Dosar GDPR

Exemplu Magazin Online SRL

CUI 00000000, Nr. Reg. Com. J00/0000/2026

Sediul: Str. Exemplului nr. 1, București

Domeniul: Magazin online, magazin.example

Data emiterii: 16.11.2026

Versiunea șabloanelor: 2026.1

Documentele din acest dosar aplică Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 (Regulamentul general privind protecția datelor), numit în continuare GDPR, și Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679. Ele sunt completate cu răspunsurile dvs. din chestionar.

EXEMPLU

Cuprins

Cod	Document	Ce faceți cu el
DP-00	Copertă, cuprins și mod de folosire	Păstrați și completați la nevoie
DP-01	Ghid de implementare	Păstrați și completați la nevoie
DP-02	Decizia administratorului	Semnați și păstrați
DP-03	Politica internă de protecție a datelor	Semnați și păstrați
DP-04	Registrul activităților de prelucrare	Păstrați și completați la nevoie
DP-05	Informarea angajaților	Semnați și păstrați
DP-07	Procedura pentru cererile persoanelor vizate	Păstrați și completați la nevoie
DP-08	Procedura pentru încălcarea securității datelor	Păstrați și completați la nevoie
DP-09	Politica de păstrare și distrugere	Semnați și păstrați
DP-10	Angajamentul de confidențialitate	Semnați și păstrați
DP-11	Reguli de securitate	Semnați și păstrați
DP-12	Proces-verbal de instruire	Semnați și păstrați
DP-13	Model de contract art. 28 cu furnizorii	Semnați și păstrați
DP-14	Lista destinatarilor și matricea de roluri	Păstrați și completați la nevoie
DP-15	Fișa de verificare DPIA	Păstrați și completați la nevoie
DP-16	Teste de interes legitim	Păstrați și completați la nevoie
DP-M1	Politica de confidențialitate a site-ului	Publicați pe site
DP-M2	Politica de cookie-uri	Publicați pe site
DP-M3	Texte pentru site și formulare	Publicați pe site
DP-M4	Marketing direct	Păstrați și completați la nevoie
DP-M6	Pixeli publicitari	Păstrați și completați la nevoie
DP-M7	Recenzii	Păstrați și completați la nevoie

EXEMPLU

Cum folosiți dosarul

1. Verificați denumirea, CUI-ul și adresa firmei de pe copertă și din antetul paginilor. Dacă un răspuns din chestionar nu mai corespunde, corectați-l și generați din nou dosarul.
2. Urmați ghidul de implementare (DP-01) în ordinea zilelor și bifați fiecare pas după ce l-ați făcut.
3. Semnați întâi decizia administratorului (DP-02), pentru că ea adoptă celelalte documente. Apoi semnați documentele marcate în cuprins cu „Semnați și păstrați”.
4. Publicați pe site documentele marcate cu „Publicați pe site”.
5. Completați de mână spațiile marcate cu linie: numere, date, nume și semnături. Arhiva conține fiecare document și în format DOCX, pe care îl puteți modifica în orice editor de text.
6. Păstrați documentele semnate la sediul firmei, pe hârtie sau scanate. Registrul activităților și celelalte documente se pun la dispoziția Autorității Naționale de Supraveghere a Prelucrării

Datelor cu Caracter Personal (ANSPDCP) la cererea ei, potrivit art. 30 alin. (4) și art. 31 GDPR.
7. Revizuiți dosarul o dată pe an și la fiecare schimbare din firmă, după regulile de mai jos.

> **Avertisment**
>
> - Documentele din dosar sunt un model de documentație, completat automat cu răspunsurile dvs. Ele descriu firma corect doar dacă răspunsurile sunt corecte și complete.
> - Dosarul nu reprezintă consultanță juridică. Nu am analizat situația firmei dincolo de răspunsurile din chestionar.
> - Dosarul nu reprezintă o certificare. Generarea lui nu dovedește că firma respectă GDPR: respectarea se vede în felul în care aplicați documentele în activitatea de zi cu zi.

Revizuirea dosarului

Legea nu stabilește un termen de valabilitate pentru documentele de protecție a datelor. Ele trebuie însă să corespundă în orice moment cu ce se întâmplă în firmă. Art. 24 alin. (1) GDPR cere ca măsurile tehnice și organizatorice să fie revizuite și actualizate dacă este necesar, art. 30 cere un registru al activităților ținut la zi, iar art. 32 alin. (1) lit. d) cere testarea și evaluarea periodică a măsurilor de securitate.

Vă recomandăm o revizuire o dată pe an și o revizuire la orice schimbare: furnizor nou, activitate nouă, camere de supraveghere, angajați noi sau primul angajat. Ghidul de implementare (DP-01) arată ce faceți la revizuire.

Cât timp contul dvs. CookiePanel are o perioadă activă, puteți modifica răspunsurile din chestionar și puteți genera din nou dosarul. Documentele generate rămân ale dvs. și după încheierea perioadei, iar fișierele DOCX se pot actualiza manual.

EXEMPLU

Ce rămâne la consultanță

Dosarul nu tratează situațiile de mai jos. Pentru ele vă recomandăm o consultanță de specialitate, pe care o puteți cere din pagina de contact a site-ului consultanta-gdpr.ro.

Situații pe care dosarul nu le acoperă pentru niciun magazin

- Redactarea termenilor și condițiilor, a formularului de retragere și a politicii de retur și garanție. Ele țin de dreptul consumatorului. Dosarul conține doar clauza de date personale pentru termenii și condițiile magazinului (DP-M3).
- Evaluarea completă a impactului asupra protecției datelor (art. 35 GDPR), atunci când fișa de verificare (DP-15) arată că este necesară.
- Testul de interes legitim pentru profilarea clienților pe scară largă.
- Obligațiile de securitate cibernetică pe care legea le impune, separat de GDPR, firmelor medii și mari din anumite sectoare de activitate.
- Firmele cu 50 de angajați sau mai mulți. Dosarul este gândit pentru firme mai mici.

Anexă. Surse legale

Actele și ghidurile citate în documentele acestui dosar, cu adresa la care pot fi consultate.

Nr.	Sursa și adresa la care poate fi consultată
1	Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 (Regulamentul general privind protecția datelor) https://eur-lex.europa.eu/eli/reg/2016/679/oj
2	Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 https://legislatie.just.ro/Public/DetaliiDocument/203151
3	art. 12 alin. (2) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice https://legislatie.just.ro/Public/DetaliiDocument/56973
4	art. 4 alin. (5) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice https://legislatie.just.ro/Public/DetaliiDocument/56973
5	art. 10^{1} alin. (3) din Ordonanța de urgență a Guvernului nr. 120/2021 privind administrarea, funcționarea și implementarea sistemului național privind factura electronică RO e-Factura și factura electronică în România https://legislatie.just.ro/Public/DetaliiDocument/247243
6	art. 4 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 https://legislatie.just.ro/Public/DetaliiDocument/203151
7	art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare https://legislatie.just.ro/Public/DetaliiDocument/1576
8	art. 35 alin. (3) din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare https://legislatie.just.ro/Public/DetaliiDocument/1576
9	art. 2517 din Codul civil https://legislatie.just.ro/Public/DetaliiDocument/109884
10	art. 9 alin. (1) din Ordonanța de urgență a Guvernului nr. 140/2021 privind anumite aspecte referitoare la contractele de vânzare de bunuri https://legislatie.just.ro/Public/DetaliiDocument/250044
11	Hotărârea Curții de Justiție a Uniunii Europene din 29 iulie 2019, cauza C-40/17, Fashion ID https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:62017CJ0040
12	art. 12 alin. (1) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice https://legislatie.just.ro/Public/DetaliiDocument/56973
13	Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal https://legislatie.just.ro/Public/DetaliiDocument/206331
14	Ghidul Grupului de lucru Articolul 29 privind evaluarea impactului asupra protecției datelor (WP248 rev.01), preluat de Comitetul European pentru Protecția Datelor https://www.edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines_en

EXEMPLU

Nr.	Sursa și adresa la care poate fi consultată
15	art. 7 alin. (6) și anexa nr. 1 pct. 26 și 27 din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor, modificată prin Ordonanța de urgență a Guvernului nr. 58/2022 https://legislatie.just.ro/Public/DetaliiDocument/88290
16	art. 2 din Ordinul președintelui Autorității Naționale pentru Protecția Consumatorilor nr. 449/2022 privind unele măsuri de informare a consumatorilor cu privire la soluționarea alternativă a litigiilor, modificat prin Ordinul nr. 270/2026 https://legislatie.just.ro/Public/DetaliiDocument/257649
17	Regulamentul (UE) 2024/3228 al Parlamentului European și al Consiliului din 19 decembrie 2024 de abrogare a Regulamentului (UE) nr. 524/2013 https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R3228
18	Ghidul EDPB 2/2023 privind domeniul tehnic de aplicare a art. 5 alin. (3) din Directiva 2002/58/CE, versiunea 2.0, adoptată la 7 octombrie 2024 https://www.edpb.europa.eu/system/files/documents/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf

EXEMPLU

Ghid de implementare

Ghidul arată, pe zile, ce faceți cu documentele din dosar după ce l-ați primit. Zilele sunt orientative și le puteți comprima sau întinde după timpul disponibil. Pașii care nu se aplică firmei Exemplu Magazin Online SRL au fost scoși din tabel. Bifați fiecare pas după ce l-ați făcut și păstrați ghidul completat împreună cu dosarul.

Pașii de implementare

Ziua	Ce faceți	Document	☐
1	Citiți coperta, cuprinsul și avertismentul. Verificați denumirea, CUI-ul și adresa firmei din antetul paginilor.	DP-00	☐
1	Completați numărul și data deciziei, apoi semnați-o. Decizia adoptă documentația și stabilește că Ion Popescu îndeplinește și funcția de responsabil intern.	DP-02	☐
1	Semnați politica internă de protecție a datelor.	DP-03	☐
2	Publicați politica de confidențialitate pe o pagină separată a site-ului. Puneți linkul în subsolul fiecărei pagini și lângă formularele care colectează date.	DP-M1	☐
2	Publicați politica de cookie-uri pe o pagină separată, cu link în subsolul fiecărei pagini.	DP-M2	☐
2	Instalați bannerul de cookie-uri din contul CookiePanel, după pașii din pagina de instalare: urcați fișierul pe server, includeți scriptul primul în antetul paginilor, blocați scripturile opționale până la acord și adăugați linkul prin care vizitatorul își schimbă opțiunea.	DP-M2	☐
2	Deschideți site-ul într-o fereastră privată a browserului și verificați că instrumentele de măsurare și de publicitate nu pornesc înainte ca vizitatorul să accepte.	DP-M2	☐
3	Puneți textele de informare în formularele site-ului: comanda, crearea contului, abonarea la newsletter și formularul de contact.	DP-M3	☐
3	Adăugați clauza de date personale în termenii și condițiile magazinului.	DP-M3	☐
3	Parcurgeți lista de verificare: linkurile obligatorii de pe site și câmpurile de la checkout. Scoateți câmpurile de care comanda nu are nevoie.	DP-M3	☐
4	Dați fiecărui angajat informarea privind datele lui și cereți semnătura pe fișa de luare la cunoștință.	DP-05	☐
4	Cereți semnarea angajamentului de confidențialitate de către fiecare persoană care are acces la datele clienților și nu lucrează pentru un furnizor cu contract de prelucrare.	DP-10	☐
5	Aplicați regulile de securitate: autentificarea în doi pași pentru conturile de administrare, actualizările platformei și ale modulelor, copiile de siguranță.	DP-11	☐
5	Organizați instruirea angajaților și a colaboratorilor care lucrează cu date. Dați testul, corectați-l după barem și semnați procesul-verbal.	DP-12	☐

EXEMPLU

Ziua	Ce faceți	Document	☐
6–10	Încheiați contractul de prelucrare (art. 28 GDPR) cu furnizorii împuterniciți din listă: Agenția Exemplu Web SRL, Contabilitate Exemplu SRL, Google Cloud EMEA Limited, Google Ireland Limited, Hostico, Intelligent IT S.R.L., The Rocket Science Group LLC. Dacă un furnizor are propriul acord de prelucrare, acceptat online, păstrați o copie a lui în locul contractului.	DP-13, DP-14	☐
6–10	Pentru furnizorii al căror rol depinde de termenii lor (de exemplu curierii și procesatorii de plăți): Delivery Solutions S.A., FAN Courier Express S.R.L., NETOPIA Financial Services S.A.. Citiți termenii fiecăruia și verificați dacă au un acord de prelucrare pe care trebuie să îl acceptați.	DP-14	☐
6–10	Pentru ceilalți destinatari din listă, verificați rolul trecut în dreptul lor.	DP-14	☐
10	Citiți registrul activităților de prelucrare și verificați că descrie ce face firma. Dacă lipsește ceva, corectați răspunsurile din chestionar și generați din nou dosarul.	DP-04	☐
10	Puneți procedura pentru cereri și procedura pentru incidente la îndemâna persoanei care citește e-mailul de contact (gdpr@magazin.example).	DP-07, DP-08	☐
10	Citiți fișa de verificare DPIA. Dacă fișa recomandă consultanță, cereți-o înainte de a începe prelucrarea respectivă.	DP-15	☐
10	Citiți testele de interes legitim și confirmați că descriu ce faceți.	DP-16	☐

După implementare

Legea nu stabilește un termen de valabilitate pentru documente, dar ele trebuie să descrie în orice moment ce face firma. Revizuiți dosarul o dată pe an, de exemplu la data la care ați semnat decizia (DP-02). Revizuiți-l și la orice schimbare: furnizor nou, activitate nouă, camere de supraveghere, angajați.

La revizuire, actualizați răspunsurile din chestionar și generați din nou dosarul. Semnați documentele care s-au schimbat și păstrați versiunea anterioară împreună cu cea nouă.

Data ultimei revizuiri: _____ Semnătura responsabilului intern: _____

EXEMPLU

Decizia administratorului privind protecția datelor cu caracter personal

Nr. _____ din data _____

Ion Popescu, administrator al societății Exemplu Magazin Online SRL, CUI 00000000, cu sediul în Str. Exemplului nr. 1, București, în calitate de reprezentant legal,

având în vedere:

- art. 24 din Regulamentul (UE) 2016/679 (GDPR), care obligă operatorul să aplice măsuri tehnice și organizatorice adecvate, inclusiv politici de protecție a datelor atunci când este proporțional, și să poată demonstra că prelucrarea respectă regulamentul;
- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679;
- activitatea de comerț online a societății, desfășurată prin magazinul magazin.example,

în temeiul actului constitutiv al societății,

decide:

Art. 1. Adoptarea documentației

(1) Se adoptă documentația de protecție a datelor cu caracter personal a societății, formată din documentele următoare, în versiunea 2026.1 din 16.11.2026:

EXEMPLU

Cod	Document
DP-00	Copertă, cuprins și mod de folosire
DP-01	Ghid de implementare
DP-02	Decizia administratorului
DP-03	Politica internă de protecție a datelor
DP-04	Registrul activităților de prelucrare
DP-05	Informarea angajaților
DP-07	Procedura pentru cererile persoanelor vizate
DP-08	Procedura pentru încălcarea securității datelor
DP-09	Politica de păstrare și distrugere
DP-10	Angajamentul de confidențialitate
DP-11	Reguli de securitate
DP-12	Proces-verbal de instruire
DP-13	Model de contract art. 28 cu furnizorii
DP-14	Lista destinatarilor și matricea de roluri
DP-15	Fișa de verificare DPIA
DP-16	Teste de interes legitim
DP-M1	Politica de confidențialitate a site-ului

Cod	Document
DP-M2	Politica de cookie-uri
DP-M3	Texte pentru site și formulare
DP-M4	Marketing direct
DP-M6	Pixeli publicitari
DP-M7	Recenzii

(2) Documentele se aplică de la data semnării prezentei decizii. Toate persoanele care prelucrează date în numele societății le respectă în activitatea lor.

Art. 2. Responsabilul intern cu protecția datelor

(1) Funcția de responsabil intern cu protecția datelor este îndeplinită de reprezentantul legal, Ion Popescu, administrator, care poate fi contactat la gdpr@magazin.example.

(2) Responsabilul intern are următoarele atribuții:

- ține la zi documentația adoptată la art. 1 și propune actualizarea ei;
- primește cererile persoanelor vizate și urmărește ca ele să primească răspuns în termenul din art. 12 alin. (3) GDPR, după procedura DP-07;
- primește semnalările despre incidentele de securitate și aplică procedura DP-08, inclusiv notificarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) în termenul și în condițiile din art. 33 GDPR;
- organizează instruirea persoanelor care lucrează cu date (DP-12) și păstrează angajamentele de confidențialitate (DP-10);
- verifică, înainte de folosirea unui furnizor nou, rolul furnizorului și, dacă este persoană împuternicită, existența contractului de prelucrare (DP-13), apoi îl trece în lista destinatarilor (DP-14);
- ține legătura cu ANSPDCP în numele societății, la cererea reprezentantului legal.

EXEMPLU

(3) Responsabilul intern nu este responsabil cu protecția datelor (DPO) în sensul art. 37 GDPR. Desemnarea lui este o măsură internă de organizare. Răspunderea pentru respectarea GDPR rămâne a societății, ca operator.

(4) Dacă activitatea societății ajunge să îndeplinească una din condițiile art. 37 alin. (1) GDPR, societatea desemnează un responsabil cu protecția datelor și modifică prezenta decizie.

Art. 3. Revizuirea documentației

(1) Documentația se revizuiește cel puțin o dată pe an și la orice schimbare: furnizor nou, activitate nouă, camere de supraveghere, angajați.

(2) Responsabilul intern propune modificările. Reprezentantul legal le aprobă prin semnarea documentelor actualizate.

Art. 4. Comunicarea deciziei

(1) Decizia se comunică responsabilului intern, angajaților și colaboratorilor care au acces la datele prelucrate de societate.

(2) Decizia intră în vigoare la data semnării.

Aprobat,
Administrator
Nume: _____
Semnătura: _____
Ștampila (opțional)

EXEMPLU

Politica internă de protecție a datelor

1. Scop și domeniu de aplicare

Politica stabilește regulile după care Exemplu Magazin Online SRL (denumită în continuare „societatea”) prelucrează datele cu caracter personal în activitatea magazinului online magazin.example. Ea pune în aplicare art. 24 alin. (2) din Regulamentul (UE) 2016/679 (GDPR), care cere operatorului politici adecvate de protecție a datelor atunci când este proporțional.

Politica privește datele clienților și ale vizitatorilor site-ului, ale persoanelor de contact de la furnizori, ale angajaților și ale oricărei alte persoane care se adresează societății.

Politica se aplică reprezentantului legal, responsabilului intern, angajaților și colaboratorilor care lucrează cu date în numele societății. Ea acoperă datele în orice formă: în platforma magazinului, în e-mail, în programul de facturare, în fișiere pe calculator sau în cloud și pe hârtie. Termenii folosiți au sensul din art. 4 GDPR.

