

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. _____

din _____
Chișinău

pentru aprobarea Conceptului Sistemului informațional BeeProtect și a Regulamentului privind modul de funcționare și utilizare a Sistemului informațional BeeProtect

În temeiul art. 7, 9, 11, alin. (7) și 13, alin. (5), lit. a) din Legea apiculturii nr. 70/2006 (Monitorul Oficial al Republicii Moldova, 2010, nr. 247-251, art. 754), art. 22, lit. b), c) și d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), Guvernul HOTĂRĂȘTE:

1. Se instituie Sistemul informațional BeeProtect.
2. Se aprobă:
 - 1) Conceptul Sistemului informațional BeeProtect, conform anexei nr. 1;
 - 2) Regulamentul privind modul de funcționare și utilizare a Sistemului informațional BeeProtect, conform anexei nr. 2.
3. Agenția Națională pentru Siguranța Alimentelor:
 - 1) va asigura condițiile juridice, financiare și organizatorice necesare, precum și va asigura crearea, administrarea, mentenanța și dezvoltarea Sistemului informațional BeeProtect;
 - 2) va asigura utilizarea gratuită a Sistemului informațional BeeProtect de către apicultori și producătorii agricoli.
4. În scopul implementării prezentei hotărâri, Agenția Națională pentru Siguranța Alimentelor, va evalua anual costurile necesare administrării și dezvoltării continue a Sistemului informațional BeeProtect și va înainta propuneri de solicitare a mijloacelor financiare Ministerului Finanțelor în conformitate cu prevederile Legii finanțelor publice și responsabilității bugetar-fiscale nr. 181/2014, pentru a fi incluse în Legea bugetului de stat pe anul respectiv.

Prim-ministru

NATALIA GAVRILIȚĂ

Contrasemnează:

**Ministrul agriculturii
și industriei alimentare**

Vladimir Bolea

Ministrul finanțelor

Dumitru Budianschi

CONCEPTUL

Sistemului informațional BeeProtect

Capitolul I

DISPOZIȚII GENERALE

1. Sistemul informațional „BeeProtect” (în continuare – *BeeProtect*) este un sistem informațional de stat, sub formă de aplicație web, destinată utilizării de către apicultori, producătorii agricoli și utilizatorii produselor de uz fitosanitar și fertilizanților pentru protejarea albinelor de otrăviri cu produse de uz fitosanitar. BeeProtect asigură schimbul interactiv de informații între apicultori, producătorii agricoli și utilizatorii produselor de uz fitosanitar și fertilizanți și organele de control referitor la aplicarea produselor de uz fitosanitar și fertilizanți în procesul lucrărilor agricole/silvice și al amplasării stupinelor.

2. BeeProtect constituie o modalitate uniformă și continuă de expediere a notificărilor în cadrul sistemului informațional deținut de Agenția Națională pentru Siguranța Alimentelor (în continuare - ANSA), prin diverse canale de notificare, în scopul facilitării interacțiunii dintre apicultori, producători agricoli și utilizatori ai produselor de uz fitosanitar și fertilizanților.

3. BeeProtect reprezintă o soluție tehnologică compatibilă cu platforma tehnologică guvernamentală comună (MCloud) și este destinat furnizării eficiente către ANSA și administrația publică locală de nivelul I (în continuare - APL) a platformelor informatice de nivel central și a altor sisteme informaționale relevante, inclusiv date furnizate de către apicultori, producători agricoli și utilizatori a produselor de uz fitosanitar și fertilizanților, cu scopul realizării interoperabilității și asigurării accesului instant, care va contribui la digitizarea funcțiilor ANSA.

4. În sensul prezentului Concept vor fi utilizate următoarele noțiuni de bază:

1) *BeeProtect* – reprezintă o interfață pentru utilizator, unde oricare din utilizatorii sistemului informațional, în funcție de drepturile de acces stabilite, gestionează date în conformitate cu contururile funcționale implementate în BeeProtect;

2) *resursă BeeProtect* – reprezintă un set de obiecte informaționale al aplicației BeeProtect formate din totalitatea atributelor asupra cărora utilizatorii acestuia pot efectua operații de citire, de modificare sau de suprimare. Vor fi distinse două tipuri de resurse:

a) *externe*, furnizate de sistemele informaționale externe prin intermediul

platformei de interoperabilitate (MConnect) și prin inserările făcute de utilizatorii producători agricoli și apicultori;

b) *locale*, reprezintă obiecte informaționale constituite și păstrate în stocul local de date al aplicației BeeProtect;

3) *utilizator producător agricol* – persoană fizică sau juridică care activează în sectorul agricol și care efectuează lucrări de aplicare a produselor de uz fitosanitar și fertilizanți în procesul lucrărilor agricole și silvice, care are obligația de a notifica APL de nivelul I pe teritoriul căreia au loc lucrările de aplicare a produselor respective, precum și a notifica apicultorii amplasați pe teritoriul acelui APL, conform Legii nr. 70/2006 și a Codului contravențional;

4) *utilizator apicultor* – persoană fizică sau juridică care activează în sectorul de producere a mierii de albine, care are obligația de a notifica APL de nivel I pe teritoriul căreia își amplasează sau își scoate stupina în/din staționar sau pastoral.

5. Destinația BeeProtect este implementarea unei soluții informatice interconectate cu toate sursele de date relevante externe, care vor furniza în regim automatizat datele necesare pentru susținerea activităților relevante ANSA și APL de nivelul I. De asemenea, BeeProtect urmează să asigure accesul public la seturi de date pentru a fi consumate în regim automatizat de aplicații externe în vederea prelucrării lor și furnizării de valoare adăugată.

6. Scopul aplicației BeeProtect constă în asigurarea ANSA, APL de nivelul I și a celorlalți utilizatori cu o soluție informatică (scalabilă, configurabilă, conectată la resursele informaționale de stat și compatibilă cu ulterioarele dezvoltări și integrări), care va facilita evidența notificărilor făcute prin intermediul BeeProtect de către utilizatorii producători agricoli și apicultori, precum și va asigura accesul imediat la date prin interoperabilitatea cu resursele informaționale de stat. BeeProtect va oferi un model tehnologic de referință și interfețe program pentru scalarea sistemelor informaționale de la nivelul central ANSA la nivelul local pentru subdiviziunile teritoriale ANSA și APL de nivelul I.

7. Obiectivele BeeProtect sunt:

1) implementarea unei soluții tehnologice din categoria Guvern către Guvern și Guvern către Business, compatibilă cu platforma tehnologică guvernamentală comună (MCloud) în sensul scalării la nivelul subdiviziunilor teritoriale ANSA și a APL de nivelul I a sistemelor informaționale relevante disponibile la nivel central și a celor din spațiul funcțional al BeeProtect care urmează să fie dezvoltate ulterior;

2) reutilizarea sistemelor informaționale partajate și a sistemelor informaționale de stat pentru raționalizarea procesului de prestare a serviciilor ANSA și pentru digitalizarea evidenței notificărilor utilizatorilor agricultori și apicultori de către ANSA și APL de nivelul I;

3) reducerea costurilor operaționale, sporirea calității mijloacelor de comunicare și asigurarea accesului rapid la date prin elaborarea unei soluții care poate fi ușor accesată de către aparatul central ANSA, subdiviziunile teritoriale ANSA, APL de nivelul I, utilizatorii producători agricoli și apicultori;

4) asigurarea scalabilității prin implementarea unei soluții informatice configurabile, cu o arhitectură orientată spre servicii care vor permite actualizări viitoare după modelul de dezvoltare iterativă;

5) celeritatea transmiterii/recepționării notificărilor, astfel, încât destinatarii acestora să afle în timp real informațiile referitoare la aplicarea produselor de uz fitosanitar și a fertilizanților în procesul lucrărilor agricole/silvice și a amplasării stupinelor.

