

**DEPARTAMENTUL DE STUDII PARLAMENTARE ȘI POLITICI UE
DIRECȚIA STUDII ȘI DOCUMENTARE LEGISLATIVĂ**

REGLEMENTAREA CASELOR DE MARCAT ELECTRONICE VIRTUALE ÎN STATE MEMBRE UE

studiu documentar

noiembrie 2025

Materialele elaborate în cadrul Direcției studii și documentare legislativă au caracter documentar și nu reprezintă punctul de vedere al Camerei Deputaților.

Documentele legislative oficiale au fost consultate în limba de origine, iar traducerea informațiilor relevante selectate nu reprezintă o traducere oficială, fiind furnizată ca un mijloc de înțelegere a unui document original, scris în altă limbă.

Baza de date cuprinzând totalitatea studiilor elaborate de Direcția studii și documentare legislativă poate fi accesată prin intermediul paginii de Intranet a Camerei Deputaților la adresa:

Documentare și sinteză: Any-Mary Jula, consilier parlamentar
Consilier parlamentar - Direcția studii și documentare legislativă
Palatul Parlamentului, str. Izvor nr.2-4, sect.5, București
Tel: 021.316.03.65; 021.414.13.50/ 51, Interior 1350/1349, camera 5070
E-mail: doc@cdep.ro

CUPRINS

ASPECTE COMPARATIVE.....	4
AUSTRIA.....	4
BELGIA	8
FRANȚA	12
GERMANIA	15
ITALIA	18
SPANIA	22
SUEDIA	25
UNGARIA	28
WEBOGRAFIE	31

Conceptul de „[virtual electronic cash register solution](#)” (adesea denumită POS virtual sau POS bazat pe cloud) a apărut și evoluat în principal între anii 2000 și 2010. Această schimbare a făcut parte din tranziția mai amplă de la casele de marcat electronice (ECR) tradiționale, greoaie, locale, la sisteme POS (Point of Sale - punct de vânzare) bazate pe software și cloud-native. În timp, adoptarea pe scară largă a POS-urilor virtuale (VPOS) și a POS-urilor mobile s-a consolidat, oferind funcții precum raportare în timp real, gestionarea stocurilor și costuri de pornire mai mici, făcându-le accesibile unei game mai largi de afaceri. Impactul evoluției POS-urilor asupra afacerilor a constat, în principal, în eficientizarea tranzacțiilor și îmbunătățirea experienței clienților. Reglementările privind casele de marcat electronice virtuale sunt foarte specifice și variază semnificativ în funcție de țară sau regiune, deoarece sunt stabilite în principal de autoritățile fiscale pentru a combate evaziunea fiscală și a asigura transparența financiară.

ASPECTE COMPARATIVE

AUSTRIA

Reglementarea sistemelor de înregistrare a vânzărilor din Austria se face prin Ordonanța de Securitate a Caselor de Marcat - [Registrierkassensicherheitsverordnung - RKSV](#), intrată în vigoare la 1 aprilie 2017. RKSV nu impune utilizarea exclusivă a unei case de marcat fizice, ci mandatează un mecanism tehnic de securitate care poate fi implementat fie hardware, fie virtual (software/cloud).

Legea austriacă urmărește să se asigure că toate tranzacțiile în numerar (inclusiv plățile cu cardul) sunt înregistrate complet și protejate împotriva oricărei modificări ulterioare, creând o "sigilare digitală" a datelor.

Casele de marcat electronice virtuale sau sistemele Cloud POS sunt permise și recunoscute legal în Austria, cu condiția să îndeplinească următoarele cerințe esențiale:

- Semnătura Digitală Obligatorie: fiecare tranzacție (bon fiscal) trebuie să fie semnată electronic, utilizând un certificat de semnătură calificată emis de un furnizor de servicii de încredere (Trust Service Provider) acreditat în UE (de exemplu, A-Trust, GlobalTrust). De importanță în acest aspect este Unitatea de Creare a Semnăturii Securizate (Sicherheits- und Signaturerstellungseinheit - SSEE) - Aceasta este elementul central al fiscalizării în Austria și poate fi virtual (o soluție software sau un serviciu cloud);
- Lanțul de Securitate: semnătura digitală a fiecărui bon trebuie să includă o referință la semnătura bonului anterior, creând un lanț criptografic neîntrerupt. Orice tentativă de ștergere sau modificare a unui bon ar rupe acest lanț și ar semnaliza imediat fraudă.

- Implementare Flexibilă - SSEE poate fi:
 - Un modul hardware (de obicei, o cartelă criptografică tip *chip-card*).
 - Un modul software/cloud (soluții virtuale) care oferă funcția de semnare și gestionare a lanțului. Aceste soluții cloud sunt cele mai utilizate în prezent, deoarece oferă flexibilitate maximă (utilizarea pe tablete, telefoane, etc.).

Bonul Fiscal cu Cod QR - Bonul fiscal emis (fie pe hârtie, fie electronic) trebuie să conțină un Cod QR lizibil de mașină. Acest Cod QR include informații esențiale despre tranzacție și semnătura digitală, permițând autorităților (și chiar clienților, prin aplicația BMF Belegcheck) să verifice integritatea datelor.

Protocolul de Înregistrare a Datelor (Datenerfassungsprotokoll - DEP) - Toate datele tranzacțiilor trebuie stocate într-un protocol de înregistrare a datelor (DEP) în format electronic, securizat și inalterabil, pentru a fi prezentat autorităților fiscale la cerere (în timpul unui audit).

Înregistrarea la FinanzOnline - Operatorul economic are obligația de a înregistra sistemul de înregistrare a vânzărilor și Unitatea de Creare a Semnăturii Securizate (fie ea hardware sau virtuală) pe portalul online al Ministerului Federal al Finanțelor (FinanzOnline).

Certificarea Modulului de Semnătură (SSEE) - -ceasta este cea mai importantă componentă, care oferă garanția de securitate. Certificarea nu se aplică *softului* casei de marcat, ci modulului de creare a semnăturii (Sicherheits- und Signaturerstellungseinheit - SSEE). Acest modul trebuie să utilizeze un Certificat de Semnătură Calificată emis de un furnizor de servicii de încredere (Trust Service Provider) autorizat la nivel european (ex. A-Trust, GlobalTrust).

În cazul soluțiilor virtuale (Cloud POS), certificatul (sau cheia privată asociată) este gestionat de un serviciu cloud securizat (Middleware), care asigură semnarea fiecărui bon fiscal. Certificatul atestă că tranzacțiile sunt semnate cu algoritmi criptografici securizați (ex. AES 256) și că ele fac parte dintr-un lanț neîntrerupt (prin includerea unui hash al bonului precedent).

Înregistrarea Sistemului la FinanzOnline - odată ce sistemul (software-ul POS și modulul de securitate) este instalat la comerciant, urmează procedura obligatorie de înregistrare pe portalul autorității fiscale austriece, FinanzOnline (FON):

Înregistrarea Contribuabilului: contribuabilul trebuie să aibă un cont activ pe portalul FinanzOnline.

Crearea Utilizatorului Serviciului Web al Casei de Marcat: comerciantul creează un utilizator dedicat pe FON pentru a permite comunicarea automată între sistemul POS și autoritatea fiscală.

Înregistrarea Casei de Marcat: se înregistrează datele de identificare ale sistemului de marcat (ID-ul casei de marcat, data punerii în funcțiune) prin interfața serviciului web al FON.

Înregistrarea Certificatului: Se înregistrează numărul de serie al certificatului de semnătură digitală utilizat de SSEE.

Verificarea Inițială și Raportarea Periodică

Procedurile nu se termină la înregistrare, ci implică și mecanisme de control continuu:

- Imediat după punerea în funcțiune și înregistrare, sistemul emite un bon de start cu valoare zero, care are semnătura digitală a primului document fiscal.
- Comerciantul trebuie să trimită datele acestui bon de start către FinanzOnline în decurs de 7 zile de la punerea în funcțiune, fie printr-un serviciu web automatizat, fie manual folosind o aplicație a Ministerului Finanțelor (BMF Belegcheck App), care scanează Codul QR. Aceasta confirmă oficial că sistemul funcționează corect și că semnătura este validă.
- Lunar și anual, sistemul trebuie să genereze un bon de închidere (Monatsbeleg/Jahresbeleg), care confirmă integritatea lanțului criptografic. Bonul anual trebuie verificat cu aplicația BMF și transmis către FinanzOnline până la 15 februarie a anului următor.

Autoritățile austriece nu certifică software-ul POS în sine, ci certifică securitatea criptografică a procesului de înregistrare a tranzacțiilor, bazându-se pe standarde de semnătură electronică calificată. Orice sistem software (virtual sau nu) care integrează corect acest modul de securitate certificat este considerat legal conform (RKS-compliant).

Modalitățile de emitere, transmitere și arhivare a bonurilor fiscale electronice în Austria sunt reglementate de **Ordonanța de Securitate a Caselor de Marcat (RKS)**. Sistemul austriac se bazează pe securitatea criptografică a fiecărui bon, recunoscând bonul electronic ca document fiscal oficial, fără a necesita neapărat o transmitere individuală a fiecărui bon către autoritatea fiscală.

Bonul fiscal electronic este recunoscut ca document oficial, cu condiția să îndeplinească următoarele criterii de securitate și conținut:

Bonul trebuie generat de un sistem de înregistrare a vânzărilor (POS) care utilizează o Unitate de Creare a Semnăturii Securizate (SSEE).

Fiecare bon emis trebuie să fie semnat digital utilizând un certificat calificat. Semnătura include o referință la tranzacția precedentă, asigurând un lanț criptografic neîntrerupt și garantând că datele nu pot fi modificate ulterior.

Bonul, fie pe hârtie, fie electronic, trebuie să includă:

- Data, ora și locul emiterii.
- Identificatorul unic al sistemului de marcat.
- Codul QR: Acesta conține datele cheie ale tranzacției și, cel mai important, semnătura digitală (valoarea *hash*) a bonului, permițând verificarea integrității sale.

Bonurile pot fi puse la dispoziția clientului în format electronic, de exemplu, prin e-mail, aplicație mobilă sau afișate pe un ecran, atâta timp cât conțin toate elementele obligatorii, inclusiv Codul QR securizat.

Arhivarea Bonului Fiscal Electronic

Arhivarea datelor bonurilor fiscale este obligatorie și se realizează prin mecanisme interne securizate:

- Protocolul de Înregistrare a Datelor (Datenerfassungsprotokoll - DEP): Sistemul POS (inclusiv cele virtuale) trebuie să stocheze toate datele tranzacțiilor în acest protocol electronic securizat.
- Datorită lanțului criptografic neîntrerupt, acest registru este considerat inalterabil și servește ca bază pentru auditurile fiscale.
- Operatorii economici sunt obligați să păstreze datele (DEP) pentru o perioadă de 7 ani în format electronic.