2. Principii de prelucrare

Societatea aplică principiile din art. 5 GDPR în fiecare activitate:

- „Legalitate, echitate și transparență” (art. 5 alin. (1) lit. a)): fiecare prelucrare are un temei din art. 6 GDPR, iar persoanele află din politica de confidențialitate a site-ului (DP-M1) ce date folosim, de ce și cât timp.
- „Limitări legate de scop” (lit. b)): datele colectate pentru o comandă se folosesc pentru comandă. Folosirea lor într-un scop nou, de exemplu pentru marketing, cere o verificare a temeiului înainte.
- „Reducerea la minimum a datelor” (lit. c)): cerem doar datele de care avem nevoie pentru scopul declarat. Secțiunea 5 aplică regula la formularul de comandă.
- „Exactitate” (lit. d)): corectăm fără întârziere datele greșite, inclusiv la cererea persoanei.
- „Limitări legate de stocare” (lit. e)): păstrăm datele doar cât prevede politica de păstrare (DP-09) și le ștergem sau le distrugem la sfârșitul termenului.
- „Integritate și confidențialitate” (lit. f)): protejăm datele împotriva accesului neautorizat, a pierderii și a distrugerii, prin regulile de securitate (DP-11).
- „Responsabilitate” (art. 5 alin. (2)): societatea poate demonstra că respectă principiile de mai sus. Dovezile sunt documentele din dosar, semnate și ținute la zi.

EXEMPLU

3. Roluri și responsabilități

Societatea este operator, în sensul art. 4 pct. 7 GDPR, pentru datele pe care le prelucrează în scopurile proprii: vânzare, livrare, facturare, relația cu clienții, relația de muncă.

Reprezentantul legal, Ion Popescu, aprobă documentația, asigură resursele necesare și răspunde de aplicarea politicii.

Reprezentantul legal îndeplinește și funcția de responsabil intern cu protecția datelor, cu atribuțiile din decizia DP-02.

Responsabilul intern nu este responsabil cu protecția datelor (DPO) în sensul art. 37 GDPR. Persoanele vizate și Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) se pot adresa societății la gdpr@magazin.example.

Angajații și colaboratorii au acces doar la datele de care au nevoie pentru sarcinile lor. Ei respectă angajamentul de confidențialitate (DP-10) și regulile de securitate (DP-11). Orice cerere primită de la o persoană vizată și orice incident de securitate se anunță imediat responsabilului intern.

Furnizorii care prelucrează date în numele societății sunt persoane împuternicite (art. 28 GDPR). Ei folosesc datele doar după instrucțiunile societății, pe baza unui contract de prelucrare (DP-13). Pentru pixelii publicitari, societatea și furnizorul pixelului pot fi operatori asociați (art. 26 GDPR), după cum descrie DP-M6.

4. Temeiuri de prelucrare

Societatea prelucrează date numai când există unul din temeiurile din art. 6 alin. (1) GDPR. În activitatea magazinului se folosesc următoarele temeiuri:

- Executarea contractului (lit. b)): preluarea, livrarea și returnarea comenzilor, contul de client, relația cu furnizorii.
- Obligația legală (lit. c)): facturarea și contabilitatea, salarizarea, securitatea și sănătatea în muncă, răspunsul la cererile persoanelor vizate și ale autorităților.
- Interesul legitim (lit. f)): mesajele primite prin formularul de contact și prin e-mail; prevenirea fraudei la plată; jurnalele serverului și securitatea site-ului; ofertele prin e-mail către clienții existenți, pentru produse similare, în condițiile excepției din art. 12 alin. (2) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice; verificarea recenziilor. Fiecare activitate bazată pe interes legitim are un test de echilibru în DP-16, făcut înainte de începerea ei.
- Consimțământul (lit. a)): măsurarea audienței site-ului; publicitatea online și măsurarea conversiilor; abonarea la newsletter; publicarea recenziilor. Cookie-urile care nu sunt strict necesare se folosesc doar cu acord, potrivit art. 4 alin. (5) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice. Consimțământul se cere înainte, se poate dovedi și se retrage la fel de ușor cum s-a dat (art. 7 alin. (3) GDPR).

EXEMPLU

Temeiul fiecărei activități este trecut în registrul activităților de prelucrare (DP-04). O activitate nouă începe numai după ce i s-a stabilit temeiul și a fost trecută în registru.

Categoriile speciale de date (art. 9 GDPR), de exemplu datele de sănătate din certificatele de concediu medical, se prelucrează doar în condițiile art. 9 alin. (2) GDPR și doar de persoanele care au nevoie de ele pentru sarcina lor.

5. Minimizarea datelor la checkout

- Formularul de comandă cere doar datele necesare livrării, facturării și contactului legat de comandă: numele, adresa de livrare, telefonul și adresa de e-mail.
- Formularul nu cere titlul de politețe, data nașterii, sexul sau codul numeric personal (CNP).
- Societatea nu cere CNP-ul pentru factură. Dacă clientul persoană fizică nu îl comunică, factura se emite cu codul format din 13 cifre de zero, potrivit art. 10^{1} alin. (3) din Ordonanța de urgență a Guvernului nr. 120/2021 privind administrarea, funcționarea și implementarea sistemului național privind factura electronică RO e-Factura și factura electronică în România.
- CNP-ul se cere numai când o lege îl impune. Prelucrarea lui respectă și art. 4 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679.
- Câmpurile care nu sunt necesare comenzii sunt marcate ca opționale. Căsuțele de acord pentru marketing nu sunt bifate dinainte.

- Contul de client se creează doar cu datele necesare autentificării și comenzilor. Clientul își poate șterge contul, după procedura DP-07.
- Lista de verificare din DP-M3 se parcurge la fiecare modificare a formularului de comandă.

6. Drepturile persoanelor vizate

Persoanele vizate au dreptul de acces, de rectificare, de ștergere, de restricționare a prelucrării, de portabilitate a datelor și de opoziție (art. 15–21 GDPR), precum și dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată (art. 22 GDPR). Când prelucrarea se bazează pe consimțământ, persoana îl poate retrage oricând.

Cererile se tratează după procedura pentru cererile persoanelor vizate (DP-07). Societatea răspunde fără întârziere și în cel mult o lună de la primirea cererii. Termenul se poate prelungi cu două luni pentru cereri complexe sau numeroase, cu informarea persoanei în prima lună (art. 12 alin. (3) GDPR). Răspunsul este gratuit, cu excepțiile din art. 12 alin. (5) GDPR.

Orice persoană din societate care primește o cerere, pe orice canal, o trimite în aceeași zi responsabilului intern. Identitatea solicitantului se verifică, de regulă, cu datele pe care societatea le are deja, de exemplu adresa de e-mail a contului sau numărul comenzii.

7. Securitatea datelor

Societatea aplică măsuri tehnice și organizatorice potrivite riscului, după art. 32 GDPR. Regulile concrete sunt în DP-11 și cuprind:

- acces la date pe bază de cont personal, numai pentru cine are nevoie de el;
- autentificarea în doi pași pentru conturile de administrare a magazinului și pentru e-mail;
- actualizarea la timp a platformei magazinului, a temelor și a modulelor;
- copii de siguranță regulate, verificate prin restaurare;
- retragerea accesului în ziua în care o persoană sau un furnizor nu mai lucrează cu societatea.

EXEMPLU

Măsurile se testează și se evaluează periodic, cel puțin la revizuirea anuală a dosarului (art. 32 alin. (1) lit. d) GDPR).

8. Incidente de securitate

Un incident de securitate este orice încălcare a securității care duce la distrugerea, pierderea, modificarea, divulgarea sau accesul neautorizat la date, în sensul art. 4 pct. 12 GDPR. Exemple pentru un magazin online: un modul compromis, un cont de administrare preluat de altcineva, un export de clienți trimis din greșeală.

Oricine observă un incident îl anunță imediat responsabilului intern. Responsabilul aplică procedura pentru încălcarea securității datelor (DP-08):

- notifică ANSPDCP fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore de la momentul în care societatea a aflat de incident, cu excepția cazului în care este puțin probabil ca incidentul să genereze un risc pentru drepturile și libertățile persoanelor (art. 33 GDPR);
- informează persoanele afectate fără întârziere nejustificată, când incidentul prezintă un risc ridicat pentru ele (art. 34 GDPR);
- trece fiecare incident în registrul incidentelor, inclusiv pe cele care nu se notifică (art. 33 alin. (5) GDPR).

9. Păstrarea și distrugerea datelor

Datele se păstrează pe durata prevăzută în politica de păstrare și distrugere (DP-09). Unele termene vin din lege. De exemplu, registrele și documentele justificative contabile se păstrează 5 ani, potrivit art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare. Celelalte termene sunt stabilite de societate și sunt marcate ca atare în DP-09.

La sfârșitul termenului, datele se șterg din sisteme sau se anonimizează, iar documentele pe hârtie se distrug astfel încât să nu poată fi refăcute. Distrugerea se consemnează în procesul-verbal din DP-09.

10. Furnizori și destinatari

Destinatarii datelor sunt trecuți în lista destinatarilor și matricea de roluri (DP-14), cu rolul fiecăruia: persoană împuternicită, operator independent sau operator asociat.

Înainte de a folosi un furnizor nou care primește date, responsabilul intern verifică rolul lui, existența unui contract de prelucrare (DP-13) sau a acordului de prelucrare publicat de furnizor și țara în care sunt prelucrate datele. Dacă datele ajung în afara Spațiului Economic European, transferul trebuie să aibă o garanție din capitolul V GDPR (art. 44–49). Furnizorul se adaugă apoi în DP-14 și, dacă este cazul, în registrul activităților (DP-04).

11. Instruirea

Fiecare persoană care lucrează cu date este instruită înainte să primească acces și apoi cel puțin o dată pe an. Instruirea cuprinde această politică, regulile de securitate și modul de recunoaștere a unei cereri sau a unui incident. Ea se consemnează în procesul-verbal de instruire (DP-12), împreună cu rezultatul testului.

EXEMPLU

12. Încălcarea regulilor

Încălcarea politicii de către un angajat se analizează disciplinar, potrivit contractului individual de muncă și regulamentului intern. Încălcarea de către un colaborator se tratează potrivit contractului încheiat cu el și poate duce la retragerea accesului la date.

Cine semnalează cu bună-credință o încălcare a regulilor sau un incident nu suferă nicio consecință negativă pentru semnalare.

13. Revizuirea politicii

Politica se revizuiește cel puțin o dată pe an și la orice schimbare: furnizor nou, activitate nouă, camere de supraveghere, angajați. Responsabilul intern propune modificările, iar reprezentantul legal le aprobă prin semnarea versiunii noi. Politica se aplică de la data deciziei de adoptare a documentației (DP-02).

Aprobat,
Administrator
Nume: _____
Semnătura: _____
Ștampila (opțional)

Registrul activităților de prelucrare

Registrul cuprinde activitățile prin care Exemplu Magazin Online SRL prelucrează date cu caracter personal, cu informațiile cerute de art. 30 alin. (1) GDPR. Se ține în format electronic sau pe hârtie (art. 30 alin. (3) GDPR) și se pune la dispoziția Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), la cerere (art. 30 alin. (4) GDPR).

Scutirea din art. 30 alin. (5) GDPR, pentru firmele cu mai puțin de 250 de angajați, nu se aplică atunci când prelucrarea nu este ocazională. Datele clienților unui magazin online se prelucrează în mod constant, de aceea societatea ține registrul.

Datele operatorului

Operatorul	Exemplu Magazin Online SRL, CUI 00000000, Nr. Reg. Com. J00/0000/2026, cu sediul în Str. Exemplului nr. 1, București
Date de contact	gdpr@magazin.example, telefon 0700000000
Reprezentantul legal	Ion Popescu, Administrator
Responsabilul intern cu protecția datelor	Ion Popescu, Administrator, gdpr@magazin.example
Responsabilul cu protecția datelor (DPO)	Nu a fost desemnat un responsabil cu protecția datelor în sensul art. 37 GDPR. Responsabilul intern de mai sus nu are această calitate.
Reprezentantul în Uniune (art. 27 GDPR)	Nu este cazul: operatorul este stabilit în România.
Operatorii asociați	Platformele de publicitate și datele lor de contact sunt în lista destinatarilor (DP-14). Au publicat acorduri de operator asociat: Meta Platforms Ireland Limited.
Data ultimei actualizări	16.11.2026, versiunea 2026.1

EXEMPLU

Cum se folosește registrul

Fiecare activitate are o fișă. Fișa arată scopul, persoanele vizate, categoriile de date, temeiul juridic, destinatarii, transferurile în afara Spațiului Economic European (SEE), termenul de păstrare și măsurile de securitate. Destinatarii sunt descriși pe larg în lista destinatarilor (DP-14), iar termenele de păstrare în politica de păstrare și distrugere (DP-09).

Responsabilul intern actualizează registrul când apare o activitate nouă, un furnizor nou sau un termen nou și îl verifică cel puțin o dată pe an. Modificările se trec în tabelul de la sfârșitul registrului.

Activitățile din registru:

1. Gestionarea personalului și salarizarea
2. Securitatea și sănătatea în muncă, prevenirea incendiilor
3. Contabilitatea
4. Relația cu furnizorii
5. Cererile persoanelor vizate
6. Mesajele primite prin formularul de contact și prin e-mail
7. Comenzile și livrarea

8. Facturarea
9. Contul de client
10. Retururile
11. Garanția și reclamațiile
12. Plățile online
13. Prevenirea fraudei la plată
14. Jurnalele serverului și securitatea site-ului
15. Măsurarea audienței site-ului
16. Publicitatea online și măsurarea conversiilor
17. Newsletterul și ofertele prin e-mail
18. Recenziile produselor

Fișa 1. Gestionarea personalului și salarizarea

Scopul prelucrării	Încheierea și executarea contractelor de muncă, calculul și plata salariilor, declarațiile către autorități.
Persoanele vizate	angajați; membrii de familie ai angajaților, pentru deduceri
Categoriile de date	nume și prenume, CNP și datele din actul de identitate, adresă, date de contact, funcție și salariu, cont bancar, concedii și absențe, certificatele de concediu medical, date despre persoanele în întreținere
Temeiul juridic	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale); art. 6 alin. (1) lit. b) GDPR (executarea contractului), pentru contractul de muncă; pentru datele privind sănătatea din certificatele de concediu medical, art. 9 alin. (2) lit. b) GDPR (obligațiile operatorului în domeniul ocupării forței de muncă și al securității sociale și protecției sociale)
Destinatarii	• Contabilitate Exemplu SRL, pentru ținerea contabilității • Banca prin care se plătesc salariile, pentru plata salariilor • Agenția Națională de Administrare Fiscală (ANAF), pentru îndeplinirea obligațiilor fiscale • Inspectoratul teritorial de muncă (registrul general de evidență a salariaților, Revisal), pentru evidența salariaților • Casa de asigurări de sănătate (certificatele de concediu medical), pentru decontarea indemnizațiilor de concediu medical • Instanțele și autoritățile publice, la cerere legală, pentru răspunsul la solicitările legale ale autorităților
Transferurile în afara SEE	• Contabilitate Exemplu SRL, țara și garanția se verifică în termenii furnizorului
Termenul de păstrare	5 ani pentru statele de salarii; restul dosarului de personal: termen stabilit de operator. Temeiul termenului: art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare.
Măsurile de securitate	• Dosarele de personal se păstrează în dulap încuiat sau în dosare electronice cu acces restrâns. • Accesul este limitat la persoanele care au nevoie de date pentru această activitate. • Se aplică și regulile de securitate ale societății (DP-11).

EXEMPLU

Fișa 2. Securitatea și sănătatea în muncă, prevenirea incendiilor

Scopul prelucrării	Instruirea angajaților, evidența controalelor medicale de medicina muncii și a incidentelor.
Persoanele vizate	angajați
Categoriile de date	nume și prenume, funcție, fișele de instruire, fișa de aptitudine de la medicina muncii, date despre accidentele de muncă
Temeiul juridic	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale); pentru datele privind sănătatea legate de accidentele de muncă, art. 9 alin. (2) lit. b) GDPR (obligațiile operatorului în domeniul ocupării forței de muncă și al securității sociale și protecției sociale); pentru fișa de aptitudine emisă de medicul de medicina muncii, art. 9 alin. (2) lit. h) GDPR (medicina muncii și evaluarea capacității de muncă)
Destinatarii	• Furnizorul de servicii de medicina muncii, pentru supravegherea sănătății lucrătorilor prin medicina muncii • Instanțele și autoritățile publice, la cerere legală, pentru răspunsul la solicitările legale ale autorităților
Transferurile în afara SEE	Destinatarii acestei activități sunt stabiliți în SEE. Garanțiile pentru transferurile pe care furnizorii le fac mai departe, în afara SEE, sunt în DP-14.
Termenul de păstrare	termen stabilit de operator, în limitele legislației privind securitatea și sănătatea în muncă.
Măsurile de securitate	• Fișele de aptitudine se păstrează separat de restul dosarului de personal. • Accesul este limitat la persoanele care au nevoie de date pentru această activitate. • Se aplică și regulile de securitate ale societății (DP-11).

EXEMPLU

Fișa 3. Contabilitatea

Scopul prelucrării	Înregistrarea operațiunilor în contabilitate și întocmirea situațiilor financiare.
Persoanele vizate	clienți; furnizori; angajați
Categoriile de date	nume sau denumire, adresă, datele din facturi și din documentele de plată
Temeiul juridic	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale)
Destinatarii	• Contabilitate Exemplu SRL, pentru ținerea contabilității • Agenția Națională de Administrare Fiscală (ANAF), pentru îndeplinirea obligațiilor fiscale
Transferurile în afara SEE	• Contabilitate Exemplu SRL, țara și garanția se verifică în termenii furnizorului
Termenul de păstrare	5 ani pentru registre și documentele justificative; 10 ani pentru situațiile financiare anuale. Temeiul termenului: art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare; art. 35 alin. (3) din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare.

Măsurile de securitate	• Documentele contabile se arhivează pe ani, cu acces doar pentru contabil și administrator. • Se aplică și regulile de securitate ale societății (DP-11).

Fișa 4. Relația cu furnizorii

Scopul prelucrării	Încheierea și executarea contractelor cu furnizorii și colaboratorii.
Persoanele vizate	persoanele de contact ale furnizorilor; colaboratori persoane fizice
Categoriile de date	nume și prenume; funcție; date de contact; cont bancar, pentru colaboratorii persoane fizice
Temeiul juridic	art. 6 alin. (1) lit. b) GDPR (executarea contractului)
Destinatarii	• Contabilitate Exemplu SRL, pentru ținerea contabilității • Google Cloud EMEA Limited, pentru e-mailul firmei și stocarea documentelor în cloud
Transferurile în afara SEE	• Contabilitate Exemplu SRL, țara și garanția se verifică în termenii furnizorului
Termenul de păstrare	durata contractului și 3 ani după încetarea lui. Temeiul termenului: art. 2517 din Codul civil.
Măsurile de securitate	• Accesul este limitat la persoanele care au nevoie de date pentru această activitate. • Se aplică și regulile de securitate ale societății (DP-11).

EXEMPLU

Fișa 5. Cererile persoanelor vizate

Scopul prelucrării	Primirea cererilor privind drepturile din GDPR, răspunsul la ele și dovada răspunsului.
Persoanele vizate	clienți; vizitatori ai site-ului; alte persoane care trimit cereri
Categoriile de date	nume și prenume, date de contact, conținutul cererii și al răspunsului
Temeiul juridic	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale), art. 12-22 GDPR
Destinatarii	• Google Cloud EMEA Limited, pentru e-mailul firmei și stocarea documentelor în cloud • Instanțele și autoritățile publice, la cerere legală, pentru răspunsul la solicitările legale ale autorităților
Transferurile în afara SEE	Destinatarii acestei activități sunt stabiliți în SEE. Garanțiile pentru transferurile pe care furnizorii le fac mai departe, în afara SEE, sunt în DP-14.
Termenul de păstrare	3 ani de la răspuns. Temeiul termenului: art. 2517 din Codul civil.
Măsurile de securitate	• Cererile se înregistrează în registrul cererilor, cu data primirii și data răspunsului. • Identitatea solicitantului se verifică înainte de a transmite date. • Se aplică și regulile de securitate ale societății (DP-11).