8. Pentru asigurarea obiectivelor înaintate soluției informatice, la re-proiectarea, completarea și implementarea BeeProtect trebuie să se țină cont de următoarele principii de bază:

1) *legalitate*, care presupune crearea și exploatarea sistemului informațional în conformitate cu cadrul normativ național, precum și cu normele și standardele internaționale recunoscute în domeniu;

2) *divizarea arhitecturii pe nivele*, constă în proiectarea independentă a subsistemelor BeeProtect în conformitate cu standardele de interfață dintre nivele;

3) *arhitectura bazată pe servicii*, constă în distribuirea funcționalității aplicației în unități mai mici, distincte, numite servicii, care pot fi distribuite într-o rețea și pot fi utilizate împreună pentru a crea aplicații destinate implementării funcțiilor de business ale sistemului informațional;

4) *expansibilitate*, care oferă posibilitatea lărgirii și completării sistemului informațional cu noi funcții sau îmbunătățirea celor existente;

5) *scalabilitate*, care presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului informațional;

6) *securitate prin design*, care presupune integrarea BeeProtect în sistemele de servicii electronice de stat, în cunoștință de cauză cu privire la riscurile de securitate a informației ce pot afecta buna funcționare a acesteia. Cerințele legale aplicabile pentru implementarea mecanismelor de asigurare a securității informației trebuie luate în considerare la etapa de re-proiectare, completare și integrare a BeeProtect. BeeProtect va asigura accesarea controlată, transparentă și responsabilă a datelor;

7) *date sigure*, care prezumă introducerea datelor în sistem doar prin canalele autorizate și autentificate;

8) *simplitatea și comoditatea utilizării*, care presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor sistemului, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție;

9) *furnizarea datelor doar o singură dată (once only)*, care presupune că

beneficiarii de servicii publice furnizează datele solicitate autorităților/instituțiilor publice o singură dată, iar acestea sunt obligate să se asigure că datele sunt reutilizabile și că pot fi accesate de toți prestatorii de servicii publice, în limitele competențelor și în scopul prestării serviciilor;

10) *auto-servire*, constă în delegarea funcțiilor administrative, de configurare și control către persoanele-cheie din cadrul ANSA, evitând în acest sens concentrarea funcției și puterii într-un punct central și, în același timp, evitând crearea blocajelor și a unor puncte unice de eșec;

11) *implementarea unei soluții client-server „Web based”* cu acces autorizat la interfață și la date.

9. Implementarea BeeProtect va furniza ANSA, APL de nivelul I, utilizatorilor producători agricoli și apicultori un instrument eficient ca punct unic de intrare și acces la resursele informaționale de stat. Sarcinile principale ale BeeProtect sunt următoarele:

1) implementarea unei soluții tehnologice compatibile cu platforma tehnologică guvernamentală comună (MCloud), care să asigure acces centralizat pentru ANSA, APL de nivelul I, utilizatorilor producători agricoli și apicultori la sisteme informaționale de stat. Asigurarea unei interfețe pentru accesarea de către utilizatori a sistemelor și a serviciilor electronice disponibile pentru evidența notificărilor între utilizatori;

2) asigurarea accesării sistemelor informaționale de la nivelul oficiului central ANSA prin care subdiviziunile teritoriale ANSA și APL de nivelul I vor obține drepturile necesare pentru gestiunea datelor aferente obiectelor informaționale ale BeeProtect;

3) implementarea mecanismelor de integrare a BeeProtect cu soluțiile informatice și cu registrele de la nivel central și ANSA pentru facilitarea schimbului de date între utilizatori și alte entități publice;

4) dezvoltarea facilităților de configurare a drepturilor de acces la date și înregistrarea acestora în resursele informaționale de stat, precum și alte soluții informatice cu scopul realizării funcțiilor de business ale ANSA și APL de nivelul I;

5) asigurarea accesului la date privind serviciile publice prestate de ANSA și alte servicii de stat prin furnizarea datelor pentru emiterea și deținerea pașapoartelor electronice ale stupinelor.

Capitolul II

Cadrul normativ al BeeProtect

10. Cadrul normativ pentru instituirea BeeProtect este constituit din următoarele acte:

- 1) Legea nr. 982/2000 privind accesul la informație;
- 2) Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;
- 3) Legea nr. 71/2007 cu privire la registre;

- 4) Legea nr. 239/2008 privind transparența în procesul decizional;
- 5) Legea nr. 133/2011 privind protecția datelor cu caracter personal;
- 6) Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;
- 7) Legea nr. 234/2021 cu privire la serviciile publice;
- 8) Hotărârea Guvernului nr. 272/2002 despre măsurile privind crearea sistemului informațional automatizat “Registrul de stat al unităților de drept”;
- 9) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;
- 10) Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- 11) Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
- 12) Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
- 13) Hotărârea Guvernului nr. 375/2020 privind platforma tehnologică guvernamentală comună (MPower);
- 14) Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);
- 15) Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;
- 16) Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);
- 17) Regulamentul privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcționarii persoanelor juridice de drept public în cadrul circulației electronice ale acestora, aprobat prin Hotărârea Guvernului nr. 1141/2017;
- 18) Regulamentul privind modul de ținere a Registrului împuternicirilor de reprezentare în baza semnăturii electronice, aprobat prin Hotărârea Guvernului nr. 375/2020;
- 19) Regulamentul privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify), aprobat prin Hotărârea Guvernului nr. 376/2020;
- 20) Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123/2010;

21) Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017;

22) Reglementarea tehnică „Procese ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006;

23) Metodologia publicării datelor guvernamentale deschise, aprobată prin Hotărârea Guvernului nr. 701/2014;

24) Regulamentul privind administrarea conținutului portalului guvernamental unic al serviciilor public și integrarea în portal a serviciilor publice electronice, aprobat prin Hotărârea Guvernului nr. 657/2012.

Capitolul III

Spațiul funcțional al BeeProtect

11. ANSA dispune de o multitudine de competențe, iar prezentul Concept stabilește mecanismele de bază prin care va fi asigurată furnizarea eficientă a resurselor informaționale pentru îndeplinirea atribuțiilor ANSA, a subdiviziunilor teritoriale ANSA, APL de nivelul I, precum și a obligațiilor utilizatorilor producători agricoli și apicultori de a proteja albinele de intoxicații cu produse de uz fitosanitar și fertilizanți în procesul lucrărilor agricole/silvice și de amplasare a stupinelor. Pentru asigurarea spațiului funcțional, BeeProtect va oferi instrumente tehnologice de integrare a soluțiilor informatice de stat existente la nivel central, inclusiv celor care urmează a fi dezvoltate pe parcurs, cu scopul scalării acestora la nivelul oficiului central și subdiviziunilor teritoriale ANSA, APL de nivelul I, utilizatorii producători agricoli și apicultori. Nivelul de cooperare a resurselor informaționale BeeProtect (interogate atât din surse externe, cât și locale) va îndeplini funcția de suport pentru realizarea sarcinilor ANSA și a subdiviziunilor sale teritoriale prin instrumentele puse la dispoziție de aplicațiile implementate în interfața utilizator BeeProtect.

12. BeeProtect trebuie să asigure realizarea funcțiilor de bază ale unui sistem informațional prevăzute în cadrul normativ, precum și a funcțiilor specifice care rezultă din destinația sistemului. În BeeProtect se vor implementa următoarele componente funcționale de bază:

1) gestionarea resurselor informaționale prin intermediul interfeței utilizator BeeProtect – prin intermediul căreia utilizatorii lansează aplicațiile implementate în sistem pentru a obține acces și a gestiona resursele informaționale disponibile. Această componentă va furniza instrumente necesare pentru căutarea, vizualizarea și descărcarea datelor relevante necesităților utilizatorilor în baza unei interogări definite de utilizator și a drepturilor de acces oferite. În funcție de interogare, BeeProtect va încărca datele din baza de date locală și va realiza interpelările necesare pentru a prelua date din sistemele

informaționale externe;

2) gestionarea înregistrărilor – reprezintă setul de funcționalități implementate în aplicațiile BeeProtect și disponibile utilizatorilor în funcție de drepturile de acces ale acestora. Utilizatorii vor putea lansa interogări pentru a obține detalii suplimentare despre unele obiecte informaționale. Gestionarea datelor va fi realizată în conformitate cu operațiunile permise asupra resurselor informaționale. Astfel, unele resurse vor admite doar operațiuni de accesare a datelor pentru citire, iar altele vor permite operațiuni de descărcare, inclusiv de creare sau de suprimare a datelor;

3) administrarea și funcționalități de sistem – reprezintă o componentă funcțională a BeeProtect, care furnizează funcționalitățile-cheie de administrare, de configurare și de control al accesului. Având în vedere modelul de partajare a funcționalităților BeeProtect între ANSA, subdiviziunile teritoriale ANSA, APL de nivelul I, utilizatorii producători agricoli și apicultori după principiul autoservirii, acest contur funcțional oferă pentru utilizatorii cu drepturi de administrare următoarele instrumente:

a) gestionarea drepturilor de acces la resursele BeeProtect – pentru a configura accesul utilizatorilor la resursele informaționale prin intermediul aplicațiilor disponibile în BeeProtect. ANSA va dispune de instrumente de configurare a accesului la setul de resurse informaționale necesare și disponibile în BeeProtect. ANSA va putea configura spațiul de lucru în BeeProtect cu setul de funcționalități oportune și va putea ulterior adăuga alte funcționalități;

b) gestiunea utilizatorilor și rolurilor – care implementează funcționalitățile destinate gestiunii profilurilor utilizatorilor și alocării drepturilor de acces la resursele și datele BeeProtect. Aceasta va furniza funcționalitățile necesare gestiunii grupurilor/rolurilor și atribuirea drepturilor de acces utilizatorilor BeeProtect. Drepturile de acces la aplicațiile și la resursele informaționale ale BeeProtect vor fi acordate grupului/rolului aferent utilizatorului sau explicit fiecărui utilizator în parte;

c) administrarea centralizată a metadatelor;

d) asigurarea continuității de funcționare sau restabilirea funcționării BeeProtect.