Bonul fiscal electronic (Beleg) este recunoscut ca document fiscal oficial datorită lanțului de securitate criptografică.

Semnătura digitală a bonului, verificabilă prin Codul QR, servește ca dovadă legală a tranzacției, asigurând autenticitatea și integritatea datelor.

Bonul este valabil pentru deducerea cheltuielilor și a TVA-ului (în cazul în care cumpărătorul este o persoană juridică), deși, similar cu alte state UE, pentru sume mari sau pentru o documentare completă, companiile solicită adesea facturi fiscale separate.

Sistemul austriac pune accentul pe autentificarea la sursă (bonul) prin criptografie, delegând responsabilitatea verificării lanțului de securitate către operatorul economic, sub controlul BMF.

Mecanismele de control, securitate și trasabilitate utilizate în Austria pentru protejarea datelor fiscale și prevenirea evaziunii (conform RKS - Registrierkassensicherheitsverordnung) sunt bazate, în principal, pe criptografie și pe responsabilitatea operatorului economic de a menține un lanț de securitate neîntrerupt al tranzacțiilor.

Securitatea datelor este asigurată la nivelul fiecărei tranzacții prin următoarele:

- Semnătura Digitală Calificată:
- Lanțul Criptografic (Chaining):
- Codul QR pe Bon:

Trasabilitatea se bazează pe registre interne securizate:

- **Protocolul de Înregistrare a Datelor (Datenerfassungsprotokoll - DEP):** Toate tranzacțiile, inclusiv bonurile și rapoartele, trebuie stocate secvențial într-un registru electronic securizat (DEP). Acesta este obligatoriu inalterabil și servește ca registru primar pentru audit.
- **Identificarea Sistemului:** fiecare sistem POS este înregistrat cu un ID Unic pe portalul FinanzOnline al Ministerului Federal al Finanțelor (BMF), asigurând trasabilitatea tranzacțiilor până la sistemul exact care le-a emis.
- **Certificatul de Semnătură:** numărul de serie al certificatului de semnătură digitală este, de asemenea, înregistrat la FinanzOnline, legând securitatea criptografică de comerciant și de sistemul său.

Mecanisme de Control și Prevenire a Evaziunii (BMF)

Controlul se realizează prin verificarea integrității lanțului de tranzacții și nu prin monitorizarea în timp real a fiecărui bon:

- **Verificarea Bonului de Start și a Bonului Anual:** comerciantul trebuie să transmită (să verifice prin scanarea Codului QR) datele Bonului de Start (la fiscalizare) și ale Bonului Anual (la încheierea anului fiscal) către FinanzOnline. Această verificare periodică confirmă că lanțul criptografic a început corect și a fost menținut pe tot parcursul anului.
- **Aplicația BMF Belegcheck:** autoritatea fiscală pune la dispoziția publicului o aplicație (și o interfață web) prin care clienții și inspectorii pot scana Codul QR de pe bon pentru a verifica instantaneu dacă valoarea *hash* (semnătura) se potrivește cu datele înregistrate și dacă bonul este valid conform RKSv.
- **Audituri bazate pe DEP:** în timpul inspecțiilor fiscale, autoritățile solicită acces la Protocolul de Înregistrare a Datelor (DEP). Analiza DEP și a lanțului criptografic permite detectarea rapidă a oricăror lacune sau modificări neautorizate ale înregistrărilor fiscale.

Spre deosebire de România, unde accentul cade pe transmiterea online a datelor către ANAF, modelul austriac se concentrează pe integritatea datelor la sursă, garantată criptografic, făcând manipularea datelor aproape imposibilă fără a rupe lanțul de securitate.

BELGIA

Statutul juridic al caselor de marcat electronice (inclusiv al sistemelor POS virtuale sau bazate pe software) în Belgia este strict reglementat, în special pentru sectorul Horeca (Hoteluri, Restaurante, Catering)¹.

Sistemul belgian nu se bazează pe o simplă casă de marcat electronică (AMEF), ci pe un sistem integrat de fiscalizare, cunoscut sub numele de Sistemul Certificat al Caselor de Marcat (*Système de Caisse Enregistreuse* – SCE) sau "Cutia Neagră" (Black Box).

Soluțiile de vânzare (POS) virtuale sunt permise, dar statutul lor legal depinde de integrarea lor cu componentele de securitate hardware/criptografice impuse de guvern.

Legea belgiană obligă anumite întreprinderi din Horeca (cele cu o cifră de afaceri din alimentație, exclusiv băuturi, care depășește 25.000 EUR pe an) să utilizeze SCE, care este compus din trei elemente esențiale:

- **Sistemul POS Certificat (Caisse Enregistreuse Certifiée).** Acesta este softul sau aplicația de vânzare (inclusiv soluțiile virtuale sau cloud) care trebuie

¹ [Loi du 30 juillet 2013 relative à la certification d'un système de caisse enregistreuse](#)

să fie certificată de Serviciul Public Federal de Finanțe (SPF Finances) pentru a asigura că respectă specificațiile de înregistrare a datelor.

- **Modulul Fiscal de Date (Fiscal Data Module – FDM).** Acesta este elementul central de securitate, adesea numit "Cutia Neagră". Este un dispozitiv hardware certificat care trebuie să fie conectat permanent la sistemul POS. Funcția sa principală este de a înregistra, de a securiza și de a genera un hash (cod unic) pentru fiecare comandă și bon, asigurând astfel integritatea datelor.
- **Cardul de Semnare TVA Personalizat (VAT Signing Card – VSC).** Acesta este un card electronic personalizat, emis de guvern, care conține datele de identificare ale angajatorului/managerului. VSC-ul trebuie introdus în Modulul Fiscal de Date (FDM) pentru a-l activa și pentru a semna digital tranzacțiile, asigurând trasabilitatea operațiunilor.

O soluție de casă de marcat electronică virtuală (adică un software POS care rulează pe tabletă, PC sau în cloud) este legală în Belgia doar dacă este capabilă să se integreze și să comunice corect cu Modulul Fiscal de Date (FDM) hardware certificat și să utilizeze Cardul VSC pentru fiscalizare.

Nu există o "casă de marcat virtuală" pur software care să înlocuiască complet FDM-ul hardware, așa cum se întâmplă în unele alte state europene (unde fiscalizarea se face exclusiv prin cloud/criptografie software).

În esență, soluția virtuală (software-ul POS) este doar interfața de vânzare, iar FDM-ul (Cutia Neagră) rămâne nucleul de securitate fiscală impus de lege.

Procedurile de omologare și certificare pentru casele de marcat electronice (inclusiv soluțiile virtuale) în Belgia sunt complexe și se axează pe certificarea a două elemente distincte: software-ul POS (interfața virtuală) și Modulul Fiscal de Date (FDM), adesea numit "Cutia Neagră".

Aceste proceduri sunt stabilite de Serviciul Public Federal de Finanțe (SPF Finances), în cadrul sistemului cunoscut sub numele de SCE (Système de Caisse Enregistreuse - Sistemul Certificat al Caselor de Marcat).

Această procedură vizează omologarea aplicației (software-ului) de vânzare care rulează pe un dispozitiv virtual (PC, tabletă, cloud). Software-ul trebuie să respecte specificațiile funcționale și poate comunica corect cu Modulul Fiscal de Date (FDM). Producătorul/Dezvoltatorul de Software (sau distribuitorul) depune o cerere oficială la SPF Finances. Se prezintă documentația tehnică detaliată a aplicației, inclusiv modul în care gestionează tranzacțiile, modificările de preț, anulările și, cel mai important, interfața de comunicare cu FDM-ul. Autoritatea fiscală sau un organism de certificare desemnat efectuează teste funcționale asupra software-ului pentru a se asigura că acesta înregistrează datele corecte și că nu permite manipulări. În final se obține unui Număr de Certificare pentru sistemul POS. Odată ce software-ul și FDM-ul sunt certificate individual, ele sunt activate la sediul comerciantului prin fiscalizare:

- Comerciantul achiziționează softul POS certificat și un FDM certificat.
- Comerciantul solicită și primește de la autoritatea fiscală Cardul de Semnare TVA (VSC), care este un card personalizat (similar unui card bancar) și conține certificatul digital al operatorului.

- Softul POS virtual este conectat fizic (de obicei prin cablu sau IoT Box) la FDM. Cardul VSC este introdus în cititorul FDM, activând modulul fiscal și permițând semnarea tranzacțiilor.
- Sistemul generează și raportează tranzacțiile zilnice în mod securizat către FDM, care le arhivează și le face disponibile pentru inspecțiile fiscale, asigurând trasabilitatea.

În concluzie, în Belgia, "casa de marcat electronică virtuală" (softul POS) este omologată doar ca interfață, în timp ce securitatea fiscală și integritatea datelor sunt certificate exclusiv de un dispozitiv hardware obligatoriu (FDM).

Modalitățile de emitere, transmitere și arhivare a bonurilor fiscale electronice în Belgia sunt strict legate de utilizarea Sistemului Certificat al Caselor de Marcat (SCE), cunoscut și ca sistemul "Cutia Neagră" (Black Box), în special pentru sectorul Horeca.

Bonurile fiscale electronice sunt recunoscute ca documente fiscale oficiale deoarece îndeplinesc cerințele de integritate impuse de lege prin intermediul Modulului Fiscal de Date (FDM) și al Cardului de Semnare TVA (VSC).

Emiterea bonului (numit Note Intermédiaire sau Ticket TVA) este generată de sistemul POS virtual, dar securitatea este garantată de componentele hardware. Bonul este generat de softul POS (soluția virtuală) care este conectat permanent la Modulul Fiscal de Date (FDM), "Cutia Neagră" certificată. FDM-ul preia datele tranzacției, le securizează și generează un cod de securitate (hash) unic pentru fiecare bon sau comandă. Acest proces de securizare este activat și validat prin intermediul Cardului de Semnare TVA (VSC) al operatorului, care trebuie să fie introdus în FDM. Bonul trebuie să conțină toate elementele standard plus numărul unic de identificare al FDM-ului și informații despre securizare.