Fișa 6. Mesajele primite prin formularul de contact și prin e-mail

Scopul prelucrării	Răspunsul la întrebările vizitatorilor și ale clienților.
Persoanele vizate	vizitatori ai site-ului; clienți
Categoriile de date	nume; adresă de e-mail; telefon, dacă este dat; conținutul mesajului
Temeiul juridic	art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului)
Destinatarii	• Google Cloud EMEA Limited, pentru e-mailul firmei și stocarea documentelor în cloud • Hostico, pentru găzduirea site-ului
Transferurile în afara SEE	• Hostico, țara și garanția se verifică în termenii furnizorului
Termenul de păstrare	12 luni de la ultimul mesaj, termen stabilit de operator.
Măsurile de securitate	• Datele se șterg sau se anonimizează la sfârșitul termenului de păstrare. • Se activează autentificarea în doi pași pentru căsuța de e-mail (DP-11). • Se aplică și regulile de securitate ale societății (DP-11).

Fișa 7. Comenzile și livrarea

Scopul prelucrării	Preluarea comenzilor, confirmarea lor și livrarea produselor.
Persoanele vizate	clienți; destinatarii coletelor
Categoriile de date	nume și prenume, adresa de livrare, telefon, adresă de e-mail, produsele comandate și valoarea comenzii
Temeiul juridic	art. 6 alin. (1) lit. b) GDPR (executarea contractului)
Destinatarii	• Agenția Exemplu Web SRL, pentru administrarea tehnică a site-ului • Delivery Solutions S.A., pentru livrarea comenzilor • FAN Courier Express S.R.L., pentru livrarea comenzilor • Hostico, pentru găzduirea site-ului
Transferurile în afara SEE	• Agenția Exemplu Web SRL, țara și garanția se verifică în termenii furnizorului • Hostico, țara și garanția se verifică în termenii furnizorului
Termenul de păstrare	3 ani de la livrare. Temeiul termenului: art. 2517 din Codul civil.
Măsurile de securitate	• Curierul primește doar datele necesare livrării. • Accesul este limitat la persoanele care au nevoie de date pentru această activitate. • Conturile de administrare au parole unice și sunt închise când persoana pleacă. • Se aplică și regulile de securitate ale societății (DP-11).

EXEMPLU

Fișa 8. Facturarea

Scopul prelucrării	Emiterea facturilor și transmiterea lor în sistemul RO e-Factura.

Persoanele vizate	clienți
Categoriile de date	nume și prenume sau denumire; adresă; produsele facturate și valoarea; codul fiscal, doar pentru clienții care au unul
Temeiul juridic	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale)
Destinatarii	• Contabilitate Exemplu SRL, pentru ținerea contabilității • Intelligent IT S.R.L., pentru emiterea facturilor • Agenția Națională de Administrare Fiscală (ANAF), pentru îndeplinirea obligațiilor fiscale
Transferurile în afara SEE	• Contabilitate Exemplu SRL, țara și garanția se verifică în termenii furnizorului
Termenul de păstrare	5 ani de la 1 iulie a anului următor încheierii exercițiului financiar. Temeiul termenului: art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare.
Măsurile de securitate	• Pentru persoanele fizice nu se cere CNP-ul; factura se emite cu codul format din 13 cifre de zero. • Accesul este limitat la persoanele care au nevoie de date pentru această activitate. • Se aplică și regulile de securitate ale societății (DP-11).

Fișa 9. Contul de client

Scopul prelucrării	Crearea și administrarea contului, istoricul comenzilor și adresele salvate.
Persoanele vizate	clienți cu cont
Categoriile de date	nume și prenume; adresă de e-mail; parola, stocată criptat; adresele salvate; istoricul comenzilor
Temeiul juridic	art. 6 alin. (1) lit. b) GDPR (executarea contractului)
Destinatarii	• Agenția Exemplu Web SRL, pentru administrarea tehnică a site-ului • Hostico, pentru găzduirea site-ului
Transferurile în afara SEE	• Agenția Exemplu Web SRL, țara și garanția se verifică în termenii furnizorului • Hostico, țara și garanția se verifică în termenii furnizorului
Termenul de păstrare	până la ștergerea contului sau după 36 de luni de inactivitate, termen stabilit de operator.
Măsurile de securitate	• Parolele se stochează doar sub formă criptată ireversibil. • Clientul își poate șterge contul din pagina contului sau printr-o cerere. • Se aplică și regulile de securitate ale societății (DP-11).

Fișa 10. Retururile

Scopul prelucrării	Primirea produselor returnate în termenul de retragere și rambursarea banilor.
Persoanele vizate	clienți persoane fizice

EXEMPLU

Categoriile de date	nume și prenume, date de contact, comanda și produsele returnate, contul bancar pentru rambursare
Temeiul juridic	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale); art. 6 alin. (1) lit. b) GDPR (executarea contractului)
Destinatarii	• Delivery Solutions S.A., pentru livrarea comenzilor • FAN Courier Express S.R.L., pentru livrarea comenzilor • Intelligent IT S.R.L., pentru emiterea facturilor • NETOPIA Financial Services S.A., pentru procesarea plăților cu cardul
Transferurile în afara SEE	Destinatarii acestei activități sunt stabiliți în SEE. Garanțiile pentru transferurile pe care furnizorii le fac mai departe, în afara SEE, sunt în DP-14.
Termenul de păstrare	3 ani de la rambursare. Temeiul termenului: art. 2517 din Codul civil.
Măsurile de securitate	• Contul bancar pentru rambursare se folosește doar pentru această plată. • Accesul este limitat la persoanele care au nevoie de date pentru această activitate. • Se aplică și regulile de securitate ale societății (DP-11).

Fișa 11. Garanția și reclamațiile

EXEMPLU

Scopul prelucrării	Soluționarea reclamațiilor privind neconformitatea produselor.
Persoanele vizate	clienți persoane fizice
Categoriile de date	nume și prenume, date de contact, produsul și descrierea problemei, fotografiile trimise de client
Temeiul juridic	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale)
Destinatarii	• Delivery Solutions S.A., pentru livrarea comenzilor • FAN Courier Express S.R.L., pentru livrarea comenzilor • Google Cloud EMEA Limited, pentru e-mailul firmei și stocarea documentelor în cloud
Transferurile în afara SEE	Destinatarii acestei activități sunt stabiliți în SEE. Garanțiile pentru transferurile pe care furnizorii le fac mai departe, în afara SEE, sunt în DP-14.
Termenul de păstrare	durata garanției și 3 ani după încetarea ei. Temeiul termenului: art. 9 alin. (1) din Ordonanța de urgență a Guvernului nr. 140/2021 privind anumite aspecte referitoare la contractele de vânzare de bunuri; art. 2517 din Codul civil.
Măsurile de securitate	• Reclamațiile se înregistrează cu data primirii și soluția dată. • Accesul este limitat la persoanele care au nevoie de date pentru această activitate. • Se aplică și regulile de securitate ale societății (DP-11).

Fișa 12. Plățile online

Scopul prelucrării	Încasarea plăților cu cardul sau în rate.

Persoanele vizate	clienți
Categoriile de date	nume, valoarea plății, starea tranzacției, tokenul cardului sau ultimele 4 cifre
Temeiul juridic	art. 6 alin. (1) lit. b) GDPR (executarea contractului)
Destinatarii	• NETOPIA Financial Services S.A., pentru procesarea plăților cu cardul
Transferurile în afara SEE	Destinatarii acestei activități sunt stabiliți în SEE. Garanțiile pentru transferurile pe care furnizorii le fac mai departe, în afara SEE, sunt în DP-14.
Termenul de păstrare	durata tranzacției și a eventualelor contestații, termen stabilit de operator.
Măsurile de securitate	• Magazinul nu vede și nu păstrează numărul complet al cardului. • Datele cardului sunt introduse doar pe pagina procesatorului de plăți. • Se aplică și regulile de securitate ale societății (DP-11).

Fișa 13. Prevenirea fraudei la plată

Scopul prelucrării	Identificarea comenzilor și a plăților suspecte.
Persoanele vizate	clienți
Categoriile de date	adresa IP, datele comenzii, rezultatul verificării făcute de procesatorul de plăți
Temeiul juridic	art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului)
Destinatarii	• NETOPIA Financial Services S.A., pentru procesarea plăților cu cardul
Transferurile în afara SEE	Destinatarii acestei activități sunt stabiliți în SEE. Garanțiile pentru transferurile pe care furnizorii le fac mai departe, în afara SEE, sunt în DP-14.
Termenul de păstrare	12 luni de la comandă, termen stabilit de operator.
Măsurile de securitate	• Datele se șterg sau se anonimizează la sfârșitul termenului de păstrare. • Se aplică și regulile de securitate ale societății (DP-11).

EXEMPLU

Fișa 14. Jurnalele serverului și securitatea site-ului

Scopul prelucrării	Funcționarea site-ului, depistarea erorilor și a atacurilor.
Persoanele vizate	vizitatori ai site-ului
Categoriile de date	adresa IP, data și ora accesării, pagina accesată, browserul folosit
Temeiul juridic	art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului)
Destinatarii	• Agenția Exemplu Web SRL, pentru administrarea tehnică a site-ului • Hostico, pentru găzduirea site-ului
Transferurile în afara SEE	• Agenția Exemplu Web SRL, țara și garanția se verifică în termenii furnizorului • Hostico, țara și garanția se verifică în termenii furnizorului
Termenul de păstrare	90 de zile, termen stabilit de operator.

Măsurile de securitate	• Jurnalele se șterg automat după 90 de zile. • Conturile de administrare au parole unice și sunt închise când persoana pleacă. • Se aplică și regulile de securitate ale societății (DP-11).

Fișa 15. Măsurarea audienței site-ului

Scopul prelucrării	Statistici despre folosirea site-ului, cu acordul vizitatorului.
Persoanele vizate	vizitatori ai site-ului care acceptă cookie-urile de analiză
Categoriile de date	identificatorii din cookie-uri, paginile vizitate, dispozitivul și browserul, țara sau orașul aproximativ
Temeiul juridic	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate), cerut de art. 4 alin. (5) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice
Destinatarii	• Google Ireland Limited, pentru măsurarea audienței site-ului
Transferurile în afara SEE	Destinatarii acestei activități sunt stabiliți în SEE. Garanțiile pentru transferurile pe care furnizorii le fac mai departe, în afara SEE, sunt în DP-14.
Termenul de păstrare	durata fiecărui cookie, afișată în politica de cookie-uri sau în panoul „Setări cookie-uri”, termen stabilit de operator.
Măsurile de securitate	• Instrumentele pornesc doar după acordul dat în bannerul de cookie-uri. • Vizitatorul își poate retrage acordul din panoul de setări al bannerului. • Se aplică și regulile de securitate ale societății (DP-11).

EXEMPLU

Fișa 16. Publicitatea online și măsurarea conversiilor

Scopul prelucrării	Afișarea de reclame și măsurarea vânzărilor obținute din reclame.
Persoanele vizate	vizitatori ai site-ului care acceptă cookie-urile de marketing
Categoriile de date	identificatorii din cookie-uri, paginile vizitate, produsele adăugate în coș, comenzile finalizate
Temeiul juridic	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate); operator asociat cu platforma de publicitate, conform art. 26 GDPR
Destinatarii	• Meta Platforms Ireland Limited, pentru publicitatea online și măsurarea conversiilor
Transferurile în afara SEE	Destinatarii acestei activități sunt stabiliți în SEE. Garanțiile pentru transferurile pe care furnizorii le fac mai departe, în afara SEE, sunt în DP-14.
Termenul de păstrare	durata fiecărui cookie, afișată în politica de cookie-uri sau în panoul „Setări cookie-uri”, termen stabilit de operator.

Măsurile de securitate	• Pixelii pornesc doar după acordul dat în bannerul de cookie-uri. • Acordul de operator asociat sau, unde platforma nu îl oferă, termenii ei de operator se păstrează la dosar. • Se aplică și regulile de securitate ale societății (DP-11).
Operatorii asociați	Pentru colectarea datelor prin pixeli și transmiterea lor către platformele de publicitate, societatea și fiecare platformă sunt operatori asociați în sensul art. 26 GDPR (a se vedea Hotărârea Curții de Justiție a Uniunii Europene din 29 iulie 2019, cauza C-40/17, Fashion ID). Pentru ce face ulterior cu datele, platforma este singurul operator. Platformele: Meta Platforms Ireland Limited (Meta Pixel). Acordurile de operator asociat, pentru platformele care le oferă, termenii celorlalte și datele de contact ale platformelor sunt în DP-14.

Fișa 17. Newsletterul și ofertele prin e-mail

Scopul prelucrării	Trimiterea de oferte și noutăți prin e-mail.
Persoanele vizate	abonați la newsletter; clienți care au cumpărat produse similare
Categoriile de date	adresă de e-mail; nume, dacă este dat; data și sursa abonării; dezabonarea
Temeiul juridic	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate), pentru abonați, cerut de art. 12 alin. (1) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice; pentru ofertele către clienții existenți, art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului), în condițiile excepției din art. 12 alin. (2) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice
Destinatarii	• The Rocket Science Group LLC, pentru trimiterea newsletterului
Transferurile în afara SEE	• The Rocket Science Group LLC, Statele Unite ale Americii: Cadrul UE-SUA privind protecția datelor (DPF)
Termenul de păstrare	până la dezabonare, termen stabilit de operator.
Măsurile de securitate	• Fiecare mesaj are un link de dezabonare gratuită. • Data și sursa abonării se păstrează ca dovadă a acordului. • Se aplică și regulile de securitate ale societății (DP-11).

EXEMPLU

Fișa 18. Recenziile produselor

Scopul prelucrării	Colectarea, verificarea și publicarea recenziilor.
Persoanele vizate	clienți care scriu recenzii
Categoriile de date	numele afișat, adresă de e-mail, textul și nota recenziei, comanda verificată

Temeiul juridic	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate), pentru publicare; art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului), pentru verificarea recenziilor
Destinatarii	Datele nu se comunică altor destinatari.
Transferurile în afara SEE	Nu este cazul.
Termenul de păstrare	cât timp recenzia este publicată, termen stabilit de operator.
Măsurile de securitate	• Adresa de e-mail nu se publică. • Clientul își poate șterge recenzia printr-o cerere. • Se aplică și regulile de securitate ale societății (DP-11).

Istoricul actualizărilor

Data	Ce s-a modificat	Cine a modificat
16.11.2026	Întocmirea registrului, versiunea 2026.1	Ion Popescu

EXEMPLU

Informarea angajaților privind prelucrarea datelor cu caracter personal

Prin acest document vă informăm, potrivit art. 13 din Regulamentul (UE) 2016/679 (GDPR), ce date personale prelucrăm despre dvs. în legătură cu contractul individual de muncă, în ce scopuri, pe ce temei și cât timp le păstrăm. Informarea se predă fiecărui angajat la angajare și ori de câte ori se modifică. Primirea ei se confirmă prin semnătură pe fișa din anexă.

1. Cine prelucrează datele

Operatorul datelor este Exemplu Magazin Online SRL, CUI 00000000, Nr. Reg. Com. J00/0000/2026, cu sediul în Str. Exemplului nr. 1, București (denumită în continuare „societatea”). Ne puteți contacta la gdpr@magazin.example sau la telefonul 0700000000.

Pentru orice întrebare despre datele dvs. vă puteți adresa responsabilului intern cu protecția datelor, Ion Popescu, la gdpr@magazin.example. Responsabilul intern nu este responsabil cu protecția datelor (DPO) în sensul art. 37 GDPR.

2. Gestionarea personalului și salarizarea

Scopul	Încheierea și executarea contractelor de muncă, calculul și plata salariilor, declarațiile către autorități.
Persoanele vizate	angajați; membrii de familie ai angajaților, pentru deduceri
Datele	nume și prenume, CNP și datele din actul de identitate, adresă, date de contact, funcție și salariu, cont bancar, concedii și absențe, certificatele de concediu medical, date despre persoanele în întreținere
Temeiul	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale); art. 6 alin. (1) lit. b) GDPR (executarea contractului), pentru contractul de muncă; pentru datele privind sănătatea din certificatele de concediu medical, art. 9 alin. (2) lit. b) GDPR (obligațiile operatorului în domeniul ocupării forței de muncă și al securității sociale și protecției sociale)
Durata de păstrare	5 ani pentru statele de salarii; restul dosarului de personal: termen stabilit de operator. Temeiul termenului: art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare

EXEMPLU

Când ne comunicați date despre membrii familiei sau despre persoanele aflate în întreținerea dvs., pentru deduceri sau pentru alte drepturi, vă rugăm să le spuneți că le-ați transmis societății și în ce scop.

Destinatarii datelor:

- Contabilitate Exemplu SRL, pentru ținerea contabilității;
- Banca prin care se plătesc salariile, pentru plata salariilor;
- Agenția Națională de Administrare Fiscală (ANAF), pentru îndeplinirea obligațiilor fiscale;
- Inspectoratul teritorial de muncă (registrul general de evidență a salariaților, Revisal), pentru evidența salariaților;
- Casa de asigurări de sănătate (certificatele de concediu medical), pentru decontarea indemnizațiilor de concediu medical;

- Instanțele și autoritățile publice, la cerere legală, pentru răspunsul la solicitările legale ale autorităților.

3. Securitatea și sănătatea în muncă, prevenirea incendiilor

Scopul	Instruirea angajaților, evidența controalelor medicale de medicina muncii și a incidentelor.
Datele	nume și prenume, funcție, fișele de instruire, fișa de aptitudine de la medicina muncii, date despre accidentele de muncă
Temeiul	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale); pentru datele privind sănătatea legate de accidentele de muncă, art. 9 alin. (2) lit. b) GDPR (obligațiile operatorului în domeniul ocupării forței de muncă și al securității sociale și protecției sociale); pentru fișa de aptitudine emisă de medicul de medicina muncii, art. 9 alin. (2) lit. h) GDPR (medicina muncii și evaluarea capacității de muncă)
Durata de păstrare	termen stabilit de operator, în limitele legislației privind securitatea și sănătatea în muncă

Fișa de aptitudine o primim de la medicul de medicina muncii. Societatea nu cere diagnosticul medical și păstrează doar concluzia privind aptitudinea pentru post.

Destinatarii datelor:

- Furnizorul de servicii de medicina muncii, pentru supravegherea sănătății lucrătorilor prin medicina muncii;
- Instanțele și autoritățile publice, la cerere legală, pentru răspunsul la solicitările legale ale autorităților.

EXEMPLU

4. Dacă datele sunt obligatorii

Datele cerute pentru salarizare și pentru securitatea și sănătatea în muncă sunt necesare pentru încheierea contractului de muncă și pentru obligațiile legale ale societății. Fără ele, contractul nu poate fi încheiat sau executat, iar societatea nu își poate îndeplini obligațiile față de autorități. Datele cerute pentru deduceri sau pentru alte drepturi opționale le comunicați numai dacă doriți să beneficiați de aceste drepturi.

5. Transferuri în afara Spațiului Economic European

Dacă un furnizor prelucrează datele dvs. în afara Spațiului Economic European, transferul se face numai cu una dintre garanțiile din capitolul V GDPR (art. 44–49). Furnizorii, țara în care prelucrează datele și garanția transferului sunt trecuți în lista destinatarilor (DP-14), pe care o puteți consulta la responsabilul intern.

