerate mai sus.

Măsurile de securitate dispuse de conducerea ICMPP trebuie să îndeplinească o serie de cerinţe minimale, între care:

- capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor de prelucrare;
- capacitatea de a restabili disponibilitatea dcp şi accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- un proces pentru testarea, evaluarea şi aprecierea periodică a eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea prelucrării.

Periodic, DPO - cu sprijinul specialiştilor din cadrul ICMPP, desemnaţi în acest sens de conducere, va realiza activităţi de evaluare a nivelului adecvat de securitate, ţinând seama de riscurile prezentate de tipurile de prelucrări şi categorii de date prelucrate, care pot fi generate în mod accidental sau ilegal de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în orice mod.

7.2. Confidenţialitatea datelor cu caracter personal

Confidenţialitatea dcp presupune că documentele care conţin dcp să fie văzute doar de cei care au atribuţii de prelucrare şi să nu ajungă la destinatari care nu au competenţa legală sau funcţională de a le primi/prelucra.

Angajaţilor ICMPP li se interzice să utilizeze dcp în scopuri private sau comerciale, să le dezvăluie persoanelor neautorizate sau să le pună la dispoziţie în orice alt mod. Superiorii ierarhici îşi informează angajaţii la începutul relaţiei de muncă cu privire la obligaţia de a proteja secretul datelor.

La nivelul ICMPP vor fi active în permanenţă şi alte măsuri tehnice şi organizatorice corespunzătoare domeniului de aplicare, tipurilor de riscuri pe care le pot genera activităţile specifice de prelucrare asupra drepturilor şi libertăţilor persoanelor vizate, astfel încât să se asigure un nivel de securitate corespunzător fiecărui tip de risc, incluzând printre altele, după caz, pseudonomizarea şi criptarea dcp.

Toţi utilizatorii de dcp trebuie să se asigure că toate dcp pe care le deţin sunt păstrate în siguranţă. Aceştia trebuie să se asigure că datele nu sunt divulgate niciunei părţi terţe neautorizate sub nici o formă, fie accidental, fie în alt mod. Securitatea datelor trebuie să fie asigurată în conformitate cu Politica de securitate a informaţiei şi cu politicile şi procedurile aferente acesteia.

8. Păstrarea datelor

Fiecare entitate organizatorică din cadrul ICMPP este responsabilă de asigurarea perioadelor corespunzătoare de păstrare a informaţiilor pe care le deţine şi le administrează, pe baza nomenclatorului arhivistic al instituţiei, a legislaţiei muncii, a legislaţiei financiar-contabile şi a altor prevederi legale incidente activităţilor specifice ale

ICMPP și structurilor sale componente.

Dcp trebuie păstrate numai pentru perioada de timp necesară efectuării prelucrării pentru care au fost colectate. În situația în care Legea Arhivelor Naționale nr. 16/1996 (republicată în 2014) și/sau legislația în vigoare din domeniu nu stabilește termene pentru anumite documente - aflate pe suport fizic sau în harduri/zone temporare de stocare informatică - ce se prelucrează și care conțin date cu caracter personal, fiecare utilizator care gestionează respectivele documentele are obligația de a stabili/propune și argumenta, în mod formalizat și cu aprobarea șefului ierarhic superior și a conducerii ICMPP, termene de păstrare. Termenele stabilite în temeiul prezentei politici, trebuie să fie rezonabile avându-se în vedere necesitatea asigurării faptului că dcp nu trebuie păstrate mai mult timp decât este necesar. Perioada maximă de păstrare a dcp pentru care nu este stabilit un termen este de maxim 1 an. Este obligatorie respectarea perioadelor de păstrare prevăzute în *Evidența activităților de prelucrare a datelor cu caracter personal*.

De asemenea, utilizatorii care gestionează documente care conțin dcp au obligația de a verifica în mod responsabil documentele aflate în gestiunea lor, pe suport fizic sau în harduri/zone temporare de stocare informatică, în vederea selecției lor pentru distrugere/arhivare/anonimizare etc.

La sfârșitul perioadei de păstrare, dcp sunt șterse sau distruse după caz, într-un mod în care să facă imposibilă accesarea lor ulterioară.

Odată ce informația nu mai este necesară, ar trebui eliminată în siguranță. Înregistrările pe hârtie trebuie să fie fragmentate în deșeuri care să nu mai permită citirea informațiilor iar înregistrările electronice trebuie șterse definitiv conform unei proceduri ce urmează a fi realizată de operator.

În cazul în care datele sunt complet anonime, nu există limite de timp pentru stocare din punct de vedere al protecției datelor.

