**Politica de protecție a datelor cu caracter personal**

**IGUS INNOVATIVE SOLUTIONS SRL**

Noi la IGUS INNOVATIVE SOLUTIONS SRLse angajează să prelucreze datele personale în siguranță și să respecte confidențialitatea persoanelor în cauză.

|  |  |
| --- | --- |
| Numărul versiunii și data ultimei actualizări: | v. 1.0.  25 septembrie 2021 |
| Aprobat de: | ORSOS PATRICK-EMANUEL, CEO IGUS INNOVATIVE SOLUTIONS SRL |
| Această politică va fi revizuită anual sau de fiecare dată când apar modificările procesării noastre de date. | |

## **Cuprins**

|  |  |
| --- | --- |
| 1. Domeniu de aplicare și definiții………………………………………………………………………… ... | 3 |
| 1. Principii de prelucrare a datelor…………………………………………………………………………… | 6 |
| 1. Accesul la datele personale. Temeiuri și scopuri legale……………………………………………………………………………. | 8 |
| 1. Terți………………………………………………………………………………. | 10 |
| 1. Transferuri internaționale……………………………………………………………………………. | 11 |
| 1. Drepturile persoanelor vizate. ……………………………………………………………………………. | 12 |
| 1. Noi activități de prelucrare a datelor………………………………………………………………………… .. | 17 |
| 1. Păstrarea datelor…………………………………………………………………. …… ... | 19 |
| 1. Securitate…………………………………………………………………………… ... | 19 |
| 1. Procedura de răspuns la încălcarea datelor. ……………. ……………………………………………………………. | 20 |

## **Domeniu de aplicare și definiții**

* 1. **Domeniul de aplicare**. AcestPersonalPolitica de protecție a datelor („Politica”) descrie regulile interne IGUS INNOVATIVE SOLUTIONS SRL pentru prelucrarea și protecția datelor cu caracter personal. Politica se aplică IGUS INNOVATIVE SOLUTIONS SRL, inclusiv angajaților și contractanților IGUS INNOVATIVE SOLUTIONS SRL („noi”, „noi”, „noștri”, „IGUS INNOVATIVE SOLUTIONS SRL”). Conducerea fiecărei entități este în cele din urmă responsabilă de implementarea acestei politici, precum și de a asigura, la nivel de entitate, existența unor proceduri adecvate și eficiente pentru implementarea acesteia și monitorizarea continuă a aderării acesteia. În sensul prezentei politici, angajații și contractanții sunt denumiți împreună „angajații”.

* 1. **Manager de confidențialitate**. Privacy Manager este un angajat al IGUS INNOVATIVE SOLUTIONS SRL responsabil pentru respectarea protecției datelor cu caracter personal în cadrul IGUS INNOVATIVE SOLUTIONS SRL („Managerul de confidențialitate”). Managerul de confidențialitate este responsabil de îndeplinirea obligațiilor impuse de această politică și de supravegherea altor angajați, care fac obiectul prezentei politici, cu privire la aderarea la această politică. Managerul de confidențialitate trebuie să fie implicat în toate proiectele într-o etapă timpurie, pentru a ține seama de aspectele privind protecția datelor cu caracter personal încă din faza de planificare.

Managerul de confidențialitate desemnat la IGUS INNOVATIVE SOLUTIONS SRL este Giurgi Bogdan, Silviu Manzur.

* 1. **Definiții**.

|  |  |
| --- | --- |
| **Autoritatea de supraveghere competentă** | înseamnă o autoritate publică care este responsabilă pentru reglementarea și supravegherea protecției datelor cu caracter personal în ceea ce privește activitățile IGUS INNOVATIVE SOLUTIONS SRL. |
| **Încălcarea datelor** | înseamnă o încălcare a securității și / sau confidențialității care duce la distrugerea accidentală sau ilegală, pierderea, modificarea, divulgarea neautorizată sau accesul la datele personale transmise, stocate sau prelucrate în alt mod.  Aceasta include, dar nu se limitează la e-mailuri trimise către o listă incorectă sau divulgată de destinatari, o publicare ilegală a datelor cu caracter personal, pierderea sau furtul de înregistrări fizice și accesul neautorizat la informații personale. |
| **Operator de date** | înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu alte persoane, determină (ia o decizie) scopurile și mijloacele prelucrării datelor cu caracter personal. |
| **Procesor de date** | înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau alt organism care prelucrează datele cu caracter personal în numele operatorului de date. |
| **Legile privind protecția datelor** | înseamnă orice legi și reguli legale privind utilizarea și protecția datelor cu caracter personal aplicabile activităților IGUS INNOVATIVE SOLUTIONS SRL, inclusiv, dar fără a se limita la 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 libera circulație a acestor date și abrogarea Directivei 95/46 / CE (Regulamentul general privind protecția datelor, GDPR). |
| **Solicitarea subiectului datelor (DSR)** | înseamnă orice solicitare din partea persoanei vizate și referitoare la datele lor personale și / sau drepturile persoanei vizate. |
| **Persoană vizată** | înseamnă o persoană fizică, ale cărei date personale le prelucrăm. Persoanele vizate includ, dar nu se limitează la, utilizatorii, vizitatorii site-ului web, angajații, contractanții și partenerii IGUS INNOVATIVE SOLUTIONS SRL. |
| **Date personale** | înseamnă orice informație referitoare la o persoană vizată identificată sau identificabilă; o persoană vizată poate fi identificată prin referire la un identificator, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online sau la unul sau combinația de factori specifici fizic, fiziologic, genetic, mental, economic, cultural sau social identitatea persoanei vizate. |
| **Prelucrare** | înseamnă orice operațiune sau set de operațiuni efectuate de IGUS INNOVATIVE SOLUTIONS SRL pe date cu caracter personal, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, recuperarea, consultarea, utilizarea, divulgarea prin transmisie, diseminare sau punerea la dispoziție în alt mod , alinierea sau combinarea, restricționarea, ștergerea sau distrugerea. |
| **Clauze contractuale standard** | înseamnă Decizia Comisiei Europene din 5 februarie 2010 privind clauzele contractuale standard pentru transferul de date cu caracter personal către procesatori stabiliți în țări terțe în temeiul Directivei 95/46 / CE a Parlamentului European și a Consiliului (2010/87 / UE). |
| **Terț** | înseamnă o persoană fizică sau juridică, care accesează Datele cu caracter personal pentru prelucrare ulterioară și nu este angajat, membru sau afiliat corporativ al IGUS INNOVATIVE SOLUTIONS SRL. Această definiție nu se aplică persoanelor fizice care furnizează servicii la IGUS INNOVATIVE SOLUTIONS SRL în calitate de contractori în mod regulat. |
| **Utilizator** | înseamnă o persoană vizată care utilizează serviciile noastre furnizate pe site-ul web IGUS INNOVATIVE SOLUTIONS SRL. |

## **Principii de prelucrare a datelor**

* 1. Activitățile de prelucrare ale IGUS INNOVATIVE SOLUTIONS SRL trebuie să fie în conformitate cu principiile specificate în această secțiune. Managerul de confidențialitate trebuie să se asigure că documentația de conformitate a IGUS INNOVATIVE SOLUTIONS SRL, precum și activitățile de prelucrare a datelor, sunt conforme cu principiile de protecție a datelor.

* 1. Trebuie să prelucrăm datele cu caracter personal în conformitate cu următoarele principii:
     1. În mod legal, corect și transparent (**legalitate, corectitudine și transparență**). Vom avea întotdeauna un temei legal pentru prelucrare (descris în secțiunea 3 a acestei politici), vom colecta cantitatea de date adecvată scopului și temeiurilor legale și ne asigurăm că persoanele vizate sunt la curent cu prelucrarea;
     2. Colectate pentru scopuri specificate, explicite și legitime și care nu sunt prelucrate ulterior într-un mod care este incompatibil cu aceste scopuri (**limitarea scopului**). Nu trebuie să prelucrăm datele cu caracter personal în scopuri nespecificate în documentația noastră de conformitate fără a obține aprobarea specifică a Managerului de confidențialitate;
     3. Adecvate, relevante și limitate la ceea ce este necesar în scopurile pentru care sunt procesate (**minimizarea datelor**). Ne asigurăm întotdeauna că datele pe care le colectăm nu sunt excesive și limitate de necesitatea strictă;
     4. Exact și, acolo unde este necesar, actualizat (**precizie)**.Ne străduim să ștergem date inexacte sau false despre persoanele vizate și ne asigurăm că actualizăm datele. Persoanele vizate ne pot cere o corectare a datelor cu caracter personal;
     5. Păstrat într-un formular care permite identificarea persoanelor vizate pentru o perioadă mai lungă decât este necesar pentru scopurile pentru care sunt prelucrate datele cu caracter personal (limitarea perioadei de stocare). Perioadele de stocare trebuie să fie limitate conform prevederilor legilor privind protecția datelor și a prezentei politici; și
     6. Procesați într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și a pierderii, distrugerii sau deteriorării accidentale, utilizând măsuri tehnice sau organizaționale adecvate (**confidențialitate, integritate și disponibilitate**).