13. Funcționalitățile de bază ale BeeProtect sunt:

1) Formarea repozitorului de date (baza de date) necesare pentru susținerea activității ANSA și a utilizării utile de către producătorii agricoli, apicultorii și autoritățile publice – funcții de introducere a datelor, modificări și/sau ștergeri, arhivare ale acestora. Funcțiile de bază în procesul de formare a bazei de date a BeeProtect sînt următoarele:

a) de înregistrare - înregistrarea inițială a obiectelor informaționale se efectuează automat la introducerea datelor proprii de către acestea. Totodată, fiecărui obiect informațional luat în evidență i se atribuie un identificator unic, care rămâne neschimbat pe toată perioada existenței obiectului în sistem;

b) de adăugare date de către obiectele informaționale - după înregistrare, obiectul

informațional adaugă date specifice adăugătoare, care rămân neschimbate până când nu sunt actualizate de către obiectul informațional;

c) de actualizare a datelor - actualizarea datelor BeeProtect constă în reînnoirea datelor proprii de către obiectele informaționale în cazul schimbării sau completării atributelor obiectelor de evidență;

d) de stocare și structurare a datelor - datele introduse de către obiectele informaționale sunt menținute și structurate în baza de date a BeeProtect;

e) de generare a rapoartelor - obiectul informațional generează rapoarte în baza datelor din sistem. Informațiile din baza de date a BeeProtect sunt oferite în funcție de nivelul de acces stabilit. Beneficiarii datelor din sistem sunt obligați să le folosească doar în scopuri legale;

f) de scoatere din evidență a obiectelor informaționale (schimbarea statutului obiectului) - scoaterea din evidență a obiectului informațional constă în schimbarea automată a statutului obiectului, în baza condițiilor de utilizare, prin aplicarea unei mențiuni speciale, fapt care nu semnifică eliminarea fizică a datelor despre obiect;

g) informația se șterge fizic numai după expirarea termenului de păstrare a informației în arhiva electronică (10 ani).

4) Generarea de Rapoarte pentru administrator, sub-diviziuni teritoriale, primării, utilizatori apicultori, producători agricoli, prestatori de servicii de aplicare a produselor de uz fitosanitar și fertilizanți. Sistemul are un modul care permite realizarea de rapoarte analitice sau statistice, în funcție de rolul și responsabilitățile fiecărui utilizator:

a) asigurarea accesului la rapoarte prin intermediul pupitrelor de control a utilizatorilor, inclusiv rapoarte privind logările (pentru Administrator);

b) asigurarea aplicării filtrelor în baza seturilor de date pentru care este oferit acces;

c) generarea fișierelor rapoartelor și asigurarea posibilității de descărcare conform accesului și a drepturilor atribuite de Administrator.

5) Organizarea accesului la date. Datele conținute în stocul de date a BeeProtect sunt puse la dispoziția ANSA, persoanelor fizice și juridice, pentru organizarea procesului de schimb informațional. Fiecare utilizator de date ale sistemului urmează să utilizeze aceste date numai în scopuri legale în conformitate cu drepturile utilizatorului.

6) Utilizarea instrumentelor interactive de lucru cu harta:

a) căutarea locației;

b) mărire, micșorare, navigare pe hartă;

c) delimitarea suprafețelor de teren spre prelucrare cu atribuirea perimetrului;

d) alegerea tipului de hartă utilizată;

e) efectuarea măsurărilor pe hartă;

f) vizualizarea granițelor parcelelor de teren și a numerelor cadastrale;

g) vizualizarea amplasării culturilor cu inflorescențe pe hartă;

h) amplasarea pe hartă și radierea locației stupinei.

- 7) Expediere notificări, realizate, cel puțin, prin următoarele canale de notificare:
- a) poșta electronică (e-mail);
 - b) serviciul mesaje scurte (sms);
 - c) aplicația Viber (printr-un ViberBot)
 - d) jurnalizare evenimente de notificare.

8) Schimb de date cu sistemele informaționale externe – realizat prin consumarea interfețelor destinate schimbului reciproc de date prin platforma de interoperabilitate (MConnect), precum și integrarea sistemelor informaționale partajate (MPass, MSign, MPower, MNotify, MLog).

9) Executare proceduri automate – reprezintă funcționalități de declanșare și funcționare în regim automat a unui șir de funcționalități ale BeeProtect în vederea utilizării raționale a resurselor server, a lansării serviciilor specifice funcționării acestuia și a furnizării la momentul oportun a datelor pentru utilizatori.

14. Funcțiile BeeProtect, determinate de destinația acestora, sunt grupate în următoarele contururi funcționale (module):

1) administrarea, verificarea, monitorizarea și controlul acțiunilor obiectelor informaționale:

- a) asigurarea integrității logice a BeeProtect;
- b) administrarea bazelor de date ale BeeProtect;
- c) delimitarea drepturilor de acces pentru utilizatori, introducerea sistemului de parole;
- d) asigurarea securității, protecției și păstrării informației în sistem conform standardelor internaționale SM ISO/CEI 27002 „Tehnologii informaționale. Cod de bună practică pentru managementul securității informaționale” și SM ISO/CEI 15408 „Tehnologii Informaționale. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației”;
- e) asigurarea respectării cerințelor BeeProtect privind protecția datelor cu caracter personal.

2) Gestionarea împuternicirilor pentru prestarea serviciilor de către personalul Oficiului central ANSA și a subdiviziunilor teritoriale:

- a) importul împuternicirilor de reprezentare din MPower;
- b) gestionarea (crearea, modificarea și radierea) tipurilor de împuterniciri;
- c) verificarea validității împuternicirii de reprezentare;
- d) evidența verificărilor validității împuternicirilor de reprezentare.

3) Înregistrarea datelor proprii de către fiecare tip de utilizator:

- a) completarea datelor la înregistrarea în BeeProtect;
- b) introducerea datelor adăugătoare solicitate de sistem pentru lansarea utilizării anumitor funcționalități;
- c) poziționarea locației pe hartă a câmpului prelucrat sau stupinei a obiectului

informațional.

4) Logarea în BeeProtect, precum și asigurarea logării utilizatorilor în BeeProtect.

5) Emiterea și gestionarea pașaportului electronic al stupinei:

a) completarea pașaportului cu datele cerute la înregistrarea în BeeProtect;

b) verificarea solicitării și a datelor introduse de solicitant, asigurarea completării datelor;

c) eliberarea numărului pașaportului electronic al stupinei;

d) generarea automată a fișierului electronic descarcabil al pașaportului electronic al stupinei, cu toate înscrisurile provenite din baza de date a BeeProtect;

e) asigurarea aplicării semnăturii digitale a emitentului și a sub-diviziunii teritoriale pe fișierul electronic al pașaportului electronic al stupinei;

f) asigurarea efectuării înscrisurilor periodice în pașaportul electronic al stupinei de către deținătorul pașaportului și de către inspectorii ANSA prin ferestre dedicate.

6) Gestionarea documentelor, care asigură funcții de evidență a:

a) documentelor de intrare;

b) documentelor tehnologice;

c) documentelor de ieșire.

15. BeeProtect va oferi o interfață ergonomică, intuitivă și accesibilă tuturor tipurilor de utilizatori prin intermediul unui explorator Web. Interfața utilizator a BeeProtect va reprezenta un design grafic, echilibrat, distinct și adaptabil pentru majoritatea dispozitivelor utilizate (calculator desktop, notebook, tabletă, smartphone).

16. BeeProtect va furniza o interfață în limba română.

17. Pentru facilitarea utilizării BeeProtect, soluția informatică va dispune de un ghid de utilizare, disponibil online la nivelul fiecărei interfețe utilizator.

18. În funcție de categoriile utilizatorilor (drepturile și rolurile acestora), BeeProtect va furniza o interfață personalizată fiecărei categorii de utilizator și aplicații.

