

1. Prezentare generală

VOGO eBS GDPR and Privacy identifică, clasifică și protejează datele cu caracter personal din documentele și fluxurile organizației. Componenta descoperă datele personale în text și în imagini, le clasifică pe categorii și scopuri, aplică mascarea, pseudonimizarea, anonimizarea sau redactarea ireversibilă pe copii derivate și păstrează originalul protejat, cu acces restrâns.

Componenta rulează integral în infrastructura beneficiarului, pe CPU, fără transmiterea documentelor către servicii externe.

Produs dezvoltat de VOGO TECHNOLOGY (denumire anterioară VIPTeSS) parte a suitei VOGO eBS, înregistrată la ORDA în Registrul Național al Programelor pentru Calculator cu certificatul seria 478196BV nr. 13869, sub marca Uniunii Europene VOGO.me înregistrată la EUIPO cu nr. 019103505 / 15.04.2025 - <https://euipo.europa.eu/eSearch/#details/trademarks/019103505>.

Produs	VOGO eBS GDPR and Privacy
Suita	VOGO eBS — Enterprise Business Suite
Detectare	Text și coordonate din modulul de captură și OCR, motor de identificare pe biblioteci open, cu suport enterprise asigurat de Ofertant, reguli deterministe pentru identificatori naționali, model lingvistic local
Acțiuni	Mascare, pseudonimizare, anonimizare, redactare ireversibilă pe copie derivată
Original	Rămâne protejat și nemodificat, cu acces restrâns și jurnalizat
Control uman	Rezultatele incerte sunt validate de un utilizator autorizat înainte de aplicare
Execuție	Local, pe CPU, fără servicii externe

2. Detectarea datelor cu caracter personal

- ▶ Analiza textului extras și a coordonatelor din documente scanate, astfel încât marcajul să poată fi aplicat exact pe zona din imagine.
- ▶ Motor de identificare a entităților personale, completat cu reguli deterministe pentru identificatorii naționali și cu un model lingvistic local pentru limba română.
- ▶ Categoriile acoperite: nume, adrese, identificatori naționali, date de contact, date financiare, date de sănătate și alte categorii configurabile.
- ▶ Pentru fiecare fișier se păstrează categoria datelor, scopul prelucrării, marcasele detectate, scorul de încredere și validarea utilizatorului autorizat.
- ▶ Rezultatele sub pragul de încredere configurat nu se aplică automat, ci intră în validare umană.

3. Protejarea datelor

Mascare	Ascunderea parțială a valorii în versiunea consultabilă, cu păstrarea formatului
Pseudonimizare	Înlocuirea identificatorului cu un substitut reversibil, controlat prin drepturi
Anonimizare	Eliminarea legăturii cu persoana, fără posibilitate de reconstituire

Toate acțiunile se aplică pe o copie derivată. Originalul rămâne protejat, nemodificat și accesibil numai persoanelor desemnate, iar fiecare consultare este jurnalizată.

4. Registrul prelucrărilor și drepturile persoanelor

- ▶ Registrul activităților de prelucrare: scopuri, temeuri, categorii de date, categorii de persoane vizate, destinatari, transferuri și termene de păstrare.
- ▶ Evaluări de impact asupra protecției datelor, legate de activitățile pe care le privesc.
- ▶ Cererile persoanelor vizate — acces, rectificare, ștergere, restricționare, portabilitate, opoziție — cu termene, responsabili și dovada răspunsului.
- ▶ Evidența consimțământului și a retragerii lui, cu efectul asupra prelucrărilor în curs.
- ▶ Evidența incidentelor de securitate cu impact asupra datelor personale, cu notificările aferente.
- ▶ Păstrarea pentru litigii, care suspendă ștergerea pe perioada stabilită.

5. Rolul responsabilului cu protecția datelor

Rolul de responsabil cu protecția datelor este nativ și distinct de rolurile administrative. Accesul este justificat, temporar, configurabil și auditat — niciodată nelimitat automat. Responsabilul vede registrul prelucrărilor, cererile, incidentele și rapoartele, fără a primi implicit acces la conținutul documentelor.

6. Conflictul dintre ștergere și obligația de păstrare

O cerere de ștergere pentru un document aflat sub obligație legală de păstrare nu se execută tăcut. Componenta anonimizează datele personale în versiunea consultabilă, păstrează originalul în arhivă cu acces restrâns și consemnează operațiunea în registrul prelucrărilor. Conflictul se rezolvă printr-o decizie juridică documentată și auditată, nu prin ștergerea înregistrării.