* 1. **Responsabilitate**.
     1. Vom putea demonstra conformitatea noastră cu legile privind protecția datelor (**principiul responsabilității**). În special, trebuie să asigurăm și să documentăm toate procedurile, eforturile, consultările interne și externe relevante privind protecția datelor cu caracter personal, inclusiv:
        + faptul numirii unei persoane responsabile pentru respectarea protecției datelor IGUS INNOVATIVE SOLUTIONS SRL;
        + acolo unde este necesar, o înregistrare a unei evaluări a impactului procesării datelor;
        + a elaborat și a implementat notificări, politici și proceduri, cum ar fi Notificarea de confidențialitate, această politică sau procedura de răspuns la încălcarea datelor;
        + faptul instruirii personalului cu privire la respectarea legilor privind protecția datelor; și
        + evaluarea, implementarea și testarea măsurilor organizaționale și tehnice de protecție a datelor.
     2. Managerul de confidențialitate trebuie să mențină evidența activităților de prelucrare a IGUS INNOVATIVE SOLUTIONS SRL, care este un document de responsabilitate care descrie activitățile de prelucrare a datelor cu caracter personal ale IGUS INNOVATIVE SOLUTIONS SRL, întocmit în conformitate cu art. 30 din GDPR („Înregistrările activităților de prelucrare”). Înregistrările activităților de prelucrare trebuie să păstreze, cel puțin, următoarele informații despre fiecare activitate de prelucrare:
        + detaliile de contact ale IGUS INNOVATIVE SOLUTIONS SRL, reprezentantul UE și, după caz, al responsabilului cu protecția datelor;
        + denumirea activității, scopurile și baza legală a acesteia împreună cu, dacă este cazul, interesele legitime ale IGUS INNOVATIVE SOLUTIONS SRL;
        + persoanele vizate și categoriile de date cu caracter personal în cauză;
        + perioade de păstrare a datelor;
        + descrierea generală a măsurilor de securitate aplicabile;
        + destinatarii, inclusiv operatorii comuni, procesatorii și contractanții implicați, precum și faptul transferului internațional de date cu garanțiile aplicate transferului;
        + dacă este cazul, o trimitere la evaluarea impactului prelucrării datelor;
        + acolo unde este cazul, o referință la înregistrarea încălcării datelor care a avut loc cu privire la datele cu caracter personal;
        + dacă IGUS INNOVATIVE SOLUTIONS SRL acționează ca procesator de date, informațiile care trebuie furnizate includ numele și datele de contact ale operatorilor, numele și datele de contact ale reprezentantului operatorului (dacă este cazul), categoriile de prelucrare (activități), numele țărilor terțe sau internaționale organizații cărora li se transferă datele cu caracter personal (dacă este cazul), garanții pentru transferuri excepționale de date cu caracter personal către țări terțe sau organizații internaționale (dacă este cazul) și descrierea generală a măsurilor de securitate tehnică și organizațională.

## **Accesul la datele personale. Temeiuri și scopuri legale**

* 1. **Temeiuri legale**.
     1. Fiecare activitate de prelucrare trebuie să aibă unul dintre motivele legale specificate în această secțiune pentru prelucrarea datelor cu caracter personal. Dacă nu avem niciuna dintre cele descrise, nu putem colecta sau prelucra datele personale.
     2. În cazul în care IGUS INNOVATIVE SOLUTIONS SRL este destinat să utilizeze datele cu caracter personal în alte scopuri decât cele specificate în Evidența activităților de prelucrare, Managerul de confidențialitate trebuie să evalueze, să determine și, dacă este necesar, să colecteze / să înregistreze baza legală adecvată pentru aceasta.
     3. **Executarea contractului**.În cazul în care IGUS INNOVATIVE SOLUTIONS SRL are un contract cu persoana vizată, de ex. Termenii de utilizare a site-ului web sau contractul de muncă, iar contractul necesită furnizarea de date cu caracter personal de la persoana vizată, temeiul juridic aplicabil va fi executarea contractului.
     4. **Consimţământ**. Pentru a procesa datele cu caracter personal pe baza consimțământului, trebuie să obținem consimțământul înainte de Procesare și să păstrăm dovada consimțământului cu înregistrările Datelor personale ale persoanei vizate. Managerul de confidențialitate trebuie să se asigure că consimțământul colectat de la persoanele vizate îndeplinește cerințele legilor privind protecția datelor și ale acestei politici. În special, Managerul de confidențialitate trebuie să se asigure că:
        + Persoana vizată trebuie să fie liberă să dea sau să refuze acordul.
        + consimțământul este sub forma unei indicații active de la persoana vizată, adică caseta de selectare a consimțământului nu trebuie bifată în prealabil pentru utilizator.
        + solicitarea consimțământului articulează în mod clar scopurile prelucrării, iar alte informații specificate în subsecțiunea 6.2 sunt disponibile persoanei vizate.
        + Persoana vizată trebuie să fie liberă să își dea consimțământul sau să o revoce.
     5. **Interese legitime**. Avem dreptul de a utiliza datele personale în „interesele noastre legitime”. Interesele pot include scopurile justificate de natura activităților noastre comerciale, cum ar fi analiza de marketing a datelor cu caracter personal. Pentru ca IGUS INNOVATIVE SOLUTIONS SRL să utilizeze interese legitime ca temei legal pentru prelucrare, Managerul de confidențialitate trebuie să se asigure că:
        + interesul legitim pentru prelucrare este clar definit și înregistrat în Evidența activităților de prelucrare;
        + sunt identificate orice riscuri prevăzute pentru drepturile și interesele persoanei vizate. Exemplele de riscuri pot fi găsite în subsecțiunea 7.2 .;
        + persoanele vizate au așteptări rezonabile cu privire la prelucrare și se iau măsuri de protecție suplimentare pentru a aborda riscurile;
        + sub rezerva condițiilor din subsecțiunea 6.7 (Dreptul de a obiecta împotriva prelucrării), persoanei vizate i se oferă posibilitatea de a renunța la prelucrare pentru interesele legitime descrise.

Dacă cel puțin una dintre condițiile de mai sus nu este îndeplinită de IGUS INNOVATIVE SOLUTIONS SRL, Managerul de confidențialitate trebuie să aleagă și să propună un alt temei juridic pentru prelucrare, cum ar fi consimțământul.

* + 1. **Conformitate legală și interes public**.În afară de motivele menționate anterior, am putea fi solicitați de legile Uniunii Europene sau de legile statului membru UE să prelucrăm datele cu caracter personal ale utilizatorilor noștri. De exemplu, ni se poate cere să colectăm, să analizăm și să monitorizăm informațiile utilizatorilor pentru a respecta legislația financiară sau a muncii.

Ori de câte ori avem o astfel de obligație, trebuie să ne asigurăm că:

* + - * prelucrăm datele personale strict în conformitate cu cerințele legale relevante;
      * nu folosim sau stocăm datele personale colectate în alte scopuri decât conformitatea legală; și
      * Persoanele vizate sunt informate în mod corespunzător și în timp util cu privire la obligațiile noastre, domeniul de aplicare și condițiile de prelucrare a datelor cu caracter personal.

**Important:** În cazul în care IGUS INNOVATIVE SOLUTIONS SRL are cerințele legale din altă țară pentru prelucrarea datelor cu caracter personal, Managerul de confidențialitate trebuie să propună utilizarea unui alt temei legal pentru prelucrarea conform legilor privind protecția datelor, cum ar fi interesele legitime sau consimțământul.

* 1. **Accesul la datele personale**.
     1. Angajații trebuie să aibă acces la datele cu caracter personal pe baza „necesității de a ști”. Datele pot fi accesate numai dacă este strict necesar să efectuați una dintre activitățile specificate în Evidența activităților de prelucrare. Angajații și contractanții vor avea acces la Datele cu caracter personal numai dacă au acreditările necesare pentru aceasta.
     2. Șefii departamentelor din cadrul IGUS INNOVATIVE SOLUTIONS SRL sunt responsabili pentru accesul angajaților lor și prelucrarea datelor cu caracter personal. Șefii trebuie să mențină lista angajaților care au dreptul de a accesa și prelucra datele cu caracter personal. Managerul de confidențialitate va avea dreptul să revizuiască lista și, dacă este necesar, să solicite modificările pentru a îndeplini cerințele prezentei politici.
     3. Șefii departamentelor din cadrul IGUS INNOVATIVE SOLUTIONS SRL trebuie să se asigure că angajații aflați sub supravegherea lor sunt la curent cu legile privind protecția datelor și respectă regulile stabilite în această politică. Pentru a ne asigura că angajații noștri sunt în măsură să respecte cerințele privind protecția datelor, trebuie să le oferim instruire adecvată în domeniul protecției datelor.
     4. Toți angajații care accesează datele cu caracter personal trebuie să păstreze o confidențialitate strictă cu privire la datele pe care le accesează. Angajații care accesează datele cu caracter personal trebuie să utilizeze numai acele mijloace (software, spații etc.) pentru prelucrare care au fost prescrise de IGUS INNOVATIVE SOLUTIONS SRL. Datele nu trebuie divulgate sau puse la dispoziție în alt mod din instrucțiunile de gestionare.
     5. Angajații din competența lor trebuie să asiste reprezentanții IGUS INNOVATIVE SOLUTIONS SRL, inclusiv Managerul de confidențialitate, în orice efort privind respectarea legilor privind protecția datelor și / sau a prezentei politici.
     6. Atunci când un angajat detectează sau crede că există activitate suspectă, încălcare a datelor, nerespectarea legilor privind protecția datelor și / sau a prezentei politici sau un DSR nu a fost direcționat către departamentul competent din cadrul IGUS INNOVATIVE SOLUTIONS SRL, angajatul trebuie să raporteze o astfel de activitate către Managerul de confidențialitate.
     7. Angajații care nu sunt siguri dacă pot prelucra sau dezvălui în mod legitim datele cu caracter personal trebuie să solicite sfatul administratorului de confidențialitate înainte de a întreprinde orice acțiune.
     8. Orice acces ocazional la date cu caracter personal pentru activități care nu sunt specificate în Evidența activităților de prelucrare este interzis. Dacă există o strictă necesitate pentru acces imediat, Managerul de confidențialitate trebuie să aprobe mai întâi accesul.