6. Drepturile dvs.

În legătură cu datele dvs. aveți următoarele drepturi:

- dreptul de acces, adică să aflați ce date prelucrăm și să primiți o copie (art. 15 GDPR);
- dreptul la rectificarea datelor inexacte sau incomplete (art. 16 GDPR);
- dreptul la ștergerea datelor, când nu mai există un temei pentru păstrarea lor (art. 17 GDPR);
- dreptul la restricționarea prelucrării (art. 18 GDPR);

- dreptul la portabilitatea datelor pe care ni le-ați furnizat, pentru prelucrările bazate pe contract și făcute automat (art. 20 GDPR);
- dreptul de opoziție față de prelucrările bazate pe interesul legitim al societății (art. 21 GDPR).

Societatea nu ia decizii bazate exclusiv pe prelucrarea automată a datelor dvs. care să producă efecte juridice asupra dvs. (art. 22 GDPR).

Cererile se adresează responsabilului intern, la gdpr@magazin.example, sau în scris, la sediul societății. Răspundem fără întârziere și în cel mult o lună de la primirea cererii. Termenul se poate prelungi cu două luni pentru cereri complexe sau numeroase, cu informarea dvs. în prima lună (art. 12 alin. (3) GDPR).

Dacă apreciați că datele dvs. sunt prelucrate cu încălcarea GDPR, aveți dreptul să depuneți o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), potrivit art. 77 GDPR.

7. Modificarea informării

Informarea se actualizează la orice schimbare a datelor prelucrate, a scopurilor sau a destinatarilor, inclusiv înainte de instalarea unor camere de supraveghere. Versiunea nouă se predă fiecărui angajat și se semnează din nou pe fișa de luare la cunoștință.

Versiunea 2026.1 din 16.11.2026.

Aprobat,
Administrator
Nume: _____
Semnătura: _____
Ștampila (opțional)

EXEMPLU

Anexă. Fișa de luare la cunoștință

Subsemnații, angajați ai societății Exemplu Magazin Online SRL, declarăm că am primit și am citit informarea privind prelucrarea datelor cu caracter personal, versiunea 2026.1 din 16.11.2026.

Nr.	Nume și prenume	Funcția	Data	Semnătura
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

EXEMPLU

Procedura pentru cererile persoanelor vizate

> Procedura arată cum primește și cum rezolvă societatea cererile prin care o persoană își exercită drepturile din Regulamentul (UE) 2016/679 (GDPR). Anexele conțin formularul de cerere, modelele de răspuns și registrul cererilor. Registrul se completează la fiecare cerere, chiar dacă răspunsul este un refuz.

1. Domeniul de aplicare

Procedura se aplică cererilor primite de Exemplu Magazin Online SRL (denumită în continuare „societatea”) de la clienți, vizitatori ai site-ului magazin.example, abonați, angajați și orice altă persoană ale cărei date le prelucrăm. Ea acoperă drepturile de la art. 15–22 GDPR și retragerea consimțământului (art. 7 alin. (3) GDPR).

2. Cine se ocupă de cereri

Cererile le rezolvă responsabilul intern cu protecția datelor, Ion Popescu, Administrator (gdpr@magazin.example). Angajatul care primește o cerere, pe orice cale, o transmite responsabilului intern în cel mult 2 zile lucrătoare și nu răspunde singur. Furnizorii care prelucrează date în numele societății transmit cererile primite direct în cel mult 5 zile lucrătoare, potrivit contractului DP-13.

Termenele interne din această procedură sunt stabilite de societate. Termenele din GDPR curg de la primirea cererii de către oricare angajat sau colaborator, deci întârzierea internă scurtează timpul de răspuns.

EXEMPLU

3. Primirea cererii

O cerere poate veni pe orice cale: e-mail la gdpr@magazin.example, telefon la 0700000000, scrisoare la sediul societății din Str. Exemplului nr. 1, București, mesaj prin formularul de contact al site-ului sau prin chat. Persoana nu este obligată să folosească formularul din Anexa 1 și nici să numească articolul din GDPR. Orice mesaj din care reiese că persoana vrea să își vadă, să își corecteze sau să își șteargă datele, să se opună prelucrării sau să își retragă acordul se tratează ca cerere.

La primire, responsabilul intern:

1. trece cererea în registrul din Anexa 3, cu data primirii și termenul de răspuns;
2. trimite confirmarea primirii, după modelul 1 din Anexa 2, în cel mult 3 zile lucrătoare;
3. verifică identitatea solicitantului, potrivit secțiunii 4;
4. caută datele persoanei în toate locurile în care se păstrează: platforma magazinului, programul de facturare, e-mailul, platforma de newsletter, exporturile și documentele salvate și dosarele furnizorilor din DP-14.

4. Identificarea solicitantului

Datele se comunică numai persoanei căreia îi aparțin. Când există îndoieli rezonabile privind identitatea solicitantului, societatea poate cere informații suplimentare, potrivit art. 12 alin. (6) GDPR. Se cer doar informațiile necesare pentru identificare:

- cererea trimisă de pe adresa de e-mail folosită la comandă sau în contul de client se consideră, de regulă, suficientă;
- pentru o cerere trimisă de pe altă adresă, se cere numărul unei comenzi și confirmarea de pe adresa cunoscută;
- copia actului de identitate nu se cere în mod obișnuit. Dacă este totuși necesară, de exemplu pentru o cerere trimisă prin poștă, se cere cu datele neesențiale acoperite și se distruge după verificare;
- răspunsul se trimite doar la adresa de e-mail sau la adresa poștală cunoscute ale persoanei, nu la o adresă nouă indicată în cerere.

Cererea făcută prin reprezentant se rezolvă numai dacă reprezentantul prezintă împuternicirea. Termenul de răspuns curge de la primirea cererii, dar responsabilul intern trece în registru data la care a cerut informații suplimentare și data la care le-a primit.

5. Termenul de răspuns

Societatea răspunde fără întârzieri nejustificate și în cel mult o lună de la primirea cererii (art. 12 alin. (3) GDPR). Termenul se poate prelungi cu încă două luni, atunci când este necesar, ținând seama de complexitatea și numărul cererilor. Prelungirea se comunică în prima lună, cu motivele întârzierii, după modelul 3 din Anexa 2.

Dacă societatea nu dă curs cererii, informează persoana fără întârziere și în cel mult o lună de la primire despre motive și despre dreptul de a depune o plângere la ANSPDCP și de a se adresa instanței (art. 12 alin. (4) GDPR). Refuzul se scrie după modelul 4 din Anexa 2.

EXEMPLU

6. Gratuitatea

Răspunsul și măsurile luate sunt gratuite (art. 12 alin. (5) GDPR). Numai când o cerere este vădit nefondată sau excesivă, în special prin caracterul ei repetitiv, societatea poate cere o taxă rezonabilă, calculată după costurile administrative, sau poate refuza cererea. Societatea trebuie să poată dovedi caracterul vădit nefondat sau excesiv, de aceea motivele se notează în registru. Pentru copii suplimentare ale datelor, cerute de aceeași persoană, se poate percepe o taxă rezonabilă (art. 15 alin. (3) GDPR).

7. Drepturile și cum se aplică în magazin

Dreptul de acces (art. 15 GDPR)

Persoana primește confirmarea că îi prelucrăm datele și o copie a lor: datele de identificare și de contact, comenzile și facturile, datele din contul de client, abonarea la mesajele comerciale și mesajele trimise societății. Răspunsul cuprinde și informațiile de la art. 15 alin. (1) GDPR: scopurile, categoriile de date, destinatarii, durata de păstrare, drepturile persoanei, dreptul de a depune plângere și sursa datelor, dacă nu au fost colectate de la ea. Când datele se transferă în afara Spațiului Economic European, răspunsul arată și temeiul și garanțiile transferului (art. 15 alin. (2), art. 45–46 GDPR): The Rocket Science Group LLC, Statele Unite ale Americii: Cadrul UE-SUA privind protecția datelor (DPF). Dacă unul dintre destinatarii marcați în DP-14 pentru verificare transferă datele în afara SEE, răspunsul arată și temeiul și garanțiile transferului. Pentru aceste informații se folosesc registrul activităților (DP-04) și lista destinatarilor (DP-14).

Dreptul la rectificare (art. 16 GDPR)

Datele inexacte se corectează, iar cele incomplete se completează, de exemplu adresa de livrare, numele sau numărul de telefon. Clientul cu cont își poate modifica singur o parte dintre date, din pagina contului. Datele unei facturi emise nu se modifică direct; dacă factura conține o eroare, se aplică regulile de corectare a facturilor.

Dreptul la ștergere (art. 17 GDPR)

Datele se șterg în situațiile de la art. 17 alin. (1) GDPR, de exemplu când nu mai sunt necesare, când persoana își retrage acordul și nu există alt temei, când persoana se opune și nu există motive legitime care să prevaleze sau când prelucrarea este ilegală. Cel mai frecvent caz este ștergerea contului de client: contul, adresele salvate și preferințele se șterg din platforma magazinului, iar persoana este scoasă din listele de marketing.

Ștergerea nu se aplică datelor pe care legea obligă societatea să le păstreze (art. 17 alin. (3) lit. b) GDPR) și celor necesare pentru constatarea, exercitarea sau apărarea unui drept în instanță (art. 17 alin. (3) lit. e) GDPR). De exemplu, facturile se păstrează 5 ani de la 1 iulie a anului următor încheierii exercițiului financiar, potrivit art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare. În răspuns se spune ce date s-au șters și ce date se păstrează, cu temeiul și termenul.

Dreptul la restricționarea prelucrării (art. 18 GDPR)

Datele se marchează și nu se mai folosesc, în afara stocării, cât timp se verifică exactitatea lor sau o opoziție, ori când persoana cere păstrarea lor pentru o acțiune în instanță în locul ștergerii.

EXEMPLU

Notificarea destinatarilor (art. 19 GDPR)

Rectificarea, ștergerea sau restricționarea se comunică destinatarilor cărora le-au fost transmise datele, de exemplu curierului pentru o comandă în curs sau platformei de newsletter, cu excepția cazului în care comunicarea este imposibilă sau cere eforturi disproporționate. La cerere, persoana află cine sunt acești destinatari.

Dreptul la portabilitatea datelor (art. 20 GDPR)

Persoana poate primi datele pe care ni le-a furnizat, prelucrate automat pe baza contractului sau a consimțământului, într-un format structurat, utilizat în mod curent și care poate fi citit automat. În magazin, acesta este, de obicei, istoricul comenzilor: produsele, datele comenzilor, adresele de livrare și datele de contact, exportate din platforma magazinului în format CSV sau într-un alt format electronic similar. La cerere și dacă este posibil tehnic, datele se transmit direct altui operator.

Dreptul la opoziție (art. 21 GDPR)

Persoana se poate opune prelucrărilor bazate pe interesul legitim al societății, de exemplu: mesajele primite prin formularul de contact și prin e-mail; prevenirea fraudei la plată; jurnalele serverului și securitatea site-ului; ofertele prin e-mail către clienții existenți, pentru produse similare, în condițiile excepției din art. 12 alin. (2) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice; verificarea recenziilor. Prelucrarea încetează, cu excepția cazului în care societatea demonstrează motive legitime și imperioase care prevalează sau prelucrarea este necesară pentru un drept în instanță. Testele de interes legitim din DP-16 ajută la această analiză. Opoziția față de

marketingul direct se respectă întotdeauna, fără analiză: adresa se scoate imediat din listele de marketing (art. 21 alin. (3) GDPR).

Decizia individuală automatizată (art. 22 GDPR)

Societatea nu ia decizii bazate exclusiv pe prelucrarea automată care să producă efecte juridice asupra persoanelor sau să le afecteze în mod similar. Dacă o asemenea decizie se introduce, procedura se completează înainte.

Retragerea consimțământului (art. 7 alin. (3) GDPR)

Acordul dat pentru newsletter, pentru cookie-uri sau pentru alte prelucrări se poate retrage oricând, la fel de simplu cum a fost dat. Retragerea nu afectează prelucrarea făcută înainte de ea.

8. Răspunsul

Răspunsul se dă în scris, pe e-mail sau pe calea folosită de persoană, dacă ea nu cere altfel, într-un limbaj clar și simplu. Se folosesc modelele din Anexa 2. După trimitere, responsabilul intern completează în registru data răspunsului și rezultatul. Cererea, răspunsul și dovada trimiterii se păstrează 3 ani de la răspuns, potrivit art. 2517 din Codul civil.

9. Plângerea

Orice persoană nemulțumită de răspuns poate depune o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), potrivit art. 77 GDPR, sau se poate adresa instanței, potrivit art. 79 GDPR. Această informație apare în orice refuz.

Versiunea 2026.1 din 16.11.2026.

EXEMPLU

Aprobat,
Administrator
Nume: _____
Semnătura: _____
Ștampila (opțional)

Anexa 1. Formularul de cerere

Către Exemplu Magazin Online SRL, Str. Exemplului nr. 1, București, gdpr@magazin.example

Nume și prenume: _____

Adresa de e-mail folosită la comandă sau în cont: _____

Telefon (opțional): _____

Numărul unei comenzi (opțional, ajută la identificare): _____

Solicit, în temeiul GDPR:

☐ accesul la datele mele și o copie a lor (art. 15)
☐ rectificarea datelor (art. 16): _____
☐ ștergerea datelor și a contului de client (art. 17)
☐ restricționarea prelucrării (art. 18)
☐ primirea istoricului comenzilor într-un format electronic (art. 20)
☐ încetarea prelucrării bazate pe interesul legitim (art. 21)
☐ să nu mai primesc mesaje comerciale (art. 21 alin. (3))
☐ retragerea acordului pentru: _____
☐ altă cerere: _____

Detalii: _____

Doresc răspunsul: ☐ pe e-mail ☐ prin poștă, la adresa: _____

Data: _____ Semnătura: _____

Datele din formular se folosesc doar pentru rezolvarea cererii și se păstrează 3 ani de la răspuns. Dacă identitatea dvs. nu poate fi verificată din datele de mai sus, vă putem cere informații suplimentare (art. 12 alin. (6) GDPR).

EXEMPLU

Anexa 2. Modele de răspuns

Completați spațiile libere și trimiteți răspunsul de pe adresa societății. Modelele se adaptează la cerere; nu se trimit cu spații necompletate.

Modelul 1. Confirmarea primirii cererii

Stimate/Stimată _____ _____,

Am primit pe data _____ _____ cererea dvs. privind dreptul exercitat _____. Cererea a fost înregistrată cu nr. _____ _____. Vă răspundem în cel mult o lună de la primire, potrivit art. 12 alin. (3) GDPR. Pentru siguranța datelor dvs., vă rugăm să confirmați cererea de pe adresa de e-mail asociată contului sau comenzilor.

Cu stimă,
Ion Popescu, Exemplu Magazin Online SRL

Modelul 2. Răspunsul la cererea de acces

Stimate/Stimată _____ _____,

Ca răspuns la cererea dvs. din data _____ _____, vă confirmăm că Exemplu Magazin Online SRL prelucrează date cu caracter personal care vă privesc. În anexa acestui mesaj găsiți copia datelor: datele transmise _____.

Prelucrăm aceste date în scopurile _____ _____, pe temeiul _____ _____. Destinatarii lor sunt _____ _____. Datele se păstrează _____ _____. Datele au fost colectate de la dvs..

Unele date se transferă în afara Spațiului Economic European, cu următorul temei și următoarele garanții ale transferului (art. 15 alin. (2), art. 45–46 GDPR): The Rocket Science Group LLC, Statele Unite ale Americii: Cadrul UE-SUA privind protecția datelor (DPF).

Aveți dreptul să cereți rectificarea sau ștergerea datelor, restricționarea prelucrării, portabilitatea lor și să vă opuneți prelucrării. Puteți depune o plângere la ANSPDCP (art. 77 GDPR). Prima copie este gratuită.

Cu stimă,
Ion Popescu, Exemplu Magazin Online SRL

Modelul 3. Prelungirea termenului de răspuns

Stimate/Stimată _____ _____,

Cererea dvs. din data _____ _____ necesită mai mult timp, din următorul motiv: complexitatea și numărul cererilor _____. Potrivit art. 12 alin. (3) GDPR, prelungim termenul de răspuns cu una sau două _____ luni. Vă vom răspunde până la data _____ _____.

Cu stimă,
Ion Popescu, Exemplu Magazin Online SRL

Modelul 4. Refuzul motivat

Stimate/Stimată _____ _____,

EXEMPLU

Am analizat cererea dvs. din data _____ privind dreptul exercitat _____. Nu putem da curs cererii în tot sau în parte _____, din următorul motiv:
de exemplu, obligația legală de păstrare și temeiul ei, identitatea neconfirmată sau cererea vădit nefondată ori excesivă _____
.

Potrivit art. 12 alin. (4) GDPR, aveți dreptul să depuneți o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) și să vă adresați instanței.

Cu stimă,
Ion Popescu, Exemplu Magazin Online SRL

EXEMPLU

Anexa 3. Registrul cererilor

Nr.	Data primirii	Solicitantul	Dreptul exercitat	Termenul de răspuns	Data răspunsului	Rezultatul
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Rezultatul se notează ca „admisă”, „admisă parțial” sau „respinsă”, cu motivul. Când registrul se umple, continuați pe o foaie nouă, cu numerotarea în continuare.

EXEMPLU

Procedura pentru încălcarea securității datelor

> Procedura spune ce se face când date personale sunt pierdute, furate, modificate sau văzute de persoane neautorizate. Termenul de notificare către ANSPDCP este de 72 de ore și curge de când societatea a aflat de incident, inclusiv în weekend și în zilele libere. Anexele conțin fișa de evaluare, scrisoarea către persoanele afectate și registrul incidentelor.

1. Ce este o încălcare a securității datelor

Încălcarea securității datelor este orice incident care duce, accidental sau ilegal, la distrugerea, pierderea, modificarea, divulgarea neautorizată ori accesul neautorizat la date personale (art. 4 pct. 12 GDPR). Exemple pentru Exemplu Magazin Online SRL (denumită în continuare „societatea”): un e-mail cu lista clienților trimis greșit, un laptop cu exporturi de comenzi pierdut, un cont de administrare preluat de altcineva, un site infectat care copiază datele introduse de clienți, ștergerea comenzilor fără copie de rezervă.

2. Anunțarea internă

Oricine observă un posibil incident, angajat sau colaborator, îl anunță imediat responsabilului intern cu protecția datelor, Ion Popescu (gdpr@magazin.example), telefon 0700000000, cel târziu în 24 de ore de la constatare. Termenul este stabilit de societate și lasă timp pentru evaluare în cele 72 de ore din GDPR. Incidentul nu se ascunde și nu se rezolvă pe cont propriu, fără a-l anunța.

Furnizorii care prelucrează date în numele societății o anunță în cel mult 48 de ore, potrivit contractului DP-13 (art. 33 alin. (2) GDPR).

EXEMPLU

3. Pașii procedurii

3.1. Constatarea

Responsabilul intern trece incidentul în registrul din Anexa 3 și notează data și ora la care societatea a aflat de el. De la acest moment curg cele 72 de ore. Apoi deschide fișa de evaluare din Anexa 1.

3.2. Izolarea

Incidentul se oprește cât mai repede: se schimbă parolele expuse, se închid conturile compromise, se dezactivează pluginul sau aplicația vulnerabilă, se cere ștergerea datelor trimise greșit. Pentru site se contactează Agenția Exemplu Web SRL, care administrează tehnic site-ul, firma de găzduire Hostico. Dovezile se păstrează: jurnalele serverului, capturile de ecran, mesajele primite. Nu se șterg fișiere înainte de a fi salvate pentru analiză.