7. Integrare cu celelalte componente

VOGO eBS ECM	Preluarea textului și a coordonatelor, aplicarea protecției pe copii derivate, păstrarea originalului
VOGO eBS AI	Redactarea informațiilor sensibile înainte de orice prelucrare de inteligență artificială
VOGO eBS BPM	Sarcini de validare umană pentru rezultatele incerte și pentru cererile persoanelor vizate
Componenta de securitate	Transmiterea evenimentelor de acces, de anonimizare și de incident

8. Audit și dovezi

- ▶ Fiecare detectare, validare, aplicare de protecție și consultare a originalului este jurnalizată, cu autor, moment și motiv.
- ▶ Jurnalul este append-only și poate fi exportat pentru audit intern, pentru auditul autorității de supraveghere sau pentru un litigiu.
- ▶ Rapoartele arată volumul documentelor procesate, categoriile detectate, rata de validare umană și cererile soluționate în termen.

9. Funcționalitățile în aplicație

Protecția datelor cu caracter personal este integrată în ecranele platformei VOGO eBS, de la definirea metadatelor până la cererile persoanelor vizate.

Metadate și documente:

- ▶ În librăria de metadate, fiecare câmp poate fi marcat ca dată cu caracter personal, cu categoria datelor personale pe care o conține.
- ▶ Proprietățile fiecărui document au o secțiune dedicată datelor cu caracter personal, salvată separat și jurnalizată.
- ▶ Nivelul de securitate al câmpului și al documentului limitează cine vede datele.

Detectare și protecție:

- ▶ Regulile de detectare a datelor personale se administrează în aplicație, iar potrivirile găsite rămân evidențiate pe document până la validare.
- ▶ Execuțiile de anonimizare sunt urmărite, cu documentul, regula aplicată și rezultatul.

Registre și evidențe:

- ▶ Profilurile de date personale, activitățile de prelucrare, cererile persoanelor vizate și evaluările de impact se gestionează în ecrane dedicate.
- ▶ Incidentele de securitate a datelor au evidența entităților afectate și a notificărilor transmise.
- ▶ Păstrarea pentru litigii se aplică pe documente anume și suspendă ștergerea până la ridicarea ei.
- ▶ Deciziile în conflictele dintre dreptul la ștergere și obligația de păstrare sunt consemnate, cu motivul.

Responsabilul cu protecția datelor și informațiile clasificate:

- ▶ Cererile de acces ale responsabilului cu protecția datelor și accesul acordat acestuia sunt evidențiate separat.
- ▶ Documentele au niveluri de clasificare, compartimente de securitate și autorizări pe persoane; schimbările de clasificare, distribuirea și copiile controlate sunt urmărite.

10. Livrare, suport și operare

VOGO livrează și integrează componenta, regulile de detectare, modelele lingvistice locale, configurațiile, imaginile de container și documentația de administrare, împreună cu procedurile de calibrare a pragurilor și de validare a rezultatelor.

Modelul de suport operațional este asigurat de VOGO pe întreaga perioadă de implementare și de garanție — instalare, configurare, actualizări de securitate, remedierea incidentelor, documentare, compatibilitate cu infrastructura beneficiarului și transfer operațional. Absența costului de licență pentru componentele open-source integrate nu diminuează niciuna dintre aceste obligații.

11. Suport enterprise

Suportul pentru VOGO eBS GDPR and Privacy este un serviciu enterprise asigurat de Ofertant pentru întreaga stivă livrată, inclusiv pentru componentele open-source integrate, pe toată perioada de implementare și de garanție. Beneficiarul are un singur punct de contact pentru toate componentele produsului, indiferent de originea lor.

Disponibilitate	24 × 7 × 365, pentru incidentele critice; program extins pentru solicitările de nivel funcțional
Call center	Punct unic de contact telefonic și prin e-mail, în limba română, cu preluare și înregistrare a fiecărei solicitări
Ticketing	Sistem de ticketing pus la dispoziția beneficiarului, cu portal web, înregistrare, clasificare, urmărire, istoric complet și rapoarte periodice

Niveluri de suport	Nivel 1 în call center, nivel 2 tehnic pe produs, nivel 3 la echipa de dezvoltare a Ofertantului, cu escaladare automată pe severitate
Acord de nivel al serviciului	Timpi de răspuns și de restabilire asumați pe clase de severitate, conform nivelurilor din contract
Acoperire	Produsul, modulele sale și componentele open-source integrate; absența costului de licență nu diminuează niciuna dintre obligațiile de suport

Serviciul include, fără costuri suplimentare pe perioada acoperită:

- ▶ Preluarea, clasificarea și soluționarea incidentelor, cu notificarea beneficiarului la fiecare schimbare de stare.
- ▶ Actualizări de securitate și corecții de defecte, testate de Ofertant și livrate cu note de versiune și procedură de aplicare.
- ▶ Mentenanță preventivă, verificări periodice de stare și recomandări de optimizare a configurației.
- ▶ Asistență la operațiunile planificate: actualizări de versiune, migrări, extinderi de capacitate, exerciții de restaurare.
- ▶ Documentație de administrare și operare, actualizată la fiecare versiune livrată.
- ▶ Instruirea administratorilor beneficiarului și transfer operațional la finalul perioadei de garanție.
- ▶ Rapoarte periodice de disponibilitate, incidente, timpi de soluționare și acțiuni corective.