## **Terți**

* 1. Înainte de a partaja date cu caracter personal cu orice persoană din afara IGUS INNOVATIVE SOLUTIONS SRL, Managerul de confidențialitate trebuie să se asigure că acest terț are un nivel adecvat de protecție a datelor și să ofere garanții suficiente de protecție a datelor în conformitate cu legile privind protecția datelor, inclusiv, dar fără a se limita la procesare cerințele (articolul 28 din GDPR) și conformitatea cu transferurile internaționale (secțiunea 5 din GDPR). Dacă este necesar, Managerul de confidențialitate trebuie să se asigure că IGUS INNOVATIVE SOLUTIONS SRL încheie contractul corespunzător de protecție a datelor cu terțul.

* 1. Un angajat poate partaja date cu caracter personal cu terți numai dacă și în măsura în care a fost direct prescris de manager și specificat în Evidența activităților de prelucrare.

* 1. În cazul în care ni se cere să ștergem, să modificăm sau să oprim prelucrarea datelor cu caracter personal, trebuie să ne asigurăm că părțile terțe, cu care am partajat datele cu caracter personal, vor îndeplini aceste obligații în consecință.

* 1. Ori de câte ori IGUS INNOVATIVE SOLUTIONS SRL este angajat ca procesator de date în numele altei entități, Managerul de confidențialitate trebuie să se asigure că IGUS INNOVATIVE SOLUTIONS SRL respectă obligația de procesare. În special, trebuie să existe un acord adecvat de prelucrare a datelor, în conformitate cu legile privind protecția datelor. Managerul de confidențialitate trebuie să supravegheze conformitatea cu instrucțiunile de prelucrare a datelor de la operator, inclusiv în ceea ce privește sfera activităților de prelucrare, implicarea subprocesorilor, transferurile internaționale, stocarea și eliminarea ulterioară a datelor personale procesate. Datele cu caracter personal prelucrate sub rolul de procesor nu trebuie prelucrate în alte scopuri decât cele specificate în instrucțiunile relevante, acordul sau alt act juridic care reglementează relațiile cu operatorul.

## **Transferuri internaționale**

* 1. Dacă avem angajați, contractanți, afiliați corporativi sau procesatori de date în afara SEE și le transferăm date cu caracter personal pentru prelucrare, responsabilul de confidențialitate trebuie să se asigure că IGUS INNOVATIVE SOLUTIONS SRL ia toate garanțiile necesare și adecvate în conformitate cu datele Legile de protecție.

* 1. Managerul de confidențialitate trebuie să evalueze garanțiile disponibile și să propună conducerii IGUS INNOVATIVE SOLUTIONS SRL garanția adecvată pentru fiecare transfer internațional. Următoarele regimuri se aplică transferurilor de date cu caracter personal în afara UE:
     + - în cazul în care Comisia Europeană decide că țara are un nivel adecvat de protecție a datelor cu caracter personal, transferul nu necesită luarea unor garanții suplimentare. Lista completă a jurisdicțiilor adecvate poate fi găsită pe pagina relevantă a site-ului web al Comisiei Europene[[1]](#footnote-1).
       - pentru a transfera date cu caracter personal contractanților sau partenerilor noștri (procesatori sau controlori de date) din alte țări terțe, trebuie să încheiem clauze contractuale standard cu acea parte. Proiectul de versiune împreună cu îndrumările pot fi găsite pe pagina relevantă a site-ului web al Comisiei Europene[[2]](#footnote-2);
       - dacă avem o filială corporativă sau o entitate în alte țări, putem alege să adoptăm reguli corporative obligatorii în conformitate cu articolul 47 din GDPR sau un cod de conduită aprobat în conformitate cu articolul 40 din GDPR;
       - de asemenea, putem transfera date cu caracter personal către entități care au o certificare aprobată în conformitate cu articolul 42 din GDPR, care certifică un nivel adecvat de protecție a datelor companiei.

* 1. Ca parte a obligațiilor de informare, IGUS INNOVATIVE SOLUTIONS SRL trebuie să informeze persoanele vizate că datele lor personale sunt transferate în alte țări, precum și să le furnizeze informații despre garanțiile utilizate pentru transfer. Obligația de informare trebuie îndeplinită în conformitate cu subsecțiunea 6.2.

* 1. În cazuri excepționale („Derogarea”), în care nu putem aplica garanțiile menționate anterior și trebuie să transferăm datele cu caracter personal, trebuie să luăm un consimțământ explicit (declarație activă) de la persoana vizată sau trebuie să fie strict necesar pentru efectuarea din contractul dintre noi și persoana vizată sau alte condiții de derogare se aplică în conformitate cu legile privind protecția datelor. Managerul de confidențialitate trebuie să aprobe în prealabil orice transfer de derogare și să documenteze derogările aprobate, precum și justificarea acestora.

## **Drepturile persoanelor vizate**

* 1. **Responsabilitățile noastre**.
     1. Managerul de confidențialitate este în cele din urmă responsabil pentru predarea tuturor DSR primite de IGUS INNOVATIVE SOLUTIONS SRL. În cazul primirii oricărui DSR restant sau neobișnuit, angajatul trebuie să solicite sfatul de la Managerul de confidențialitate înainte de a întreprinde orice acțiune.
     2. Suport tehnic în cadrul IGUS INNOVATIVE SOLUTIONS SRL este responsabil pentru manipularea DSR-urilor de la utilizatorii IGUS INNOVATIVE SOLUTIONS SRL zilnic. Departamentul Resurse Umane este responsabil pentru gestionarea DSR de la angajații IGUS INNOVATIVE SOLUTIONS SRL.
     3. Toate DSR-urile de la utilizatori trebuie să fie adresate la și să primească răspuns de la următoarea adresă de e-mail: gopackcontact@gmail.com. DSR de la angajați poate fi adresat direct managerului de resurse umane sau la adresa gopackcontact@gmail.com.
     4. Angajatul responsabil trebuie să răspundă la DSR în termen de o (1) lună de la primirea cererii. Dacă respectarea DSR durează mai mult de o lună, angajatul responsabil trebuie să solicite sfatul managerului de confidențialitate și, dacă este necesar, să informeze persoana vizată despre prelungirea termenului de răspuns cu până la două (2) luni suplimentare.
     5. Angajatul responsabil trebuie să analizeze DSR-ul primit pentru următoarele criterii:
        + **Identificarea subiectului datelor**. Înainte de a lua în considerare conținutul DSR, angajatul responsabil trebuie să se asigure că persoana vizată este aceeași persoană despre care pretinde că este. În acest scop, trebuie stabilită legătura dintre înregistrările datelor cu caracter personal și persoana vizată.

Pentru aceasta trebuie utilizate următoarele metode: verificarea adresei de e-mail a persoanei vizate - în general, adresa de e-mail trebuie să fie aceeași pe care IGUS INNOVATIVE SOLUTIONS SRL o are despre utilizatorul în cauză; dacă adresa de e-mail este diferită de înregistrarea din baza de date, trebuie să fie consultat Managerul de confidențialitate, după aprobarea căruia angajatul responsabil poate solicita detalii suplimentare din cont pentru identificare, precum data nașterii, adresa și adresa de e-mail abordare.

În cazul în care persoana vizată nu a fost supusă verificării, Managerul de confidențialitate trebuie să refuze efectuarea cererii și să informeze persoana vizată despre aceasta fără întârziere nejustificată, dar nu mai târziu de o (1) lună de la primirea cererii.