1) Utilizatorii sistemului informațional vor dispune de câteva nivele de acces la interfața utilizator și date (seturile de drepturi și roluri atribuite acestora, precum și numărul optim de grupuri de acces vor putea fi configurate de administratorul de sistem) și anume:

a) *administrator de sistem* – nivel caracteristic utilizatorului cu privilegii de administrare a accesului, configurare, audit și depănare în cadrul BeeProtect. Acest nivel de acces, dat fiind rolul său de a administra buna funcționare a soluției informatice, va asigura accesul la toate funcționalitățile interfeței utilizator și conținutul bazei de date livrate de interfața utilizator;

b) *funcționar ANSA din oficiul central și din subdiviziunile teritoriale* – nivel de acces asigurat funcționarilor ANSA care va oferi funcționalități specifice necesare pentru gestiunea resurselor informaționale BeeProtect și asigurarea accesului automat la interfața utilizator a sistemelor informaționale externe, din care face parte și controlul

accesului la aplicațiile implementate în BeeProtect. Funcționarul ANSA va dispune de acces la interfața utilizator BeeProtect și funcționalitățile oferite de aceasta în funcție de drepturile de acces configurate în BeeProtect. În funcție de specificul și necesitățile oficiului central ANSA și a subdiviziunilor teritoriale, BeeProtect va permite configurarea rolurilor distincte pentru funcționarii oficiului central ANSA, șefii subdiviziunilor teritoriale, a inspectorilor teritoriali, etc;

c) *funcționar APL de nivelul I* - nivel de acces asigurat angajaților din APL de nivelul I, cu privilegii specifice pentru vizualizarea informației corespunzător rolului său și în perimetrul de date al APL pe care îl reprezintă;

d) *utilizator de sistem* – nivel de acces asigurat utilizatorilor apicoli și producători agricoli pentru introducerea și actualizarea datelor, precum și vizualizarea informației și a notificărilor, inclusiv din surse externe;

19. Utilizatorii sistemului informațional – apicultorii sau producătorii agricoli, care vor plasa informații de avertizare privind plasarea stupinelor, respectiv utilizarea produselor de uz fitosanitar și fertilizanți, au, astfel, o calitate dublă, după caz, de expeditor, fie destinat al notificărilor.

Capitolul IV

Structura organizațională a BeeProtect

20. Funcțiile de bază privind formarea și exploatarea BeeProtect sunt divizate între:

- 1) proprietarul sistemului;
- 2) posesorul sistemului;
- 3) deținătorul sistemului;
- 4) utilizatorii sistemului;
- 5) administratorul tehnic al sistemului.

21. Proprietarul sistemului informațional BeeProtect este statul care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din acesta. Resursele financiare pentru dezvoltarea sistemului informațional sunt asigurate din bugetul de stat, din proiecte de asistență internațională și din alte mijloace financiare, conform cadrului normativ.

22. Posesorul și deținătorul BeeProtect este Agenția Națională pentru Siguranța Alimentelor. Rolul de posesor al sistemului reflectă aspectul administrativ ce ține de competențele deținute și necesare administrării și dezvoltării continue a sistemului informațional. Agenția va fi responsabilă de dezvoltarea și de implementarea BeeProtect, iar beneficiarii finali ai acesteia vor fi ANSA, inclusiv subdiviziunile teritoriale ANSA, APL de nivelul I și mediul de afaceri din sectorul agricol și apicol. Deținătorul BeeProtect asigură crearea, administrarea, mentenanța și dezvoltarea sistemului informațional.

23. Utilizatorii BeeProtect sunt funcționarii și angajații ANSA, ai APL de nivelul

I, apicultorii și producătorii agricoli, care vor utiliza funcționalitățile sistemului informațional în scopurile prevăzute de prezentul Concept. Nivelul de acces al utilizatorilor este diferențiat în funcție de atribuțiile, responsabilitățile, drepturile de acces la date și se configurează de către administratorul BeeProtect. Gestionarea resurselor informaționale furnizate prin intermediul BeeProtect va fi realizată în funcție de perimetrul de date la care un utilizator are acces sigur și în conformitate cu serviciile externe pentru datele captate.

24. Registratorul datelor în BeeProtect este ANSA prin intermediul oficiului central și a subdiviziunilor teritoriale. Ca posesor a resursei și sistemului informațional, ANSA va asigura înscrierea, actualizarea și radierea resurselor și a informațiilor aferente acestora.

25. Furnizorii de date care vor livra date aferente obiectelor informaționale ale BeeProtect sunt:

- a) apicultorii și producătorii agricoli;
- b) oficiul central și subdiviziunile teritoriale ale ANSA.

26. Destinatarii datelor din BeeProtect sunt:

- a) ANSA (oficiul central și subdiviziunile teritoriale);
- b) producătorii agricoli și apicultorii.

27. Administratorul tehnic al BeeProtect este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care își exercită atribuțiile în conformitate cu Regulamentul privind administrarea tehnică și menținerea resurselor și sistemelor informaționale de stat, aprobat prin anexa nr. 5 la Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat.

Capitolul V

Documentele BeeProtect

28. În funcție de faza procesului de executare, documentele de bază ale BeeProtect se clasifică, după cum urmează:

- 1) documente de intrare, precum:
 - a) introducerea și confirmarea în BeeProtect de către producătorul agricol a datelor privind evenimentul de aplicare planificată sau anulare a aplicării produselor de uz fitosanitar sau fertilizanților;
 - b) introducerea și confirmarea în BeeProtect de către apicultor a datelor privind evenimentul de amplasare sau ștergere a stupinei;
 - c) solicitări din partea apicultorului privind eliberarea pașaportului electronic al stupinei;

d) solicitări din partea subdiviziunilor teritoriale ANSA către oficiul central ANSA privind eliberarea numărului de pașaport al stupinei și emiterea pașaportului electronic al stupinei.

2) documente de ieșire, precum:

a) notificarea privind înregistrarea sau anularea evenimentul de aplicare planificată sau anulare a aplicării produselor de uz fitosanitar sau fertilizanților;

b) notificarea privind evenimentul de amplasare sau ștergere a unei stupine;

c) emiterea pașaportul electronic al stupinei semnat prin MSign de către Oficiul Central ANSA;

d) extrase din baza de date și rapoartele analitice și sintetice generate în baza filtrelor alese,

3) documente tehnologice, care includ:

a) semnăturile documentelor și înregistrărilor semnate electronic;

b) certificatele electronice cu care au fost produse semnăturile electronice;

c) imaginile scanate ale documentelor;

d) lista utilizatorilor și drepturilor acestora;

e) înregistrările de audit ale activității sistemului și utilizatorilor;

f) versiunile documentelor și istoricul modificărilor;

g) documentele tehnologice privind parametrii de sistem;

h) rapoartele și statisticile agregate privind utilizarea sistemului;

i) ghidul de utilizare;

j) termenii și condițiile de utilizare;

k) politica privind Cookies.

Capitolul VI

Spațiul informațional al BeeProtect

29. Spațiul informațional al BeeProtect este format din totalitatea resurselor informaționale cuprinse în gama de responsabilități ale ANSA. Aceste resurse pot fi atât locale, cât și externe (interpelate din sisteme informaționale externe pentru a fi gestionate local, actualizate în resursele externe și la necesitate salvate temporar în baza de date BeeProtect).

30. Ținând cont de scopul și de obiectivele BeeProtect, au fost identificate obiectele informaționale de care trebuie să se țină cont la re-proiectarea, completarea și integrarea sistemului.

Orice modificare a datelor – creare, modificare, ștergere, schimbare statut etc. trebuie să fie înregistrată într-un registru special (fișiere log) arătând momentul de timp și utilizatorul care a efectuat modificarea.

Identificarea obiectelor informaționale în cadrul BeeProtect se efectuează prin utilizarea, pentru fiecare dintre ele, a unui cod de identificare unic, inclusiv a celui atribuit

la formarea/înregistrarea primară a obiectului informațional în cadrul stocului de date al BeeProtect sau în cadrul altor sisteme informaționale furnizoare de date, în scopul realizării sarcinilor sistemului informațional.

31. Obiectele informaționale de bază, care reprezintă resursa informațională a BeeProtect, se determină în funcție de destinația acestora și includ:

- a) Oficiul Central ANSA (posesor, deținător, registrator și furnizor de informație);
- b) subdiviziunea teritorială ANSA (furnizor de informație);
- c) apicultorul sau producătorul agricol (furnizor de informație);
- d) pașaportul electronic al stupinei (furnizor de informație).

32. Obiectele informaționale vor fi validate prin intermediul următorilor identificatori:

- a) identificator al obiectului informațional „Oficiul Central ANSA” este numărul de identificare de stat al persoanei juridice (IDNO);
- b) identificator al obiectului informațional „Subdiviziunea teritorială ANSA” este numărul de identificare de stat al persoanei juridice (IDNO);
- c) identificator al obiectului informațional „Apicultorul sau producătorul agricol” este numărul de identificare de stat al persoanei juridice (IDNO);
- d) identificator al obiectului informațional „Rapoarte personalizate” este constituit dintr-un cod alfanumeric, generat în mod aleatoriu de BeeProtect;
- e) identificatorul obiectului informațional „Pașaportul electronic al stupinei” îl constituie un cod alfanumeric, generat în mod aleatoriu de BeeProtect pentru pașaportul electronic stupină, iar ”numărul” reprezintă numărul atribuit de ANSA pentru pașaportul stupinei.