Transmiterea către Autoritatea Fiscală (SPF Finances). Spre deosebire de România, Belgia nu impune transmiterea online, în timp real, a fiecărui bon individual către Serviciul Public Federal de Finanțe (SPF Finances). Controlul se bazează pe capacitatea autorității de a extrage date direct din Modulul Fiscal de Date (FDM) în timpul inspecțiilor. Sistemul (FDM) generează rapoarte periodice (de exemplu, la schimbarea de tură sau zilnic) care însumează tranzacțiile. Aceste date pot fi transmise electronic, la cerere, sau extrase de inspectori.

Bonurile pot fi puse la dispoziția clientului în format electronic (prin e-mail sau afișare pe dispozitiv mobil), cu condiția ca acestea să fie o copie fidelă și lizibilă a datelor securizate de FDM. Bonul tipărit rămâne modalitatea standard, iar majoritatea sistemelor oferă ambele opțiuni.

Arhivarea datelor bonurilor fiscale se realizează centralizat și securizat în cadrul sistemului fiscal. Datele tuturor tranzacțiilor sunt stocate în Modulul Fiscal de Date (FDM) într-un format criptat și inalterabil. FDM-ul acționează ca un jurnal electronic securizat. Operatorul economic trebuie să păstreze o copie a registrului de date (Fișierul FDM) pe un mediu secundar securizat. Datele fiscale din FDM trebuie păstrate timp de 7 ani, conform legislației contabile și fiscale belgiene.

Bonul fiscal (ticket TVA) emis de un sistem SCE este recunoscut oficial ca document fiscal în Belgia datorită garanțiilor de securitate. Utilizarea FDM-ului și a VSC-ului asigură integritatea și autenticitatea datelor tranzacției, deoarece orice încercare de manipulare ar fi detectată. Bonul fiscal servește ca dovadă a încasării TVA-ului pentru tranzacțiile B2C (tranzacții cu clienți finali). Pentru tranzacțiile B2B (între companii), deși bonul poate fi utilizat ca dovadă primară a plății, documentul necesar pentru deducerea TVA-ului și justificarea cheltuielilor este factura fiscală completă.

În concluzie, în Belgia, recunoașterea legală a bonului electronic nu provine din transmiterea lui către autoritate, ci din faptul că datele sale au fost înregistrate și securizate criptografic de un modul hardware certificat (FDM).

Mecanismele de control, securitate și trasabilitate utilizate în Belgia pentru protejarea datelor fiscale și prevenirea evaziunii sunt integrate în Sistemul Certificat al Caselor de Marcat (SCE) - "Cutia Neagră" (Black Box). Acest sistem este obligatoriu în special pentru sectorul Horeca (cu anumite praguri de cifră de afaceri) și se bazează pe o combinație de hardware securizat și autentificare personală.

Modulul Fiscal de Date (FDM) – "Cutia Neagră" este elementul central de securitate. Este un dispozitiv tip hardware certificat și sigilat care este interfața obligatorie între softul POS (soluția virtuală) și înregistrarea finală a datelor fiscale. FDM-ul este conceput să fie inviolabil; orice încercare de a deschide sau manipula fizic modulul duce la blocarea permanentă a acestuia. FDM-ul criptează datele și aplică un cod hash fiecărei tranzacții și comenzi. Acest *hash* garantează că datele nu au fost modificate între momentul înregistrării și cel al inspecției. **Cardul de Semnare TVA** (VAT Signing Card – VSC) este un card electronic, personalizat și emis de Guvern (similar unui card bancar cu cip), care asigură autentificarea operatorului economic sau a managerului. FDM-ul funcționează doar când cardul VSC este introdus, asigurând că tranzacțiile sunt semnate digital sub responsabilitatea unei persoane identificate.

Trasabilitatea este asigurată de înregistrarea detaliată și permanentă a operațiunilor: FDM-ul acționează ca un jurnal electronic securizat, stocând toate datele tranzacțiilor (inclusiv comenzile anulate, modificările și bonurile emise) într-un format criptat și nealterabil. Fiecare bon emis poartă numărul unic de identificare al FDM-ului (seria Cutiei Negre) și identificatorul VSC-ului utilizat. Acest lucru asigură trasabilitatea completă a tranzacției până la sistemul și operatorul responsabil. FDM-ul generează fișiere de audit standardizate (adesea în format XML) care pot fi extrase de inspectori și analizate.

Controlul se realizează prin inspecții bazate pe datele stocate: În timpul controalelor fiscale, inspectorii nu se bazează pe transmiterea online de date, ci extrag direct fișierele de audit (FDM data) din Modulul Fiscal de Date. Datorită faptului că FDM-ul înregistrează și hash-ul tuturor comenzilor (nu doar al bonurilor finale), autoritățile pot detecta dacă o comandă a fost luată, dar ulterior anulată sau modificată în mod nejustificat pentru a ascunde veniturile.

Faptul că orice soft POS (inclusiv soluțiile virtuale) trebuie să fie certificat și conectat la FDM-ul hardware elimină posibilitatea utilizării unui soft POS neomologat care să includă funcții ascunse de fraudă (așa-numitele "softuri Zapper").

Sistemul belgian este, așadar, un model de securitate bazat pe hardware certificat și autentificare strictă, cu accent pe auditarea datelor inalterabile stocate local de FDM, fiind diferit de modelul bazat pe transmiterea online a fiecărui bon ca în România sau de cel bazat exclusiv pe criptografie software (Austria).

FRANȚA

În Franța, sistemele de tip „casă de marcat electronică virtuală” (software- de tip POS / sistem de încasare computerizat) au un statut juridic specific, reglementat în principal prin legea anti-fraudă la TVA, dar nu există o obligație generală ca toate firmele să dețină un sistem de casă de marcat. Mai jos sunt cele mai importante aspecte:

Conform art. 286 I-3 bis din Codul fiscal general - [Code général des impôts \(CGI\)](#), un software/sistem POS - „logiciel ou système de caisse” (software sau sistem de casă de marcat) este definit drept sistem informatic care prevede înregistrarea plăților încasate în schimbul livrărilor de bunuri sau prestațiilor de servicii.

În practică: dacă un profesionist (persoană fizică sau juridică) este plătitor de TVA și înregistrează plăți de la clienți neplătitori de TVA (persoane fizice) la care folosește un sistem de casă de marcat software sau hardware, atunci sistemul respectiv trebuie să respecte anumite condiții de securitate: inalterabilitatea, securizarea datelor, conservarea, arhivarea.

Legea de finanțe și reglementările ulterioare au introdus obligativitatea utilizării unui software/sistem de casă de marcat certificat (« logiciel ou système de caisse certifié ») pentru comercianții care încheie tranzacții cu publicul larg și care utilizează un sistem de casă de marcat.

Totodată, nu este obligatoriu pentru toți comercianții să aibă o casă de marcat. Legea nu impune tuturor profesioniștilor să utilizeze automat un sistem de casă de marcat.

Dacă se folosește un sistem software de casă de marcat, atunci acesta trebuie să respecte:

- Inalterabilitatea datelor (nu pot fi modificate după înregistrare)
- Securizarea datelor originale, modificărilor și justificativelor aferente
- Conservarea datelor cumulate, recapitulare, închideri zilnice/lunare/anuale²
- Arhivarea datelor astfel încât să existe dată certă („date certaines”) și integritate în timp
- Certificarea (sau în curs de certificare) a software-ului/casa de marcat – în Franța se utilizează norma «NF525» și este în curs de tranziție spre certificare prin organism acreditat, fără auto-certificare³.
- Sancțiuni în caz de neconformitate: o amendă de 7 500 € pentru fiecare sistem neconform (art. 1770 duodécies CGI).

² <https://www.ionos.fr/startupguide/gestion/nouvelle-reglementation-pour-les-caisses-enregistreuses/>

³ <https://www.sumup.com/fr-fr/gerer-son-entreprise/paiements/caisse-enregistreuse-obligatoire/?>

Procedurile de omologare și certificare a caselor de marcat electronice virtuale (sistemele software sau Cloud POS) în Franța nu se bazează pe o omologare guvernamentală directă, ci pe o certificare a software-ului de către entități terțe sau pe atestarea dezvoltatorului, conform Articolul 88 din Legea nr. 2015-1785 din 29 decembrie 2015 privind finanțele pentru anul 2016 2016 - Loi n° 2015-1785 du 29 décembre 2015 de finances pour 2016⁴ (aplicabil de la 1 ianuarie 2018). Legea nu impune un modul fiscal hardware, ci cere ca softul să garanteze inalterabilitatea, securitatea și arhivarea datelor de încasare.

Există două modalități principale prin care un sistem virtual poate obține statutul juridic de conformitate:

- **Certificarea de către un Organism Acreditat.**

Software-ul de încasare este supus unui audit complet de către un organism independent, acreditat de stat, cum ar fi LNE (Laboratoire National de métrologie et d'Essais) sau AFNOR Certification.

Organismul efectuează teste detaliate pentru a verifica dacă funcțiile software-ului (înregistrarea, anularea, modificarea și arhivarea tranzacțiilor) respectă cerințele legale de inalterabilitate.

În final se obține un Certificat de Conformitate oficial, care trebuie prezentat autorităților fiscale la cerere.

- **Atestarea Individuală a Editorului**

Dacă software-ul nu este certificat de un organism terț, dezvoltatorul (editorul) trebuie să își asume responsabilitatea. Editorul emite o Atestare Individuală de Conformitate (Attestation Individuelle de Conformité). Prin această atestare, dezvoltatorul garantează, sub propria răspundere, că software-ul îndeplinește toate condițiile de inalterabilitate și securitate impuse de legislația franceză.

Indiferent de calea aleasă, certificarea se axează pe verificarea următoarelor mecanisme implementate în software-ul virtual:

- Datele tranzacțiilor trebuie înregistrate cronologic și continuu.
- Datele înregistrate trebuie să fie protejate prin tehnici de criptografie (hashing sau *chaining*), făcând imposibilă modificarea lor ulterioară.
- Software-ul trebuie să efectueze închideri zilnice, lunare și anuale, sigilând definitiv datele fiscale din acele perioade.
- Trebuie să existe o funcționalitate care să permită exportul securizat al datelor arhivate într-un format standard (FAFEC - Fichier des Écritures Comptables), necesar în caz de control fiscal.

Comerciantul care utilizează un sistem virtual trebuie să dețină fie Certificatul de Conformitate, fie Atestarea Individuală a editorului.

Dacă la un control fiscal, contribuabilul nu poate prezenta unul dintre aceste două documente, se aplică o amendă fixă de €7.500 per sistem de încasare necertificat.

Bonul fiscal este recunoscut ca document oficial dacă este emis de un sistem certificat și securizat.