* + - * **Date personale**. Angajatul responsabil trebuie să verifice dacă IGUS INNOVATIVE SOLUTIONS SRL are acces la datele personale solicitate. În cazul în care IGUS INNOVATIVE SOLUTIONS SRL nu are datele cu caracter personal sub control, angajatul responsabil trebuie să informeze persoana vizată și, dacă este posibil, să instruiască pașii suplimentari cu privire la modul de accesare a datelor în cauză;
      * **Conținutul cererii**. În funcție de conținutul DSR, angajatul responsabil trebuie să definească tipul cererii și să verifice dacă îndeplinește condițiile prevăzute de această politică și legile privind protecția datelor. Tipurile de cereri și condițiile respective pentru fiecare dintre acestea pot fi consultate în subsecțiunile 6.3-6.9. În cazul în care solicitarea nu îndeplinește criteriile descrise, angajatul responsabil trebuie să refuze respectarea DSR și să informeze persoana vizată despre motivele refuzului;
      * **Gratuit.** În general, toate cererile persoanelor vizate și exercitarea drepturilor acestora sunt gratuite. În cazul în care angajatul responsabil constată că persoana vizată își exercită drepturile într-un mod excesiv sau nefondat (de exemplu, intenționat să dăuneze sau să întrerupă activitățile comerciale ale IGUS INNOVATIVE SOLUTIONS SRL), angajatul trebuie să solicite sfatul de la Managerul de confidențialitate și, la primirea acesta din urmă, poate fie să perceapă persoanei vizate o taxă rezonabilă, fie să refuze să se conformeze cererii;
      * **Documentarea**. Ori de câte ori IGUS INNOVATIVE SOLUTIONS SRL primește DSR, Managerul de confidențialitate trebuie să se asigure că datele și ora, persoana vizată, tipul cererii și decizia luată cu privire la aceasta sunt bine documentate. În cazul refuzului de a se conforma cererii, trebuie documentate și motivele refuzului;
      * **Destinatari**. Când se adresează DSR, Managerul de confidențialitate trebuie să se asigure că toți destinatarii în cauză au fost informați cu privire la acțiunile necesare.

* 1. **Dreptul de a fi informat**.
     1. IGUS INNOVATIVE SOLUTIONS SRL trebuie să notifice fiecare subiect de date cu privire la colectarea și prelucrarea ulterioară a datelor cu caracter personal.
     2. Informațiile care trebuie furnizate includ: numele și datele de contact ale IGUS INNOVATIVE SOLUTIONS SRL; scopuri generice și baza legală pentru colectarea datelor și prelucrarea ulterioară; categorii de date personale colectate; destinatari / categorii de destinatari; perioade de păstrare; informații despre drepturile persoanei vizate, inclusiv dreptul de a depune plângere la autoritatea de supraveghere competentă; consecințele cazurilor în care datele sunt necesare pentru executarea contractului și persoana vizată nu furnizează datele solicitate; detalii despre garanțiile în care datele cu caracter personal sunt transferate în afara SEE; și orice sursă terță parte a datelor cu caracter personal, fără specificarea cazului particular (cu excepția cazului în care primim solicitarea directă de la persoana vizată).
     3. Utilizatorii trebuie informați prin Politica de confidențialitate accesibilă pe site-ul web IGUS INNOVATIVE SOLUTIONS SRL și furnizată în timpul înregistrării utilizatorului. Angajații și contractanții trebuie informați printr-o declarație de confidențialitate independentă a angajaților, care explică detaliile descrise la p. 6.2.2 într-o manieră bazată pe cazuri, descriind scopurile și activitățile specifice.
     4. IGUS INNOVATIVE SOLUTIONS SRL trebuie să informeze persoanele vizate despre prelucrarea datelor, inclusiv orice activitate de prelucrare nouă introdusă la IGUS INNOVATIVE SOLUTIONS SRL în termenul următor:
        + dacă datele cu caracter personal sunt colectate direct de la persoana vizată, persoana vizată trebuie să fie informată în momentul colectării datelor cu caracter personal de la persoanele vizate, arătând persoanei vizate declarația noastră de confidențialitate;
        + dacă datele cu caracter personal sunt colectate din alte surse: (a) în termen de o lună de la colectarea acestora; (b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată; sau (c) dacă este prevăzută o divulgare către un alt destinatar, cel târziu la data publicării pentru prima dată a datelor cu caracter personal.
        + la cererea persoanei vizate; și
        + în termen de o (1) lună după orice modificare a practicilor noastre de date cu caracter personal, schimbarea operatorului de date cu caracter personal sau după modificări semnificative în declarațiile noastre de confidențialitate.

* 1. **Dreptul de a accesa informațiile**.
     1. Persoana vizată trebuie să fie furnizată numai cu acele înregistrări de date cu caracter personal specificate în cerere. Dacă persoana vizată solicită accesul la toate datele personale care o privesc, angajatul trebuie să solicite mai întâi sfatul managerului de confidențialitate, pentru a se asigura că toate datele personale ale persoanei vizate sunt mapate și furnizate.
     2. O persoană vizată are dreptul la:
        + aflați dacă prelucrăm datele personale ale persoanei vizate;
        + obține dezvăluire cu privire la aspecte ale prelucrării, inclusiv informații detaliate și specifice cazului cu privire la scopuri, categorii de date cu caracter personal, destinatari / categorii de destinatari, perioade de păstrare, informații despre drepturile cuiva, detalii despre garanțiile relevante în cazul în care datele cu caracter personal sunt transferate în afara SEE , și orice sursă terță parte a datelor cu caracter personal; și
        + obțineți o copie a datelor cu caracter personal în curs de prelucrare la cerere.

* 1. **Dreptul de a verifica informațiile persoanei vizate și de a solicita rectificarea acestora**. Informațiile pe care le colectăm pot fi / devin inexacte sau depășite (de exemplu, greșeli de naționalitate, data nașterii, informații despre datorii, activități economice). Dacă dezvăluim că datele personale sunt inexacte sau persoana vizată ne solicită acest lucru, trebuie să ne asigurăm că corectăm toate greșelile și actualizăm informațiile relevante.

* 1. **Dreptul de a restricționa prelucrarea**.
     1. Restricționarea prelucrării permite persoanelor vizate să oprească temporar utilizarea informațiilor lor pentru a preveni posibilele daune cauzate de o astfel de utilizare.
     2. Acest drept se aplică atunci când persoana vizată:
        + contestă acuratețea datelor cu caracter personal;
        + consideră că prelucrăm datele cu caracter personal în mod ilegal; și
        + se opune procesării și dorește să nu prelucrăm datele cu caracter personal în timp ce analizăm solicitarea.
     3. În cazul primirii cererii de restricție, nu trebuie să prelucrăm datele cu caracter personal în cauză în alt scop decât stocarea acestora sau în scopuri de conformitate legală până când circumstanțele restricției nu mai există.

* 1. **Dreptul de a retrage consimțământul**.Pentru activitățile care necesită consimțământul, persoana vizată își poate revoca consimțământul în orice moment. Dacă persoana vizată revocă consimțământul, trebuie să înregistrăm modificările și nu trebuie să prelucrăm datele cu caracter personal în scopuri bazate pe consimțământ. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate înainte de retragere.

* 1. **Dreptul de a obiecta împotriva prelucrării**.
     1. Dacă prelucrăm informațiile în interesele noastre legitime, de exemplu, pentru e-mailuri de marketing direct sau în scopurile noastre de cercetare de marketing, persoana vizată poate obiecta împotriva prelucrării.
     2. În cazul primirii cazului cererii de obiecție, trebuie să luăm în considerare solicitarea persoanei vizate și, în cazul în care nu avem interese imperioase, să oprim prelucrarea în scopurile specificate. În cazul în care datele cu caracter personal urmează să fie procesate în alte scopuri, Managerul de confidențialitate trebuie să se asigure că baza de date are o înregistrare că datele nu pot fi prelucrate în continuare pentru activitățile obiectate.
     3. Cererea de obiecție poate fi refuzată numai dacă datele cu caracter personal în cauză sunt utilizate în scopuri de cercetare științifică / istorică sau în scopuri statistice și au fost protejate corespunzător, adică prin tehnici de anonimizare sau pseudonimizare.

* 1. **Dreptul la ștergere / la uitare**.
     1. Persoanele vizate au dreptul să ne ceară să le ștergem datele personale dacă sunt îndeplinite una dintre următoarele condiții:
        + Datele cu caracter personal nu mai sunt necesare în scopul colectării. De exemplu, un utilizator a furnizat date cu caracter personal pentru o activitate unică, cum ar fi validarea datelor sau participarea la un concurs, iar scopul este deja îndeplinit;
        + Persoana vizată își revocă consimțământul sau se opune prelucrării (acolo unde este cazul) și nu există un alt temei legal pentru prelucrare; sau
        + prelucrăm datele cu caracter personal în mod ilegal sau ștergerea acestora este cerută de legislația aplicabilă a Uniunii Europene sau a uneia dintre țările membre ale Uniunii Europene.
     2. Condiții în care avem dreptul de a refuza ștergerea:
        + Datele cu caracter personal sunt prelucrate în scopuri științifice / istorice sau statistice și sunt protejate corespunzător, adică pseudonimizate sau anonimizate;
        + Datele cu caracter personal sunt încă necesare pentru respectarea legii (de exemplu, respectarea legislației financiare sau a muncii).
     3. Trebuie șterse numai acele înregistrări de date cu caracter personal care au fost specificate în cerere. Dacă persoana vizată solicită ștergerea tuturor datelor cu caracter personal care o privesc, angajatul trebuie să solicite mai întâi sfatul administratorului de confidențialitate, pentru a se asigura că toate datele despre persoana vizată sunt mapate și pot fi șterse.
     4. Dacă Utilizatorul are încă un cont la noi și solicită ștergerea informațiilor necesare menținerii contului, trebuie să îl informăm pe utilizator că ștergerea va afecta experiența utilizatorului sau poate duce la închiderea contului.

