UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

PROTECȚIA DATELOR CU CARACTER PERSONAL

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
Mob: 0744423188
Birou: Clădirea Juventus, birou 4,
Parcul Sportiv "Iuliu Haţieganu"
dpo@ubbcluj.ro
www.ubbcluj.ro

Nr. DPO .... din 2022

INSTRUCȚIUNI
privind protecția datelor cu caracter personal a persoanelor care participă la proiectul de cercetare „Monitorizarea problemelor de mediu cu ajutorul Informațiilor Geografice Voluntare prin implicarea comunităților locale (EcoVoce)" *derulat de către* Facultatea de Știința și Ingineria Mediului *a* Universității Babeș-Bolyai din Cluj-Napoca

Desfășurarea activităților din cadrul proiectului de cercetare cu denumirea **Monitorizarea problemelor de mediu cu ajutorul Informațiilor Geografice Voluntare prin implicarea comunităților locale (EcoVoce)** impune tuturor persoanelor implicate în activitățile specifice respectarea unor măsuri de securitate pentru asigurarea protecției datelor cu caracter personal prelucrate[1] cu această ocazie.

Măsurile trecute în prezenta listă de recomandări nu exclud celelalte măsuri de securitate fizică, a informațiilor, a personalului, a documentelor, informatice și a comunicațiilor pe care fiecare angajat este dator să le adopte conform reglementărilor naționale și ale UBB Cluj.

1. Baze legale:

- **Regulamentul (UE) 2016/679** al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei95/46/CE (Regulamentul general privind protecția datelor), denumită în continuare **GDPR**, Art. 35 GDPR (Motivarea 89);
- **Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 (GDPR)** al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- **Directiva 2002/58/CE** a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice);
- **Legea nr. 506 din 17 noiembrie 2004** privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice;
- **SR EN ISO/IEC 27001:2015**, Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației.
- HCA 16772 privind Politica utilizării serviciului de mesagerie electronică (e-mail) instituțional
- GHID de utilizare în siguranță a serviciului de mesagerie electronică al Universității Babeș-Bolyai

[1] „**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 (art. 4 GDPR);

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
Mob: 0744423188
Birou: Clădirea Juventus, birou 4,
Parcul Sportiv "Iuliu Haţieganu"
dpo@ubbcluj.ro
www.ubbcluj.ro

2. Principiile care trebuie respectate pentru desfășurarea în deplină legalitate a activității de protecție a datelor cu caracter personal (DCP[2]) sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată **(„legalitate, echitate și transparență"**). Explicație: *Consimțământul Informat[3] privind PDCP[4] asigură legalitatea, echitatea și transparența. Aceasta trebuie pus la dispoziția tuturor participanților în format online (anterior furnizării datelor cu caracter personal) și* ***letric în timpul derulării activităților față în față de înscriere în Proiect****;*

(b) **colectate în scopuri determinate, explicite și legitime** și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri. Explicație: *În Consimțământul Informat privind PDCP sunt trecute explicit scopurile în care sunt prelucrate DCP, mijloacele de prelucrare, temeiurile legale, durata de păstrare;*

(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate **(„reducerea la minimum a datelor").** Explicație: *Aplicația EcoVoce va conține doar datele necesare bunei desfășurări a procesului de înscriere în Proiect. Nu se vor solicita date care nu sunt necesare sau care nu sunt înscrise în bazele legale ale Proiectului*;

d) **exacte și, în cazul în care este necesar, să fie actualizate**; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere (**"exactitate"**). Explicație: *se va oferi tot concursul pentru corectarea și completarea fără întârziere a datelor furnizate de către participanți la cererea acestora sau din proprie inițiativă. Datele vor fi șterse imediat ce legea o impune – conform termenului de păstrare- vezi Nomenclator Arhivistic*;

(e) **păstrate într-o formă care permite identificarea persoanelor vizate** pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele **("limitări legate de stocare"**); Explicație: *datele vor fi păstrate în sistemele informatice și letric în formate care permit identificarea persoanelor. DCP vor fi păstrate conform procedurii stabilite prin Regulamentul Proiectului fără a exceda scopului prelucrării conform perioadei stabilite prin Nomenclatorul arhivistic al UBB. Pe toată perioada vor fi instituite măsuri de securitate adecvate;*