⁴ <https://bofip.impots.gouv.fr/bofip/10693-PGP.html/identifiant%3DACTU-2016-00190>

Bonul trebuie să fie generat de un software de încasare care deține fie un Certificat de Conformitate emis de un organism acreditat (AFNOR, LNE), fie o Atestare Individuală de Conformitate emisă de editor.

Bonul este considerat oficial deoarece datele sale sunt înregistrate imediat și inalterabil în sistem. Odată emis, softul nu permite modificarea sau ștergerea datelor tranzacției.

Bonul trebuie să conțină toate informațiile fiscale necesare (TVA, detalii comerciant, prețuri). Deși legea nu impune un Cod QR fiscal pe bon, sistemul trebuie să înregistreze în jurnalul său elemente de securitate criptografică.

Transmiterea bonurilor fiscale (tranzacții B2C) se face exclusiv către client, întrucât nu există o obligație de transmitere online, în timp real, a fiecărui bon către autoritatea fiscală franceză (Direction générale des Finances publiques - DGFIP).

Sistemul francez se bazează pe controlul intern al integrității software-ului și pe audituri ulterioare, nu pe monitorizarea continuă.

În caz de control, contribuabilul trebuie să furnizeze datele fiscale arhivate (inclusiv bonurile) în format electronic standard (FAFEC - Fichier des Écritures Comptables).

Bonurile pot fi puse la dispoziția clientului în format electronic (ex. trimise prin e-mail, afișate pe dispozitiv mobil) sau tipărite, cu condiția ca ele să fie o copie fidelă și lizibilă a datelor înregistrate securizat de sistemul certificat.

Legea vizează eliminarea tipăririi automate a bonurilor pe hârtie (cu excepții), promovând astfel implicit transmiterea electronică.

Arhivarea este un pilon central al conformității și securității datelor. Sistemul de încasare certificat trebuie să stocheze toate bonurile într-un jurnal electronic (journal des ventes) sau un fișier securizat. Software-ul trebuie să efectueze închideri periodice (zilnice, lunare, anuale) care sigilează definitiv datele fiscale din acele perioade. Datele sigilate nu mai pot fi accesate sau modificate. Documentele și registrele contabile, inclusiv datele bonurilor fiscale arhivate în sistemul certificat, trebuie păstrate pentru o perioadă de 6 ani.

Bonul fiscal electronic (Ticket de Caisse) este recunoscut ca document fiscal oficial în Franța. Recunoașterea provine din faptul că bonul a fost generat de un sistem al cărui software a fost certificat ca fiind inalterabil și securizat conform cerințelor DGFIP. Bonul servește ca dovadă a încasării și a colectării TVA în tranzacțiile B2C. Pentru tranzacțiile B2B (între companii), bonul simplu nu este suficient pentru deducerea TVA-ului, fiind necesară emiterea unei facturi complete.

Securitatea se realizează prin funcționalitățile obligatorii ale softului certificat:

- Sistemul software trebuie să garanteze că, odată ce o tranzacție (bon, anulare, retur) este înregistrată, aceasta nu mai poate fi modificată sau ștearsă. Orice ajustare trebuie efectuată printr-o tranzacție ulterioară, transparentă și inversă.
- Software-ul trebuie să utilizeze tehnici de securizare (criptografie) pentru a proteja datele înregistrate. De exemplu, prin utilizarea unor funcții hash sau a unui lanț de legătură (chaining) care să conecteze logic și cronologic tranzacțiile, asigurând o "plumbuire digitală" (similar cu modelul austriac).

- Toate tranzacțiile trebuie înregistrate cronologic și continuu în jurnalul electronic, fără lacune.
- Softul este obligat să efectueze închideri (zilnice, lunare, anuale). Aceste închideri sigilează definitiv datele fiscale ale perioadei respective, făcându-le inalterabile.

Mecanisme de Control și Trasabilitate

Controlul se bazează pe documentele de certificare și pe extragerea datelor în caz de audit.

Principalul mecanism de control este obligația ca operatorul economic să prezinte la control fie Certificatul de Conformitate emis de un organism terț (ex. LNE, AFNOR), fie Atestarea Individuală emisă de dezvoltator. Acest document garantează că mecanismele de securitate de mai sus sunt implementate.

Sistemul trebuie să permită extragerea tuturor datelor contabile și fiscale într-un format electronic standardizat, numit FAFEC (Fichier des Écritures Comptables). Acest fișier conține toate înregistrările necesare pentru un audit detaliat.

Autoritatea fiscală (DGFIP) efectuează audituri bazate pe analiza FAFEC, verificând integritatea lanțului de înregistrări, coerența datelor și prezența tuturor închiderilor fiscale.

Sistemul francez de prevenire a evaziunii se focalizează pe securitatea internă a software-ului, transferând responsabilitatea garantării inalterabilității datelor de la hardware (placă fiscală) la aplicația de vânzare.

GERMANIA

În Germania, sistemele de casă de marcat electronice (inclusiv cele virtuale sau bazate pe software) sunt reglementate strict din punct de vedere fiscal.

Codul fiscal german ([Abgabenordnung](#) – AO), la § 146a impune ca sistemele electronice de înregistrare să îndeplinească anumite cerințe tehnice și să fie raportate autorităților fiscale.

Regulamentul privind stabilirea cerințelor tehnice pentru sistemele electronice de înregistrare și securitate în tranzacțiile comerciale ([KassenSicherungsverordnung](#) - KassenSichV stabilește cerințele privind securitatea tehnică a sistemelor de marcat/POS – de exemplu introducerea unui modul de securitate tehnologică certificat TSE⁵.

De la 1 ianuarie 2025, a intrat în vigoare o obligație de raportare pentru aceste sisteme: fiecare sistem de casă de marcat electronică trebuie declarat organului fiscal pentru fiecare punct de vânzare.⁶

Dacă o firmă utilizează un sistem de înregistrare electronică (software, aplicație, tabletă, POS-app) care funcționează ca registru de casă (adică înregistrează tranzacții

⁵ <https://www.fiskaly.com/blog/kassensichv-and-tss-fiscalization-in-germany?utm>

⁶ <https://assets.kpmg.com/content/dam/kpmg/de/pdf/Themen/2025/05/KPMG-electronic-cash-register-systems-2025.pdf>

legate de vânzare de bunuri/servicii) și emite chitanțe sau înregistrează plăți, atunci acest sistem poate să cadă sub obligațiile de mai sus.

Sistemul trebuie să fie dotat cu TSE certificat (modulul de securitate tehnologică) sau dacă este cazul, să respecte alte reglementări corespunzătoare. Chiar dacă este “virtual” (cloud, software), nu se scutește de obligație dacă funcționează ca registru de casă.

Cum trebuie procedat dacă se implementează sistemul german:

- Se verifică dacă sistemul este considerat „casă de marcat electronică” conform definiției (adică, dacă înregistrează vânzări, emite chitanțe, etc.).
- Comerciantul se asigură că sistemul are o TSE (modulul de securitate) certificat de Bundesamt für Sicherheit in der Informationstechnik (BSI). ([BSI](#))
- Se raportează sistemul autorității fiscale via portalul „Mein ELSTER” sau interfața ERiC. Deadlines: pentru sistemele achiziționate înainte de 1 iulie 2025 — raportare până la 31 iulie 2025. Pentru cele după 1 iulie 2025 — în termen de o lună. ([winheller.com](#))
- Se păstrează evidențe complete, transparente și imuabile — sistemul trebuie să permită audit de către autorități.

În concluzi, casele de marcat electronice virtuale (cash-register / POS pur software, inclusiv cloud) sunt permise în Germania, dar intră sub același regim fiscal ca orice sistem electronic de înregistrare și trebuie să respecte trei piloni federali:

- Baza legală federală menționată mai sus
- TSE și soluții cloud - TSE poate fi hardware sau cloud, dar trebuie să fie certificată BSI (lista oficială a produselor/serviciilor TSE).
- Obligația de raportare (din 2025) - Fiecare sistem electronic de înregistrare și TSE folosită se raportează electronic prin Mein ELSTER (formularul Notificarea sistemelor electronice de înregistrare prevăzut la §146a paragraful 4 din Codul Fiscal German (AO)) - Mitteilung über elektronische Aufzeichnungssysteme⁷):
Alte obligații federale relevante
- chitanță obligatorie (electronică sau pe hârtie) pentru toate sistemele menționate la §146a AO.
- cerințe de export/audit ale datelor (conform AEAO la § 146a AO – ghid de aplicare al Ministerului Finanțelor).

Certificarea se aplică doar modulului de securitate TSE (Technische Sicherheitseinrichtung). O „casă de marcat virtuală” este legală dacă integrează o TSE certificată BSI, respectă KassenSichV și poate exporta datele în format DSFinV-K.

TSE este certificată conform ghidului tehnic BSI TR-03153⁸; certificarea este emisă/listată de BSI (Bundesamt für Sicherheit in der Informationstechnik).

⁷ <https://www.bundesfinanzministerium.de/Content/DE/Downloads/Steuern/FAQ-Ausfuellanleitung.html>

⁸ <https://www.tuvit.de/en/services/norms-standards-guidelines/bsi-tr-03153/>

Proiectare conform TR-03153 include cerințe pentru semnarea/încapsularea fiecărei tranzacții, jurnalizare imuabilă, marcaj temporal, protecții anti-manipulare și interfața standardizată către sistemul de înregistrare⁹.

Se face o evaluare conform TR-03153. Laboratoare recunoscute (ISO/IEC 17025) efectuează testele și emit raportul tehnic.

Pe baza raportului de încercare, BSI emite certificatul TSE (cu perioadă de valabilitate) și îl publică pe lista oficială. Există și reguli tranzitorii/documente de menținere a certificării în situații justificate.

Actualizările majore de firmware/software ale TSE pot necesita reevaluare. Producătorul trebuie să mențină conformitatea pe toată durata certificării. ([BSI](#))

Emiterea bonurilor fiscale electronice

Fiecare tranzacție înregistrată de casa de marcat (inclusiv virtuală) trebuie să genereze automat un bon fiscal

Bonul poate fi tipărit pe hârtie sau emis electronic (eBon), cu consimțământul clientului.

Trebuie să includă: – denumirea comerciantului și adresa – data și ora – numărul de serie al TSE – semnătura digitală și codul *hash* – suma totală și TVA – tipul de plată (cash/card/digital)

Fiecare bon fiscal trebuie "semnat" TSE, ceea ce îi oferă validitate fiscală

Bonul electronic (eBon) este considerat **emis** atunci când clientul poate **vizualiza sau descărca** documentul electronic (ex: link QR, e-mail, PDF, app).