* 1. **Portabilitatea datelor**.
     1. Persoanele vizate ne pot cere să transferăm toate datele personale și / sau partea sa într-un format care poate fi citit de mașină către o terță parte. Acest drept se aplică în două cazuri:
        + datele personale au fost colectate în scopul furnizării serviciilor noastre (executarea contractului); sau
        + colectate pe baza consimțământului.
     2. Pentru a determina dacă una dintre condițiile de la p.6.9.1 este îndeplinită, angajatul trebuie să solicite sfatul managerului de confidențialitate și să verifice baza legală aplicabilă în Evidența activităților de prelucrare. În cazul în care răspunsul este negativ, solicitarea poate fi refuzată de IGUS INNOVATIVE SOLUTIONS SRL, iar Managerul de confidențialitate trebuie să decidă dacă să respecte cererea în mod voluntar.
     3. Pentru a respecta cererea, angajatul responsabil trebuie să consolideze datele personale solicitate și să trimită datele în formatul cu care lucrăm de obicei către organizația solicitată. Persoana vizată trebuie să furnizeze datele de contact necesare ale organizației.

## **Noi activități de prelucrare a datelor**

* 1. **Notificare către Managerul de confidențialitate**
     1. Înainte de a introduce orice activitate nouă care implică prelucrarea datelor cu caracter personal, un angajat responsabil de implementarea acestuia trebuie să informeze Managerul de confidențialitate.
     2. La primirea informațiilor despre o nouă activitate, Managerul de confidențialitate trebuie:
        + stabiliți dacă este necesară evaluarea impactului procesării datelor (DPIA) și / sau consultarea cu autoritatea de supraveghere. Dacă răspunsul este pozitiv, Managerul de confidențialitate trebuie să se asigure că DPIA este efectuat și / sau Autoritatea de supraveghere este consultată în conformitate cu cerințele acestei secțiuni și cu legile privind protecția datelor;
        + să stabilească baza legală pentru prelucrare și, dacă este necesar, să ia măsuri suplimentare pentru fixarea acesteia;
        + asigurați-vă că activitatea de prelucrare se realizează în conformitate cu această politică, cu alte politici IGUS INNOVATIVE SOLUTIONS SRL, precum și cu legile privind protecția datelor;
        + adăugați activitatea de procesare la Evidența activităților de procesare;
        + modifică declarațiile de confidențialitate și, dacă este necesar, informează persoana vizată în consecință.

* 1. **Evaluarea impactului procesării datelor**
     1. Pentru a ne asigura că activitățile noastre actuale sau prospective de prelucrare nu încalcă / nu vor încălca drepturile persoanelor vizate, IGUS INNOVATIVE SOLUTIONS SRL trebuie, acolo unde este impus de legile privind protecția datelor, să efectueze Evaluarea impactului procesării datelor (DPIA), o evaluare bazată pe riscuri a procesării și căutării măsurilor de atenuare a riscurilor. Managerul de confidențialitate trebuie să se asigure că DPIA se desfășoară în conformitate cu această secțiune.
     2. Managerul de confidențialitate, unde este necesar, implicând angajații competenți și / sau consilieri externi, trebuie să efectueze un DPIA dacă sunt îndeplinite cel puțin una dintre următoarele condiții:
        + prelucrarea implică utilizarea noilor tehnologii, cum ar fi inteligența artificială, utilizarea dispozitivelor conectate și autonome etc., care creează anumite efecte juridice, economice sau similare persoanei vizate;
        + evaluăm și evaluăm sistematic aspectele personale ale persoanelor vizate pe baza profilării automate, alocând scorul / rata personală și creăm efecte juridice sau similare pentru persoana vizată prin această activitate;
        + prelucrăm date sensibile la scară largă, care includ date personale referitoare la condamnări și infracțiuni penale, datele despre persoanele vulnerabile, datele cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, credințele religioase sau filozofice sau apartenența la sindicat și prelucrarea datelor genetice, a datelor biometrice în scopul identificării unice a unei persoane fizice, a datelor privind sănătatea sau a datelor privind viața sexuală sau orientarea sexuală a unei persoane fizice;
        + colectăm sau prelucrăm date personale dintr-o zonă accesibilă publicului sau surse publice pe scară largă, sau combinăm sau potrivim două seturi de date diferite; și
        + Autoritatea de supraveghere din lista sa publică necesită efectuarea unui DPIA pentru un anumit tip de activitate în care suntem implicați. Lista activităților de prelucrare care necesită efectuarea DPIA poate fi găsită pe site-ul web al fiecărei autorități de supraveghere.
     3. Evaluarea conține cel puțin următoarele detalii:
        + o descriere sistematică a operațiunilor de prelucrare și a scopurilor prelucrării, inclusiv, dacă este cazul, interesul legitim urmărit de noi. Descrierea trebuie să includă categoriile de date și persoanele vizate vizate, amploarea activităților de prelucrare, precum frecvența, volumul, numărul preconizat de înregistrări etc .; destinatarii datelor, perioadele de păstrare și, după caz, transferurile internaționale;
        + o evaluare a necesității și proporționalității operațiunilor de prelucrare în raport cu scopurile. DPIA trebuie să explice dacă activitatea este necesară în acest scop și dacă scopul poate fi atins prin metode mai puțin intruzive;
        + o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate, inclusiv drepturile persoanelor vizate cu privire la datele lor personale.
        + Exemplele de riscuri sunt prelucrarea care ar putea duce la daune fizice, materiale sau nemateriale, în special: în cazul în care prelucrarea poate duce la discriminare, furt de identitate sau fraudă, pierderi financiare, deteriorarea reputației, pierderea confidențialității personalului date protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau orice alt dezavantaj economic sau social semnificativ; în cazul în care persoanele vizate ar putea fi private de drepturile și libertățile lor sau împiedicate să exercite controlul asupra datelor lor personale; în cazul în care sunt prelucrate date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența la sindicat și prelucrarea datelor genetice, a datelor privind sănătatea sau a datelor privind viața sexuală sau condamnările și infracțiunile penale sau măsurile de securitate conexe; acolo unde sunt evaluate aspectele personale, în special analizând sau prezicând aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau mișcările, pentru a crea sau utiliza profiluri personale; în cazul în care datele personale ale persoanelor fizice vulnerabile, în special ale copiilor, sunt prelucrate; sau în cazul în care prelucrarea implică o cantitate mare de date cu caracter personal și afectează un număr mare de persoane vizate; și sau în cazul în care prelucrarea implică o cantitate mare de date cu caracter personal și afectează un număr mare de persoane vizate; și sau în cazul în care prelucrarea implică o cantitate mare de date cu caracter personal și afectează un număr mare de persoane vizate; și
        + măsurile de abordare a riscurilor, inclusiv măsuri de protecție, măsuri de securitate și mecanisme pentru a asigura protecția datelor cu caracter personal și pentru a demonstra conformitatea cu prezentul regulament.
     4. În cazul în care DPIA nu a furnizat modalități de abordare eficientă a riscurilor, Managerul de confidențialitate trebuie să inițieze consultarea cu autoritatea de supraveghere competentă pentru a primi ajutor în căutarea soluției. În acest caz, IGUS INNOVATIVE SOLUTIONS SRL nu trebuie să desfășoare activitatea înainte ca Autoritatea de Supraveghere să aprobe activitatea de prelucrare în cauză.

## **Păstrarea datelor**

* 1. **Regula generala**.
     1. Managerul de confidențialitate trebuie să se asigure că IGUS INNOVATIVE SOLUTIONS SRL a definit în mod clar perioadele de stocare a datelor și / sau criteriile pentru determinarea perioadelor de stocare pentru fiecare activitate de procesare pe care o are. Perioadele pentru fiecare activitate de prelucrare trebuie specificate în Evidența activităților de prelucrare.
     2. Fiecare departament din cadrul IGUS INNOVATIVE SOLUTIONS SRL trebuie să respecte perioadele de stocare a datelor în conformitate cu programul de păstrare prevăzut în Evidența activităților de prelucrare. Managerul de confidențialitate trebuie să supravegheze fiecare departament și să se asigure că respectă această cerință.
     3. După încheierea perioadei de stocare, datele cu caracter personal trebuie eliminate de la dispoziția departamentului responsabil cu prelucrarea sau, în cazurile în care datele nu sunt necesare în alte scopuri, trebuie distruse complet, inclusiv din copiile de rezervă și din alte suporturi.
     4. Ori de câte ori perioada de stocare pentru o activitate de prelucrare s-a încheiat, dar datele cu caracter personal prelucrate sunt necesare în alte scopuri de prelucrare, directorul departamentului trebuie să se asigure că datele personale nu sunt utilizate pentru activitatea de prelucrare încetată, iar angajații responsabili nu au acces la acesta, cu excepția cazului în care este necesar pentru orice altă activitate.

* 1. **Scutiri**. Regulile specificate în subsecțiunea 8.1 au următoarele excepții:
     1. **Nevoi de afaceri**. Perioadele de păstrare a datelor pot fi prelungite, dar nu mai mult de 60 de zile, în cazul în care ștergerea datelor va întrerupe sau va afecta afacerea noastră în desfășurare. Managerul de confidențialitate trebuie să aprobe orice prelungire neprevăzută;
     2. **Imposibilitate tehnică**. Unele informații sunt din punct de vedere tehnic imposibile sau disproporționat de șterse. De exemplu, ștergerea informațiilor poate duce la încălcarea integrității sistemului sau este imposibilă ștergerea informațiilor din copiile de rezervă. Într-un astfel de caz, informațiile pot fi stocate în continuare, sub rezerva aprobării de către Managerul de confidențialitate și a modificărilor respective la Evidența activităților de prelucrare; și
     3. **Anonimizare**.Datele cu caracter personal pot fi prelucrate în continuare în orice scop (de exemplu, marketing) dacă anonimizăm complet aceste date după expirarea perioadei de păstrare. Aceasta înseamnă că toți identificatorii personali și conexiunile la aceștia vor fi șterse din date. Pentru a considera datele personale anonime, trebuie să fie imposibil să reidentificați persoana vizată din setul de date.