3.3. Evaluarea riscului

Riscul pentru persoane se evaluează cu fișa din Anexa 1, după tipul și volumul datelor, numărul persoanelor, cât de ușor pot fi identificate și consecințele posibile: frauda, furtul de identitate, pierderea financiară, umilința, mesajele de tip phishing. Rezultatul este unul dintre următoarele:

- riscul este puțin probabil, de exemplu când datele erau criptate și cheia nu a fost expusă: incidentul se trece doar în registru;

- există un risc pentru persoane: se notifică ANSPDCP;
- riscul este ridicat, de exemplu pentru datele cardului, parole sau date sensibile: se notifică ANSPDCP și se informează persoanele afectate.

3.4. Notificarea către ANSPDCP (art. 33 GDPR)

Când incidentul poate genera un risc pentru drepturile și libertățile persoanelor, societatea îl notifică Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) fără întârzieri nejustificate și, dacă este posibil, în cel mult 72 de ore de la constatare (art. 33 alin. (1) GDPR). Notificarea făcută după 72 de ore se trimite cu motivele întârzierii.

Notificarea se face prin formularul online publicat de ANSPDCP pe site-ul său oficial. Ea cuprinde cel puțin informațiile de la art. 33 alin. (3) GDPR:

- natura incidentului, categoriile și numărul aproximativ de persoane și de înregistrări afectate;
- numele și datele de contact ale responsabilului intern;
- consecințele probabile;
- măsurile luate sau propuse, inclusiv cele pentru reducerea efectelor.

Dacă nu toate informațiile sunt cunoscute în 72 de ore, notificarea se trimite cu ce se știe, iar restul se completează pe etape, fără întârzieri nejustificate (art. 33 alin. (4) GDPR). O copie a notificării și numărul de înregistrare primit se păstrează lângă fișa incidentului.

3.5. Informarea persoanelor afectate (art. 34 GDPR)

Când incidentul poate genera un risc ridicat, persoanele afectate sunt informate fără întârzieri nejustificate (art. 34 alin. (1) GDPR), cu scrisoarea din Anexa 2. Ea descrie, într-un limbaj clar și simplu, natura incidentului, persoana de contact, consecințele probabile și măsurile luate, plus ce poate face persoana ca să se protejeze (art. 34 alin. (2) GDPR).

EXEMPLU

Informarea nu este necesară în cazurile de la art. 34 alin. (3) GDPR:

- lit. a): datele erau protejate prin măsuri care le fac neinteligibile pentru persoanele neautorizate, de exemplu criptarea;
- lit. b): societatea a luat ulterior măsuri care fac puțin probabil riscul ridicat;
- lit. c): informarea individuală ar cere un efort disproporționat. În acest caz, persoanele se informează printr-un anunț public, de exemplu pe site, la fel de eficient.

ANSPDCP poate cere informarea persoanelor chiar dacă societatea a apreciat că nu este necesară (art. 34 alin. (4) GDPR).

3.6. Registrul incidentelor (art. 33 alin. (5) GDPR)

Orice incident se trece în registrul din Anexa 3, chiar dacă nu a fost notificat: faptele, efectele și măsurile de remediere. Registrul arată, la un control, cum a fost tratat fiecare incident. Fișele de evaluare se păstrează lângă registru.

3.7. După incident

Responsabilul intern analizează cauza și propune măsuri care să prevină repetarea: o regulă nouă în DP-11, o instruire, schimbarea unui furnizor. Măsurile se notează în registru.

4. Scenarii pentru magazinul online

Skimming la plată

Un cod rău intenționat introdus în paginile de plată copiază datele cardului sau datele de contact introduse de clienți. Datele cardului se introduc pe pagina procesatorului de plăți, deci verificarea începe cu paginile coșului și ale comenzii, unde codul poate devia clientul sau poate copia datele.

1. Puneți site-ul în mentenanță sau dezactivați plata online până la curățare.
2. Cereți lui Agenția Exemplu Web SRL să verifice fișierele site-ului și să compare codul cu o versiune curată.
3. Anunțați procesatorul de plăți (NETOPIA Financial Services S.A.) și cereți informații despre tranzacțiile suspecte.
4. Stabiliți perioada în care codul a fost activ și comenzile plasate în acest interval.
5. Tratați riscul ca ridicat: datele de plată pot fi folosite pentru fraudă. Notificați ANSPDCP și informați clienții, cu recomandarea de a-și contacta banca.

Preluarea conturilor

Conturile clienților sunt accesate cu parole furate de pe alte site-uri, iar atacatorul vede adresele și istoricul comenzilor sau plasează comenzi. Un cont de administrare al magazinului este preluat după o parolă slabă sau un e-mail de tip phishing.

1. Blocați conturile afectate și resetați parolele.
2. Verificați jurnalele de autentificare: de unde și când s-a intrat în conturi.
3. Verificați comenzile recente din conturile afectate și adresele de livrare modificate. Verificați dacă au apărut conturi de administrare noi.
4. Activați autentificarea în doi pași pentru conturile de administrare și limitarea încercărilor de autentificare.
5. Evaluați riscul după datele vizibile în conturi și informați persoanele afectate să își schimbe parola și pe alte site-uri unde au folosit-o.

EXEMPLU

Plugin sau extensie compromisă

Un plugin al magazinului WooCommerce are o vulnerabilitate publicată sau a fost modificat de un atacator și permite accesul la baza de date.

1. Dezactivați pluginul sau actualizați-l la versiunea corectată.
2. Verificați lista conturilor de administrare și schimbați parolele de administrare și cheile de acces folosite de pluginuri.
3. Verificați în jurnale ce date au fost accesate.
4. Dacă fișierele site-ului au fost modificate, restaurați site-ul dintr-o copie de rezervă curată.
5. Evaluați riscul după datele din baza de date: nume, adrese, telefoane, parole criptate.

Exportul de clienți scăpat

Un fișier cu clienții sau cu comenzile ajunge unde nu trebuie: e-mail trimis greșit, link de partajare public.

1. Cereți destinatarului să șteargă fișierul și să confirme ștergerea în scris.
2. Opriți linkul de partajare sau schimbați permisiunile în Google Workspace.
3. Pentru un dispozitiv pierdut, blocați-l sau ștergeți-l de la distanță și schimbați parolele salvate pe el.

4. Stabiliți ce coloane conținea fișierul și câte persoane sunt afectate.
5. Un fișier trimis unui singur destinatar cunoscut, care confirmă ștergerea, are de regulă un risc redus; un fișier public sau furat are un risc mai mare.

Versiunea 2026.1 din 16.11.2026.

Aprobat,
Administrator
Nume: _____
Semnătura: _____
Ștampila (opțional)

EXEMPLU

Anexa 1. Fișa de evaluare a incidentului

Nr. din registru	_____
Data și ora constatării	_____
Cine a constatat și cum	_____
Ce s-a întâmplat	_____
Tipul încălcării	☐ confidențialitate (acces sau divulgare) ☐ integritate (modificare) ☐ disponibilitate (pierdere sau distrugere)
Datele afectate	☐ nume și contact ☐ adrese ☐ comenzi ☐ parole ☐ date de plată ☐ date sensibile ☐ altele: _____
Numărul aproximativ de persoane și de înregistrări	_____
Datele erau criptate?	☐ da ☐ nu
Consecințele probabile	_____
Măsurile de izolare luate	_____
Riscul	☐ puțin probabil ☐ risc ☐ risc ridicat
Notificarea ANSPDCP	☐ da, la data _____, nr. _____ ☐ nu, motivul: _____
Informarea persoanelor	☐ da, la data _____ ☐ nu, motivul (art. 34 alin. (3) GDPR): _____
Întocmit de	Ion Popescu, Semnătura _____

EXEMPLU

Anexa 2. Scrisoarea către persoanele afectate

Subiect: Informare privind un incident de securitate care vă privește

Stimate/Stimată _____ _____,

Vă informăm că pe data _____ _____ Exemplu Magazin Online SRL a constatat un incident de securitate care a afectat datele dvs. personale: ce s-a întâmplat, pe scurt _____.

Datele afectate sunt: _____ _____. Consecințele posibile sunt: de exemplu, mesaje de tip phishing sau tentative de fraudă _____.

Am luat următoarele măsuri: _____ _____. Am notificat incidentul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

Vă recomandăm: de exemplu, să vă schimbați parola, să vă verificați extrasele de cont, să nu deschideți linkuri din mesaje neașteptate _____.

Pentru întrebări ne puteți contacta la gdpr@magazin.example sau la telefonul 0700000000. Persoana de contact este Ion Popescu, responsabilul intern cu protecția datelor.

Cu stimă,
Exemplu Magazin Online SRL

EXEMPLU

Anexa 3. Registrul incidentelor

Nr.	Data constatării	Descrierea	Datele și persoanele afectate	Riscul	ANSPDCP (data)	Persoanele informate (data)	Măsurile
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

Registrul cuprinde toate incidentele, inclusiv pe cele nenotificate (art. 33 alin. (5) GDPR). Când se umple, continuați pe o foaie nouă, cu numerotarea în continuare.

EXEMPLU

Politica de păstrare și distrugere a datelor cu caracter personal

Politica stabilește cât timp păstrează Exemplu Magazin Online SRL (denumită în continuare „societatea”) datele cu caracter personal și cum le șterge sau le distruge la sfârșitul termenului. Ea pune în aplicare principiul limitării legate de stocare din art. 5 alin. (1) lit. e) GDPR: datele se păstrează într-o formă care permite identificarea persoanelor doar cât este necesar pentru scopul în care au fost colectate.

1. Domeniul de aplicare

Politica se aplică tuturor datelor cu caracter personal prelucrate de societate, oriunde s-ar afla: în platforma magazinului online magazin.example, în căsuțele de e-mail, în serviciile de stocare în cloud și în copiile de rezervă. Ea se aplică și persoanelor care lucrează pentru societate, iar furnizorilor care prelucrează date în numele societății li se aplică prin contractul de prelucrare (DP-13).

2. Regulile de păstrare

- Fiecare activitate are un termen de păstrare, trecut în tabelul de la punctul 3 și în registrul activităților de prelucrare (DP-04).
- Unele termene sunt stabilite de lege, iar sursa lor este citată în tabel. Celelalte sunt stabilite de societate, după scopul prelucrării, și sunt marcate „termen stabilit de operator”.
- Termenul curge de la evenimentul arătat în tabel, de exemplu livrarea comenzii, ultimul mesaj sau încheierea exercițiului financiar.
- Dacă datele sunt necesare într-un litigiu, într-un control sau pentru a răspunde unei cereri a unei autorități, ștergerea lor se amână până la încheierea procedurii. Amânarea o decide responsabilul intern și o consemnează în scris.
- Când aceleași date servesc mai multor activități, se aplică termenul cel mai lung. De exemplu, datele de pe factură rămân în evidența contabilă și după ce comanda nu mai are nevoie de ele.
- În locul ștergerii, datele pot fi anonimizate, dacă după anonimizare nu mai pot fi legate de o persoană. Datele anonimizate se pot folosi pentru statistici.

EXEMPLU

3. Termenele de păstrare

Activitatea	Termenul de păstrare	Temeiul termenului
Gestionarea personalului și salarizarea	5 ani pentru statele de salarii; restul dosarului de personal: termen stabilit de operator	art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare
Securitatea și sănătatea în muncă, prevenirea incendiilor	termen stabilit de operator, în limitele legislației privind securitatea și sănătatea în muncă	termen stabilit de operator

Activitatea	Termenul de păstrare	Temeiul termenului
Contabilitatea	5 ani pentru registre și documentele justificative; 10 ani pentru situațiile financiare anuale	art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare; art. 35 alin. (3) din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare
Relația cu furnizorii	durata contractului și 3 ani după încetarea lui	art. 2517 din Codul civil
Cererile persoanelor vizate	3 ani de la răspuns	art. 2517 din Codul civil
Mesajele primite prin formularul de contact și prin e-mail	12 luni de la ultimul mesaj, termen stabilit de operator	termen stabilit de operator
Comenzile și livrarea	3 ani de la livrare	art. 2517 din Codul civil
Facturarea	5 ani de la 1 iulie a anului următor încheierii exercițiului financiar	art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare
Contul de client	până la ștergerea contului sau după 36 de luni de inactivitate, termen stabilit de operator	termen stabilit de operator
Retururile	3 ani de la rambursare	art. 2517 din Codul civil
Garanția și reclamațiile	durata garanției și 3 ani după încetarea ei	art. 9 alin. (1) din Ordonanța de urgență a Guvernului nr. 140/2021 privind anumite aspecte referitoare la contractele de vânzare de bunuri; art. 2517 din Codul civil
Plățile online	durata tranzacției și a eventualelor contestații, termen stabilit de operator	termen stabilit de operator
Prevenirea fraudei la plată	12 luni de la comandă, termen stabilit de operator	termen stabilit de operator
Jurnalele serverului și securitatea site-ului	90 de zile, termen stabilit de operator	termen stabilit de operator
Măsurarea audienței site-ului	durata fiecărui cookie, afișată în politica de cookie-uri sau în panoul „Setări cookie-uri”, termen stabilit de operator	termen stabilit de operator
Publicitatea online și măsurarea conversiilor	durata fiecărui cookie, afișată în politica de cookie-uri sau în panoul „Setări cookie-uri”, termen stabilit de operator	termen stabilit de operator
Newsletterul și ofertele prin e-mail	până la dezabonare, termen stabilit de operator	termen stabilit de operator
Recenziile produselor	cât timp recenzia este publicată	termen stabilit de operator

EXEMPLU

4. Verificarea periodică

Responsabilul intern, Ion Popescu, verifică cel puțin o dată la 6 luni dacă există date al căror termen s-a încheiat și dispune ștergerea sau distrugerea lor. Datele cu termene scurte (jurnalele serverului) se șterg automat, din setările platformei sau ale serverului, unde este posibil. Verificarea se face și la încetarea relației cu un furnizor sau cu un angajat.

5. Procedura de ștergere și distrugere

În platforma magazinului

- Comenzile și conturile de client cu termenul încheiat se șterg din panoul de administrare sau se anonimizează, dacă platforma păstrează comenzile pentru rapoarte.
- Se șterg și exporturile făcute din platformă (liste de comenzi, liste de clienți), oriunde au fost salvate.
- Conturile de client se șterg la cererea clientului sau după perioada de inactivitate din tabel. Înainte de ștergere, clientul poate fi anunțat prin e-mail.
- Adresele de e-mail ale persoanelor care s-au dezabonat sau și-au retras acordul se păstrează doar pe lista de excludere, ca să nu mai primească mesaje.

În căsuțele de e-mail

Mesajele cu date personale se șterg după termenul din tabel, inclusiv din dosarul „Elemente trimise” și din coșul de gunoi. Atașamentele cu date (facturi, documente de identitate, CV-uri) nu se păstrează în e-mail după ce au fost salvate în locul lor.

EXEMPLU

În cloud

- Fișierele se șterg și din coșul de gunoi al serviciului, iar versiunile anterioare ale fișierului se șterg acolo unde serviciul le păstrează.
- Se retrag linkurile de partajare și accesul persoanelor din afara firmei la dosarele cu date.
- Furnizorul serviciului șterge copiile lui de rezervă după termenul din acordul de prelucrare. Termenul se verifică în acord, al cărui link este în DP-14.

Copiile de rezervă

Datele șterse din sisteme dispar din copiile de rezervă pe măsură ce acestea sunt înlocuite. Dacă o copie de rezervă se restaurează, datele care trebuiau șterse se șterg din nou imediat după restaurare.

6. Evidența ștergerii și a distrugerii

Ștergerile curente din platformă și din e-mail nu se consemnează una câte una. Se consemnează în procesul-verbal din anexă:

- distrugerea documentelor pe hârtie;
- distrugerea sau ștergerea prin suprascriere a suporturilor de date (discuri, stickuri, calculatoare);
- ștergerea unui set mare de date la verificarea periodică, de exemplu comenzile unui an întreg.

Procesul-verbal se semnează de persoana care a făcut distrugerea și de responsabilul intern și se păstrează împreună cu această politică.

7. Revizuirea politicii

Politica se revizuiește o dată pe an și ori de câte ori apare o activitate nouă, un termen legal nou sau un loc nou de păstrare a datelor.

Versiunea 2026.1 din 16.11.2026.

Aprobat,
Administrator
Nume: _____
Semnătura: _____
Ștampila (opțional)

EXEMPLU

Anexă. Proces-verbal de distrugere a documentelor și a suporturilor de date

Nr. _____ din data _____

Încheiat astăzi, data _____, la sediul societății Exemplu Magazin Online SRL, CUI 00000000, de către:

- Nume și prenume _____, persoana care a făcut distrugerea;
- Nume și prenume _____, responsabilul intern cu protecția datelor.

Am distrus documentele și suporturile de date de mai jos, al căror termen de păstrare s-a încheiat, potrivit politicii de păstrare și distrugere:

Nr.	Documentele sau suportul	Activitatea și perioada	Cantitatea	Metoda de distrugere
1				
2				
3				
4				
5				
6				
7				
8				

EXEMPLU

Metoda de distrugere: ☐ distrugător de documente; ☐ predare către o firmă specializată, cu documentul de predare nr. _____; ☐ ștergere prin suprascriere; ☐ distrugerea fizică a suportului.

Documentele și datele distruse nu mai pot fi refăcute.

Persoana care a făcut distrugerea,
Nume și prenume _____
Semnătura _____

Responsabilul intern,
Nume și prenume _____
Semnătura _____

Angajament de confidențialitate privind datele cu caracter personal

Angajamentul se semnează de angajații, colaboratorii și persoanele de la furnizori sau agenții care au acces la datele prelucrate de Exemplu Magazin Online SRL, înainte de a primi acces. Fiecare persoană semnează un exemplar separat, care se păstrează de responsabilul intern cu protecția datelor.

Subsemnatul/Subsemnata _____, în calitate de:

- ☐ angajat al societății, în funcția de _____;
- ☐ colaborator al societății, pe baza contractului nr. _____;
- ☐ persoană desemnată de un furnizor sau de o agenție care lucrează pentru societate, de exemplu agenția care administrează site-ul: denumirea furnizorului _____;

mă angajez față de Exemplu Magazin Online SRL, CUI 00000000 (denumită în continuare „societatea”), să păstrez confidențialitatea datelor cu caracter personal la care am acces în activitatea magazinului online magazin.example și în orice altă activitate pentru societate.

1. Datele la care se referă angajamentul

Angajamentul privește orice dată care identifică o persoană fizică sau o poate identifica: datele clienților și ale comenzilor, adresele de livrare, mesajele primite de la clienți, datele furnizorilor și ale colegilor. Nu contează forma în care se află datele: în platforma magazinului, în e-mail, în exporturi, în fișiere sau pe hârtie.