33. Scenariile de bază reprezintă lista evenimentelor aferente obiectelor informaționale aferente BeeProtect și sunt următoarele:

1) Scenarii referitoare la obiectul informațional „Oficiul Central ANSA”:

- a) punerea inițială la evidență – realizată de către registrator:
 - la aprobarea actului juridic, care determină necesitatea creării obiectului informațional;
 - la înscrierea obiectului informațional deja existent.

b) actualizarea datelor – realizată de către registrator, la necesitatea modificării sau completării informației despre obiectul informațional;

c) scoaterea din evidență – de către registrator, în cazul lichidării obiectului informațional.

2) Scenarii referitoare la obiectul informațional „Subdiviziunea teritorială ANSA”:

- a) punerea inițială la evidență – realizată de către registrator:
 - la aprobarea actului juridic, care determină necesitatea creării obiectului informațional;
 - la înscrierea obiectului informațional deja existent.

b) actualizarea datelor – realizată de către registrator, la necesitatea

modificării sau completării informației despre obiectul informațional;

c) scoaterea din evidență – de către registrator, în cazul scoaterii din exploatare a obiectului informațional.

3) Scenarii referitoare la obiectul informațional „Apicultorul sau producătorul agricol”:

a) punerea inițială la evidență – realizată de către apicultorul sau producătorul agricol la înregistrarea acestora în BeeProtect;

b) actualizarea datelor – realizată de către apicultor sau producătorul agricol, la necesitatea modificării sau completării informației despre obiectul informațional;

c) scoaterea din evidență – de către registrator, în cazul scoaterii din exploatare a obiectului informațional.

4) Scenarii referitoare la obiectul informațional „Pașaportul electronic al stupinei”:

a) punerea inițială la evidență – realizată de către registrator la emiterea pașaportului electronic stupină în BeeProtect;

b) actualizarea datelor – realizată de către apicultor sau producătorul agricol și subdiviziunea teritorială ANSA la necesitatea modificării sau completării informației despre obiectul informațional;

c) scoaterea din evidență – de către registrator, în cazul scoaterii din exploatare a obiectului informațional.

34. Fluxul de date aferent mecanismului de interoperabilitate al BeeProtect este descris în Figura 1. Acesta cuprinde procesele de furnizare a datelor de către utilizatori și interpelare din surse externe, combinarea acestora și formarea obiectelor informaționale specifice BeeProtect, precum și procesul de gestiune a resurselor acestuia prin intermediul interfeței utilizator sau prin furnizarea lor către sisteme informaționale externe prin intermediul platformei de interoperabilitate (MConnect). BeeProtect va recepționa/actualiza datele necesare din surse oficiale exclusiv prin intermediul platformei de interoperabilitate (MConnect).

Indiferent de sursă, toate datele interpellate din exterior vor fi trecute printr-un proces de mapare la obiecte informaționale specifice BeeProtect și, în caz de necesitate, vor fi combinate date din surse diferite. De asemenea, structurile de date recepționate vor fi adaptate în conformitate cu schema relațională a bazei de date BeeProtect pentru a facilita gestionarea datelor în interfața utilizator a sistemului informațional. În urma acestui proces de extragere-transformare, obiectele informaționale vor fi stocate, după caz, temporar sau permanent în baza de date BeeProtect.

35. Structurile de date cu care va opera BeeProtect vor fi formate din următoarele tipuri de date:

1) clasificatoare și nomenclatoare;

2) tabele de corespondență utilizate de mecanismul de adaptare a structurilor de date furnizate de sistemele informaționale externe la structurile obiectelor informaționale

gestionate de BeeProtect;

3) registre locale;

4) structuri de date recepționate din surse externe.

36. Conform diagramei fluxului de date din Figura 1, BeeProtect va permite utilizarea datelor din stocul său de date prin intermediul facilităților furnizate de interfața utilizator și accesibile utilizatorilor BeeProtect. Interfața utilizator BeeProtect va furniza mai multe aplicații specifice prin intermediul cărora utilizatorii vor avea acces la instrumente de gestiune a datelor (citire, actualizare, creare și ștergere). La actualizarea datelor, în funcție de resursa accesată, BeeProtect va interpela interfețele specifice pentru a actualiza datele în sistemele informaționale externe sau/și le va salva în stocul de date local.

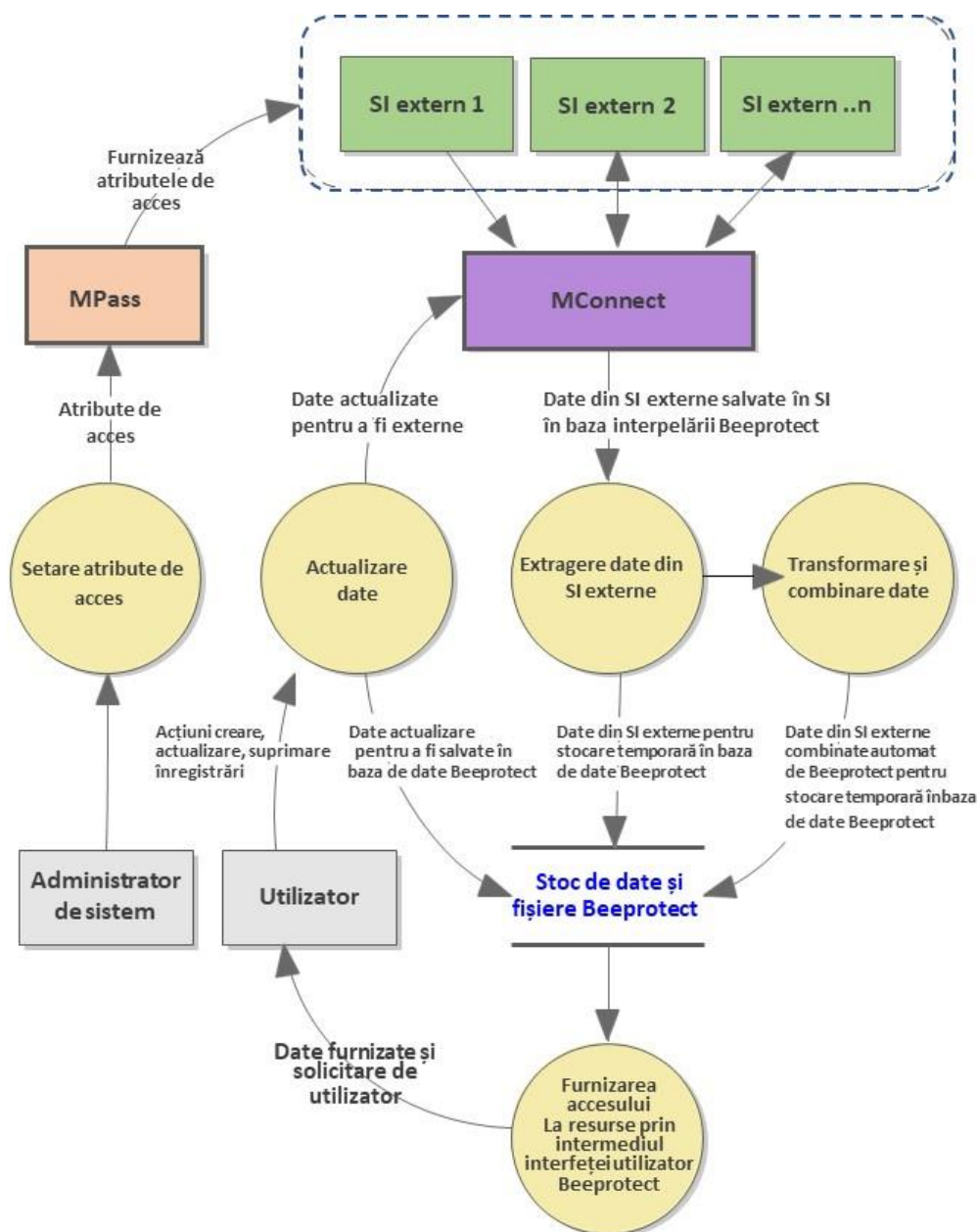


Figura 1. Fluxurile de date în cadrul spațiului funcțional al BeeProtect

37. Integrarea cu alte sisteme informaționale a BeeProtect presupune implementarea unui mecanism de interoperabilitate cu următoarele sisteme informaționale:

- 1) Registrul de stat al unităților de drept;
- 2) Registrul de stat al populației;
- 3) Registrul de stat al unităților administrativ-teritoriale și al adreselor;
- 4) Registrul produselor de uz fitosanitar și al fertilizanților (www.pesticide.md);
- 5) Platforma de interoperabilitate (MConnect);
- 6) Serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- 7) Serviciul electronic guvernamental integrat de semnătură electronică (MSign);
- 8) Serviciul guvernamental de notificare electronică (MNotify);
- 9) Serviciul electronic guvernamental de jurnalizare (MLog);
- 10) Portalul guvernamental unic de date deschise (www.date.gov.md);
- 11) Portalul serviciilor publice (www.servicii.gov.md).