## **Securitate**

* 1. Fiecare departament din cadrul IGUS INNOVATIVE SOLUTIONS SRL va lua toate măsurile tehnice și organizatorice adecvate care protejează împotriva accesului neautorizat, ilegal și / sau accidental, distrugerii, modificării, blocării, copierii, distribuției, precum și împotriva altor acțiuni ilegale ale persoanelor neautorizate cu privire la date cu caracter personal aflate sub responsabilitatea lor.

* 1. Angajatul responsabil cu supravegherea după securitatea datelor cu caracter personal în cadrul IGUS INNOVATIVE SOLUTIONS SRL va fi specialist IT. Această persoană pune în aplicare liniile directoare și alte specificații privind protecția datelor și securitatea informațiilor în zona sa de responsabilitate. El / ea sfătuiește conducerea IGUS INNOVATIVE SOLUTIONS SRL cu privire la planificarea și implementarea securității informațiilor în IGUS INNOVATIVE SOLUTIONS SRL și trebuie să fie implicat în toate proiectele într-un stadiu incipient pentru a lua în considerare aspectele legate de securitate încă din faza de planificare. .

## **Procedura de răspuns la încălcarea datelor**

* 1. **Echipa de răspuns**.
     1. În cazul dezvăluirii încălcării datelor, CEO-ul IGUS INNOVATIVE SOLUTIONS SRL va forma urgent echipa de răspuns la încălcarea datelor („Echipa de răspuns”), care se va ocupa de încălcarea datelor, va notifica persoanele corespunzătoare și va atenua riscurile acesteia.
     2. Echipa de răspuns trebuie să fie un grup multidisciplinar condus de CEO-ul IGUS INNOVATIVE SOLUTIONS SRL și format din Managerul de confidențialitate, specialist în legislația privind confidențialitatea (fie el intern sau extern) și specialiști cu cunoștințe de specialitate și securitate a informațiilor din cadrul IGUS INNOVATIVE SOLUTIONS SRL sau profesioniști în externalizare , daca este necesar. Echipa trebuie să se asigure că toți angajații și contractanții / procesatorii angajați aderă la prezenta politică și să ofere un răspuns imediat, eficient și abil la orice încălcare suspectată / presupusă sau efectivă a datelor care afectează IGUS INNOVATIVE SOLUTIONS SRL.
     3. Membrii potențiali ai echipei de răspuns trebuie să fie pregătiți să răspundă la o încălcare a datelor. Echipa de răspuns va îndeplini toate responsabilitățile IGUS INNOVATIVE SOLUTIONS SRL menționate în prezenta politică. Sarcinile echipei de răspuns sunt:
        + să comunice încălcarea datelor către autoritatea (autoritățile) de supraveghere competentă;
        + în caz de risc ridicat pentru drepturile și libertățile persoanelor vizate, să comunice încălcarea datelor către persoana vizată;
        + dacă IGUS INNOVATIVE SOLUTIONS SRL obține date de la orice terță parte în calitate de procesator, iar o încălcare a datelor implică datele obținute, pentru a informa terții despre încălcarea datelor;
        + să comunice contractanților IGUS INNOVATIVE SOLUTIONS SRL sau oricărei alte părți terțe care prelucrează datele cu caracter personal implicate în încălcarea datelor; și
        + să ia toate măsurile tehnice și organizaționale adecvate pentru a înceta încălcarea datelor și pentru a atenua consecințele acesteia;
        + să înregistreze încălcarea datelor în Evidența activităților de prelucrare și să înregistreze un raport intern de încălcare a datelor care descrie evenimentul.
     4. Echipa de răspuns își va îndeplini sarcinile până când vor fi luate toate măsurile necesare cerute de prezenta politică.

* 1. **Notificare către autoritatea de supraveghere**.
     1. IGUS INNOVATIVE SOLUTIONS SRL va informa Autoritatea competentă de supraveghere cu privire la încălcarea datelor fără întârzieri nejustificate și, acolo unde este posibil, nu mai târziu de 72 de ore după ce a luat cunoștință de încălcarea datelor.
     2. Autoritatea competentă de supraveghere este determinată de reședința persoanelor vizate, ale căror informații au fost implicate în încălcarea datelor. În cazul în care încălcarea datelor se referă la datele cu caracter personal ale persoanelor vizate din mai multe țări, IGUS INNOVATIVE SOLUTIONS SRL va informa toate autoritățile de supraveghere competente.
     3. Pentru a adresa notificarea autorității, echipa de răspuns ar trebui să utilizeze anexa 1 la prezenta politică. Anexa 1 conține toate informațiile de contact necesare ale autorităților de supraveghere ale UE. În cazul în care încălcarea datelor se referă la persoane vizate din alte țări decât UE, echipa de răspuns va cere sfatul unui specialist competent în domeniul confidențialității.
     4. Notificarea către autoritatea de supraveghere competentă conține cel puțin următoarele informații:
        + **natura încălcării datelor** inclusiv acolo unde este posibil, categoriile și un număr aproximativ de persoane vizate și înregistrări de date cu caracter personal în cauză;
        + numele și detaliile de contact ale echipei de răspuns, Managerul de confidențialitate sau, dacă nu este cazul, al directorului executiv;
        + consecințele probabile ale încălcării datelor. Explicați punctul de vedere al IGUS INNOVATIVE SOLUTIONS SRL asupra scopurilor și posibilelor riscuri ulterioare ale încălcării datelor. De exemplu, datele cu caracter personal pot fi furate pentru vânzare ulterioară, activități de fraudă sau șantajarea persoanelor vizate; și
        + **măsurile luate sau propuse** care urmează să fie luate de IGUS INNOVATIVE SOLUTIONS SRL pentru a aborda încălcarea datelor, inclusiv, după caz, măsuri de atenuare a posibilelor sale efecte adverse.
     5. Pentru a depune o notificare, echipa de intervenție ar trebui să utilizeze formularul de notificare privind încălcarea datelor către IGUS INNOVATIVE SOLUTIONS SRL către autoritatea de supraveghere.

* 1. **Notificări către persoanele vizate**.
     1. În cazul în care încălcarea datelor poate avea drept rezultat un risc ridicat pentru drepturile și libertățile persoanelor vizate (de exemplu, furtul de fonduri, active, informații de proprietate), trebuie să comunicăm, de asemenea, încălcarea datelor persoanelor vizate fără întârzieri nejustificate. Managerul de confidențialitate trebuie să stabilească dacă există un risc ridicat pe baza factorilor de risc specificați în subsecțiunea 7.2.3 din prezenta politică.
     2. Notificarea conține următoarele informații:
        + descrierea încălcării datelor - ce s-a întâmplat și ce a condus la încălcarea datelor, cum ar fi o încălcare a securității, neglijența angajaților, erori în funcționarea sistemului. Dacă echipa de răspuns a decis să nu dezvăluie cauzele încălcării datelor, atunci această clauză nu trebuie menționată;
        + măsurile luate de IGUS INNOVATIVE SOLUTIONS SRL cu privire la încălcarea datelor, inclusiv măsuri de securitate, investigații interne și notificarea autorității de supraveghere;
        + recomandări pentru persoanele vizate vizate cum să atenueze riscurile și posibilele consecințe, cum ar fi liniile directoare privind modul de restabilire a accesului la un cont, prevenirea măsurilor (schimbarea unei parole); și
        + informațiile de contact ale echipei de răspuns sau ale unuia dintre membrii acesteia.
     3. Notificarea către persoanele vizate trebuie efectuată prin scrisoarea prin e-mail sau, în cazul în care este imposibil de utilizat, prin alte mijloace de comunicare disponibile.
     4. **Scutiri**.Nu trebuie să trimitem notificarea persoanelor vizate dacă sunt îndeplinite oricare dintre următoarele condiții:
        + IGUS INNOVATIVE SOLUTIONS SRL a implementat măsuri de protecție tehnică și organizațională adecvate, iar aceste măsuri au fost aplicate Datelor cu caracter personal afectate de încălcarea datelor, în special celor care lasă datele cu caracter personal inaccesibile oricărei persoane care nu este autorizată să le acceseze, astfel ca criptare;
        + IGUS INNOVATIVE SOLUTIONS SRL a luat măsuri ulterioare care să asigure că riscul ridicat pentru drepturile și libertățile persoanelor vizate menționate în această secțiune nu se mai poate materializa; sau
        + ar presupune un efort disproporționat de a comunica cu fiecare persoană vizată. Într-un astfel de caz, va exista în schimb o comunicare publică sau o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficient.

În cazul în care aplicăm una dintre scutiri, trebuie să documentăm circumstanțele, motivul pentru care nu informăm și măsurile întreprinse pentru a îndeplini una dintre scutiri.