9. Temeiurile prelucrării datelor

Institutul de Chimie Macromoleculară „Petru Poni" - Iași prelucrează dcp în baza următoarelor temeiuri:

a) Persoana vizată și-a dat consimțământul;

b) Prelucrarea este necesară în baza unui contract;

c) Prelucrarea este necesară din cauza unei obligații legale;

d) Prelucrarea este necesară pentru protejarea intereselor vitale ale unei persoane (adică situația de viață sau de deces);

e) Prelucrarea este necesară pentru îndeplinirea unei sarcini realizate în interes public sau în exercitarea autorității publice a operatorului;

f) Prelucrarea este necesară pentru interesele legitime ale operatorului sau ale unei terțe părți și nu interferează cu drepturile și libertățile persoanei vizate (această condiție nu poate fi utilizată de autoritățile publice în îndeplinirea sarcinilor lor publice).

Întreaga prelucrare a dcp efectuată de către ICMPP trebuie să se bazeze pe un temei legal, în acord cu obiectivele instituției și scopurile prelucrării.

În plus prelucrarea „categoriilor speciale" de date cu caracter personal necesită condiții suplimentare, mai stricte, care trebuie îndeplinite în conformitate cu art. 9 din RGPD.

9.1. Consimțământul ca temei al prelucrarii datelor

Atunci cand este necesar consimțământul persoanelor vizate, dcp pot fi prelucrate după primirea acordului persoanei vizate. În acest caz, ICMPP trebuie să fie în măsură să demonstreze că persoana fizică vizată și-a dat consimțământul pentru prelucrarea dcp. Consimțământul trebuie obținut în scris.

În cazul în care consimțământul este exprimat printr-o declarație scrisă care se referă și la alte aspecte, cererea privind consimțământul va fi prezentată într-o formă care o va diferenția de celelalte aspecte, folosind exprimări inteligibile și ușor accesibile.

La nivelul ICMPP va fi implementată o procedură de exercitare a drepturilor care va asigura persoanelor vizate posibilitatea de a-și retrage în orice moment consimțământul, în condițiile prevăzute de RGPD.

În cazul angajaților, consimțământul nu ar trebui utilizat pentru prelucrările de bază din cauza dezechilibrului existent în relația dintre operator și persoana vizată. În aceste cazuri, este puțin probabil să poată fi considerat liber acordat consimțământul. Prin urmare, atunci când este posibil, ICMPP ar trebui să identifice criterii alternative pentru prelucrare.

ICMPP poate utiliza ca temei de prelucrare consimțământul în anumite situații ca de exemplu: atunci când, în procesul de cercetare sunt necesare activități care presupun prelucrarea datelor cu caracter personal (anchete de teren, chestionare, înregistrări audio/foto etc.) sau atunci când intenționează să realizeze prelucrări ce sunt în interesul angajatului - cum ar fi acordarea unor beneficii personale/membrilor de familie/copiilor angajaților, iar în acest caz va solicita consimțământul părinților.

RGPD explică faptul că tăcerea, căsuțele pre-bifate sau inactivitatea nu constituie un consimțământ.

Orice persoană care şi-a dat consimţământul are dreptul să-şi retragă consimţământul în orice moment. ICMPP va implementa condiţiile tehnice şi organizatorice necesare pentru ca persoanele vizate să îşi poată exercita dreptul de a-şi retrage consimţământul acordat pentru prelucrările care se bazează pe acest temei.

9.2. Prelucrarea datelor pentru relaţia de muncă

În relaţiile de muncă, dcp pot fi prelucrate pentru iniţierea, executarea şi încetarea contractului individual de muncă. La iniţierea unui raport de muncă, datele personale ale candidaţilor vor fi procesate. În cazul în care candidatul este respins, datele sale trebuie şterse în conformitate cu perioada de păstrare legală.

9.3. Prelucrarea datelor pentru executarea unui contract

Datele personale ale persoanelor de contact şi reprezentanţilor partenerilor contractuali pot fi procesate pentru a încheia, executa şi înceta un contract. Înainte de semnarea contractului - în timpul fazei de iniţiere a contractului - datele personale pot fi prelucrate pentru a pregăti ofertele sau comenzile de cumpărare sau pentru a îndeplini alte cerinţe din perspectiva care se referă la încheierea contractului. Persoanele de contact pot fi contactate în timpul procesului de pregătire a contractului, utilizând doar informaţiile pe care acestea le-au furnizat pentru contactare. Orice restricţii solicitate de persoanele de contact respective trebuie să fie respectate.

9.4. Prelucrarea datelor în conformitate cu obligatia legală

Prelucrarea dcp este permisă şi în cazul în care legislaţia aplicabila solicită, impune sau permite acest lucru. Tipul şi amploarea procesării datelor trebuie să fie necesare pentru activitatea legală instituţională de prelucrare a datelor şi trebuie să respecte dispoziţiile legale relevante. Dacă există o anumită flexibilitate juridică, trebuie luate în considerare interesele persoanei vizate.