(f) **prelucrate într-un mod care asigură securitatea** adecvată a DCP, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate"). Explicație: *Vor fi respectate toate măsurile de securitate fizică a informațiilor, a personalului, a documentelor, informatice și a comunicațiilor pe care fiecare angajat este dator să le adopte conform reglementărilor naționale și ale UBB Cluj.*

[2] DCP - date cu caracter personal
[3] Este postată pe platforma de admitere și pe site-ul UBB
[4] PDCP - protecția datelor cu caracter personal

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
Mob: 0744423188
Birou: Clădirea Juventus, birou 4,
Parcul Sportiv "Iuliu Hațieganu"
dpo@ubbcluj.ro
www.ubbcluj.ro

În vederea respectării principiilor mai sus prezentate orice echipă de proiect este obligată să instituie măsuri tehnice și organizatorice pentru a asigura protecția datelor cu caracter personal.

3. Reguli privind asigurarea securității fizice a DCP:

- activitățile specifice proiectului se vor desfășura exclusiv în spațiile puse la dispoziție de UBB și stabilite de către conducerea Facultății de Știința și Ingineria Mediului în colaborare cu directorul de proiect. Prin activități specifice se înțelege atât cele care se desfășoară fizic cât și cele care se desfășoară online;
- spațiile în care se vor desfășura activitățile de derulare a proiectului trebuie să îndeplinească criteriile specifice impuse de măsurile de securitate fizică stabilite pentru încăperile respective prin evaluările de risc la securitate fizică și incluse în planurile de pază *(Ex: încăperile vor fi dotate cu încuietori - cheia păstrată la formațiunea de pază; sistemul de supraveghere video activat – dacă este prevăzut; geamurile închise în afara orelor de program; cheile de acces vor fi predate structurii de pază, etc.);*
- deschiderea încăperilor va fi permisă doar persoanelor care au dreptul de acces stabilit de Decanul facultății și managerul de proiect. Numele persoanelor care au acces în acele încăperi trebuie să fie notificat la structura de pază;
- accesul personalului pentru curățenie și efectuarea acesteia se va face doar în condițiile stabilite de regulamentele UBB;
- documentele, ciornele, copiile sau alte documente care conțin înscrisuri cu date cu caracter personal vor fi închise în afara orelor de program în dulapuri sau sertare prevăzute cu încuietori;
- ciornele, copiile sau alte documente care conțin înscrisuri cu date cu caracter personal și care nu mai trebuie incluse în documentele privind proiectul de cercetare vor fi distruse astfel încât să nu poată fi reconstituite informațiile incluse pe acestea;
- se va evita accesul în încăperi a altor persoane care nu sunt incluse în activitățile proiectului.

4. Reguli privind asigurarea securității informațiilor/DCP:

- accesul personalului la informații (DCP) va fi permis pe principiul nevoii de a cunoaște (acces doar la DCP/informațiile de care are nevoie membrul echipei de proiect);
- persoanele implicate în proiect vor avea în vedere să nu disemineze date cu caracter personal înspre persoane terțe indiferent de formă: verbal, documente, înscrisuri, pe suport electronic, letric, online, telefonic, etc.;
- nu se vor solicita alte date cu caracter personal în afara celor trecute în procedurile de derulare a proiectului.

5. Reguli privind asigurarea securității informatice și a comunicațiilor:

- activitățile din cadrul proiectului se vor desfășura folosind doar echipamentele informatice (laptop-uri, PC-uri, tablete electronice, smartphone-uri, etc.) și suporturile de memorie externă (hard disk extern, CD, DVD, card de memorie, memorie USB, etc) puse la dispoziție de către UBB;

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
Mob: 0744423188
Birou: Clădirea Juventus, birou 4,
Parcul Sportiv "Iuliu Hațieganu"
dpo@ubbcluj.ro
www.ubbcluj.ro