Arhivarea bonurilor electronice. Perioada de păstrare a bonurilor este de minimum **10 ani** de la data emiterii. Bonurile trebuie păstrate **în format neschimbabil (WORM)** – nu PDF reeditabil.

Autoritățile fiscale pot solicita exportul complet al bonurilor, semnăturilor TSE și jurnalului fiscal (DSFinV-K)

eBon-ul are aceeași valoare juridică ca bonul tipărit, dacă:

- Este generat de un sistem de înregistrare electronică conform § 146a AO.
- Include semnătura digitală TSE (hash + certificat valid).
- Poate fi auditat integral prin export DSFinV-K.

Mecanismele de securitate tehnică (Technische Sicherheitseinrichtung – TSE). TSE este nucleul sistemului de protecție — un modul hardware sau cloud certificat de BSI (Bundesamt für Sicherheit in der Informationstechnik).

Componentele TSE îndeplinesc următoarele funcții:

- înregistrează, semnează și sigilează fiecare tranzacție prin algoritmi asimetrici;
- păstrează jurnalul criptat al tuturor operațiunilor, cu verificare hash-chain;

⁹ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Schutz-vor-Manipulation-an-digitalen-Grundaufzeichnungen/Informationen-zur-Zertifizierung/Informationen-zur-zertifizierung_node.html?utm

- Conectează sistemul de marcat cu TSE printr-un canal criptat (TLS).

Măsurile de securitate:

- Semnătură digitală pentru fiecare înregistrare (tranzacție, anulare, retur).
- Hash-chain pentru detectarea oricărei modificări.
- Timestamp sincronizat și certificat.
- Certificat TSE emis și validat de BSI.
- Mecanism anti-replay și anti-tampering (detectie intervenție fizică sau logică).

Mecanisme de control administrativ și audit fiscal:

- Inspectorii pot accesa DSFinV-K, verifica TSE, exporta jurnalele și semnăturile;
- Analiză a datelor exportate, verificarea coerenței hash-urilor, testarea software-ului;
- Analizează pattern-uri de evaziune (vânzări lipsă, date șterse, timpi anormali).
- Fiecare TSE și sistem POS trebuie raportat și identificat la fisc.

Germania utilizează o combinație de instrumente tehnice (criptografie, semnătură digitală, hash-chain) și măsuri administrative (raportare, audit, inspecții inopinate) pentru a asigura:

- Integritatea și imuabilitatea datelor fiscale;
- Trasabilitatea completă a tranzacțiilor;
- Detectarea automată a manipulărilor;
- Responsabilizarea fiecărui operator economic;
- Reducerea masivă a evaziunii bazate pe numerar.

ITALIA

În Italia, sistemul normal pentru punerea în evidență a încasărilor la vânzarea de bunuri/prestarea de servicii este cel al „Registratore Telematico” (RT) — un registrator de casă conectat telematic către Agenzia delle Entrate, autoritatea fiscală italiană.

Obligația a fost introdusă prin DECRETUL LEGISLATIV nr. 127 din 5 august 2015 Transmiterea electronică a tranzacțiilor cu TVA și controlul vânzărilor de bunuri efectuate prin intermediul automatelor de vânzare, în temeiul articolului 9, alineatul 1, lit. d) și g), din Legea nr. 23 din 11 martie 2014. (15G00143) - [Decreto Legislativo 127/2015](#), care a stabilit principiul memorizării electronice și transmiterii telematice a încasărilor pentru comercianți.

Legea italiană prevede că datele privind încasările trebuie să fie memorizate electronic și transmise telematic către Agenzia delle Entrate.

Casele de marcat electronice sunt permise și (de fapt impuse) ca sisteme de înregistrare electronică (registratori telematici) pentru majoritatea comercianților.

Versiunea „virtuală” (software/cloud) devine posibilă și recunoscută dacă îndeplinește cerințele tehnice legale (memorizare, transmitere telematică, inalterabilitate).

Sistemul tradițional hardware (registrator telematic) încă este standardul, dar legislația evoluează spre software/soluție virtuală.

Casa de marcat electronică virtuală (soluție software care memorează și transmite telematic încasările) este legală și are propriile proceduri oficiale. Există două trasee paralele, în funcție de tipul soluției folosite:

- Registratore Telematico (RT) clasic (hardware/embedded) – modele omologate de Agenzia delle Entrate;
- Soluție software alternativă (noua opțiune națională) – cu specificații tehnice oficiale publicate de Agenzia delle Entrate în 2025, operațională din 2026.
- Procedurile de omologare și certificare pentru casele de marcat electronice virtuale (incluse în categoria Registratori Telematici - RT) în Italia sunt reglementate de Agenzia delle Entrate (ADE) și se concentrează pe aprobarea modelului de către autoritatea fiscală.

Procedura italiană impune omologarea prealabilă a modelului de software/echipament înainte de a fi introdus pe piață:

- Producătorul de software (editorul soluției virtuale) sau importatorul depune o cerere de omologare (aprobare a modelului) la Agenzia delle Entrate.
- Se anexează documentația tehnică detaliată a soluției, care descrie arhitectura software, modul de funcționare, mecanismele de memorizare inalterabilă, protocoalele de comunicare și implementarea semnăturii digitale.
- ADE examinează modelul (inclusiv prin teste practice) pentru a verifica dacă îndeplinește cerințele de securitate, memorizare și transmitere electronică. Această etapă include verificarea: a) Capacității de a semna digital bonul; b) Inalterabilității jurnalului electronic; c) Protocoalelor de comunicare cu serverele ADE.
- Dacă verificarea este pozitivă, ADE emite o Decizie de Aprobare (Provvedimento di Approvazione), care autorizează modelul respectiv de Registrator Telematic (fie fizic, fie software/virtual) pentru utilizare fiscală.

După omologarea modelului, urmează etapele de certificare a unității individuale și punerea în funcțiune.

Doar tehnicienii acreditați (Laboratori de Verificare sau "Technical Assistance Centres") pot efectua instalarea și activarea.

La instalarea la comerciant (pentru soluția virtuală, la activarea softului), se efectuează o Verificare Inițială pentru a confirma că sistemul funcționează conform modelului omologat și că poate comunica securizat.

Sistemul virtual primește un Certificat Digital de Echipament (Certificato Dispositivo) de la ADE. Acest certificat este utilizat pentru semnarea digitală a bonurilor fiscale electronice, garantând autenticitatea și integritatea fiecărei tranzacții.

Registratorii Telematici (inclusiv soluțiile virtuale) sunt supuși unor verificări periodice obligatorii (de obicei, la fiecare doi ani) pentru a reconfirma funcționarea corectă a mecanismelor de memorizare și securizare a datelor.

În esență, sistemul italian necesită aprobarea prealabilă a modelului de către autoritatea fiscală (ADE) și certificarea unității individuale prin atribuirea unui certificat digital fiscal (pas esențial pentru funcția de semnare a bonurilor).

Modalitățile de emitere, transmitere și arhivare a bonurilor fiscale electronice în Italia sunt guvernate de sistemul Registratoarelor Telematici (RT) și de cerința de Memorizare și Transmitere Electronică (MTT) a datelor către Agenzia delle Entrate (ADE). Bonul electronic (numit Documento Commerciale Online) este pe deplin recunoscut ca document fiscal oficial.

Bonul electronic este documentul fiscal oficial care a înlocuit bonul fiscal pe hârtie (scontrino fiscale). Bonul este generat de un Registrator Telematic (RT) certificat (care poate fi o soluție software virtuală sau un aparat fizic). RT-ul aplică automat o semnătură electronică calificată bonului, utilizând un certificat digital al dispozitivului emis de ADE. Această semnătură asigură integritatea și autenticitatea (plumbuirea digitală) datelor bonului în momentul emiterii. Bonul electronic semnat digital este recunoscut ca document fiscal oficial în scopuri TVA și contabile.

Deși bonul oficial este cel electronic securizat, clientului i se poate oferi o copie pe hârtie, o chitanță electronică (prin e-mail, aplicație) sau un Cod QR. Totuși, doar bonul electronic semnat digital transmis la ADE este documentul fiscal valid.

Registratorul Telematic (RT) are obligația de a transmite automat datele agregate ale bonurilor fiscale (jurnalul electronic) către serverele centrale ale Agenziei delle Entrate (ADE). De obicei, transmiterea se face zilnic, la momentul închiderii fiscale (Rapporto di chiusura giornaliera), sau imediat, în cazul soluțiilor complet online. Transmisia folosește un protocol de comunicare securizat și criptat, garantând că datele ajung la ADE în siguranță.

Arhivarea se realizează pe două niveluri:

- **Arhivarea de către RT (Local)** - Registratorul Telematic (RT), fie el fizic sau virtual, are o memorie inalterabilă destinată stocării copiei electronice a bonurilor emise (jurnal electronic), conform specificațiilor tehnice impuse de ADE.
- **Arhivarea Centralizată (ADE)** - Odată transmise, datele bonurilor fiscale sunt stocate și arhivate centralizat pe serverele Agenziei delle Entrate. Contribuabilii pot accesa și consulta aceste date arhivate pe portalul lor fiscal (Fisconline). Documentele și registrele fiscale trebuie păstrate pentru o perioadă de 10 ani în scopuri contabile și fiscale.

Bonul electronic este recunoscut necondiționat ca document fiscal oficial, datorită următoarelor garanții: Bonul electronic are o semnătură digitală calificată aplicată de RT certificat, care îi conferă valoare legală și asigură non-repudierea (comerciantul nu poate nega emiterea) și integritatea. Servește ca dovadă a încasării și a colectării TVA în tranzacțiile B2C. Pentru deducerea TVA și justificarea cheltuielilor de către companii (B2B), deși bonul poate fi o dovadă inițială a plății, documentul primar necesar este Fatura Electronică (e-Fattura), pe care Italia o impune obligatoriu în relațiile B2B și B2C (la cererea clientului).

Mecanismele de control, securitate și trasabilitate utilizate în Italia sunt printre cele mai avansate din Europa și se bazează pe o strategie fiscală duală: fiscalizarea la sursă prin Registratori Telematici (RT) și monitorizarea centralizată prin Facturarea Electronică (e-Fattura). Ambele sisteme sunt gestionate de Agenzia delle Entrate (ADE).