9.5. Prelucrarea datelor în baza unui interes legitim

Dcp pot fi procesate şi în cazul în care acest lucru este necesar pentru un interes legitim al ICMPP. Interesele legitime sunt în general de natură juridică (de exemplu, depunerea, aplicarea sau apărarea împotriva unor actiuni legale, recuperarea unor debite restante) sau comerciale (de exemplu, evitarea încălcării prevederilor contractuale). Dcp nu pot fi prelucrate în scopul unui interes legitim dacă, în cazuri individuale, există dovezi conform cărora interesele persoanei vizate merită protecţie şi că aceasta are prioritate. Înainte de prelucrarea datelor, este necesar să se determine dacă există interese care merită protejate.

Interesele justificate ale ICMPP (de exemplu, respectarea dispoziţiilor legale şi a reglementarilor interne ale instituţiei) trebuie să fie cântărite în raport cu interesele angajatului care trebuie protejate. Interesul legitim al instituţiei şi orice interese ale angajatului care merită protejate trebuie să fie identificate şi documentate înainte de luarea oricăror măsuri. În plus, trebuie luate în considerare orice cerinţe suplimentare din legislaţia naţională (de exemplu, drepturile de co-decizie pentru reprezentanţii angajaţilor şi drepturile de informare ale persoanelor vizate).

10. Înregistrarea activităţilor de prelucrare

În calitate de operator de date, ICMPP trebuie să ţină o evidenţă a activităţilor de prelucrare a datelor personale efectuate. Responsabilul cu protecţia datelor de la nivelul ICMPP are sarcina de a întocmi, actualiza şi păstra, în format scris/listat şi în format electronic, *Evidenţa activităţilor de prelucrare a datelor cu caracter personal.*

Evidenţa activităţilor de prelucrare realizate de ICMPP va cuprinde: scopurile prelucrării, descrierea categoriilor de persoane vizate şi a categoriilor de dcp, categoriile de destinatari cărora le sunt divulgate datele personal, dacă este cazul - transferurile de date către o ţară terţă sau o organizaţie internaţională (inclusiv documentaţia care dovedeşte existenţa unor garanţii adecvate), termenele-limită preconizate pentru ştergerea diferitelor categorii de date, descrierea generală a măsurilor tehnice şi organizatorice de securitate.

ICMPP realizează activităţi de prelucrare cu privire la următoarele categorii de persoane:

- Angajaţi (potenţiali, actuali şi foşti) şi membri familiilor salariaţilor;
- Persoane vizate, altele decât candidaţi, angajaţi şi foşti angajaţi (ex. invitaţi/participanţi la evenimentele organizate de ICMPP , subiecţi ai cercetărilor care necesită completarea de chestionare, înregistrări video/audio, interviuri, părţi semnatare ale contractelor şi persoanele implicate în încheierea şi executarea contractelor, reprezentanţi ai autorităţilor, instituţiilor publice şi mass-media, studenţi aflaţi în practică, utilizatori ai serviciilor de Bibliotecă, vizitatori, persoane care accesează paginile web etc.).

Personalul care se angajează în noi activităţi care implică utilizarea dcp şi care nu este acoperit de una dintre înregistrările existente ale activităţilor de prelucrare trebuie să informeze responsabilul pentru protecţia datelor (dpo@icmpp.ro) înainte de a începe noua activitate.

11. Cercetare ştiinţifică

Obiectul de activitate al ICMPP constă în cercetarea ştiinţifică fundamentală şi avansată, pe bază de programe înscrise în planurile de cercetare ale Academiei Române, precum şi în activităţi conexe (difuzarea rezultatelor cercetărilor efectuate prin publicaţii, consultanţă, participare şi organizare de sesiuni ştiinţifice) în

chimie macromoleculară. ICMPP participă la elaborarea unor cercetări cu caracter interdisciplinar în parteneriat cu alte institute şi parteneri din ţară şi străinătate.

Prelucrarea dcp în scopuri de cercetare ştiinţifică sau istorică, în scopuri statistice ori în scopuri de arhivare în interes public se va realiza cu respectarea prevederilor şi precizărilor din art. 8 al Legii nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679, precum şi a garanţiilor şi derogărilor stabilite prin art. 89 din RGPD.

În situaţia în care, în cadrul procesului de cercetare sunt necesare activităţi prin care se prelucrează dcp (ca de exemplu: anchete de teren, interviuri, chestionare, înregistrări audio/foto etc.), cercetătorii care colectează datele în scopul cercetării vor include o notă de informare şi o formă adecvată de consimţământ în orice formular de colectare a datelor (ex: Anexa nr. 2 - Notă de informare şi Anexa nr. 3 - Formular de consimţământ), conform unor politici/proceduri interne specifice realizate şi aprobate înainte de a începe procesul de cercetare.