* 1. **Comunicarea cu terți**.
     1. În cazul în care o încălcare a datelor se referă la datele cu caracter personal partajate cu noi sau prelucrate de noi în numele unei terțe părți, trebuie să informăm terțul cu privire la aceasta în termen de 24 de ore. Dacă prelucrăm datele cu caracter personal ca procesator de date, notificarea terțului nu ne scutește de obligația de a atenua consecințele încălcării datelor, dar nu trebuie să informăm autoritatea de supraveghere competentă și persoanele vizate.
     2. În cazul primirii notificării cu privire la încălcarea datelor de la Procesorul de date sau de la alte terțe părți care au acces la datele cu caracter personal, CEO-ul IGUS INNOVATIVE SOLUTIONS SRL va face, în conformitate cu prezenta secțiune:
        + formează echipa de răspuns;
        + solicitați părții terțe să trimită informațiile menționate în subsecțiunile 10.2-3 din prezenta politică;
        + dacă este necesar, informați autoritatea (autoritățile) de supraveghere competentă și persoanele vizate; și
        + efectuați alți pași ai procedurii de răspuns la încălcarea datelor.

**ANEXA 1 LA POLITICA DE PROTECȚIE A DATELOR PERSONALE**

**Autoritățile naționale europene pentru protecția datelor**

**Austria**

**Österreichische Datenschutzbehörde**

Hohenstaufengasse 3

1010 Viena

Tel. +43 1 531 15 202525

Fax +43 1 531 15 202690

e-mail: [dsb@dsb.gv.at](mailto:dsb@dsb.gv.at)

Site web: <http://www.dsb.gv.at/>

Membru 29 Art WP: Dr. Andrea JELINEK, Director, Österreichische Datenschutzbehörde

**Belgia**

**Commission de la protection de la vie privée**

**Commissie voor de bescherming van de persoonlijke levenssfeer**

Rue de la Presse 35 / Drukpersstraat 35 1000 Bruxelles / 1000 Brussel

Tel. +32 2 274 48 00

Fax +32 2 274 48 35

e-mail: [commission@privacycommission.be](mailto:commission@privacycommission.be)

Site web: <http://www.privacycommission.be/>

Art. 29 Vicepreședintele WP: Willem DEBEUCKELAERE, președintele Comisiei belgiene pentru confidențialitate

**Bulgaria**

**Comisia pentru protecția datelor cu caracter personal**

2, bl. Prof. Tsvetan Lazarov. 1592

Tel. +359 2 915 3580

Fax +359 2 915 3525

e-mail: [kzld@cpdp.bg](mailto:kzld@cpdp.bg)

Site web: <http://www.cpdp.bg/>

Art 29 Membru WP: dl Ventsislav KARADJOV, președinte al Comisiei pentru protecția datelor cu caracter personal

Art 29 WP Membru supleant: dna Mariya MATEVA

**Croaţia**

**Agenția Croată pentru Protecția Datelor cu Caracter Personal**

Martićeva 14

10000 Zagreb

Tel. +385 1 4609 000

Fax +385 1 4609 099

e-mail: [azop@azop.hr](mailto:azop@azop.hr) sau [info@azop.hr](mailto:info@azop.hr)

Site web: <http://www.azop.hr/>

Art 29 Membru WP: Dl Anto RAJKOVAČA, Directorul Agenției Croate pentru Protecția Datelor

**Cipru**

**Comisar pentru protecția datelor cu caracter personal**

1 Iasonos Street,

1082 Nicosia

Caseta postala 23378, CY-1682 Nicosia Tel. +357 22 818 456

Fax +357 22 304 565

e-mail: [commissioner@dataprotection.gov.cy](mailto:jcommissioner@dataprotection.gov.cy)

Site web: <http://www.dataprotection.gov.cy/>

Art 29 Membru WP: Dna Irene LOIZIDOU NIKOLAIDOU

Art 29 WP Membru supleant: dl Constantinos GEORGIADES

**Republica Cehă**

**Biroul pentru protecția datelor cu caracter personal**

Urad pro ochranu osobnich udaju Pplk. Sochora 27

170 00 Praga 7

Tel. +420 234 665 111

Fax +420 234 665 444

e-mail: [posta@uoou.cz](mailto:posta@uoou.cz)

Site web: <http://www.uoou.cz/>

Art 29 Membru WP: dna Ivana JANŮ, președinte al Oficiului pentru Protecția Datelor cu Caracter Personal

Art 29 Membru alternativ WP: domnul Ivan PROCHÁZKA, consilier al președintelui biroului

**Danemarca**

**Datatilsynet**

Borgergade 28, 5

1300 Copenhaga K

Tel. +45 33 1932 00

Fax +45 33 19 32 18

e-mail: [dt@datatilsynet.dk](mailto:dt@datatilsynet.dk)

Site web: <http://www.datatilsynet.dk/>

Art 29 WP Membru: Dna Cristina Angela GULISANO, Director, Agenția Daneză pentru Protecția Datelor (Datatilsynet)

Art 29 WP Membru supleant: dl Peter FOGH KNUDSEN, șef al diviziei internaționale la Agenția daneză pentru protecția datelor (Datatilsynet)

**Estonia**

**Inspectoratul pentru protecția datelor din Estonia (Andmekaitse Inspektsioon)**

Väike-Ameerika 19

10129 Tallinn

Tel. +372 6274 135

Fax +372 6274 137

e-mail: [info@aki.ee](mailto:info@aki.ee)

Site web: <http://www.aki.ee/en>

Art. 29 WP Membru: dl Viljar PEEP, director general, Inspectoratul Estonian pentru Protecția Datelor

Art 29 WP Membru supleant: dna Maarja Kirss

**Finlanda**

**Biroul Ombudsmanului pentru Protecția Datelor**

Căsuța poștală 315

FIN-00181 Helsinki Tel. +358 10 3666 700

Fax +358 10 3666 735

e-mail: [tietosuoja@om.fi](mailto:tietosuoja@om.fi)

Site web: <http://www.tietosuoja.fi/en/>

Art 29 Membru WP: dl Reijo AARNIO, Ombudsman al Autorității finlandeze pentru protecția datelor

Art 29 WP Membru supleant: dna Elisa KUMPULA, șef de departament

**Franţa**

**Commission Nationale de l'Informatique et des Libertés - CNIL**

8 rue Vivienne, CS 30223 F-75002 Paris, Cedex 02 Tel. +33 1 53 73 22 22

Fax +33 1 53 73 22 00

Site web: <http://www.cnil.fr/>

Art 29 Membru WP: dna Isabelle FALQUE-PIERROTIN, președinte CNIL

Art 29 WP Membru supleant: dna Florence RAYNAL

**Germania**

**Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit**

Husarenstraße 30

53117 Bonn

Tel. +49 228 997799 0; +49 228 81995 0

Fax +49 228 997799 550; +49 228 81995 550

e-mail: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)

Site web: <http://www.bfdi.bund.de/>

Competența pentru reclamații este împărțită între diferite autorități de supraveghere a protecției datelor din Germania.

Autoritățile competente pot fi identificate conform listei furnizate la <https://www.bfdi.bund.de/bfdi_wiki/index.php/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte>

Art 29 Membru WP: dna Andrea VOSSHOFF, comisar federal pentru libertatea de informare

Art 29 WP Membru supleant: Prof. Dr. Johannes CASPAR, reprezentant al statelor federale

**Grecia**

**Autoritatea Elenă pentru Protecția Datelor**

Kifisias Av. 1-3, PC 11523 Ampelokipi Atena

Tel. +30 210 6475 600

Fax +30 210 6475 628

e-mail: [contact@dpa.gr](mailto:contact@dpa.gr)

Site web: <http://www.dpa.gr/>

Art 29 Membru WP: domnul Konstantinos Menoudakos, președintele APD elen

Art 29 WP Membru supleant: Dr. Vasilios ZORKADIS, director

**Ungaria**

**Autoritatea Națională pentru Protecția Datelor și Libertatea Informației**

Szilágyi Erzsébet fasor 22 / C H-1125 Budapest

Tel. +36 1 3911 400

e-mail: [peterfalvi.attila@naih.hu](mailto:peterfalvi.attila@naih.hu)

Site web: <http://www.naih.hu/>

Art 29 Membru WP: Dr. Attila PÉTERFALVI, președintele Autorității Naționale pentru Protecția Datelor și Libertatea Informației

Art 29 WP Membru supleant: dl Endre Győző SZABÓ Vicepreședinte al Autorității Naționale pentru Protecția Datelor și Libertatea Informației

**Irlanda**

**Comisar pentru protecția datelor**

Canal House Station Road Portarlington Co. Laois

Lo-Call: 1890 25 22 31

Tel. +353 57 868 4800

Fax +353 57 868 4757

e-mail: [info@dataprotection.ie](mailto:info@dataprotection.ie)

Site web: <http://www.dataprotection.ie/>

Art 29 Membru WP: dna Helen DIXON, comisar pentru protecția datelor

Art. 29 Membrii supleanți ai WP: dl John O'DWYER, comisar adjunct; Dl Dale SUNDERLAND, comisar adjunct