EXEMPLU

2. Obligațiile mele

Potrivit art. 29 și art. 32 alin. (4) din Regulamentul (UE) 2016/679 (GDPR), prelucrez datele numai la instrucțiunile societății. În acest scop mă oblig:

1. să folosesc datele numai pentru sarcinile primite de la societate și numai în măsura în care am nevoie de ele pentru aceste sarcini;
2. să nu dezvălui datele niciunei persoane, din societate sau din afara ei, care nu are dreptul să le cunoască, inclusiv curierilor, furnizorilor sau persoanelor care se prezintă drept clienți, fără verificarea cerută de procedurile societății;
3. să nu copiez datele în conturi sau pe dispozitive personale (e-mail personal, stocare în cloud personală, aplicații de mesagerie, stick-uri USB) și să nu le scot din societate fără acordul responsabilului intern;
4. să respect regulile de securitate (DP-11): folosesc doar contul meu, nu îmi împart parola, folosesc autentificarea în doi pași unde este disponibilă și blochez calculatorul când plec de la el;
5. să nu încerc să accesez date sau sisteme pentru care nu am primit acces;
6. să anunț imediat responsabilul intern, Ion Popescu (gdpr@magazin.example), despre orice incident de securitate, de exemplu un e-mail cu date trimis la o adresă greșită, un dispozitiv pierdut sau un mesaj suspect, precum și despre orice cerere primită de la o persoană cu privire la datele ei;
7. la încetarea activității pentru societate, să predau documentele și dispozitivele primite, să șterg copiile de date pe care le am și să nu mai folosesc conturile societății.

3. Durata angajamentului

Angajamentul se aplică de la data semnării, pe toată durata activității mele pentru societate. Obligațiile de confidențialitate rămân valabile și după încetarea contractului de muncă, a colaborării sau a contractului cu furnizorul, oricare ar fi motivul încetării, fără limită în timp.

4. Încălcarea angajamentului

Am luat la cunoștință că încălcarea angajamentului poate duce la retragerea imediată a accesului la date, la răspunderea disciplinară în cazul angajaților, potrivit contractului individual de muncă și regulamentului intern, și la răspunderea pentru prejudiciul cauzat societății sau persoanelor ale căror date au fost afectate, potrivit contractului încheiat cu societatea și legii.

Pentru persoanele desemnate de un furnizor care prelucrează date în numele societății, angajamentul se adaugă obligației de confidențialitate din contractul de prelucrare (art. 28 alin. (3) lit. b) GDPR).

5. Documentele primite

Declar că am primit și am citit politica internă de protecție a datelor (DP-03) și regulile de securitate (DP-11) și că am participat la instruirea consemnată în procesul-verbal de instruire (DP-12) sau că voi participa la prima instruire organizată după semnare.

EXEMPLU

Persoana care se angajează,
Nume și prenume _____
Data _____
Semnătura _____

Pentru societate,
Ion Popescu, Administrator
Semnătura _____

Reguli de securitate

> Regulile se aplică tuturor celor care lucrează cu datele Exemplu Magazin Online SRL (denumită în continuare „societatea”): administratorul, angajații și colaboratorii cu acces la site, la e-mail sau la documente. Ele fac parte din măsurile de securitate cerute de art. 32 GDPR. Secțiunea 6 este despre site-ul magazinului.

1. Reguli generale

Datele clienților și ale angajaților se folosesc doar pentru sarcinile de serviciu și doar în măsura în care sunt necesare. Orice problemă de securitate, chiar și o bănuială, se anunță responsabilului intern, Ion Popescu (gdpr@magazin.example), potrivit procedurii DP-08.

2. Parolele

- Fiecare cont are o parolă proprie, de cel puțin 12 caractere, folosită doar pentru acel cont.
- Parolele se păstrează într-un manager de parole, nu pe hârtie lipită de monitor și nici în fișiere necriptate.
- Parolele nu se comunică altor persoane, nici colegilor, nici prin e-mail sau telefon. Nicio persoană care lucrează legitim pentru societate nu are nevoie de parola altcuiva.
- Parola se schimbă imediat când există suspiciunea că a fost aflată de altcineva.

3. Dispozitivele

- Calculatoarele și telefoanele folosite pentru lucru au ecranul blocat cu parolă, PIN sau amprentă și se blochează automat după câteva minute de inactivitate.
- Sistemul de operare, browserul și programul antivirus se actualizează când apar actualizări.
- Laptopurile au discul criptat, de exemplu cu BitLocker sau FileVault.
- Pe dispozitivele de lucru nu se instalează programe din surse necunoscute și nu se conectează stickuri de proveniență necunoscută.
- Pierderea sau furtul unui dispozitiv se anunță imediat, ca incident, potrivit DP-08.

4. E-mailul

E-mailul firmei funcționează prin Google Workspace. Pentru e-mail se aplică următoarele reguli:

- contul de e-mail are autentificarea în doi pași activă;
- înainte de a trimite un mesaj cu date ale clienților, verificați destinatarii, mai ales la completarea automată a adresei;
- listele de clienți sau de comenzi nu se trimit ca atașament necriptat; se folosește un link de partajare restricționat la persoana destinatară;
- mesajele care cer parole, plăți urgente sau deschiderea unor atașamente neașteptate se tratează ca posibil phishing: nu se răspunde și nu se deschid linkurile. Mesajul se verifică pe altă cale cu expeditorul.

5. Stocarea datelor

În afara platformei magazinului, datele clienților se păstrează în locurile de mai jos, cu regulile fiecăruia:

EXEMPLU

- în cloud, în Google Workspace: dosarele cu date ale clienților se partajează doar cu persoanele care au nevoie de ele, nu prin linkuri publice, iar contul are autentificarea în doi pași activă;
- datele nu se copiază pe dispozitive personale sau în conturi personale de cloud și e-mail.

6. Site-ul magazinului

Magazinul funcționează pe platforma WooCommerce, cu găzduirea la Hostico. Site-ul trebuie să folosească doar conexiuni securizate (HTTPS), cu certificat valabil pentru toate paginile.

6.1. Conturile de administrare

Conturi de administrare au în prezent: administratorul societății, agenția Agenția Exemplu Web SRL. Pentru aceste conturi:

- fiecare persoană are propriul cont, cu numele ei; conturile comune, de tipul „admin”, nu se folosesc;
- fiecare cont are doar drepturile de care persoana are nevoie, de exemplu acces la comenzi, fără acces la setări, pentru angajații care pregătesc coletele;
- contul se închide în ziua în care persoana nu mai lucrează pentru societate;
- lista conturilor se verifică cel puțin o dată la 6 luni, termen stabilit de societate, iar conturile nefolosite se închid.

6.2. Autentificarea în doi pași

Recomandăm activarea autentificării în doi pași pentru toate conturile, inclusiv pentru contul agenției Agenția Exemplu Web SRL. În prezent, ea este activă doar pentru o parte dintre conturi. Un cont de administrare protejat doar de parolă poate fi preluat după o singură parolă aflată, iar contul dă acces la datele tuturor clienților. Autentificarea în doi pași se activează din setările platformei WooCommerce sau printr-un modul dedicat, cu o aplicație de autentificare pe telefon.

EXEMPLU

6.3. Actualizările

WooCommerce se instalează pe găzduirea societății, deci actualizările sunt în grija ei:

- platforma, tema și pluginurile se actualizează cel puțin o dată pe lună, iar actualizările de securitate în cel mult câteva zile de la apariție;
- pluginurile se instalează doar din sursele oficiale sau de la dezvoltatori cunoscuți; pluginurile nefolosite se șterg, pentru că dezactivarea lor nu este suficientă;
- versiunea de PHP și a bazei de date rămâne una susținută de furnizorul de găzduire.

6.4. Copiile de rezervă

Site-ul și baza de date se salvează automat, cel puțin zilnic, iar o copie se păstrează în afara serverului de găzduire. Copiile se păstrează criptate și cu acces limitat, la fel ca datele din site.

O dată la 6 luni, termen stabilit de societate, se verifică dacă o copie poate fi restaurată. Data verificării se notează.

6.5. Accesul agenției sau al colaboratorului independent

Agenția Exemplu Web SRL lucrează la site ca persoană împuternicită și are acces la datele clienților. Pentru acest acces:

- se încheie contractul de prelucrare a datelor DP-13 înainte de acordarea accesului;

- fiecare persoană din echipa furnizorului primește conturi nominale, cu drepturile necesare lucrării; parola administratorului societății nu se dă nimănui;
- exporturile de date ale clienților se fac doar la cererea societății, iar copiile de lucru se șterg după terminarea lucrării;
- la încetarea colaborării, conturile furnizorului se închid în aceeași zi, iar parolele și cheile de acces cunoscute de el se schimbă.

7. Verificarea regulilor

Responsabilul intern verifică aplicarea regulilor odată cu lista conturilor de administrare și le actualizează la orice schimbare: platformă nouă, furnizor nou, angajat nou, incident. Nerespectarea regulilor se tratează potrivit angajamentului de confidențialitate (DP-10).

Versiunea 2026.1 din 16.11.2026.

Aprobat,
Administrator
Nume: _____
Semnătura: _____
Ștampila (opțional)

EXEMPLU

Proces-verbal de instruire privind protecția datelor cu caracter personal

Societatea Exemplu Magazin Online SRL, CUI 00000000, a organizat instruirea privind protecția datelor cu caracter personal pentru angajații, colaboratorii și persoanele de la furnizori care au acces la datele prelucrate de societate. Instruirea este una dintre măsurile prin care societatea se asigură că persoanele cu acces la date le prelucrează numai la instrucțiunile ei (art. 32 alin. (4) din Regulamentul (UE) 2016/679, GDPR). Ea aplică secțiunea 11 din politica internă (DP-03).

1. Date despre instruire

- Data instruirii _____
- Durata (minute) _____
- Locul sau platforma online _____
- Instructor: Ion Popescu, responsabil intern cu protecția datelor
- Tipul instruirii: ☐ inițială, înainte de primirea accesului; ☐ periodică, anuală; ☐ după o schimbare sau după un incident

2. Tematica

1. Ce sunt datele cu caracter personal în activitatea magazinului online și principiile din politica internă (DP-03).
2. Confidențialitatea datelor și angajamentul de confidențialitate (DP-10).
3. Regulile de securitate (DP-11): conturi personale, parole, autentificarea în doi pași, mesajele de tip phishing, dispozitivele și exporturile de date.
4. Recunoașterea cererilor persoanelor vizate și transmiterea lor în aceeași zi responsabilului intern, după procedura DP-07.
5. Recunoașterea incidentelor de securitate și anunțarea lor imediată, după procedura DP-08.
6. Păstrarea și distrugerea datelor (DP-09).
7. Ce date primesc curierii, procesatorii de plăți și ceilalți furnizori (DP-14) și ce date nu li se transmit.
8. Datele angajaților și informarea lor (DP-05), pentru persoanele care lucrează cu dosarele de personal.
9. Testul de verificare și discutarea răspunsurilor.

EXEMPLU

3. Participanți

Fiecare participant semnează după ce a urmat instruirea și a completat testul. Punctajul se trece de instructor, după barem.

Nr.	Nume și prenume	Funcția sau calitatea	Punctaj test	Semnătura
1				
2				
3				
4				
5				

Nr.	Nume și prenume	Funcția sau calitatea	Punctaj test	Semnătura
6				
7				
8				
9				
10				

Testul este promovat cu cel puțin 7 din 10 răspunsuri corecte. Participantul care nu promovează reia instruirea și testul în cel mult 30 de zile. Până atunci, responsabilul intern decide ce acces la date păstrează.

Instructor,
Ion Popescu
Semnătura _____

Aprobat,
Administrator
Nume: _____
Semnătura: _____
Ștampila (opțional)

EXEMPLU

Anexa 1. Test de verificare

Nume și prenume _____ Data _____

Încercuiți un singur răspuns la fiecare întrebare. Testul are 10 întrebări și se promovează cu cel puțin 7 răspunsuri corecte.

1. Un client scrie pe adresa magazinului și cere ștergerea contului și a tuturor datelor sale. Ce faceți?
a) Ștergeți imediat contul, comenzile și facturile, ca cererea să fie rezolvată complet.
b) Trimiteți cererea în aceeași zi responsabilului intern; facturile se păstrează pe termenul legal.
c) Îi răspundeți că un client cu comenzi recente nu își poate șterge contul.

2. Ați pierdut laptopul de serviciu, pe care erați autentificat în platforma magazinului și aveați exporturi cu comenzi. Ce faceți?
a) Anunțați imediat responsabilul intern, care schimbă parolele și evaluează incidentul.
b) Așteptați câteva zile, pentru că laptopul poate fi găsit sau returnat.
c) Vă schimbați singur parola contului și nu mai anunțați pe nimeni.

3. Primiți un e-mail care pare trimis de platforma magazinului: contul va fi suspendat dacă nu vă autentificați în 24 de ore, prin linkul din mesaj. Ce faceți?
a) Vă autentificați prin link, ca să nu fie suspendat contul magazinului.
b) Trimiteți mesajul colegilor, ca să verifice și ei dacă linkul funcționează.
c) Nu deschideți linkul și anunțați mesajul responsabilului intern.

4. Ați trimis din greșeală un export cu comenzile din ultima lună, cu nume, adrese și telefoane, la o adresă de e-mail greșită. Ce faceți?
a) Nu faceți nimic, dacă destinatarul pare o persoană de încredere.
b) Retrimiteți exportul la adresa corectă și considerați problema rezolvată.
c) Anunțați imediat responsabilul intern și cereți destinatarului să șteargă mesajul.

5. Un curier vă cere lista completă a clienților magazinului, cu adrese și telefoane, ca să își planifice mai bine rutele. Ce faceți?
a) Trimiteți lista, pentru că firma de curierat este partenerul magazinului.
b) Refuzați; curierul primește doar datele coletelor pe care le livrează.
c) Trimiteți lista fără numerele de telefon, ca să protejați clienții.

6. Cineva sună și spune că este soțul unei cliente. Vrea să afle ce a comandat ea și la ce adresă se livrează coletul. Ce faceți?
a) Nu dați informații; datele comenzii se comunică doar clientei.
b) Îi spuneți adresa de livrare, pentru că nu este o informație secretă.
c) Îi dați informațiile, dacă știe numărul comenzii și numele clientei.

7. Un client întreabă ce date are magazinul despre el. Ce faceți?
a) Îi cereți o taxă pentru timpul necesar căutării datelor.
b) Îi spuneți că datele clienților sunt confidențiale și nu se comunică.
c) Trimiteți cererea responsabilului intern; clientul primește gratuit o copie.

8. Un abonat răspunde la newsletter cu mesajul „Nu mai vreau să primesc oferte”. Ce faceți?
a) Îl scoateți din listă cât mai repede, fără să îi cereți motivul.

EXEMPLU

b) Îl păstrați în listă până la campania următoare, ca să nu pierdeți abonați.
c) Îl întrebați mai întâi de ce se dezabonează și așteptați răspunsul.

9. O persoană de la agenția care administrează site-ul vă cere parola contului dvs. de administrare, ca să rezolve urgent o eroare. Ce faceți?
a) Îi trimiteți parola pe WhatsApp și o schimbați după ce termină.
b) Nu dați parola; agenția primește un cont propriu de la administrator.
c) Îi dictați parola la telefon, ca să nu rămână scrisă nicăieri.

10. Se propune adăugarea în formularul de comandă a unui câmp obligatoriu „Data nașterii”, pentru cupoanele de ziua clientului. Ce răspuns este corect?
a) Câmpul se adaugă ca obligatoriu, pentru că cupoanele cresc vânzările.
b) Se cere CNP-ul în locul datei nașterii, pentru că o conține.
c) Câmpul nu poate fi obligatoriu; o variantă opțională se discută cu responsabilul.

EXEMPLU

Anexa 2. Barem de corectare

Baremul se păstrează de responsabilul intern și nu se dă participanților înainte de test. Fiecare răspuns corect valorează un punct. Testul este promovat cu cel puțin 7 din 10 puncte.

Întrebarea	Răspunsul corect	Explicația
1	b)	Cererea de ștergere se tratează după procedura DP-07, în termenul din art. 12 alin. (3) GDPR. Datele pe care legea obligă societatea să le păstreze, cum sunt facturile, nu se șterg înainte de termen (art. 17 alin. (3) lit. b) GDPR).
2	a)	Pierderea unui dispozitiv cu acces la date este un incident de securitate. Se schimbă parolele și se închid sesiunile deschise. Notificarea către ANSPDCP se face în condițiile art. 33 GDPR, dacă este cazul, în cel mult 72 de ore de la aflarea incidentului.
3	c)	Mesajele care cer autentificarea urgentă printr-un link sunt o metodă frecventă de furt al conturilor (phishing). În platformă se intră doar de la adresa folosită de obicei. Regulile sunt în DP-11.
4	c)	Un export trimis greșit este o divulgare neautorizată (art. 4 pct. 12 GDPR). Responsabilul intern trece incidentul în registru, chiar dacă nu se notifică (art. 33 alin. (5) GDPR), și evaluează notificarea.
5	b)	Curierul primește doar datele necesare livrării (art. 5 alin. (1) lit. c) GDPR). Lista destinatarilor și datele pe care le primesc sunt în DP-14.
6	a)	Comunicarea datelor comenzii altei persoane decât clientul încalcă art. 5 alin. (1) lit. f) GDPR. Identitatea clientului se verifică înainte, după procedura DP-07.
7	c)	Dreptul de acces este prevăzut de art. 15 GDPR. Prima copie a datelor este gratuită (art. 15 alin. (3) GDPR), iar răspunsul se dă în cel mult o lună (art. 12 alin. (3) GDPR).
8	a)	Consimțământul se retrage la fel de ușor cum s-a dat (art. 7 alin. (3) GDPR), iar opoziția față de marketingul direct nu se motivează (art. 21 alin. (2) și (3) GDPR).
9	b)	Fiecare persoană are un cont propriu, iar parolele nu se împart (DP-11). Astfel se poate verifica cine a avut acces la date (art. 32 GDPR).
10	c)	Formularul de comandă cere doar datele necesare (art. 5 alin. (1) lit. c) și art. 25 GDPR). Un câmp opțional se adaugă doar cu scopul explicat. CNP-ul nu se cere pentru comenzi (DP-03, secțiunea 5).

EXEMPLU

Contract de prelucrare a datelor cu caracter personal (art. 28 GDPR)

> Contractul se încheie cu fiecare furnizor care prelucrează date în numele societății, ca persoană împuternicită: platforma magazinului, firma de găzduire, agenția sau colaboratorul care administrează site-ul, contabilul extern, programul de facturare, platforma de newsletter. Dacă furnizorul are propriul acord de prelucrare, folosiți-l pe acela; linkul este în DP-14.
>
> Pentru acești furnizori, lista destinatarilor (DP-14) nu are un link către un acord public de prelucrare: Agenția Exemplu Web SRL; Contabilitate Exemplu SRL; Delivery Solutions S.A.; FAN Courier Express S.R.L.; Hostico; NETOPIA Financial Services S.A.. Cereți-le acordul lor sau propuneți-le acest contract. Pentru furnizorii al căror rol depinde de termenii lor (de exemplu curierii și procesatorii de plăți), contractul se încheie doar dacă termenii lor arată că lucrează ca persoane împuternicite.
>
> Completați spațiile libere și anexele, apoi semnați contractul în două exemplare.

Nr. _____ din data _____

EXEMPLU

Părțile

Exemplu Magazin Online SRL, CUI 00000000, Nr. Reg. Com. J00/0000/2026, cu sediul în Str. Exemplului nr. 1, București, reprezentată de Ion Popescu, Administrator, în calitate de operator (denumită în continuare „operatorul”),

și

Denumirea furnizorului _____, CUI _____, Nr. Reg. Com. _____, cu sediul în _____, reprezentată de Nume și funcție _____, în calitate de persoană împuternicită (denumită în continuare „împuternicitul”),

încheie prezentul contract, în temeiul art. 28 din Regulamentul (UE) 2016/679 (GDPR).

Art. 1. Obiectul contractului

(1) Împuternicitul prelucrează date cu caracter personal în numele operatorului, pentru serviciul _____, prestat în baza contractului sau a termenilor nr. _____ din data _____ (denumit în continuare „contractul principal”).