În situaţia în care, în cadrul procesului de cercetare/documentare cercetătorii prelucrează documente care conţin dcp (ex: copii după documente care conţin dcp sau date cu caracter special ale unor persoane în viaţă - documente obţinute în procesul de documentare din instituţii precum Arhivele Naţionale ale României, Consiliul Naţional pentru Studierea Arhivelor Securităţii, Arhivele Diplomatice ale Ministerului de Externe etc.), aceştia vor proceda la soluţii precum anonimizarea/pseudonimizarea/criptarea documentelor pe care le prelucrează, conform unor politici/proceduri interne specifice realizate şi aprobate înainte de a începe procesul de cercetare.

12. Prelucrarea datelor cu caracter personal

În principal, la nivelul ICMPP scopul prelucrării dcp vizează îndeplinirea obligaţiilor legale în legătură cu obiectul de activitate al ICMPP, în exercitarea atribuţiilor prevăzute în Legea nr. 752/2001 republicată, cu modificările şi completările ulterioare şi Statutul Academiei Române.

ICMPP prelucrează dcp pe care persoanele vizate le furnizează în mod direct, date care sunt generate pe baza acestora, precum şi date din surse publice.

12.1. Categoriile de dcp prelucrate sunt:

- date de identificare - *nume, prenume, prenumele părinţilor, data şi locul naşterii, CNP, seria şi nr BI/CI/paşaport/permis de conducere;*
- date ale membrilor de familie - *sau ale unor persoane aflate în întreţinere - nume, prenume, CNP-ul copiilor (pentru deducere, ajutor de naştere, diverse ajutoare acordate de angajator), adeverinţe pentru şcoală, declaraţie pe proprie răspundere de la soţ/soţie că nu beneficiază de deducere pt copii, copie certificat căsătorie;*
- date tip adresă - *domiciliul, reşedinţă, etc.;*
- date de contact - *numere de telefon, fax, e-mail , etc.;*
- date privind studiile şi istoricul profesional - acte de studii, diplome, certificări, informaţii de la alte locuri de muncă, recomandări, caracterizări, etc.;
- date privind veniturile şi de natură bancară - *situaţia financiară, funcţie, departament, salariu bonusuri, venituri, sporuri, nr. de zile de concediu de odihnă, de concediu medical, cont bancar;*
- date privind evoluţia profesională - *evaluări ale performanţei profesionale, cercetări disciplinare, sancţiuni, reclamaţii la adresa angajatului, etc.;*
- date cu caracter special privind sănătatea - *codul de pe adeverinţa de concediu medical, elemente de identificare în legătură cu asigurările sociale;*
- date legate de securitatea şi sănătatea muncii;
- date necesare pentru echipamentele de protecţie la locul de muncă - *talia, nr. la pantofi, dioptrii pentru ochelari, etc.;*
- date de identificare informatice: adresa IP, nume de utilizator, parolă;
- date biometrice: voce, imagine;
- date colectate cu ocazia înregistrării şi participării la evenimentele organizate sau sprijinite de către ICMPP (fotografii, video, citate, postări pe pagina web şi/sau pe reţele de socializare etc.).
- date de geolocalizare auto şi terminal mobil de serviciu;
- date identificare utilizator terminal telefonic;
- date de trafic şi acces la aplicaţii;
- contacte din e-mailul alocat de angajator, date sms;

(*toate exemplele de mai sus sunt cu referire la auto şi echipamente de comunicare încredinţate de angajator)*

- semnătura (inclusiv electronică), ştampile.
- date stocate pe cartele magnetice aferente sistemului de acces controlat;
- date privind activitatea individuală la locul de muncă stocate pe memoria echipamentelor electronice.

12.2. Proceduri de prelucrare a datelor cu caracter personal

Tipurile de operaţiuni de prelucrare sunt următoarele:

Organizare = *ordonare, structurare sau sistematizare conform unor criterii prestabilite, potrivit atribuțiilor legale ale operatorului;*

Stocare = *păstrarea pe orice fel de suport a dcp, inclusiv prin efectuarea de copii de siguranță;*

Adaptare = *transformarea dcp conform unor criterii prestabilite și în acord cu scopurile pentru care au fost colectate;*

Modificare = *actualizarea, completarea, schimbarea, corectarea, refacerea dcp în scopul menținerii, corectitudinii și actualității lor;*

Extragere = *scoaterea unei părți a dcp pentru utilizarea lor separată și distinct de scopul prelucrării inițiale;*

Consultare = *vizualizarea, examinarea, interogarea, analiza dcp, în scopul efectuării unor operațiuni;*

Utilizare = *folosirea dcp, total sau parțial - de către operator, împuternicit, destinatari-inclusiv prin tipărire, copiere, scanare, multiplicare.*