- lucrul cu echipamentele informatice se va face în spațiile puse la dispoziție de UBB;
- echipamentele informatice vor fi protejate împotriva unor atacuri cibernetice (softuri antivirus, etc);
- stațiile de lucru (calculator, laptop) și suporturile de memorie externă vor fi parolate;
- în afara orelor de program stațiile de lucru portabile și suporturile de memorie externă vor sta închise în dulapuri închise cu cheie;
- în pauze sau când persoana care lucrează la stația de lucru se deplasează în altă încăpere, stația de lucru va fi închisă sau în "stand by", protejată de parolă, pentru a evita accesul altor persoane;
- conexiunile internet vor fi asigurate de către UBB;
- se vor folosi conexiuni securizate și pe cât posibil LAN (cablu) nu wi-fi;
- platformele electronice pe care se vor desfășura activități de admitere vor fi puse la dispoziție de către UBB;
- transmiterea de documente care conțin DCP va fi făcută folosind exclusiv serviciul de mesagerie electronică pus la dispoziție de către UBB (....@ubbcluj.ro). Nu se vor folosi e-mail-uri personale;
- nu se vor transmite documente care conțin DCP folosindu-se aplicațiile telefonice de mesagerie (Ex: WhatsApp, Telegram, Signal, etc);
- în cazul comunicării cu mai multe persoane se va evita folosirea opțiunii Cc, folosindu-se Bcc (evitându-se astfel diseminarea adreselor de e-mail la persoane care nu trebuie să cunoască adresele din listă);
- stocarea documentelor care conțin DCP va fi făcută pe suporți parolați;
- recomandăm folosirea criptării fișierelor atât în cazul transmiterii cât și în cazul stocării DCP;
- suporturile de memorie externă nu vor fi scoase din incinta UBB nejustificat, asigurându-se protecția acestora pe timpul deplasării între diferitele sedii ale UBB;
- parola de acces la platforma online de desfășurare a întâlnirilor va fi o combinație de minim 8 caractere care să conțină litere mari, litere mici, cifre, semn special;
- nu se vor comunica parolele de acces pe platforma de desfășurare a întâlnirilor înspre alte persoane;
- parolele folosite pentru limitarea accesului la stațiile de lucru vor fi comunicate conform procedurilor interne doar înspre persoane care prin natura activității trebuie să aibă acces la acea stație de lucru în absența titularului;
- comunicarea parolelor de decriptare a documentelor/fișierelor transmise e-mail va fi făcută folosindu-se un alt sistem de transmitere;
- anterior lansării Aplicației EcoVoce va fi realizată o Analiză de Risc și de Impact privitoare la protecția datelor cu caracter personal conform art. 35/GDPR.

6. Alte recomandări:

- membrii echipei de proiect vor folosi ca bază argumentativă - în cazul solicitării unor explicații de către participanți asupra modului de prelucrare a datelor cu caracter personal de către UBB - secțiunea *Protecția datelor cu caracter personal* de pe site-ul UBB, Ghidul privind protecția datelor pe timpul derulării activităților prin intermediul internetului (dacă se desfășoară întâlniri prin intermediul MS Teams), Consimțământul Informat care vor fi disponibile în format electronic și letric (când se fac deplasări în teren)

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
Mob: 0744423188
Birou: Clădirea Juventus, birou 4,
Parcul Sportiv "Iuliu Hațieganu"
dpo@ubbcluj.ro
www.ubbcluj.ro

- dacă solicitările participanților pe linia PDCP nu pot fi soluționate de către membri echipei de proiect, aceștia vor fi direcționați înspre DPO UBB folosindu-se datele de contact de pe site sau din acest document.

7. Procedura de soluționare a unor posibile incidente care pot afecta securitatea prelucrării DCP:

Posibile incidente (definiții):

Compromiterea DCP **–** pierderea sau alterarea, în mod accidental sau intenționat, a integrității, confidențialității și disponibilității DCP;

Confidențialitatea DCP **–** atributul DCP de a nu fi dezvăluite sau divulgate decât persoanelor sau entităților îndreptățite să le cunoască și să le acceseze în conformitate cu principiile legalității, echității, transparenței, a limitărilor legate de scop, a reducerii la minim a datelor, a exactității și a limitărilor legate de stocare;

Disponibilitatea DCP **–** calitatea DCP de a fi accesate de persoanele sau entitățile îndreptățite să le cunoască sau să le dețină în conformitate cu principiile legalității, echității, transparenței, a limitărilor legate de scop, a reducerii la minim a datelor, a exactității și a limitărilor legate de stocare;

Distrugerea neautorizată a DCP **–** situația în care DCP nu mai există sau nu sunt disponibile într-o formă în care să fie posibilă utilizarea de către UBB în conformitate cu scopurile prelucrării;