Acestea asigură că datele bonurilor (Documento Commerciale Online) sunt inalterabile. Doar modelele de RT (inclusiv soluțiile virtuale) aprobate prealabil de ADE pot fi utilizate. Aceasta garantează că sistemul include funcțiile de securitate necesare. Fiecare bon electronic este semnat digital cu un certificat digital al dispozitivului (RT). Această semnătură asigură integritatea și autenticitatea datelor, prevenind orice modificare ulterioară și asigurând non-repudierea. RT-ul (fizic sau componenta de memorizare a soluției virtuale) trebuie să dețină o memorie electronică inalterabilă (jurnal electronic) care stochează toate tranzacțiile, servind ca dovadă primară în caz de audit. În cazul RT-urilor fizice, există un sigiliu fizic. În cazul soluțiilor virtuale, echivalentul este sigiliul software al sistemului certificat și protecția datelor criptate.

Mecanisme de Control și Transmisie (MTT și e-Fattura). Acestea asigură colectarea centralizată a datelor și verificarea încrucișată:

- Datele agregate ale bonurilor fiscale (jurnalul) sunt transmise zilnic, automat de la Registratorul Telematic (RT) către serverele centrale ale ADE. Aceasta oferă Agenției o viziune completă și rapidă asupra veniturilor B2C la nivel național.
- Italia impune Factura Electronică (e-Fattura) obligatorie pentru aproape toate tranzacțiile B2B și B2C (dacă clientul o solicită). Toate facturile trec printr-un sistem centralizat numit Sistema di Interscambio (SdI).
- ADE poate compara volumele totale de vânzări B2C raportate prin RT (zilnic) cu volumele B2B raportate prin SdI. Această corelare extrem de eficientă permite identificarea imediată a discrepanțelor și a riscului de evaziune.
- Transmiterea datelor (atât de la RT, cât și de la e-Fattura) se face prin protocoale securizate și criptate, garantând confidențialitatea și integritatea în timpul transferului.

Deoarece toate tranzacțiile B2B/B2C sunt fie semnate de RT și transmise (bonuri), fie procesate centralizat (facturi), există o trasabilitate completă a fiecărui flux de venituri.

ADE utilizează datele masive primite din sistemele MTT și SdI pentru a efectua analize de risc de înaltă precizie. Aceste analize identifică sectoarele, zonele geografice sau contribuabilii cu neconcordanțe între TVA declarat, bonuri emise și facturi emise/primite.

Contribuabilii pot accesa portalul Fisconline pentru a vedea propriile date de tranzacții înregistrate de ADE, ceea ce crește transparența și încurajează conformarea voluntară.

Modelul italian este un exemplu de integrare a controlului fiscal, eliminând bonul pe hârtie și obligând la transmiterea integrală a datelor fiscale electronic, atât pentru B2B, cât și pentru B2C.

SPANIA

În Spania, statutul juridic al „caselor de marcat electronice virtuale” (sau mai exact al sistemelor electronice de emiterie/înregistrare a bonurilor/facturilor și al soft-urilor de gestiune fiscală) nu este încă **complet** uniformizat la nivel național, dar există o tendință clară către reglementare mai strictă, mai ales în scopul combaterii fraudei fiscale.

Există deja reglementări care se aplică soft-urilor de facturare / sisteme informatice de facturare (invoice-software) în Spania, de pildă, [Decretul Regal 1007/2023](#), din 5 decembrie, privind aprobarea Regulamentului care stabilește cerințele pe care trebuie să le adopte sistemele și programele informatice sau electronice care susțin procesele de facturare ale întreprinderilor și profesioniștilor și standardizarea formatelor înregistrărilor de facturare.

Astfel, dacă sistemul (inclusiv o „casă de marcat virtuală”) emite bonuri, facturi, sau ține evidența vânzărilor pentru autoritatea fiscală, atunci trebuie să respecte cerințele legale privind trasabilitatea, integritatea datelor, arhivarea și altele.

De la 1 iulie 2026 se va introduce sistemului VERIFACTU, care va impune standarde tehnice pentru softurile de facturare/emiterie din Spania, inclusiv formate XML, semnături electronice și transmiterea către autoritățile fiscale.¹⁰ De exemplu, conform informațiilor, softurile ar trebui să permită stocarea în timp real a datelor (noi, anulate) într-un format definit de lege.¹¹

Deși există reglementări stricte pentru softuri de facturare și transmiterea datelor fiscale, termenul „casă de marcat electronică virtuală” (în sensul unui dispozitiv fizic sau complet virtual într-un mediu de cloud) nu este întotdeauna tratat separat în legislație specifică — regulile se axează mai mult pe sistemele informatice care sprijină facturarea și înregistrarea vânzărilor. În anumite regiuni autonome din Spania pot exista reguli locale suplimentare privind „fiscalizarea” caselor de marcat (ex: regiuni cu sisteme proprii de control).

În Spania, „casa de marcat electronică virtuală” intră juridic în categoria SIF — Sisteme informatice de facturare reglementate de Decretul Regal 1007/2023, din 5 decembrie, privind aprobarea Regulamentului care stabilește cerințele pe care trebuie să le adopte sistemele și programele informatice sau electronice care susțin procesele de facturare ale întreprinderilor și profesioniștilor și standardizarea formatelor înregistrărilor de facturare și de Ordinul HAC/1177/2024, din 17 octombrie, care dezvoltă specificațiile tehnice, funcționale și de conținut menționate în Regulamentul care stabilește cerințele pe care trebuie să le adopte sistemele și programele informatice sau electronice care susțin procesele de facturare ale întreprinderilor și profesioniștilor și standardizarea formatelor înregistrărilor de facturare, aprobat prin Decretul Regal 1007/2023, din 5 decembrie; și în Regulamentul care reglementează obligațiile de facturare, aprobat prin Decretul Regal 1619/2012, din 30 noiembrie. Omologarea/certificarea nu este un test de stat clasic, ci se face prin Certificarea

¹⁰ <https://ticnegocios.camaravalencia.com/servicios/tendencias/cuando-entrara-en-vigor-verifactu/>

¹¹ <https://www.boe.es/buscar/act.php?id=BOE-A-2024-22138>
<https://www.boe.es/buscar/act.php?id=BOE-A-2023-24840>

producătorului (declarație pe proprie răspundere) + respectarea strictă a cerințelor tehnice, cu sancțiuni mari dacă software-ul nu corespunde.

În concluzie, statutul juridic al caselor de marcat electronice virtuale în Spania este acela de Instrumente de Facturare Electronice Certificate (SIF), care sunt obligate să integreze mecanisme de securitate criptografică la nivel de software pentru a garanta integritatea datelor, fără a mai fi necesară o componentă hardware fiscală separată.

Procedurile de omologare și certificare pentru casele de marcat electronice virtuale (adică sistemele software și Cloud POS) în Spania, stabilite de Regulamentul VERIFACTU (Real Decreto 1007/2023) se concentrează pe certificarea software-ului și pe responsabilitatea dezvoltatorului, spre deosebire de certificarea hardware.

Modalitățile de emitere, transmitere și arhivare a bonurilor fiscale electronice în Spania sunt în curs de a fi standardizate la nivel național sub regimul VERIFACTU (Real Decreto 1007/2023). Recunoașterea acestora ca documente fiscale oficiale este direct legată de integrarea mecanismelor de securitate criptografică impuse de acest regulament.

Statutul de document fiscal oficial este conferit bonului prin aplicarea securității la sursă: Bonul trebuie emis exclusiv de un Sistem de Facturare Certificat (VERIFACTU), care poate fi o soluție software virtuală (Cloud POS) sau un sistem integrat. În momentul emiterii, sistemul trebuie să aplice automat o semnătură criptografică bonului – sigilare digitală. Această semnare asigură integritatea datelor și creează un lanț de securitate (chaining) cu tranzacția precedentă.

Bonul (sau factura simplificată) trebuie să includă obligatoriu un Cod QR care conține:

- Datele esențiale ale tranzacției.
- Semnătura criptografică.
- Identificatorul sistemului software și al dezvoltatorului.
- Bonul (factura simplificată) emis conform cerințelor VERIFACTU este recunoscut ca document fiscal oficial și servește ca dovadă a tranzacției.

Sistemul VERIFACTU oferă opțiunea ca înregistrările fiscale (bonurile) să fie transmise automat, imediat sau cvasi-imediat, către serverele AEAT (Agenția de Administrare Fiscală). Deși nu este obligatoriu ca fiecare bon să fie transmis individual în timp real (ca în sistemul SII pentru facturi), această opțiune este recomandată pentru simplificare. Dacă opțiunea de transmitere imediată nu este activată, sistemul generează un fișier de înregistrări auditable (audit log) care poate fi transmis la cererea AEAT sau în cadrul unui audit.

Bonurile pot fi puse la dispoziția clientului în format electronic (ex. prin e-mail, aplicație, link), cu condiția ca acesta să fie o copie fidelă a datelor înregistrate securizat și să conțină obligatoriu Codul QR pentru verificare. Codul QR permite clientului să verifice autenticitatea bonului utilizând instrumente puse la dispoziție de autoritatea fiscală.

Arhivarea este obligatorie și trebuie să fie asigurată de sistemul software: Sistemul VERIFACTU trebuie să păstreze un registru de înregistrări *auditable* care conține toate bonurile emise, inclusiv detaliile criptografice (lanțul de securitate). Acest registru trebuie să fie inalterabil și ușor de accesat de către autorități. Contribuabilul este responsabil de

păstrarea acestor înregistrări securizate, chiar dacă utilizează un sistem Cloud POS. Documentele fiscale, inclusiv registrul de bonuri, trebuie păstrate pe o perioadă de 4 ani (termenul general de prescripție fiscală în Spania).

Bonul fiscal securizat (Factura Simplificada) servește ca dovadă legală a tranzacției și a TVA-ului colectat în tranzacțiile B2C. Pentru deducerea TVA-ului și justificarea cheltuielilor de către companii (B2B), deși bonul poate fi utilizat ca dovadă inițială, este necesară emiterea unei facturi complete (care, în multe cazuri, trebuie transmisă separat prin sistemul SII).

Respectarea standardelor VERIFACTU este ceea ce conferă bonului electronic spaniol statutul de document fiscal oficial și de încredere, fiind protejat de mecanisme de criptare la nivel de software.

Mecanismele de control, securitate și trasabilitate utilizate în Spania pentru protejarea datelor fiscale și prevenirea evaziunii sunt consolidate prin două sisteme majore gestionate de Agenția de Administrare Fiscală (AEAT): Sistemul de Furnizare Imediată a Informațiilor (SII) pentru facturare și Proiectul VERIFACTU pentru sistemele de vânzare (case de marcat/POS).