Alăturarea = *adăugarea, alipirea sau anexarea unor dcp la cele deja deținute;*

Combinarea = *îmbinarea, unirea sau asamblarea unor dcp – care inițial se aflau separate - într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri bine determinate;*

Blocarea = *întreruperea prelucrării dcp;*

Ștergerea = *eliminarea - total sau partial - a dcp din evidențe sau înregistrări, ca urmare a solicitării persoanei vizate, a unei decizii a ANSPDCP, a expirării termenului de prelucrare, etc.;*

Transformarea = *operațiuni efectuate asupra dcp având drept scop anonimizarea sau utilizarea lor în scopuri exclusiv statistice;*

Distrugerea = *aducerea în stare de neîntrebuințare – în condiții legale - definitivă și irecuperabilă, prin mijloace mecanice sau termice a suporților fizici pe care sunt stocate/prelucrate dcp;*

Dezvăluire = *facilitarea accesării de dcp de către terți prin comunicare, transmitere, diseminare în orice mod;*

Pentru a asigura un nivel ridicat de protecție a dcp, ICMPP trebuie să elaboreze proceduri interne care se garanteze respectarea protecției dcp în orice moment, luând în considerare:

- *breșele de securitate;*
- *solicitări privind exercitarea drepturilor persoanelor vizate;*
- *modificarea dcp colectate;*
- *schimbarea persoanelor împuternicite.*

13. Categorii speciale de date sau date sensibile

13.1. Sunt denumite **categorii speciale de date** sau **date sensibile:**

- date referitoare la originea rasială sau etnică;
- date referitoare la opiniile politice, convingerile religioase sau de altă natură;
- datele cu caracter personal referitoare la starea de sănătate sau viața sexuală;
- apartenența la sindicate;
- date referitoare la infracțiuni și condamnările penale.

13.2. Prelucrarea datelor sensibile

Datele sensibile pot fi procesate numai în anumite condiții. În conformitate cu legislația națională, alte categorii de date pot fi considerate sensibile sau conținutul categoriilor de date poate fi completat diferit. Mai mult, datele care se referă la o infracțiune pot fi procesate numai în conformitate cu cerințele speciale din legislația națională.

Prelucrarea trebuie permisă în mod expres sau prescrisă de legislația națională. În plus, prelucrarea poate fi permisă dacă este necesar ca autoritatea responsabilă să își îndeplinească drepturile și obligațiile în domeniul dreptului muncii. Angajatul poate, de asemenea, să consimtă în mod expres prelucrarea.

Dacă există situații de prelucrare a datelor sensibile, DPO trebuie informat în prealabil.

14. Restricționarea prelucrării datelor cu caracter personal

Restricționarea prelucrării dcp reprezintă marcarea într-un sistem a dcp stocate, cu scopul de a limita prelucrarea viitoare a acestora.

Exemple de metode de restricționare: mutarea temporară a dcp selectate, într-un alt sistem de prelucrare; anularea accesului utilizatorilor la datele selectate; înlăturarea temporară a datelor publicate pe un site.

Condiții pentru restricționarea în sistemele automatizate:

- soluția tehnică trebuie să nu permită ca dcp să poată face obiectul unor operațiuni de prelucrare ulterioară și să nu poată fi schimbate;
- faptul că prelucrarea dcp este restricționată, trebuie indicată în mod clar în sistem.

15. Ştergerea, distrugerea şi arhivarea datelor cu caracter personal

ICMPP, prin grija responsabilului IT şi a DPO, va elabora o procedură internă privind ştergerea, distrugerea şi arhivarea dcp deţinute în format electronic.

Până la elaborarea procedurii privind ştergerea, distrugerea şi arhivarea a dcp deţinute în format electronic, angajaţii care urmează să efectueze aceste operaţiuni vor consulta responsabilul cu protecţia datelor.

Distrugerea şi arhivarea documentelor fizice care conţin dcp se va face în conformitate cu Procedura de sistem ICMPP – Arhivarea documentelor şi înregistrărilor.

16. Prelucrarea prin intermediul persoanelor împuternicite de operator (PIO)

ICMPP, în calitate de operator, are obligaţia de a alege numai persoane împuternicite care oferă garanţii suficiente că aplică măsuri tehnice şi organizatorice capabile să asigure respectarea cerinţelor RGPD în cadrul operaţiunilor de prelucrare a dcp.

În toate situaţiile, între ICMPP şi PIO se va încheie un contract sau un act juridic în temeiul dreptului UE sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită. În contract se vor stipula obligaţiile părţilor cu privire la prelucrarea dcp.