Figura 2 ilustrează modelul indicativ pentru realizarea mecanismului de integrare a sistemelor informaționale externe cu platforma BeeProtect.

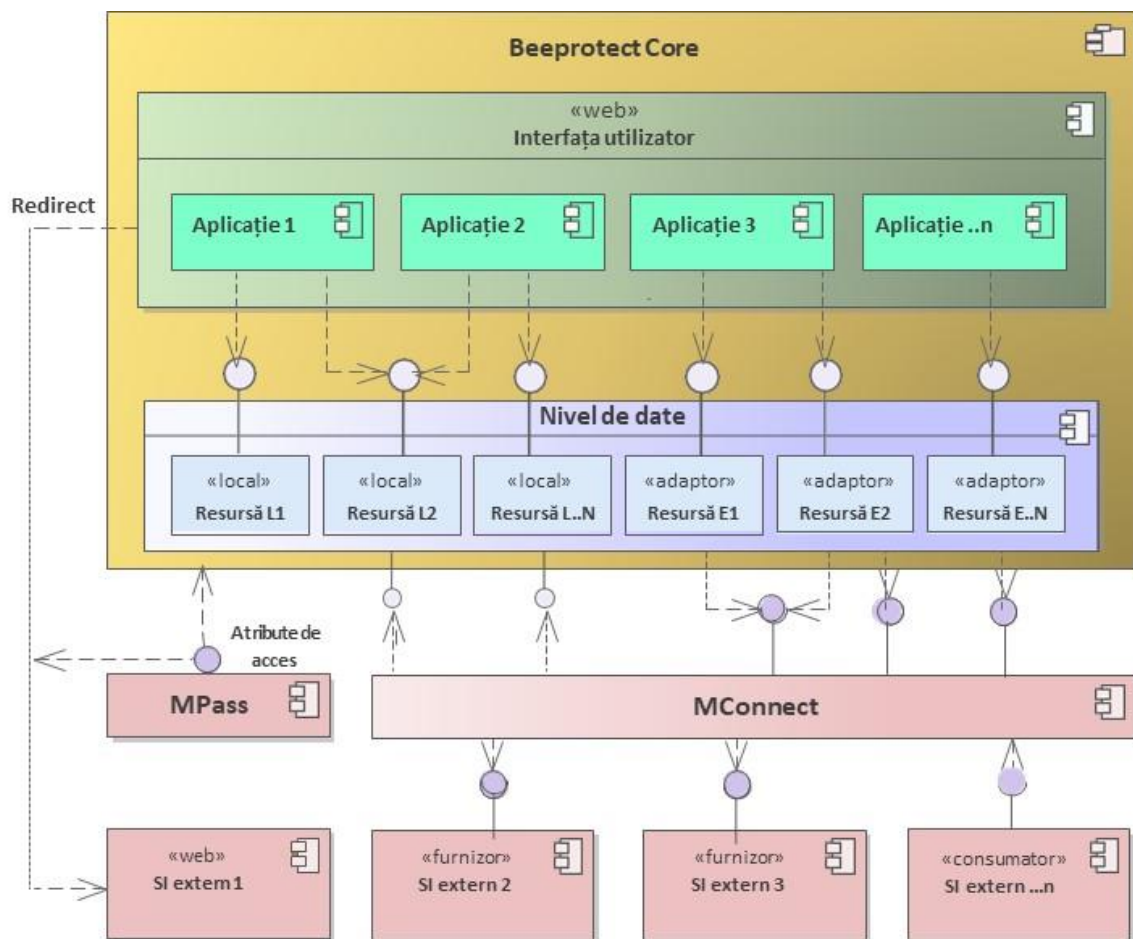


Figura 2. Model de integrare BeeProtect cu resurse externe

Capitolul VI

Spațiul tehnologic al BeeProtect

38. Pentru asigurarea unui nivel adecvat al securității informaționale, BeeProtect va permite realizarea conexiunilor securizate atât între stațiile client și serverul de aplicație, cât și între componentele BeeProtect.

39. BeeProtect urmează să se dezvolte conform planului său de dezvoltare, ținând cont de prioritățile ANSA. Din punct de vedere funcțional, având în vedere multitudinea de competențe/atribuții ale ANSA, BeeProtect urmează să se dezvolte etapizat.

40. Din punct de vedere tehnologic, se va determina o soluție fiabilă și scalabilă atât în cazul creșterii numărului de utilizatori concurenți, cât și în cazul creșterii volumului de date gestionate de aceasta.

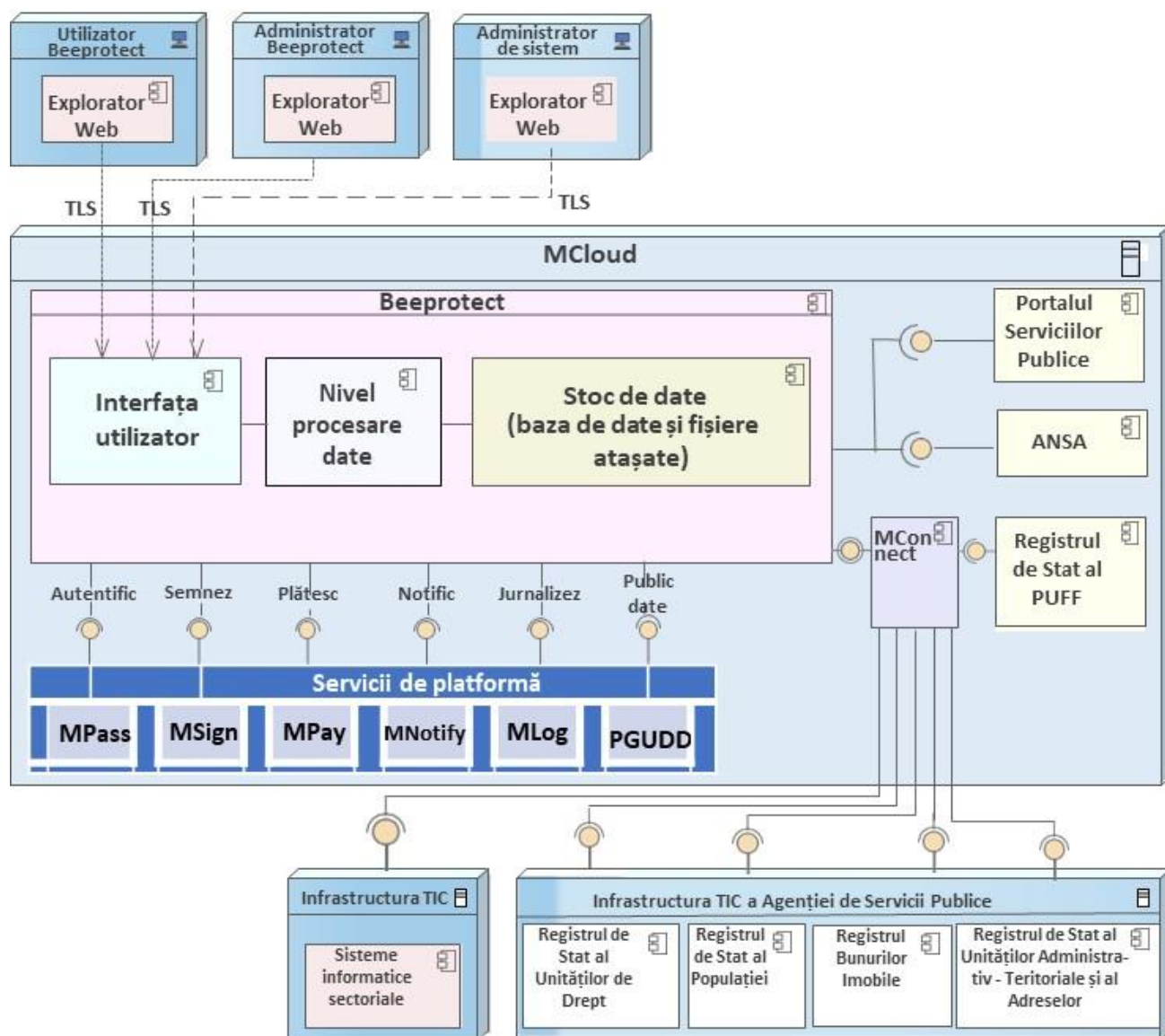


Figura 3. Arhitectura BeeProtect

În figura 3 este ilustrată arhitectura conceptuală a BeeProtect. Soluția de cooperare dintre resursele BeeProtect constă în interacțiunea dintre mai multe resurse informaționale externe și componentele acestuia.