Integritatea DCP **–** atributul DCP de a nu fi fost modificate sau alterate, accidental sau intenționat, de către operator sau persoanele împuternicite ale acestuia;

Încălcare a prevederilor legale privind PDCP – orice acțiune sau inacțiune contrară prevederilor legale și procedurale în vigoare care reglementează PDCP și care este de natură a pune în pericol integritatea, confidențialitatea și disponibilitatea DCP, fără a compromite DCP;

Încălcarea securității DCP (incident de securitate care implică DCP) - încălcare a securității 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;

Pierderea DCP – situația în care DCP nu mai sunt sub controlul sau în posesia UBB sau instituția nu mai are acces la acestea.

Aspecte specifice:

Incidentul de securitate care implică DCP poate să apară ca urmare a unei încălcări a securității DCP sau a măsurilor organizatorice sau tehnice implementate la nivelul echipei de proiect și care are ca rezultat compromiterea DCP.

Încălcarea securității DCP sau a măsurilor organizatorice sau tehnice implementate la nivelul echipei de proiect poate fi rezultatul unei acțiuni sau inacțiuni accidentale sau intenționate și care să conducă la pierderea integrității, disponibilității sau confidențialității DCP.

Compromiterea DCP are loc în situația în care acestea sunt pierdute, distruse sau modificate în mod neautorizat ori divulgate unor persoane sau entități neautorizate sau nu sunt disponibile, în conformitate cu scopurile prelucrării acestora.

În situația în care acțiunile sau inacțiunile menționate mai sus nu duc la compromiterea DCP, rezultatul este o încălcare a prevederilor legale privind PDCP.

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
Mob: 0744423188
Birou: Clădirea Juventus, birou 4,
Parcul Sportiv "Iuliu Haţieganu"
dpo@ubbcluj.ro
www.ubbcluj.ro

Managementul incidentelor de securitate care implică DCP în cadrul UBB are în vedere parcurgerii mai multor etape care vizează semnalarea incidentului de securitate, numirea unei comisii de investigare a incidentului de securitate, investigarea preliminară a incidentului de securitate, notificarea incidentului de securitate, continuarea investigațiilor, finalizarea investigațiilor și gestionarea consecințelor incidentului de securitate.

a. Semnalarea incidentului:

Încălcarea securității DCP sau a măsurilor organizatorice sau tehnice implementate la nivelul UBB pe timpul derulării proiectului se semnalează de către orice salariat sau structură organizatorică a UBB, respectiv o persoană vizată sau entitate terță, telefonic și în scris, Responsabilului cu protecția datelor cu caracter personal al UBB (DPO), Raul-Ciprian Dăncuță (0744423188, dpo@ubbcluj.ro, 0264405300 - centrala UBB).

Sesizarea se va face în timpul cel mai scurt în succesiunea: telefon mobil (sau telefon fix - centrala UBB - solicitându-se legătura cu DPO) - e-mail (cu detalii).

b. Soluționarea incidentului:

DPO informează în timpul cel mai scurt conducerea UBB și trece la investigarea incidentului ajutat de personalul din structura unde s-a produs incidentul.

DPO prezintă datele și informațiile care au dus la suspiciunea existenței unui incident de securitate, o evaluare inițială a datelor cu caracter personal asupra cărora există suspiciunea compromiterii și structurile organizatorice implicate în fluxurile care conțin datele respective.

DPO prezintă opțiunile pentru soluționarea incidentului conducerii UBB.

Pentru informații suplimentare legate de Politica de securitate privind protecția datelor cu caracter personal a UBB CLUJ vă puteți adresa Responsabilului cu protecția datelor cu caracter personal (DPO) a UBB Cluj pe adresa dpo@ubbcluj.ro sau la telefonul +40.264.405.300, fax +40.264 591 906, tel mobil +40.744.423 188; corespondență scrisă pe adresa str Mihail Kogălniceanu nr 1, Cluj-Napoca, RO-400084 sau personal la birou DPO str Pandurilor nr 7 clădire Juventus biroul nr 4.

Responsabil cu protecția datelor
cu caracter personal la UBB Cluj (DPO UBB Cluj)
dr. Raul-Ciprian Dăncuță