Situaţiile în care ICMPP încredinţează unei PIO operaţiuni de prelucrare a dcp sunt:

- plata drepturilor salariale şi alte drepturi băneşti;
- asigurarea dreptului la securitate şi sănătatea în muncă;
- drepturi acordate de angajator;
- asigurarea mentenanţei Sistemului Informatic Integrat – Infostar;
- asigurarea mentenanţei programului informatic salarizare – Naum consalt;
- asigurarea semnăturii electronice pentru persoanele împuternicite să efectueze operaţiuni în numele ICMPP;
- prestări servicii IT;
- achiziţionarea biletelor de avion necesare deplasărilor interne/externe;
- achiziţionarea materialelor necesare desfăşurării activităţii (birotică, papetărie, consumabile imprimante/copiatoare, curăţenie, etc.);
- angajaţi împuterniciţi pentru semnarea electronică a unor documente instituţionale.

Obligaţiile PIO sunt următoarele:

- Păstrarea evidenţei activităţilor de prelucrare realizate în numele operatorului;
- Obligaţia de a notifica operatorul cu privire la orice încălcare a securităţii dcp prelucrate;
- Respectarea regulilor privind transferul de date în afara ţării ori a spaţiului european.

PIO răspunde direct faţă de persoana vizată dacă acţionează în afara mandatului dat de operator ori dacă încalcă sarcini prevăzute expres de RGPD în sarcina sa.

Pentru situaţiile în care există contracte încheiate între ICMPP şi o PIO, se va completa contractul cu un Acord privind protecţia datelor cu caracter personal (conform modelului prezentat în Anexa nr. 4 - model Acord privind prelucrarea datelor cu caracter personal).

17. Categoriile de destinatari. Transferul şi divulgarea datelor

Ca regulă generală, dcp nu ar trebui să fie transmise terţilor, în special dacă acestea implică categorii speciale de dcp, dar există anumite circumstanţe când transmiterea este permisă.

În cazul în care un terţ prelucrează dcp în numele ICMPP trebuie să existe un contract scris. Un contract este, de asemenea, recomandabil atunci când datele sunt partajate din alte motive decât prelucrarea datelor, astfel încât ICMPP să aibă asigurări că cerinţele RGPD sunt îndeplinite.

Personalul trebuie să se consulte cu DPO dacă încheie un nou contract care implică partajarea sau prelucrarea dcp.

Dcp colectate de ICMPP sunt transmise către destinatari care au o obligaţie legală privind prelucrarea acestor date şi/sau pentru executarea unui contract. Aceşti destinatari sunt: Ordonatorul principal de credite, Trezoreria Municipiului Iaşi, finanţatori proiecte naţionale/fonduri externe nerambursabile/fonduri structurale/fonduri europene, Ministerul Educaţiei şi Cercetării, parteneri proiecte, Inspectoratul Teritorial de Muncă, Agenţia Naţională de Administrare Fiscală, Casa Naţională de Asigurări de Sănătate, Institutul Naţional de Statistică, BRD, RZBR, terţi (furnizori, clienţi, alţi debitori şi creditori), alte organisme de control.

ICMPP transferă dcp ale persoanei vizate către altă ţară numai la solicitarea acesteia.

Imaginile înregistrate prin intermediul sistemului de supraveghere video instalat în sediul ICMPP pot fi puse la dispoziţia organelor judiciare şi a altor instituţii abilitate de lege să solicite aceste informaţii, la cererea expresă a acestora. Orice transmitere a dcp catre un terţ operator se va face cu aprobarea conducerii ICMPP şi va fi consemnată de către responsabilul cu organizarea serviciului de pază în registrul de evidenţă al solicitărilor de înregistrări video. În situaţia în care nu există un registru de evidenţă al solicitărilor de înregistrări video, se va

proceda la constituirea acestuia.

18. Drepturile persoanelor vizate şi exercitarea acestora

18.1. În conformitate cu prevederile RGPD (art. 13 – art. 23), persoanele vizate ale căror dcp sunt prelucrate de ICMPP beneficiază de următoarele drepturi:

a) dreptul de a fi informat - să obţină de la ICMPP următoarele informaţii:

i. identitatea şi datele de contact ale ICMPP, ale reprezentanţilor, şi ale DPO;

ii. scopurile şi temeiul juridic al prelucrării dcp, interesele legitime ale ICMPP;

iii. categoriile de dcp;

iv. destinatarii dcp, inclusiv destinatarii din ţări terţe sau organizaţii internaţionale (dacă există) şi referirea la garanţiile şi mijloacele corespunzătoare;

v. perioada de stocare a dcp şi criteriile folosite pentru a determina acea perioadă, sub rezerva că ICMPP păstrează şi prelucrează dcp atâta timp cât legile şi reglementările legale impun acest lucru. Prelucrarea dcp încetează imediat dacă nu mai există niciun motiv pentru o astfel de prelucrare;

vi. din ce sursă provin datele cu caracter personal (în cazul în care datele cu caracter personal nu au fost obţinute de la persoana vizată);

vii. dacă furnizarea de date cu caracter personal este o cerinţă legală sau contractuală, sau o cerinţă necesară pentru a încheia un contract, precum şi dacă persoana vizată este obligată să furnizeze dcp şi a posibilelor consecinţe ale neîndeplinirii de furnizare a acestor date.

b) dreptul de acces la dcp - să obţină de la ICMPP confirmarea dacă dcp sunt prelucrate sau nu şi acces la datele sale cu caracter personal.