41. Arhitectura BeeProtect constă din următoarele noduri distincte:

1) platforma tehnologică guvernamentală comună (MCloud), unde vor fi găzduite componentele BeeProtect;

2) serviciile platformei tehnologice guvernamentale comune (MCloud), furnizate de următoarele soluții software: platforma de interoperabilitate (MConnect); serviciul electronic guvernamental de autentificare și control al accesului (MPass); serviciul electronic guvernamental integrat de semnătură electronică (MSign); serviciul guvernamental de notificare electronică (MNotify); serviciul electronic guvernamental de jurnalizare (MLog); Serviciului Guvernamental de Plăți Electronice (MPay);

3) infrastructura TIC a Agenției de Servicii Publice, care include: Registrul de stat al unităților de drept, Registrul de stat al populației, Registrul bunurilor imobile, Registrul de stat al unităților administrativ-teritoriale și al adreselor;

4) infrastructura TIC a organizațiilor sectoriale, care poate include sisteme informaționale care vor face schimb de date cu BeeProtect.

42. Componentele principale ale BeeProtect sunt interdependente, realizează schimb reciproc de date și sunt grupate în următoarele module:

1) administrarea, verificarea, monitorizarea și controlul acțiunilor obiectelor informaționale;

2) gestionarea împuternicirilor pentru prestarea serviciilor de către personalul oficiului central ANSA și a subdiviziunilor teritoriale;

3) înregistrarea datelor proprii de către fiecare tip de utilizator;

4) logarea în BeeProtect;

5) emiterea și gestionarea pașaportului electronic al stupinei;

6) gestionarea documentelor.

Capitolul VII

Asigurarea securității informaționale a BeeProtect

43. Securitatea informațională presupune protecția BeeProtect, în toate etapele proceselor de creare, procesare, stocare și transmitere a datelor, de acțiuni accidentale sau intenționate cu caracter artificial sau natural, care au ca rezultat cauzarea prejudiciului posesorului și utilizatorilor resurselor informaționale și infrastructurii informaționale.

44. Mecanismele principale de securitate informațională utilizate vor fi:

1) autentificarea și autorizarea accesului la date;

2) administrarea accesului la date;

3) înregistrarea acțiunilor utilizatorilor sistemului informațional;

4) criptarea datelor (după caz);

- 5) auditul informatic;
- 6) procedurile de restabilire în caz de dezastru.

45. Veriga cea mai sensibilă supusă riscului în sistemul de securitate este factorul uman. Din aceste considerente, instruirea personalului la capitolul însușirii metodologiei rezistenței la amenințări informatice este un element foarte important. În procesul de elaborare a BeeProtect, pentru asigurarea securității informaționale, se va ține cont de algoritmi și de protocoalele existente pe piață, cu respectarea cadrului normativ al Republicii Moldova.

46. BeeProtect va corespunde Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Legea nr. 133/2011, Hotărârii Guvernului nr. 1123/2010, precum și Cerințelor minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017.

47. Accesul la resursele sistemului informațional va fi asigurat și autorizat prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass). Utilizatorii BeeProtect vor dispune de drepturi distincte de acces în funcție de nivelul de securitate căruia îi corespund. Pentru fiecare categorie de acces va exista posibilitatea de a defini rolurile și drepturile utilizatorilor (inclusiv la nivelul de acces la interfața accesibilă utilizatorilor).

48. Accesul la informația bazei de date va fi limitată în funcție de drepturile și rolurile specifice utilizatorilor. Fiecare categorie de utilizatori va avea acces la o interfață personalizată (diferită de cea a altor categorii de utilizatori) pentru vizualizarea și gestionarea informației bazei de date.

49. Indiferent de nivelul de acces al utilizatorului, niciun grup de acces nu trebuie să posede dreptul de a suprima direct înregistrările bazei de date (se va schimba doar statutul corespunzător al înregistrării ce urmează a fi eliminate). De asemenea, nu se va admite modificarea directă a datelor bazei de date. Toate inserările și actualizările de date în baza de date se vor face exclusiv prin intermediul unor formulare electronice specializate, cu parcurgerea completă a unor fluxuri de lucru implementate în cadrul BeeProtect.

50. Orice modificare potențial periculoasă: modificarea informației unei înregistrări, schimbarea statutului, adăugarea unor înregistrări noi etc. va fi documentată în registre electronice speciale (fișiere log), arătând momentul de timp și utilizatorul care a efectuat modificarea potențial periculoasă. Pentru fiecare modificare potențial periculoasă, BeeProtect va salva în evenimentul jurnalizat modificarea efectuată.

51. La nivel fizic, politica de asigurare a securității informaționale va fi realizată prin intermediul unor module automate de generare a copiilor de rezervă a fișierelor, a bazelor de date și a aplicațiilor informatice aflate în producție. Administratorul BeeProtect vor dispune de posibilitatea de definire a politicii de generare automată a

copiilor de rezervă.

52. Pentru asigurarea unui nivel adecvat al securității informaționale a BeeProtect, va fi elaborată și aplicată o politică de asigurare a securității informaționale care va detalia totalitatea compartimentelor de securitate, rolurile, drepturile și obligațiile fiecărui actor al BeeProtect. Politica de securitate va fi adusă la cunoștința fiecărui utilizator și va fi semnată de acesta. Fiecare utilizator va cunoaște obligațiile în materie de respectare a securității informaționale și totalitatea procedurilor formale pe care trebuie să le respecte în strictă concordanță cu politica de securitate.

53. Pentru asigurarea veridicității informație, va fi elaborată politica care va defini mecanismele de validare a informației introduse în cadrul BeeProtect sau extrase din acesta.

54. Deținătorul BeeProtect va dispune de angajați sau va contracta personal calificat pentru efectuarea auditului securității informaționale, verificării și instruirii continue în materie de asigurare a securității informaționale.

REGULAMENT

privind modul de funcționare și utilizare al Sistemului informațional „BeeProtect”

Capitolul I

DISPOZIȚII GENERALE

1. Regulamentul privind modul de funcționare și utilizare a Sistemului informațional „BeeProtect” (în continuare - Regulament) este elaborat în vederea reglementării conținutului, modului de organizare și funcționare a Sistemului informațional „BeeProtect” (în continuare – *BeeProtect*), utilizată de către apicultori și producătorii agricoli în scopul înregistrării și notificării reciproce a informațiilor privind aplicarea produselor de uz fitosanitar și a fertilizanților și privind amplasarea stupinelor.

2. BeeProtect constituie o modalitate uniformă și continuă de expediere a notificărilor în cadrul sistemului informațional deținut de Agenția Națională pentru Siguranța Alimentelor (în continuare - ANSA), prin diverse canale de notificare, în scopul facilitării interacțiunii dintre apicultori și producătorii agricoli.

Capitolul II

SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL UTILIZĂRII BEEPROTECT

3. Subiecții din domeniul exploatării și al utilizării BeeProtect sunt:

- 1) proprietarul sistemului informațional;
- 2) posesorul și deținătorul sistemului informațional;
- 3) utilizatorii sistemului informațional;
- 4) administratorul tehnic al sistemului informațional.

4. Proprietarul BeeProtect este statul care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din aceasta. Resursele financiare pentru dezvoltarea sistemului informațional sunt asigurate din bugetul de stat, din proiecte de asistență internațională și din alte mijloace financiare, conform cadrului normativ.

5. Posesorul și deținătorul BeeProtect este ANSA, care își realizează dreptul de gestionare și de utilizare a BeeProtect. Rolul de posesor al sistemului reflectă aspectul administrativ ce ține de competențele deținute și necesare administrării și dezvoltării continue a sistemului informațional. ANSA va fi responsabilă de dezvoltarea și de

implementarea BeeProtect, iar beneficiarii finali ai acesteia vor fi ANSA, inclusiv subdiviziunile teritoriale ANSA, autoritățile publice locale de nivel I și mediul de afaceri din sectorul agricol și apicol. Deținătorul BeeProtect asigură crearea, administrarea, mentenanța și dezvoltarea sistemului informațional.

6. Utilizatorii BeeProtect sunt funcționarii și angajații ANSA care vor utiliza funcționalitățile sistemului informațional în scopurile prevăzute de prezentul Regulament. Nivelul de acces al utilizatorilor este diferențiat în funcție de atribuțiile, responsabilitățile, drepturile de acces la date și se configurează de către administratorul BeeProtect. Gestionarea resurselor informaționale furnizate prin intermediul BeeProtect va fi realizată în funcție de perimetrul de date la care un utilizator are acces sigur și în conformitate cu serviciile externe pentru datele captate.

7. De asemenea, utilizatori ai aplicației BeeProtect sunt și apicultorii și producătorii agricoli, care vor plasa informații de avertizare privind plasarea stupinelor, respectiv utilizarea produselor de uz fitosanitar, având astfel o calitate dublă, după caz, de expeditor, fie destinat al notificărilor.

8. Administratorul tehnic al BeeProtect este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care își exercită atribuțiile în conformitate cu Regulamentul privind administrarea tehnică și menținerea resurselor și sistemelor informaționale de stat, aprobat prin anexa nr. 5 la Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat.