(2) Obiectul și durata prelucrării, natura și scopul ei, tipurile de date și categoriile de persoane vizate sunt descrise în Anexa 1.

(3) În privința datelor cu caracter personal, prevederile acestui contract au prioritate față de contractul principal.

Art. 2. Obligațiile operatorului

Operatorul răspunde de existența unui temei legal pentru prelucrare, dă împuternicitului instrucțiuni scrise și îl informează despre orice modificare a lor. Instrucțiunile inițiale sunt cele din

acest contract și din Anexa 1.

Art. 3. Obligațiile împuternicitului

Împuternicitul are următoarele obligații:

a) prelucrează datele numai pe baza instrucțiunilor scrise ale operatorului, inclusiv în privința transferurilor în afara Spațiului Economic European (SEE). Dacă dreptul Uniunii sau dreptul național îl obligă la o prelucrare în afara instrucțiunilor, îl informează pe operator înainte de prelucrare, cu excepția cazului în care legea interzice informarea din motive importante de interes public (art. 28 alin. (3) lit. a) GDPR);

b) se asigură că persoanele autorizate să prelucreze datele s-au angajat să respecte confidențialitatea sau au o obligație legală de confidențialitate (art. 28 alin. (3) lit. b) GDPR);

c) aplică măsurile de securitate cerute de art. 32 GDPR, cel puțin pe cele din Anexa 2 (art. 28 alin. (3) lit. c) GDPR);

d) respectă condițiile de la art. 4 din acest contract pentru recrutarea altor persoane împuternicite (art. 28 alin. (3) lit. d) GDPR);

e) ținând seama de natura prelucrării, îl ajută pe operator, prin măsuri tehnice și organizatorice potrivite, să răspundă cererilor persoanelor vizate privind drepturile din capitolul III GDPR. Cererile primite direct de împuternicit se transmit operatorului în cel mult 5 zile lucrătoare, fără a le răspunde în numele lui (art. 28 alin. (3) lit. e) GDPR);

f) îl ajută pe operator să își îndeplinească obligațiile de la art. 32-36 GDPR: securitatea prelucrării, notificarea și comunicarea încălcărilor securității datelor, evaluarea impactului și consultarea prealabilă, ținând seama de natura prelucrării și de informațiile pe care le are (art. 28 alin. (3) lit. f) GDPR);

g) la încetarea serviciilor, șterge sau returnează operatorului toate datele, după alegerea operatorului, și șterge copiile existente, potrivit art. 7 din acest contract, cu excepția cazului în care dreptul Uniunii sau dreptul național impune păstrarea lor (art. 28 alin. (3) lit. g) GDPR);

h) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea art. 28 GDPR și permite auditurile și inspecțiile făcute de operator sau de un auditor mandatat de acesta, potrivit art. 8 din acest contract (art. 28 alin. (3) lit. h) GDPR).

Împuternicitul îl informează imediat pe operator dacă, în opinia sa, o instrucțiune încalcă GDPR sau alte dispoziții privind protecția datelor (art. 28 alin. (3) al doilea paragraf GDPR).

Art. 4. Subîmputerniciții

(1) Operatorul îi dă împuternicitului o autorizare generală scrisă de a recurge la alte persoane împuternicite (subîmputerniciți). Subîmputerniciții folosiți la data semnării sunt trecuți în Anexa 3.

(2) Împuternicitul îl informează pe operator, în scris, cu cel puțin 30 de zile înainte, despre orice subîmputernicit nou sau înlocuit. În acest termen, operatorul poate formula obiecții motivate. Dacă părțile nu ajung la o soluție, operatorul poate înceta contractul principal pentru serviciile afectate, fără penalități.

(3) Împuternicitul impune fiecărui subîmputernicit, printr-un contract scris, aceleași obligații de protecție a datelor ca în acest contract, în special garanții suficiente pentru măsurile de securitate (art. 28 alin. (4) GDPR).

EXEMPLU

(4) Împuternicitul răspunde integral față de operator pentru îndeplinirea obligațiilor subîmputerniciților săi.

Art. 5. Transferurile în afara Spațiului Economic European

(1) Împuternicitul și subîmputerniciții lui transferă date în afara SEE numai cu acordul scris al operatorului și numai cu una dintre garanțiile din capitolul V GDPR: o decizie de adecvare (art. 45 GDPR), inclusiv Cadrul UE-SUA privind protecția datelor pentru entitățile certificate, sau garanții adecvate (art. 46 GDPR), de exemplu clauzele contractuale standard adoptate de Comisia Europeană.

(2) Țările în care se prelucrează datele și garanția folosită se trec în Anexa 1 și în Anexa 3.

Art. 6. Notificarea încălcărilor securității datelor

(1) Împuternicitul îl notifică pe operator fără întârzieri nejustificate (art. 33 alin. (2) GDPR), dar cel târziu în 48 de ore după ce a luat cunoștință de o încălcare a securității datelor prelucrate pentru operator. Termenul îi permite operatorului să notifice ANSPDCP în 72 de ore, potrivit art. 33 alin. (1) GDPR.

(2) Notificarea cuprinde, în măsura în care sunt cunoscute: natura încălcării, categoriile și numărul aproximativ de persoane și de înregistrări afectate, consecințele probabile, măsurile luate sau propuse și datele de contact ale persoanei care poate da detalii (art. 33 alin. (3) GDPR). Informațiile care nu sunt disponibile imediat se transmit pe etape, fără întârzieri nejustificate.

(3) Notificarea se trimite la gdpr@magazin.example, în atenția responsabilului intern cu protecția datelor, Ion Popescu, și se confirmă telefonic la 0700000000.

EXEMPLU

Art. 7. Ștergerea sau returnarea datelor

(1) La încetarea contractului principal, operatorul alege, în scris, dacă datele se returnează sau se șterg. În lipsa unei alegeri în 15 zile de la încetare, datele se returnează.

(2) Împuternicitul returnează datele într-un format electronic structurat, utilizat în mod curent, sau le șterge, împreună cu copiile existente, inclusiv cele ale subîmputerniciților, în cel mult 30 de zile de la alegerea operatorului. Copiile de rezervă se șterg la sfârșitul ciclului lor obișnuit.

(3) Împuternicitul confirmă ștergerea în scris. Datele pe care legea îl obligă să le păstreze rămân protejate de acest contract până la ștergerea lor.

Art. 8. Auditul

(1) La cererea operatorului, împuternicitul transmite, în cel mult 15 zile, informațiile care dovedesc respectarea acestui contract, de exemplu descrierea măsurilor de securitate, rapoarte de audit sau certificări ale sistemului de securitate a informației.

(2) Operatorul sau un auditor mandatat de el, obligat la confidențialitate, poate face un audit sau o inspecție, cu o notificare prealabilă de cel puțin 15 zile, în timpul programului de lucru și fără a perturba nejustificat activitatea împuternicitului. Fiecare parte își suportă propriile costuri ale auditului.

(3) Dacă auditul constată nereguli, împuternicitul le remediază în termenul convenit cu operatorul.

Art. 9. Răspunderea

Fiecare parte răspunde pentru prejudiciile cauzate prin încălcarea obligațiilor sale din acest contract și din GDPR, potrivit art. 82 GDPR. Împuternicitul răspunde, în special, atunci când nu și-a îndeplinit obligațiile care îi revin în mod specific sau a acționat în afara instrucțiunilor legale ale operatorului ori contrar acestora.

Art. 10. Durata și dispoziții finale

(1) Contractul intră în vigoare la data semnării și se aplică pe toată durata contractului principal. Obligațiile de la art. 3 lit. b), art. 6 și art. 7 rămân valabile cât timp împuternicitul are date ale operatorului.

(2) Modificările se fac numai în scris, prin act adițional semnat de ambele părți.

(3) Contractul se completează cu prevederile GDPR și ale legislației române privind protecția datelor.

(4) Anexele 1-3 fac parte din contract. Contractul s-a încheiat în două exemplare, câte unul pentru fiecare parte.

Operatorul,
Exemplu Magazin Online SRL
Ion Popescu, Administrator
Semnătura _____

Împuternicitul,
Denumirea _____
Nume și funcție _____
Semnătura _____

EXEMPLU

Anexa 1. Detaliile prelucrării

Obiectul prelucrării	serviciul prestat _____
Durata prelucrării	Durata contractului principal și perioada de ștergere sau de returnare de la art. 7.
Natura prelucrării	☐ colectare; ☐ stocare; ☐ consultare; ☐ transmitere; ☐ modificare; ☐ ștergere; ☐ altele: _____
Scopul prelucrării	_____
Categoriile de persoane vizate	☐ clienți; ☐ vizitatori ai site-ului; ☐ abonați la newsletter; ☐ angajați; ☐ persoanele de contact ale furnizorilor; ☐ altele: _____
Tipurile de date	☐ nume și prenume; ☐ date de contact (e-mail, telefon); ☐ adresa de livrare sau de facturare; ☐ datele comenzilor; ☐ datele de plată, fără numărul complet al cardului; ☐ adresa IP și identificatori online; ☐ date din dosarul de personal; ☐ altele: _____
Locul prelucrării	Țara sau țările: _____. Garanția pentru transferurile în afara SEE: _____
Instrucțiuni speciale	_____

EXEMPLU

Anexa 2. Măsurile tehnice și organizatorice de securitate

Împuternicitul aplică cel puțin măsurile de mai jos. Bifați măsurile confirmate de furnizor și adăugați-le pe cele pe care le descrie în documentele lui.

- ☐ accesul la date se acordă numai persoanelor care au nevoie de ele pentru serviciu, cu conturi nominale;
- ☐ autentificarea în doi pași pentru conturile cu acces la datele operatorului;
- ☐ criptarea datelor în tranzit (HTTPS sau TLS) și, unde este posibil, la stocare;
- ☐ copii de rezervă regulate și testarea restaurării lor;
- ☐ actualizarea la timp a sistemelor și a aplicațiilor folosite;
- ☐ jurnale ale accesului la date și verificarea lor;
- ☐ angajamente de confidențialitate semnate de personalul cu acces la date;
- ☐ o procedură pentru încălcările securității datelor, cu notificarea operatorului potrivit art. 6;
- ☐ ștergerea sigură a datelor și a suporturilor scoase din uz;
- ☐ alte măsuri: _____

Anexa 3. Subîmputerniciții aprobați

Nr.	Denumirea	Serviciul	Țara	Garanția transferului
1				
2				
3				

Nr.	Denumirea	Serviciul	Țara	Garanția transferului
4				
5				

EXEMPLU

Lista destinatarilor și matricea de roluri

Lista cuprinde persoanele și entitățile din afara societății Exemplu Magazin Online SRL care primesc date cu caracter personal, grupate după rolul lor în GDPR. Matricea de roluri, de la sfârșitul documentului, arată cine din societate și din afara ei are acces la fiecare categorie de date.

Rolul destinatarului decide ce document trebuie să existe:

- pentru o persoană împuternicită, un contract de prelucrare potrivit art. 28 GDPR: acordul publicat de furnizor sau contractul DP-13;
- pentru un operator independent, nu se încheie contract de prelucrare, iar furnizorul răspunde singur pentru prelucrările lui;
- pentru operatorii asociați, un acord care stabilește responsabilitățile fiecăruia, potrivit art. 26 GDPR.

Pentru transferurile în afara Spațiului Economic European (SEE), coloana „Garanția transferului” arată garanția declarată de furnizor, potrivit capitolului V GDPR. Unde scrie „Verificați acordul furnizorului”, furnizorul nu publică o declarație despre transferuri; responsabilul intern o caută în acordul sau în termenii furnizorului și completează rândul. Datele despre furnizorii cunoscuți au fost verificate pe site-urile lor la 18.10.2026. Furnizorii își pot schimba termenii, de aceea rândurile se verifică din nou la revizuirea anuală a dosarului.

EXEMPLU

1. Persoanele împuternicite

Furnizorii prelucrează datele în numele societății și numai după instrucțiunile ei. Furnizorii al căror rol depinde de termenii lor (de exemplu curierii și procesatorii de plăți) apar aici cu formularea „Împuternicit sau operator independent: verificați termenii furnizorului”: unii lucrează ca persoane împuternicite, alții ca operatori independenți, după termenii lor. Responsabilul intern citește termenii, trece rolul corect și, dacă furnizorul este împuternicit, păstrează acordul lui sau încheie contractul DP-13.

Furnizor	Serviciu	Rol	Țara	Garanția transferului	Acordul de prelucrare
Agenția Exemplu Web SRL	administrarea tehnică a site-ului	Împuternicit	Țara _____	Verificați acordul furnizorului	Încheiați contractul DP-13 sau cereți acordul furnizorului
Contabilitate Exemplu SRL	contabilitate externă, pentru ținerea contabilității	Împuternicit	Țara _____	Verificați acordul furnizorului	Încheiați contractul DP-13 sau cereți acordul furnizorului

Furnizor	Serviciu	Rol	Țara	Garanția transferului	Acordul de prelucrare
Delivery Solutions S.A.	servicii de curierat (Sameday), pentru livrarea comenzilor	Împuternicit sau operator independent: verificați termenii furnizorului	România	Clauzele contractuale standard (art. 46 alin. (2) lit. c) GDPR)	Politica furnizorului; dacă este împuternicit, contractul DP-13 sau acordul lui (linkul este sub tabel)
FAN Courier Express S.R.L.	servicii de curierat (FAN Courier), pentru livrarea comenzilor	Împuternicit sau operator independent: verificați termenii furnizorului	România	Verificați acordul furnizorului	Politica furnizorului; dacă este împuternicit, contractul DP-13 sau acordul lui (linkul este sub tabel)
Google Cloud EMEA Limited	e-mail și stocare în cloud (Google Workspace), pentru e-mailul firmei și stocarea documentelor în cloud	Împuternicit	Irlanda	Clauzele contractuale standard (art. 46 alin. (2) lit. c) GDPR)	Acordul de prelucrare publicat de furnizor (linkul este sub tabel)
Google Ireland Limited	Google Analytics 4, pentru măsurarea audienței site-ului	Împuternicit	Irlanda	Cadrul UE-SUA privind protecția datelor (DPF), pentru transferurile în SUA	Acordul de prelucrare publicat de furnizor (linkul este sub tabel)
Hostico	găzduirea site-ului	Împuternicit	Țara _____	Verificați acordul furnizorului	Încheiați contractul DP-13 sau cereți acordul furnizorului
Intelligent IT S.R.L.	program de facturare online (SmartBill), pentru emiterea facturilor	Împuternicit	România	Verificați acordul furnizorului	Acordul de prelucrare publicat de furnizor (linkul este sub tabel)

EXEMPLU

Furnizor	Serviciu	Rol	Țara	Garanția transferului	Acordul de prelucrare
NETOPIA Financial Services S.A.	procesator de plăți online (NETOPIA Payments), pentru procesarea plăților cu cardul	Împuternicit sau operator independent: verificați termenii furnizorului	România	Clauzele contractuale standard (art. 46 alin. (2) lit. c) GDPR)	Politica furnizorului; dacă este împuternicit, contractul DP-13 sau acordul lui (linkul este sub tabel)
The Rocket Science Group LLC	platformă de newsletter (Mailchimp), pentru trimiterea newsletterului	Împuternicit	Statele Unite ale Americii	Cadrul UE-SUA privind protecția datelor (DPF), pentru transferurile în SUA	Acordul de prelucrare publicat de furnizor (linkul este sub tabel)

Linkurile din coloana „Acordul de prelucrare”:

- Delivery Solutions S.A.: https://sameday.ro/politica-de-confidentialitate/
- FAN Courier Express S.R.L.: https://www.fancourier.ro/politica-de-confidentialitate/
- Google Cloud EMEA Limited: https://cloud.google.com/terms/data-processing-addendum/
- Google Ireland Limited: https://business.safety.google/adsprocessorterms/
- Intelligent IT S.R.L.: https://www.smartbill.ro/termeni-si-conditii
- NETOPIA Financial Services S.A.: https://netopia-payments.com/politica-de-confidentialitate/
- The Rocket Science Group LLC: https://mailchimp.com/legal/data-processing-addendum/

EXEMPLU

2. Operatorii independenți

Acești destinatari primesc datele și le prelucrează în scopurile lor, ca operatori. Societatea îi informează pe clienți și pe angajați despre ei, dar nu le dă instrucțiuni.

Furnizor	Serviciu	Rol	Țara	Garanția transferului	Acordul de prelucrare
Banca prin care se plătesc salariile	plata salariilor	Operator independent	România	Verificați acordul furnizorului	Se completează după termenii destinatarului
Furnizorul de servicii de medicina muncii	medicina muncii, pentru supravegherea sănătății lucrătorilor prin medicina muncii	Operator independent	România	Verificați acordul furnizorului	Se completează după termenii destinatarului

3. Operatorii asociați

Pentru pixelii publicitari, societatea și platforma de publicitate stabilesc împreună scopurile și mijloacele colectării și transmiterii datelor, deci sunt operatori asociați în sensul art. 26 GDPR (a se vedea Hotărârea Curții de Justiție a Uniunii Europene din 29 iulie 2019, cauza C-40/17, Fashion

ID). Acordul de operator asociat al fiecărei platforme care îl oferă sau, în lipsa lui, termenii de operator ai platformei sunt în coloana „Acordul de operator asociat”; se acceptă din contul de publicitate și se păstrează la dosar.

Furnizor	Serviciu	Rol	Țara	Garanția transferului	Acordul de operator asociat
Meta Platforms Ireland Limited	Meta Pixel, pentru publicitatea online și măsurarea conversiilor	Operator asociat (art. 26 GDPR)	Irlanda	Cadrul UE-SUA privind protecția datelor (DPF), pentru transferurile în SUA	Acordul de operator asociat publicat de furnizor (linkul este sub tabel)

Linkurile din coloana „Acordul de operator asociat”:

- Meta Platforms Ireland Limited: https://www.facebook.com/legal/controller_addendum

4. Autoritățile publice

Autoritățile primesc date numai când legea o cere. Ele sunt operatori independenți și nu semnează contracte de prelucrare cu societatea.

Autoritatea	Serviciu	Rol	Țara	Garanția transferului	Acordul de prelucrare
Agenția Națională de Administrare Fiscală (ANAF)	administrarea fiscală, inclusiv sistemul RO e-Factura, pentru îndeplinirea obligațiilor fiscale	Autoritate publică, operator independent	România	Nu este cazul	Nu este cazul
Inspectoratul teritorial de muncă (registrul general de evidență a salariaților, Revisal)	registrul general de evidență a salariaților, pentru evidența salariaților	Autoritate publică, operator independent	România	Nu este cazul	Nu este cazul
Casa de asigurări de sănătate (certificatele de concediu medical)	decontarea concediilor medicale, pentru decontarea indemnizațiilor de concediu medical	Autoritate publică, operator independent	România	Nu este cazul	Nu este cazul
Instanțele și autoritățile publice, la cerere legală	solicitări în temeiul legii, pentru răspunsul la solicitările legale ale autorităților	Autoritate publică, operator independent	România	Nu este cazul	Nu este cazul

EXEMPLU

5. Matricea de roluri

Matricea pornește de la răspunsul din chestionar despre conturile de administrare ale magazinului. Celelalte accese sunt cele recomandate de politica internă (DP-03), după principiul accesului minim necesar. Dacă în societate se lucrează altfel, corectați matricea și regulile de securitate (DP-11).