Exercitarea dreptului de acces se va face prin completarea unei cereri-tip (Anexa nr. 5).

c) dreptul la rectificare - să obţină de la ICMPP fără întârzieri nejustificate rectificarea unor dcp inexacte cu privire la ele, completarea dcp incomplete, inclusiv prin furnizarea unei declaraţii suplimentare;

Exercitarea dreptului la rectificare se va face prin transmiterea unei cereri-tip (Anexa nr. 6).

d) dreptul la opoziţie - vizează posibilitatea de se opune în orice moment prelucrării dcp;

Exercitarea dreptului la opoziţie se va face prin transmiterea unei cereri-tip (Anexa nr. 7).

e) dreptul la ştergerea datelor ("dreptul de a fi uitat") - să obţină de la ICMPP ştergerea dcp fără întârzieri nejustificate (dacă dcp nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate; persoana vizată îşi retrage consimţământul; dcp au fost prelucrare ilegal etc.).

Exercitarea dreptului de ştergere se va face prin transmiterea unei cereri-tip (Anexa nr. 8).

f) dreptul la restricţionarea prelucrării - să obţină restricţia de procesare a datelor lor cu caracter personal în anumite cazuri, de exemplu atunci când apreciază că prelucrarea este ilegală sau contestă exactitatea datelor lor cu caracter personal, pentru o perioadă care să permită ICMPP să corecteze situaţia.

Exercitarea dreptului la restricţionarea prelucrării se va face prin transmiterea unei cereri-tip (Anexa nr. 9).

g) dreptul la portabilitatea datelor - să primească dcp pe care ni le-au furnizat, într-un format structurat, utilizat în mod curent şi care poate fi citit automat şi are dreptul de a transmite aceste dcp unui alt operator fără obstacole din partea ICMPP (dacă prelucrarea se bazează pe consimţământ sau pe un contract, iar prelucrarea este efectuată prin mijloace automate).

Exercitarea dreptului la portabilitatea datelor se va face prin transmiterea unei cereri-tip (Anexa nr. 10).

h) dreptul legat de luarea deciziilor şi profilarea automată – acest drept se referă la decizii sau profiluri automate care ar putea avea ca rezultat efecte semnificative asupra unei persoane. Profilarea este prelucrarea datelor pentru a evalua, analiza sau prezice comportamentul sau orice caracteristică a comportamentului sau preferinţelor. Persoanele vizate au dreptul să nu se supună deciziilor bazate exclusiv pe prelucrarea automată. Atunci când se utilizează profilarea, trebuie luate măsuri pentru a asigura securitatea şi fiabilitatea serviciilor. Decizia automată bazată pe date sensibile poate fi făcută numai cu acordul explicit al persoanei vizate.

18.2. ICMPP ia măsuri adecvate pentru a furniza persoanelor vizate informaţiile legale solicitate, precum şi orice notificări şi comunicări (în situaţia exercitării drepturilor de care beneficiază acestea potrivit legii) referitoare la prelucrarea dcp, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. Informaţiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic.

ICMPP *furnizează persoanei vizate informaţii privind acţiunile întreprinse în urma unei cereri prin care îşi exercită drepturile de care beneficiază în baza legii, fără întârzieri nejustificate şi în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ţinându-se seama de complexitatea şi numărul cererilor şi informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând şi motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informaţiile sunt furnizate în format electronic acolo unde este posibil, cu*

excepția cazului în care persoana vizată solicită un alt format (art. 12 alin.3 din RGPD).

Daca nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară (art. 12 alin.4 din RGPD).

Informațiile furnizate în temeiul legislației specifice și orice comunicare sau măsuri luate în baza exercitării drepturilor de care beneficiază, potrivit legii, persoana vizată, sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

a) fie să perceapă o taxa rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;

b) fie să refuze să dea curs cererii.

În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii (art. 12 alin.5 din RGPD).

În cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea prin intermediul căreia își exercită drepturile de care beneficiază, potrivit legii, persoana vizată, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

ICMPP va implementa și deține o procedură de exercitare a drepturilor, prin grija DPO.

Toate cererile de exercitare a drepturilor trebuie să fie formulate în scris, datate și semnate.