Mecanismele de control, securitate și trasabilitate utilizate în Spania pentru protejarea datelor fiscale și prevenirea evaziunii sunt consolidate prin două sisteme majore gestionate de Agenția de Administrare Fiscală (AEAT): Sistemul de Furnizare Imediată a Informațiilor (SII) pentru facturare și Proiectul VERIFACTU pentru sistemele de vânzare (case de marcat/POS).

Aceste mecanisme vizează integritatea datelor la sursă, prevenind manipularea bonurilor și a facturilor simplificate:

- Sistemul software (inclusiv soluțiile virtuale) trebuie să aplice o semnătură electronică criptografică fiecărui bon fiscal (Factura Simplificada) în momentul emiterii. Aceasta asigură că datele tranzacției sunt inalterabile – sigilare digitală;
- Se impune un mecanism de lanț de trasabilitate (similar unui registru blockchain). Fiecare bon emis poartă în semnătura sa referința criptografică (hash-ul) bonului precedent. Orice tentativă de ștergere sau modificare a unei înregistrări ar rupe lanțul, făcând fraudă detectabilă.
- Fiecare bon securizat include un Cod QR care conține informațiile cheie și valoarea criptografică (hash-ul). Acest cod permite autorităților (și clienților) să verifice rapid autenticitatea și integritatea bonului.
- Sistemul software trebuie să genereze și să stocheze un registru electronic auditabil (audit log) care să fie securizat și inalterabil, păstrând o evidență completă a tuturor tranzacțiilor.
- Bonul emis include un identificator unic al software-ului și al dezvoltatorului, asigurând trasabilitatea tranzacției până la sursa sa.

Mecanisme de Control și Transmisie (SII - Pentru Facturi). Acest sistem se aplică marilor companii și grupurilor de TVA și asigură controlul cvasi-instantaneu asupra TVA-ului:

- Companiile obligate trebuie să transmită datele esențiale din registrele lor de facturare (emise și primite) către serverele AEAT în maximum 4 zile lucrătoare de la emitere/înregistrare.
- Transmiterea se face printr-un Web Service securizat bazat pe mesaje în format XML.
- AEAT compară datele transmise de vânzător cu cele transmise de cumpărător. Această verificare încrucișată automată permite identificarea rapidă a discrepanțelor și a fraudei de tip TVA-carusel.

SII permite contribuabililor să consulte propriile registre de TVA pe portalul AEAT (parțial pre-populate) și oferă autorității fiscale o viziune completă asupra bazei de TVA la nivel național aproape în timp real.

AEAT utilizează instrumente avansate de Big Data și analiză de risc pentru a procesa volumele mari de informații primite prin SII și VERIFACTU, identificând rapid tipare suspecte și selectând contribuabilii pentru inspecție.

Faptul că sistemele software trebuie să fie conforme și certificate (VERI*FACTU) și că dezvoltatorii poartă responsabilitatea integrității datelor elimină posibilitatea utilizării softurilor de tip "Zapper" (programe de fraudă care șterg tranzacțiile).

SUEDIA

Statutul juridic al sistemelor de casă de marcat (inclusiv virtuale / software) în Suedia este într-un stadiu mai puțin "fiscalizat" decât în alte țări (ex: Italia, Germania), dar există cerințe clare și o evoluție spre digitalizare.

Este obligatoriu ca orice firmă care realizează vânzări cu numerar sau plăți cu cardul trebuie să utilizeze o casă de marcat certificată și un „control unit” (sau echivalent) aprobat de Swedish Tax Agency (Skatteverket). Bonul de casă („receipt”) trebuie emis pentru fiecare tranzacție. Poate fi pe hârtie sau electronic. Casa de marcat trebuie înregistrată la Skatteverket, fiecare unitate și/equipment cu număr de serie.¹²

Legea suedeză ([Lag \(2007:592\) om kassaregister m.m.](#), regulamentele [Skatteverket SKVFS 2014:9](#)) privind casele de marcat nu obligă tipărirea hârtiei; un bon electronic este legal dacă clientul îl poate primi. De la 1 iulie 2024, potrivit modificărilor la Legea contabilității - [Bokföringslag \(1999:1078\)](#) firmele pot păstra doar versiuni digitale ale bonurilor/facturilor - hârtia originală nu trebuie obligatoriu păstrată dacă e digitalizată. Există excepții: de exemplu mașinile automate, automatele self-service (vending) pot fi exceptate de anumite cerințe de casă de marcat.

¹²<https://www.skatteverket.se/servicelankar/otherlanguages/englishengelska/businessesandemployers/startingandrunningaswedishbusiness/cashregisters.4.57cadbbd15a3688ff44ddf9.html>

Sistemul suedez de fiscalizare nu impune o omologare directă a software-ului virtual, ci se bazează pe obligativitatea conectării oricărui sistem de vânzare (inclusiv soluțiile virtuale sau Cloud POS) la o Unitate de Control a Registrului (Kontrollenhet), care este un modul fizic de securitate.

Procedurile de omologare și certificare sunt gestionate de Skatteverket (Agenția Fiscală Suedeză) și se împart în două etape distincte:

Omologarea Unității de Control (Kontrollenhet) Aceasta este etapa principală de omologare hardware/firmware, similară cu placa fiscală din alte țări.

Producătorul Unității de Control (Kontrollenhet) solicită omologarea modelului de la Skatteverket.

Modelul este supus unor teste riguroase de către laboratoare sau experți desemnați pentru a verifica:

- Securitatea fizică (imposibilitatea de a deschide fără a lăsa urme).
- Implementarea corectă a funcțiilor de criptare și securizare a tranzacțiilor.
- Funcționalitatea protocolului de comunicare cu sistemul POS.

Dacă modelul trece testele, Skatteverket îl înregistrează și îl listează în Registrul Public al Unităților de Control Aprobate. Doar unitățile din acest registru pot fi utilizate legal în Suedia.

Certificarea Sistemului POS (Kassaregister)

- Această etapă vizează software-ul (care poate fi virtual) și interfața sa cu unitatea de control
- Furnizorul sau dezvoltatorul sistemului POS (virtual) trebuie să se asigure că software-ul funcționează corect și este compatibil cu cel puțin un model de Kontrollenhet aprobat.
- Furnizorul trimite o Declarație de Conformitate către Skatteverket, atestând că sistemul respectă toate cerințele legale (ex. includerea informațiilor corecte pe bon, protocolul de comunicare cu Kontrollenhet, etc.).
- Skatteverket menține un registru public al modelelor de Kassaregister (inclusiv soluțiile virtuale) care au depus declarația de conformitate.

Modalitățile de emitere, transmitere și arhivare a bonurilor fiscale electronice în Suedia sunt reglementate de cerințele impuse de Skatteverket (Agenția Fiscală Suedeză), centrate pe utilizarea Unității de Control a Registrului (Kontrollenhet).

Deși sistemul suedez se bazează puternic pe componente fizice de securitate, bonul fiscal electronic este recunoscut ca document fiscal oficial dacă a fost generat și securizat conform acestor reguli.

În Suedia, bonul fiscal (numit kvitto) trebuie să fie generat de un sistem de casă de marcat (Kassaregister) care este conectat la o Kontrollenhet omologată.

Sistemul POS (care poate fi o soluție virtuală) trimite datele tranzacției către Kontrollenhet. Kontrollenhet criptează datele și le generează un cod de securitate (similar cu un hash sau semnătură). Acest cod este apoi reintrodus în datele bonului.

Bonul, fie pe hârtie, fie electronic, trebuie să includă:

- Seria fiscală a sistemului de casă de marcat.
- Seria de identificare a Unității de Control (Kontrollenhet).
- Codul de Securitate: Codul unic generat de Kontrollenhet pentru a garanta că tranzacția este reală și inalterabilă.

Bonul care conține codul de securitate generat de Kontrollenhet este recunoscut ca document fiscal oficial și ca dovadă a tranzacției.

Nu există o obligație națională de transmitere zilnică sau în timp real a datelor bonurilor către Agenția Fiscală. Controlul fiscal se bazează pe capacitatea Skatteverket de a extrage datele arhivate din Kontrollenhet (sau din jurnalul electronic).

Bonurile pot fi puse la dispoziția clientului în format electronic (de exemplu, prin e-mail, aplicație, sau Cod QR), cu condiția ca acest format să fie o copie fidelă și lizibilă care să includă obligatoriu codul de securitate generat de Kontrollenhet.

Arhivarea se realizează prin două componente:

- Unitatea de Control (Kontrollenhet). Acest dispozitiv fizic acționează ca un jurnal electronic securizat. Kontrollenhet memorează datele agregate ale tuturor tranzacțiilor (nu neapărat detaliile complete ale fiecărui articol) într-un mod criptat și inalterabil. Această unitate servește ca probă principală în caz de audit.
- Jurnalul Electronic al Kassaregister-ului. Software-ul (soluția virtuală) trebuie să păstreze, de asemenea, o copie a tuturor tranzacțiilor (jurnalul).

Contribuabilii sunt obligați să păstreze datele fiscale (inclusiv cele din Kontrollenhet și Kassaregister) pe o perioadă de 7 ani.

Faptul că bonul a fost procesat și marcat cu codul de securitate generat de o Unitate de Control (Kontrollenhet) omologată de stat îi conferă statutul de document inalterabil și autentic. Codul de securitate leagă tranzacția de un sistem specific aprobat și de o oră precisă.

Mecanismele de control, securitate și trasabilitate utilizate în Suedia pentru protejarea datelor fiscale și prevenirea evaziunii sunt centrate pe utilizarea obligatorie a Unității de Control a Registrului (Kontrollenhet), care acționează ca un sigiliu hardware și un jurnal electronic securizat pentru orice sistem de vânzare (Kassaregister). Aceste mecanisme sunt reglementate strict de Skatteverket (Agenția Fiscală Suedeză).

Mecanisme de Securitate Hardware (Kontrollenhet)

Acestea asigură integritatea datelor la sursă, prevenind manipularea sistemului POS.

Doar modelele de Kontrollenhet (Unitate de Control) aprobate de Skatteverket pot fi utilizate. Această omologare garantează că dispozitivul îndeplinește standardele stricte de securitate fizică și criptografică.

Kontrollenhet este un dispozitiv fizic sigilat. Orice tentativă de deschidere sau manipulare fizică a unității o face nefuncțională sau lasă urme detectabile.

Pentru fiecare tranzacție, Kontrollenhet generează un cod de securitate criptografic unic. Acest cod este tipărit/inclus pe bonul fiscal (kvitto), acționând ca o "plumbuire digitală" care dovedește că tranzacția a fost înregistrată și securizată oficial.