Capitolul III

DREPTURILE ȘI OBLIGAȚIILE SUBIECȚILOR BEEPROTECT

Secțiunea 1

Atribuțiile ANSA. Drepturi și obligații

9. ANSA are următoarele atribuții:

- 1) să asigure condițiile juridice, organizatorice și financiare pentru crearea, funcționarea și mentenanța BeeProtect;
- 2) să aprobe proceduri, reguli și instrucțiuni pentru înregistrarea, acumularea, păstrarea, completarea, corectarea, sistematizarea și utilizarea datelor, precum și de funcționare a BeeProtect;
- 3) să stabilească scopurile și sarcinile funcționale ale BeeProtect;
- 4) să asigure dezvoltarea continuă a BeeProtect, inclusiv prin identificarea și integrarea noilor canale de notificare;
- 5) să autorizeze, suspende și revoce dreptul de acces la BeeProtect;

6) să monitorizeze procesul de înregistrare și prelucrare a datelor în cadrul BeeProtect;

7) să asigure securitatea și protecția datelor;

8) să stabilească măsurile tehnice și organizatorice de protecție și securitate;

9) să monitorizeze și ajusteze cerințele de securitate și conformitate ale aplicației BeeProtect la domeniul protecției datelor cu caracter personal;

10) să exercite alte atribuții necesare asigurării bunei funcționări a BeeProtect.

10. ANSA are dreptul:

1) să elaboreze și/sau să aprobe, conform competenței, cadrul normativ cu privire BeeProtect;

2) să supravegheze respectarea cerințelor de securitate a informației de către subiecții BeeProtect, să fixeze cazurile și tentativele de încălcare a acestora;

3) să inițieze procedura de suspendare a drepturilor de acces la BeeProtect pentru utilizatorii care nu respectă regulile, standardele și normele general acceptate în domeniul securității informaționale;

4) să verifice autenticitatea și veridicitatea datelor transmise de subiecții BeeProtect;

5) să solicite de la subiecții BeeProtect actualizarea sau corectarea datelor din baza de date a BeeProtect în caz de depistare a omisiunilor și erorilor;

6) să propună soluții pentru perfecționarea și eficientizarea procesului de funcționare a BeeProtect, precum și să le pună în aplicare după aprobarea acestora.

11. ANSA este obligat:

1) să asigure atribuirea rolurilor și drepturilor de acces la interfețele BeeProtect și datele acestuia;

2) să identifice încălcările comise și să întocmească un raport privind datele accesate;

3) să asigure funcționarea neîntreruptă a BeeProtect;

4) să acorde suportul necesar utilizatorilor, care au acces la BeeProtect, privind folosirea complexului de mijloace software aferente acestuia;

5) să stabilească condițiile tehnice de funcționare a acestuia, pentru a asigura expedierea și recepționarea notificărilor, prin intermediul canalelor de notificare, în termenele stabilite;

6) să efectueze măsurile organizatorice și tehnice necesare asigurării protecției și confidențialității informației stocate în baza de date a BeeProtect, inclusiv împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate;

7) să asigure implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu cadrul normativ în materie de protecția datelor cu caracter personal;

8) să asigure accesul securizat la informația conținută în BeeProtect, respectarea condițiilor de securitate și regulilor de exploatare a acestuia.

Secțiunea 2

Drepturile și obligațiile utilizatorului

12. Utilizatorul BeeProtect are următoarele drepturi:

1) să utilizeze BeeProtect pentru a expedia notificări în contextul activităților pe care intenționează să le desfășoare;

2) să asigure conformitatea conținutului notificărilor cu cadrul legal;

3) să se conformeze cerințelor tehnice stabilite de ANSA, în calitate de posesor al BeeProtect;

4) să încheie acorduri cu posesorul BeeProtect privind utilizarea sistemului informațional;

5) să utilizeze funcționalitățile BeeProtect, în exclusivitate conform destinațiilor acestora și în conformitate cu prezentul Regulament;

6) să solicite și să primească de la ANSA asistență metodologică și practică de utilizare a BeeProtect;

7) să înainteze către ANSA propuneri privind modificarea actelor normative care reglementează funcționarea BeeProtect;

8) să înainteze posesorului propuneri privind îmbunătățirea și sporirea eficacității funcționării BeeProtect.

13. Utilizatorul BeeProtect este obligat:

1) să asigure conformitatea conținutului notificărilor cu cadrul legal;

2) să se conformeze cerințelor tehnice stabilite de ANSA, în calitate de posesor și deținător al BeeProtect;

3) să întreprindă măsuri pentru evitarea accesului neautorizat al persoanelor terțe;

4) să prevină crearea și expedierea prin intermediul BeeProtect a notificărilor ce contravin legislației naționale, precum și a notificărilor eronate și/sau false;

5) să respecte condițiile tehnice de utilizare a BeeProtect;

6) să asigure autenticitatea și veridicitatea datelor transmise BeeProtect;

7) să efectueze acțiunile de asigurare a securității informației, să documenteze cazurile și tentativele de încălcare a acesteia, precum și să întreprindă măsurile ce se impun pentru prevenirea și lichidarea consecințelor.

Capitolul IV

ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI

14. Datele din BeeProtect fac parte din categoria datelor care necesită a fi protejate. Asigurarea securității, confidențialității și a integrității datelor prelucrate în cadrul BeeProtect se efectuează de către subiecții cu drepturi de acces la sistem cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

15. Măsurile de protecție și securitate a datelor din BeeProtect reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a BeeProtect și se actualizează de către toți subiecții BeeProtect.

16. Securitatea informațională a BeeProtect se efectuează prin aplicarea metodelor și efectuarea acțiunilor și a procedurilor operaționale.

17. Protecția datelor din BeeProtect se efectuează prin următoarele metode:

- 1) prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor;
- 2) utilizarea obligatorie a produselor de program licențiate aprobate, orice solicitare de instalare a unui produs de program trebuie coordonată cu posesorul;
- 3) monitorizarea procesului de exploatare al BeeProtect prin intermediul mecanismului de jurnalizare efectuat de administratorul tehnic al acestuia.

18. Subiecții la utilizarea și exploatarea BeeProtect, cu excepția destinatarilor, asigură implementarea normelor de securitate, aceasta urmând să conțină acte ce confirmă:

- 1) identitatea persoanei responsabile de implementarea normelor de securitate și împuternicirile acesteia;
- 2) implementarea principalelor măsuri tehnico-organizatorice necesare asigurării funcționării BeeProtect;
- 3) implementarea procedurilor interne ce exclud cazurile de modificare nesancționată a mijloacelor software și/sau a informației din BeeProtect;
- 4) informarea utilizatorilor interni și instruirea acestora cu privire la modalitățile și mecanismele de asigurare a securității informaționale;
- 5) procedurile de control intern al subiectului BeeProtect privind respectarea condițiilor de securitate informațională.

19. Schimbul informațional se efectuează cu utilizarea mijloacelor software și hardware, doar prin canale securizate, asigurând integritatea și securitatea datelor.

Capitolul V

CONTROLUL ȘI RĂSPUNDEREA

20. Crearea, organizarea și funcționarea BeeProtect este supusă controlului intern și extern. Controlul intern privind organizarea și funcționarea BeeProtect se efectuează de către ANSA. Controlul extern asupra respectării cerințelor privind crearea, organizarea și funcționarea BeeProtect se efectuează de către instituții abilitate și certificate în domeniul auditului.

21. Responsabilitatea pentru organizarea funcționării BeeProtect aparține posesorului acestuia.

22. Utilizatorii în atribuțiile cărora intră administrarea BeeProtect, introducerea datelor, furnizarea informațiilor și asigurarea funcționării BeeProtect poartă răspundere personală în conformitate cu legislația, pentru completitudinea, autenticitatea, veridicitatea, integritatea informației, precum și pentru păstrarea și utilizarea ei.

23. Toți subiecții BeeProtect poartă răspundere conform legislației pentru prelucrarea, divulgarea și transmiterea informației din sistem ce conține date cu caracter personal, persoanelor terțe, contrar prevederilor legislației.

24. Pentru asigurarea funcționalității eficiente și neîntrerupte a BeeProtect, schimbul informațional de date al BeeProtect este asigurat în regim non-stop.

25. Funcționarea BeeProtect se suspendă de către administratorul tehnic, după coordonarea prealabilă cu ANSA, în caz de apariție a uneia dintre următoarele situații:

1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al BeeProtect;

2) la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea BeeProtect;

3) în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al BeeProtect;

4) la cererea scrisă a posesorului.

26. În cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al BeeProtect din vina terțelor persoane, este posibilă suspendarea funcționării BeeProtect, cu informarea subiecților prin mijloacele tehnice disponibile.