**Italia**

**Garanție pentru protecția datelor personale**

Piazza di Monte Citorio, 121 00186 Roma

Tel. +39 06 69677 1

Fax +39 06 69677 785

e-mail: [garante@garanteprivacy.it](mailto:garante@garanteprivacy.it)

Site web: <http://www.garanteprivacy.it/>

Art 29 Membru WP: domnul Antonello SORO, președintele Garante pentru protecția datelor personale

Art 29 WP Membru supleant: dna Giuseppe BUSIA, secretar general al Garanției pentru protecția datelor personale

**Letonia**

**Directorul inspectoratului de stat al datelor: doamna Daiga Avdejanova**

Str. Blaumana. 11 / 13-15

1011 Riga

Tel. +371 6722 3131

Fax +371 6722 3556

e-mail: [info@dvi.gov.lv](mailto:info@dvi.gov.lv)

Site web: <http://www.dvi.gov.lv/>

Art 29 Membru alternativ WP: Dna Aiga BALODE

**Lituania**

**Protecția datelor de stat**

Žygimantų str. 11-6a 011042 Vilnius

Tel. + 370 5 279 14 45

Fax +370 5 261 94 94

e-mail: [ada@ada.lt](mailto:ada@ada.lt)

Site web: <http://www.ada.lt/>

Art 29 Membru WP: dl Raimondas Andrijauskas, directorul Inspectoratului de Stat pentru Protecția Datelor

Art 29 WP Membru supleant: dna Neringa KAKTAVIČIŪTĖ-MICKIENĖ, șefa diviziei de investigare a reclamațiilor și cooperare internațională

**Luxemburg**

**Commission Nationale pour la Protection des Données**

1, avenue du Rock'n'Roll L-4361 Esch-sur-Alzette Tel. +352 2610 60 1

Fax +352 2610 60 29

e-mail: [info@cnpd.lu](mailto:info@cnpd.lu)

Site web: <http://www.cnpd.lu/>

Art 29 Membru WP: Dna Tine A. LARSEN, Președintele Comisiei Naționale pentru Protecția Datelor

Art 29 WP Membru supleant: dl Thierry LALLEMANG, comisar

**Malta**

**Biroul comisarului pentru protecția datelor Comisarul pentru protecția datelor: dl Joseph Ebejer**

2, Airways House

High Street, Sliema SLM 1549 Tel. +356 2328 7100

Fax +356 2328 7198

e-mail: [commissioner.dataprotection@gov.mt](mailto:commissioner.dataprotection@gov.mt)

Site web: <http://www.dataprotection.gov.mt/>

Art 29 Membru WP: Dl Savior CACHIA, comisar pentru informare și protecția datelor

Art 29 WP Membru supleant: dl Ian DEGUARA, director - Operațiuni și implementarea programului

**Olanda**

**Autoriteit Persoonsgegevens**

60. Prins Clauslaan

Căsuța poștală 93374

2509 AJ Den Haag / Haga Tel. +31 70 888 8500

Fax +31 70 888 8501

e-mail: [info@autoriteitpersoonsgegevens.nl](mailto:info@autoriteitpersoonsgegevens.nl)

Site web: <https://autoriteitpersoonsgegevens.nl/nl>

Art 29 Membru WP: dl Aleid WOLFSEN, președinte al Autoriteit Persoonsgegevens

**Polonia**

**Biroul inspectorului general pentru protecția datelor cu caracter personal - GIODO**

ul. Stawki 2

00-193 Varșovia

Tel. +48 22 53 10 440

Fax +48 22 53 10 441

e-mail: [kancelaria@giodo.gov.pl](mailto:kancelaria@giodo.gov.pl); [desiwm@giodo.gov.pl](mailto:desiwm@giodo.gov.pl)

Site web: <http://www.giodo.gov.pl/>

Art 29 Membru WP: Dna Edyta BIELAK-JOMAA, inspector general pentru protecția datelor cu caracter personal

**Portugalia**

**Comissão Nacional de Protecção de Dados - CNPD**

R. de São. Bento, 148-3 ° 1200-821 Lisboa

Tel. +351 21 392 84 00

Fax +351 21 397 68 32

e-mail: [geral@cnpd.pt](mailto:geral@cnpd.pt)

Site web: <http://www.cnpd.pt/>

Art 29 Membru WP: dna Filipa CALVÃO, președinte, Comissão Nacional de Protecção de Dados

Art 29 Membru alternativ WP: Isabel CRUZ, secretar general al APD

**România**

**Autoritatea Națională de Supraveghere pentru Prelucrarea Datelor cu Caracter Personal Președinte: dna Ancuța Gianina Opre**

B-dul Magheru 28-30

Sectorul 1, BUCUREȘTI

Tel. +40 21 252 5599

Fax +40 21 252 5757

e-mail: [anspdcp@dataprotection.ro](mailto:anspdcp@dataprotection.ro)

Site web: <http://www.dataprotection.ro/>

Art 29 Membru WP: dna Ancuța Gianina OPRE, președinte al Autorității naționale de supraveghere pentru prelucrarea datelor cu caracter personal

Art 29 WP Membru supleant: dna Alina SAVOIU, șefa departamentului juridic și comunicare

**Slovacia**

**Oficiul pentru Protecția Datelor cu Caracter Personal din Republica Slovacă**

Hraničná 12

820 07 Bratislava 27

Tel .: + 421 2 32 31 32 14

Fax: + 421 2 32 31 32 34

e-mail: [statny.dozor@pdp.gov.sk](mailto:statny.dozor@pdp.gov.sk)

Site web:<http://www.dataprotection.gov.sk/>

Art 29 Membru WP: dna Soňa PŐTHEOVÁ, președinte al Oficiului pentru Protecția Datelor cu Caracter Personal din Republica Slovacă

Art 29 WP Membru supleant: dl Anna VITTEKOVA, vicepreședinte

**Slovenia**

**Comisar pentru informații**

Dna Mojca Prelesnik Zaloška 59

1000 Ljubljana

Tel. +386 1 230 9730

Fax +386 1 230 9778

e-mail: [gp.ip@ip-rs.si](mailto:gp.ip@ip-rs.si)

Site web:<https://www.ip-rs.si/>

Art 29 Membru WP: Dna Mojca PRELESNIK, comisar pentru informații al Republicii Slovenia

**Spania**

**Agenția de protecție a datelor**

C / Jorge Juan, 6

28001 Madrid

Tel. +34 91399 6200

Fax +34 91455 5699

e-mail: [internacional@agpd.es](mailto:internacional@agpd.es)

Site web: <https://www.agpd.es/>

Art 29 Membru WP: dna María del Mar España Martí, director al Agenției Spaniole pentru Protecția Datelor

Art 29 WP Membru supleant: dl Rafael GARCIA GOZALO

**Suedia**

**Datainspektionen**

Drottninggatan 29 Etajul 5

Caseta 8114

1. 20 Stockholm

Tel. +46 8 657 6100

Fax +46 8 652 8652

e-mail: [datainspektionen@datainspektionen.se](mailto:datainspektionen@datainspektionen.se)

Site web: <http://www.datainspektionen.se/>

Art 29 Membru WP: Dna Kristina SVAHN STARRSJÖ, Director General al Comitetului de inspecție a datelor

Art 29 WP Membru supleant: dl Hans-Olof LINDBLOM, consilier juridic șef

**Regatul Unit**

**Biroul comisarului pentru informații**

Water Lane, Wycliffe House Wilmslow - Cheshire SK9 5AF Tel. +44 1625 545 745

e-mail: [international.team@ico.org.uk](mailto:international.team@ico.org.uk)

Site web: [https://ico.org.uk](https://ico.org.uk/)

Art 29 Membru WP: Dna Elizabeth DENHAM, comisar pentru informații

Art 29 Membru alternativ WP: dl Steve WOOD, subcomisar

**ZONA EUROPEANĂ DE COMERȚ LIBER (AELS)**

**Islanda**

[Agenția islandeză pentru protecția datelor](http://personuvernd.is/) Rauðarárstíg 10

1. Reykjavík

Tel. +354 510 9600; Fax +354 510 9606

e-mail: [postur@personuvernd.is](mailto:postur@personuvernd.is)

**Liechtenstein**

[Biroul de protecție a datelor](http://www.dss.llv.li/) Kirchstrasse 8, poștă 684

9490 Vaduz

Principatul Liechtenstein Tel. +423 236 6090

e-mail: [info.dss@llv.li](mailto:info.dss@llv.li)

**Norvegia**

[Datatilsynet](http://www.datatilsynet.no/)

Inspectoratul de date

Caseta postala 8177 Dep 0034 Oslo

Tel. +47 22 39 69 00; Fax +47 22 42 23 50

e-mail: [postkasse@datatilsynet.no](mailto:postkasse@datatilsynet.no)

Autoritatea pentru protecția datelor: dl Bjørn Erik THORN

**Elveţia**

[Comisar pentru protecția datelor și informații din Elveția](http://www.edoeb.admin.ch/) Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter Dl Adrian Lobsiger

Feldeggweg 1

3003 Berna

Tel. +41 58 462 43 95; Fax +41 58 462 99 96 e-mail: [contact20@edoeb.admin.ch](mailto:contact20@edoeb.admin.ch)

1. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions\_en; [↑](#footnote-ref-1)
2. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc\_en; [↑](#footnote-ref-2)