Orice sistem de casă de marcat (Kassaregister), inclusiv soluțiile virtuale, trebuie să fie conectat permanent la Kontrollenhet pentru a putea emite bonuri legale. Trasabilitatea se bazează pe înregistrările securizate ale Unității de Control. Kontrollenhet servește ca jurnal electronic securizat, stocând datele agregate ale tuturor tranzacțiilor (vânzări, retururi, anulări) într-un mod criptat și inalterabil. Această memorie nu poate fi ștearsă sau rescrisă de către comerciant. Bonul fiscal include seria fiscală a Kontrollenhet și codul său de securitate. Acest lucru asigură trasabilitatea fiecărei tranzacții până la unitatea de control specifică și implicit, până la comerciantul care a emis-o. Sistemul POS (Kassaregister) trebuie, de asemenea, să păstreze propriul său jurnal electronic detaliat.

Controlul Skatteverket este bazat pe audituri inopinate și verificarea directă a datelor securizate: inspectorii fiscali suedezi pot efectua controale inopinate, inclusiv controale de tip "client misterios" (mystery shopping), verificând dacă bonurile emise conțin codul de securitate valid al Kontrollenhet. În timpul unui control, inspectorii pot extrage datele direct din Kontrollenhet (cu ajutorul unui cititor special). Compararea datelor din Kontrollenhet cu datele declarate de comerciant este mecanismul principal de detectare a evaziunii.

Obligativitatea conectării la hardware-ul omologat (Kontrollenhet) descurajează utilizarea de software-uri de tip "Zapper" (programe de fraudă care șterg tranzacțiile), deoarece Kontrollenhet înregistrează tranzacția înainte ca software-ul POS să o poată șterge.

UNGARIA

Statutul juridic al caselor de marcat electronice (inclusiv „virtuale”) în Ungaria este în curs de consolidare și digitalizare, fiind unul dintre cele mai avansate sisteme în Europa pentru fiscalizare.

În Ungaria funcționează de mult timp un sistem de „online cash registers” („online pénztárgépek”) conectate la Nemzeti Adó- és Vámhivatal (NAV) pentru anumite categorii de comercianți.

În 2025 a fost adoptat decretul [8/2025. \(III. 31.\) Decret NGM privind distribuirea și funcționarea caselor de marcat electronice, precum și cerințele pentru emiterea caselor de marcat electronice și a chitanțelor electronice](https://kpmg.com/hu/en/home/insights/2025/05/taxalert-2025-05-27.html?). Începând cu 1 iulie 2025, comercianții pot voluntar opta pentru „hardware-based e-cash registers”. Până la 1 iulie 2028, tranziția către noile e-cash registers devine obligatorie pentru comercianții care erau obligați să utilizeze case de marcat.

Decretul prevede obligativitatea de a emite e-bonuri (e-receipts) și de a stoca datele într-un registru de bonuri („receipt store”) gestionat de NAV pentru până la 10 ani.¹³

Soluția software sau cloud devine posibilă dacă respectă cerințele tehnice și de conexiune impuse de NAV (hardware-based e-cash register cu modul de control fiscal, sau alternativă pentru activități încă neobligate).

¹³ <https://kpmg.com/hu/en/home/insights/2025/05/taxalert-2025-05-27.html?>

Dispozitivul/soluția trebuie să fie certificată/autorizată de NAV; producătorii depun cerere de autorizare („type testing”) conform standardelor tehnice certificate.

Obligații principale pentru comercianți

- Emiterea de bon fiscal (sau e-bon) pentru fiecare tranzacție la care se aplică obligația
- Utilizarea unui registrator fiscal autorizat (online cash register) sau tranziția către nou-sistemul e-cash register
- Stocarea electronică a datelor de încasare, raportarea către NAV conform cerințelor (în multe cazuri în timp real sau aproape real-time)
- Respectarea arhivării datelor pe durata prevăzută (ex: 10 ani pentru bonuri stocate în „receipt store”).

Pașii principali pentru omologare/certificare

- **Selectarea tipului de dispozitiv sau soluție software.** NAV permite două categorii: „hardware-based e-cash register” și, în anumite condiții, soluții cloud/virtuale.
- Testare de tip („type testing”) și autorizare la NAV - Producătorul/distribuitorul trebuie să depună la NAV cererea de autorizare a dispozitivului/soluției: evaluare
- Înregistrarea operatorului/dispozitivului la NAV - Comercianții care utilizează dispozitivul aprobat trebuie să îl declare conform regulilor NAV (ex: utilizatori, serial, loc funcționare). Soluțiile cloud/virtuale vor trebui integrate în portalul NAV și în „receipt store”.

Implementarea operațională și întreținerea

Dispozitivul/soluția trebuie să emite bonuri conforme, să transmită date (unde prevăzut), să stocheze datele pe durata legală. Actualizările sau modificările majore de software pot necesita re-autorizare. Distribuitorii/producătorii trebuie să asigure service autorizat.

Bonul fiscal electronic este pe deplin recunoscut ca document fiscal oficial, deoarece integritatea sa este garantată de transmiterea imediată a datelor către NAV.

Bonul este generat de casa de marcat certificată, care are un modul fiscal sigilat și o memorie fiscală inalterabilă.

Fiecare bon emis este asociat cu un identificator unic al casei de marcat și al tranzacției.

Ungaria a introdus și conceptul de bon electronic (e-Nyugta sau DigiNyugta), care permite ca bonul să fie transmis direct către client în format digital (ex., prin e-mail, aplicație) în loc să fie tipărit. Validitatea acestui bon digital este garantată de faptul că datele au fost transmise și înregistrate de NAV.

Bonul (tipărit sau electronic) emis de o Casă de Marcat Online, ale cărui date au fost transmise cu succes către NAV, este recunoscut ca document fiscal oficial valabil.

Casele de Marcat Online sunt obligate să transmită toate datele tranzacțiilor (vânzări, anulări, retururi) către serverele centrale ale NAV. Transmiterea se încearcă în timp real (imediat după încheierea tranzacției). Dacă conexiunea la internet eșuează, datele sunt stocate temporar în memoria internă a casei de marcat și sunt transmise

automat imediat ce conexiunea este restabilă. Transmiterea se face utilizând un protocol de comunicare criptat și securizat (de obicei bazat pe comunicații mobile sau Ethernet), garantând că datele nu pot fi interceptate sau modificate pe drum.

Arhivarea este realizată pe trei niveluri pentru a garanta redundanța și integritatea. Casa de marcat are o memorie fiscală sigilată care stochează datele agregate ale vânzărilor. Sistemul software stochează, de asemenea, o copie detaliată (jurnal electronic) a tranzacțiilor. Toate datele tranzacțiilor transmise de casele de marcat sunt stocate și arhivate pe serverele fiscale. Contribuabilii pot accesa și verifica propriile date arhivate prin intermediul portalului NAV.

Documentele fiscale și registrele aferente trebuie păstrate de către contribuabil pentru o perioadă de 8 ani.

Recunoașterea bonului ca document oficial este indisolubil legată de controlul NAV. NAV monitorizează non-stop datele primite de la toate casele de marcat, analizând volumele de vânzări, tiparele de închidere și eventualele lacune de date. Ungaria are și un sistem obligatoriu de raportare online a facturilor (Online Számla). NAV poate compara automat vânzările înregistrate prin casele de marcat cu cele înregistrate prin facturarea online. NAV folosește analiza de risc pentru a identifica discrepanțele între locații similare sau abateri de la tiparul obișnuit al comerciantului, declanșând inspecții țintite.

Mecanismele de control, securitate și trasabilitate

Mecanismele de control, securitate și trasabilitate utilizate în Ungaria pentru protejarea datelor fiscale și prevenirea evaziunii sunt extrem de riguroase și sunt în mare parte centralizate, bazându-se pe sistemul de Case de Marcat Online (Online Pénztárgép) și pe sistemul de Raportare Online a Facturilor (Online Számla), ambele gestionate de Nemzeti Adó- és Vámhivatal (NAV).

Toate casele de marcat online sunt obligate să transmită datele complete ale fiecărei tranzacții (vânzări, retururi, anulări) către serverele NAV. Transmiterea se realizează imediat sau în cel mai scurt timp posibil, asigurând o monitorizare complexă și dinamică a fluxului de venituri.

Transmiterea datelor se face printr-un canal de comunicație criptat și securizat, administrat de NAV (adesea bazat pe SIM-uri fiscale sau conexiuni securizate), prevenind interceptarea sau modificarea datelor pe parcurs.

NAV folosește platforme de analiză (Big Data) pentru a procesa volumele uriașe de date primite zilnic de la toate casele de marcat. Aceasta permite identificarea în timp real a anomaliilor (ex. vânzări mult sub medie, închideri repetate, discrepanțe mari).

Ungaria impune, de asemenea, raportarea online, în timp real sau cvasi-real, a detaliilor tuturor facturilor emise, inclusiv a celor B2B.

Securitatea datelor este garantată la nivelul echipamentului de vânzare:

- Doar modelele de case de marcat online (hardware sau anumite soluții integrate) aprobate și omologate de NAV pot fi utilizate. Aceste aparate vin cu un modul fiscal sigilat și o memorie fiscală inalterabilă.

- Datele tranzacțiilor sunt stocate în memoria fiscală a aparatului. Această memorie servește ca sursă de date securizată, independentă de softul de operare, și poate fi verificată direct de inspectori.
- Aparatele sunt fizic sigilate de tehnicienii acreditați. Ruperea sigiliului indică o tentativă de fraudă sau necesitatea unei intervenții autorizate.

Mecanisme de Trasabilitate

Fiecare bon fiscal este identificat unic și este legat de un aparat fiscal specific și o oră exactă. Datorită transmiterii online, NAV are o evidență completă, inalterabilă și centralizată a fiecărui bon emis. NAV poate compara datele primite de la casele de marcat cu informațiile agregate din sistemul de raportare a facturilor (Online Számla). Se pot compara datele de TVA colectat cu datele din conturile bancare și din declarațiile fiscale. Inspectorii fiscali ungari folosesc datele din sistemele online pentru a efectua controale ținute pe baza indicatorilor de risc, concentrându-și resursele acolo unde probabilitatea de evaziune este cea mai mare.

WEBOGRAFIE

[The 2000s: Cloud-Based POS and the Rise of Mobile Retail](#)

[The Evolution Of POS Machines: From Cash Registers To Modern Payment Solutions](#)

[The History and Functionality of POS Systems](#)

[What is a Virtual POS: Definition, Benefits, and Features](#)

[6 steps to transition to digital tax accounting for cash registers](#)

[What Is Online Cash Register? How do Virtual Cash Registers Work? \(Pros & Cons\)](#)