19. Încălcarea securității datelor cu caracter personal

ICMPP va elabora și implementa, prin grija DPO, o procedură de gestionare a incidentelor de securitate, notificând persoanele vizate despre un eventual incident în legătură cu securitatea datelor, fără întârzieri nejustificate.

Până la realizarea procedurii de gestionare a incidentelor de securitate, dacă vor fi incidente de securitate raportabile, se va face o notificare.

ICMPP va monitoriza, prin intermediul DPO, riscurile noi și cele existente referitoare la protecția dcp, actualizând de îndată registrul riscurilor privind protecția datelor la nivelul ICMPP.

În cazul în care are loc o încălcare a securității dcp, ICMPP va notifica acest lucru și autorității de supraveghere, fără întârzieri nejustificate și dacă este posibil în cel mult 72 de ore de la data la care a luat la cunoștință de aceasta.

Este responsabilitatea întregului personal din cadrul ICMPP să notifice imediat șeful ierarhic superior și DPO cu privire la cazurile de încălcare a acestei politici sau cu privire la orice încălcare a securității dcp. Directorii/șefii fiecărui institut/birou/departament sunt obligați să informeze imediat conducerea ICMPP și DPO cu privire la incidentele de protecție a datelor. Atunci când DPO va considera necesar, va informa autoritatea de supraveghere despre aceste încălcări.

Directorii/șefii fiecărui institut/birou/departament din cadrul ICMPP vor fi responsabili pentru prelucrarea datelor din cadrul entității pe care o conduc și vor monitoriza riscurile noi și cele existente referitoare la protecția datelor, vor actualiza registrul riscurilor privind protecția dcp. În cazul sesizării unui risc, vor raporta, în scris, acest lucru de îndată conducerii ICMPP și DPO.

Directorii/șefii fiecărui institut/birou/departament în cadrul căruia se prelucrează dcp vor informa DPO în timp util cu privire la fiecare nouă activitate de prelucrare a datelor.

Conducerea ICMPP, împreună cu DPO se vor îngriji ca periodic să se efectueze un audit intern prin care să se verifice gestionarea riscurilor privind protecția dcp prelucrate la nivelul ICMPP.

ANSPDCP trebuie anunțată/consultată ori de câte ori este necesar iar DPO are o obligație legală în acest sens. De asemenea, în cazul unui control din partea ANSPDCP, DPO trebuie anunțat imediat.

În cazul încălcării securității dcp, angajații ICMPP pot fi sancționați în conformitate cu legislația aplicabilă și cu reglementările interne ale ICMPP.

20. Măsurile de verificare a modului în care sunt aplicate și respectate prevederile Politicii la nivelul ICMPP

Verificarea modului în care sunt aplicate și respectate prevederile politicii la nivelul ICMPP se va realiza de către DPO, prin intermediul auditurilor de protecția datelor precum și al altor controale, dispuse de conducerea ICMPP.

Scopul verificării este de a evalua modul de respectare și implementarea măsurilor tehnice și organizatorice care asigură conformitatea cu RGPD, de a adăuga valoare prin formularea recomandărilor, iar în cazul identificării unor iregularități, de corectare a acestora.

Obiectivul verificării este evaluarea stadiului de implementare / conformare a prevederilor prezentei Politici.

Tehnicile de verificare utilizate în cadrul unei activități de control sunt: listă de verificare, examinare, observarea fizică, interviu, testare, analiza datelor.

Fiecare activitate de control se finalizează cu un raport și un plan de acțiune care va conține recomandări pentru implementarea/conformarea cu cerințele tehnice și organizatorice adecvate prelucrării dcp.

21. Procedura de actualizare a Politicii

Prezenta politică poate fi actualizată ca urmare a modificării legislației relevante în domeniu sau atunci când se constată că este necesar, de către DPO. În cazul în care se fac modificări ale politicii, angajații vor fi înștiințați prin e-mail și prin afișare pe pagina web (www.icmpp.ro).

22. Contact DPO

Toate solicitările de informații suplimentare sau îndrumări referitoare la protecția datelor precum și cererile pentru exercitarea drepturilor prevăzute de legislația specifică trebuie transmise Responsabilului cu protecția datelor din cadrul Institutului de Chimie Macromoleculară „Petru Poni" - Iași la adresa de e-mail: dpo@icmpp.ro sau la următoarea adresă de corespondență:

„Institutul de Chimie Macromoleculară „Petru Poni" - Iași
În atenția Responsabilului cu protecția datelor
Aleea Grigore Ghica Vodă, nr. 41A
Cod poștal 700487, Iași".

Întocmit,
Responsabil cu protecția datelor,
Liviu Bunghez

[redacted]

Avizat,
Consilier juridic dr. ,
Raluca-Oana Andone

[redacted]