Persoana	Panoul de administrare al magazinului	Comenzile și datele clienților	Facturile și documentele contabile	E-mailul firmei	Dosarele de personal
Ion Popescu, Administrator	Da	Da	Da	Da	Da
Angajații	Nu	La nevoie	La nevoie	Da	Nu
Agenția Exemplu Web SRL	Da	La nevoie	Nu	Nu	Nu
Contabilitate Exemplu SRL	Nu	Nu	Da	Nu	Da

„Da” înseamnă acces permanent, pentru sarcinile obișnuite. „La nevoie” înseamnă acces acordat pentru o sarcină anume, de exemplu o cerere a unui client sau o verificare, și retras după aceea. „Nu” înseamnă că persoana nu are acces.

Accesul se retrage în ziua în care persoana nu mai lucrează pentru societate sau contractul cu furnizorul încetează. Responsabilul intern verifică matricea la fiecare schimbare de personal sau de furnizor și cel puțin o dată pe an.

EXEMPLU

Fișa de verificare a necesității unei evaluări de impact (DPIA)

> Fișa verifică, pe baza răspunsurilor din chestionar, dacă prelucrările Exemplu Magazin Online SRL cer o evaluare a impactului asupra protecției datelor (art. 35 GDPR). Ea nu este o evaluare de impact. Când rezultatul este „recomandăm consultanță”, evaluarea de impact se face cu un consultant, înainte de a începe prelucrarea în cauză sau, pentru o prelucrare deja începută, cât mai curând.

1. Ce se verifică

Potrivit art. 35 alin. (1) GDPR, operatorul face o evaluare de impact înainte de prelucrare când aceasta poate genera un risc ridicat pentru drepturile și libertățile persoanelor. Verificarea are două părți:

- lista operațiunilor pentru care evaluarea este obligatorie, de la art. 1 alin. (1) din Decizia Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 174/2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal (tabelul 1);
- cele nouă criterii din Ghidul Grupului de lucru Articolul 29 privind evaluarea impactului asupra protecției datelor (WP248 rev.01), preluat de Comitetul European pentru Protecția Datelor (tabelul 2). Potrivit ghidului, în cele mai multe cazuri o prelucrare care îndeplinește două criterii cere o evaluare de impact.

Criteriile se apreciază pentru fiecare prelucrare din registrul activităților (DP-04), nu pentru toate împreună.

EXEMPLU

2. Tabelul 1. Decizia ANSPDCP nr. 174/2018

Art. 1 alin. (1)	Operațiunea	Rezultat	Motivul
lit. a)	Evaluarea sistematică și cuprinzătoare a aspectelor personale, bazată pe prelucrarea automată, inclusiv crearea de profiluri, care stă la baza unor decizii ce produc efecte juridice privind persoana sau o afectează în mod similar într-o măsură semnificativă	Nu se aplică	Societatea nu ia decizii bazate exclusiv pe prelucrarea automată care să producă efecte juridice asupra persoanelor sau să le afecteze în mod similar. Profilurile folosite pentru reclame sau pentru recomandări de produse servesc marketingului, cu acordul persoanei, și nu stau la baza unor astfel de decizii.

Art. 1 alin. (1)	Operațiunea	Rezultat	Motivul
lit. b)	Prelucrarea pe scară largă a categoriilor speciale de date (art. 9 alin. (1) GDPR) sau a datelor privind condamnări penale și infracțiuni (art. 10 GDPR)	Nu se aplică	Societatea nu vinde produse care dezvăluie date sensibile despre clienți și nu prelucrează date privind condamnări penale. Datele privind sănătatea angajaților (concediile medicale, fișa de aptitudine) se prelucrează pentru obligațiile legale ale angajatorului, numai pentru angajații proprii, deci nu pe scară largă.
lit. c)	Monitorizarea sistematică, pe scară largă, a unei zone accesibile publicului, de exemplu prin supraveghere video în centre comerciale, stadioane, piețe sau parcuri	Nu se aplică	Societatea nu folosește camere video și nu monitorizează zone accesibile publicului.
lit. d)	Prelucrarea pe scară largă a datelor persoanelor vulnerabile, în special ale minorilor și ale salariaților, prin mijloace automatizate de monitorizare sau de înregistrare sistematică a comportamentului, inclusiv pentru publicitate, marketing și difuzare	Nu se aplică	Magazinul nu se adresează copiilor. Activitatea angajaților nu este monitorizată prin mijloace automatizate.
lit. e)	Prelucrarea pe scară largă prin utilizarea inovatoare sau implementarea unor tehnologii noi, mai ales dacă limitează capacitatea persoanelor de a-și exercita drepturile, de exemplu recunoașterea facială pentru accesul în diferite spații	Nu se aplică	Societatea nu folosește recunoașterea facială sau alte tehnologii noi care să limiteze exercitarea drepturilor persoanelor.
lit. f)	Prelucrarea pe scară largă a datelor generate de dispozitive cu senzori care transmit date prin internet sau prin alte mijloace (aplicații de tip „Internet of Things”)	Nu se aplică	Societatea nu prelucrează date generate de dispozitive cu senzori conectate la internet.
lit. g)	Prelucrarea pe scară largă sau sistematică a datelor de trafic ori de localizare, atunci când nu este necesară pentru un serviciu cerut de persoana vizată	Nu se aplică	Adresa de livrare și adresa IP se folosesc pentru comandă, livrare și securitatea site-ului. Societatea nu urmărește traficul sau localizarea persoanelor.

EXEMPLU

3. Tabelul 2. Criteriile din Ghidul WP248

Nr.	Criteriul	Rezultat	Motivul
1	Evaluarea sau scoring, inclusiv profilarea și preconizarea	Se aplică	Pixelii publicitari transmit platformelor de publicitate date despre navigarea pe site, din care acestea creează profiluri de marketing; pixelii se încarcă doar cu acordul vizitatorului.
2	Proces decizional automatizat cu efecte legale sau similare semnificative	Nu se aplică	Nicio decizie cu efect juridic sau cu un efect similar asupra persoanelor nu se ia exclusiv automat.
3	Monitorizare sistematică	Nu se aplică	Societatea nu observă și nu monitorizează sistematic persoanele. Instrumentele de măsurare și de publicitate de pe site se încarcă doar cu acordul vizitatorului.
4	Date sensibile sau date de natură foarte personală	Nu se aplică	Societatea nu prelucrează date sensibile despre clienți. Datele cardului se introduc doar pe pagina procesatorului de plăți. Datele privind sănătatea angajaților se limitează la ce cere legea angajatorului (concediile medicale, fișa de aptitudine).
5	Date prelucrate pe scară largă	Nu se aplică	Chestionarul nu cere numărul clienților și nici volumul datelor, deci răspunsurile nu arată o prelucrare pe scară largă. Ghidul ia în calcul numărul persoanelor, volumul datelor, durata și întinderea geografică a prelucrării. Dacă magazinul are un număr foarte mare de clienți, cereți consultanță.
6	Potrivirea sau combinarea seturilor de date	Nu se aplică	Datele din surse diferite nu se combină în afara scopurilor din registrul activităților (DP-04).
7	Date privind persoanele vizate vulnerabile	Nu se aplică	Datele angajaților se prelucrează pentru contractul de muncă și pentru obligațiile legale, fără monitorizarea activității lor. Magazinul nu se adresează copiilor.
8	Utilizare inovatoare sau implementarea unor noi soluții tehnologice sau organizaționale	Nu se aplică	Societatea folosește tehnologiile obișnuite ale unui magazin online.
9	Atunci când prelucrarea în sine „împiedică persoanele fizice să-și exercite un drept sau să utilizeze un serviciu sau un contract”	Nu se aplică	Nicio prelucrare nu decide automat dacă o persoană poate cumpăra sau își poate exercita un drept.

EXEMPLU

4. Concluzia

Pe baza răspunsurilor, nu este necesară o evaluare de impact (DPIA).

Nicio operațiune din Decizia ANSPDCP nr. 174/2018 nu se aplică, iar nicio activitate nu îndeplinește două dintre criteriile din Ghidul WP248. Fișa se păstrează ca dovadă a verificării făcute.

5. Când se reface verificarea

Verificarea se reface înainte de orice prelucrare nouă sau schimbare importantă: blocarea automată a comenzilor, vânzarea de produse care dezvăluie date sensibile, instalarea de camere video, un instrument nou de profilare sau de publicitate, un asistent automat nou, o creștere mare a numărului de clienți.

Verificat de Ion Popescu, Administrator, la data de _____ _____.

Versiunea 2026.1 din 16.11.2026.

Aprobat,
Administrator
Nume: _____
Semnătura: _____
Ștampila (opțional)

EXEMPLU

Teste de interes legitim

> Pentru fiecare activitate întemeiată, în tot sau în parte, pe interesul legitim al Exemplu Magazin Online SRL (art. 6 alin. (1) lit. f) GDPR) există mai jos o fișă de evaluare. Fișa arată de ce interesul societății nu este depășit de interesele, drepturile și libertățile persoanelor vizate. Fișele se revizuiesc cel puțin o dată la 12 luni, termen stabilit de societate, și la orice schimbare a activității.

Fiecare fișă parcurge trei verificări: dacă interesul urmărit este legitim, dacă prelucrarea este necesară pentru acest interes și dacă, după echilibrarea cu interesele și așteptările rezonabile ale persoanelor, interesul societății prevalează. Considerentul 47 al GDPR arată că trebuie avute în vedere așteptările rezonabile ale persoanelor, în funcție de relația lor cu operatorul. Persoanele se pot opune oricând prelucrării, potrivit art. 21 GDPR.

EXEMPLU

Fișa 1. Mesajele primite prin formularul de contact și prin e-mail

Scopul	Răspunsul la întrebările vizitatorilor și ale clienților.
Persoanele vizate	vizitatori ai site-ului; clienți
Datele	nume; adresă de e-mail; telefon, dacă este dat; conținutul mesajului
Temeiul	art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului)
Durata de păstrare	12 luni de la ultimul mesaj, termen stabilit de operator

1. Interesul legitim

Societatea răspunde la întrebările vizitatorilor și ale clienților care îi scriu prin formularul de contact sau prin e-mail, despre produse, livrare sau comenzi.

2. Necesitatea

Fără nume și adresă de e-mail nu se poate trimite un răspuns. Formularul cere doar aceste date și mesajul; telefonul este opțional. Datele se folosesc numai pentru răspuns.

3. Echilibrul și așteptările rezonabile

Persoana inițiază contactul și se așteaptă să primească un răspuns, deci prelucrarea corespunde așteptărilor ei rezonabile. Mesajele nu se folosesc pentru marketing fără acordul persoanei. Impactul asupra persoanei este redus.

EXEMPLU

4. Garanțiile

- Datele se șterg sau se anonimizează la sfârșitul termenului de păstrare.
- Se activează autentificarea în doi pași pentru căsuța de e-mail (DP-11).
- Persoana se poate opune prelucrării, potrivit art. 21 GDPR și procedurii DP-07.

5. Concluzia

Interesul legitim al societății prevalează, cu garanțiile de mai sus. Prelucrarea se poate face pe temeiul art. 6 alin. (1) lit. f) GDPR.

Evaluat de Ion Popescu, la data de _____.

Fișa 2. Prevenirea fraudei la plată

Scopul	Identificarea comenzilor și a plăților suspecte.
Persoanele vizate	clienți
Datele	adresa IP, datele comenzii, rezultatul verificării făcute de procesatorul de plăți
Temeiul	art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului)
Durata de păstrare	12 luni de la comandă, termen stabilit de operator

1. Interesul legitim

Societatea urmărește să prevină plățile frauduloase, de exemplu cu carduri furate, și pierderile din rambursarea lor. Interesul îi protejează și pe titularii cardurilor. Considerentul 47 al GDPR arată că prelucrarea strict necesară pentru prevenirea fraudelor este un interes legitim al operatorului.

2. Necesitatea

Verificarea folosește doar adresa IP, datele comenzii, rezultatul verificării făcute de procesatorul de plăți. Nu se folosesc date sensibile și nu se creează profiluri ale clienților în alte scopuri.

3. Echilibrul și așteptările rezonabile

Clienții se așteaptă, în mod rezonabil, ca un magazin online să verifice plățile suspecte. Pentru clientul de bună-credință, verificarea nu are efecte. O comandă suspectă este verificată de un om înainte de orice decizie.

EXEMPLU

4. Garanțiile

- Datele se șterg sau se anonimizează la sfârșitul termenului de păstrare.
- Persoana se poate opune prelucrării, potrivit art. 21 GDPR și procedurii DP-07.

5. Concluzia

Interesul legitim al societății prevalează, cu garanțiile de mai sus. Prelucrarea se poate face pe temeiul art. 6 alin. (1) lit. f) GDPR.

Evaluat de Ion Popescu, la data de _____ _____.

Fișa 3. Jurnalele serverului și securitatea site-ului

Scopul	Funcționarea site-ului, depistarea erorilor și a atacurilor.
Persoanele vizate	vizitatori ai site-ului
Datele	adresa IP, data și ora accesării, pagina accesată, browserul folosit
Temeiul	art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului)
Durata de păstrare	90 de zile, termen stabilit de operator

1. Interesul legitim

Societatea asigură funcționarea și securitatea site-ului: depistarea erorilor, a atacurilor și a accesului neautorizat. Considerentul 49 al GDPR arată că prelucrarea strict necesară pentru securitatea rețelelor și a informațiilor este un interes legitim.

2. Necesitatea

Jurnalele cuprind doar adresa IP, data și ora accesării, pagina accesată, browserul folosit, adică datele fără de care un atac nu poate fi investigat. Ele se șterg automat la sfârșitul termenului de păstrare.

3. Echilibrul și așteptările rezonabile

Vizitatorii se așteaptă, în mod rezonabil, ca un site să păstreze jurnale tehnice pentru securitate. Jurnalele nu se folosesc pentru profilare sau pentru publicitate, iar securitatea site-ului îi protejează și pe vizitatori.

EXEMPLU

4. Garanțiile

- Jurnalele se șterg automat după 90 de zile.
- Conturile de administrare au parole unice și sunt închise când persoana pleacă.
- Persoana se poate opune prelucrării, potrivit art. 21 GDPR și procedurii DP-07.

5. Concluzia

Interesul legitim al societății prevalează, cu garanțiile de mai sus. Prelucrarea se poate face pe temeiul art. 6 alin. (1) lit. f) GDPR.

Evaluat de Ion Popescu, la data de _____.

Fișa 4. Newsletterul și ofertele prin e-mail

Scopul	Trimiterea de oferte și noutăți prin e-mail.
Persoanele vizate	abonați la newsletter; clienți care au cumpărat produse similare
Datele	adresă de e-mail; nume, dacă este dat; data și sursa abonării; dezabonarea
Temeiul	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate), pentru abonați, cerut de art. 12 alin. (1) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice; pentru ofertele către clienții existenți, art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului), în condițiile excepției din art. 12 alin. (2) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice
Durata de păstrare	până la dezabonare, termen stabilit de operator

1. Interesul legitim

Societatea trimite clienților existenți oferte pentru produse similare celor cumpărate, în condițiile excepției din art. 12 alin. (2) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice. Considerentul 47 al GDPR arată că prelucrarea în scopul marketingului direct poate fi realizată în interesul legitim al operatorului.

EXEMPLU

2. Necesitatea

Se folosește doar adresa de e-mail primită de la client la cumpărare și categoria produselor cumpărate, pentru a alege oferte similare. Abonații la newsletter primesc mesaje pe baza consimțământului, nu a acestei fișe.

3. Echilibrul și așteptările rezonabile

Clientul a fost informat la colectarea adresei că poate primi astfel de oferte și a putut refuza simplu și gratuit. Un client care a cumpărat un produs se așteaptă, în mod rezonabil, la oferte pentru produse similare de la același magazin. Fiecare mesaj are o modalitate simplă de dezabonare.

4. Garanțiile

- Fiecare mesaj are un link de dezabonare gratuită.
- Data și sursa abonării se păstrează ca dovadă a acordului.
- Clientul se poate opune simplu și gratuit, la colectarea adresei și la fiecare mesaj; opoziția față de marketingul direct se respectă întotdeauna (art. 21 alin. (3) GDPR).

5. Concluzia

Interesul legitim al societății prevalează, cu garanțiile de mai sus. Prelucrarea se poate face pe temeiul art. 6 alin. (1) lit. f) GDPR.

Evaluat de Ion Popescu, la data de _____.

Fișa 5. Recenziile produselor

Scopul	Colectarea, verificarea și publicarea recenziilor.
Persoanele vizate	clienți care scriu recenzii
Datele	numele afișat, adresă de e-mail, textul și nota recenziei, comanda verificată
Temeiul	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate), pentru publicare; art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului), pentru verificarea recenziilor
Durata de păstrare	cât timp recenzia este publicată

1. Interesul legitim

Societatea verifică dacă recenziile provin de la clienți care au cumpărat produsul, ca informațiile pentru ceilalți cumpărători să fie corecte. Modul de verificare se comunică, potrivit art. 7 alin. (6) și anexa nr. 1 pct. 26 și 27 din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor, modificată prin Ordonanța de urgență a Guvernului nr. 58/2022.

2. Necesitatea

Verificarea compară adresa de e-mail a autorului cu comenzile. Nu se publică adresa de e-mail și nici detaliile comenzii.

3. Echilibrul și așteptările rezonabile

Autorul unei recenzii se așteaptă, în mod rezonabil, ca magazinul să verifice dacă a cumpărat produsul. Publicarea recenziei se face pe baza consimțământului, iar autorul poate cere oricând ștergerea recenziei.

4. Garanțiile

- Adresa de e-mail nu se publică.
- Clientul își poate șterge recenzia printr-o cerere.
- Persoana se poate opune prelucrării, potrivit art. 21 GDPR și procedurii DP-07.

5. Concluzia

Interesul legitim al societății prevalează, cu garanțiile de mai sus. Prelucrarea se poate face pe temeiul art. 6 alin. (1) lit. f) GDPR.

Evaluat de Ion Popescu, la data de _____.

Versiunea 2026.1 din 16.11.2026.

Aprobat,
Administrator
Nume: _____
Semnătura: _____
Ștampila (opțional)

EXEMPLU

Politica de confidențialitate

Această politică arată ce date personale prelucrăm când vizitați site-ul magazin.example, când comandați de la noi sau când ne scrieți, de ce le prelucrăm, cât timp le păstrăm și ce drepturi aveți. Informațiile sunt cele cerute de art. 13 și art. 14 din Regulamentul (UE) 2016/679 (Regulamentul general privind protecția datelor, „GDPR”).

Cine suntem

Operatorul datelor este Exemplu Magazin Online SRL, CUI 00000000, Nr. Reg. Com. J00/0000/2026, cu sediul în Str. Exemplului nr. 1, București. În această politică, „noi” înseamnă Exemplu Magazin Online SRL.

Pentru orice întrebare sau cerere privind datele dvs. ne puteți contacta la adresa de e-mail gdpr@magazin.example sau la telefon 0700000000, ori prin poștă, la sediul din Str. Exemplului nr. 1, București.

Persoana care se ocupă în firma noastră de protecția datelor este Ion Popescu, Administrator. Nu am desemnat un responsabil cu protecția datelor (DPO) în sensul art. 37 GDPR.

Ce date prelucrăm și de ce

Pentru fiecare activitate de mai jos arătăm scopul, datele, temeiul legal și durata de păstrare. Când temeiul este interesul nostru legitim (art. 6 alin. (1) lit. f) GDPR), interesul este chiar scopul descris la activitatea respectivă. Vă puteți opune acestei prelucrări, potrivit art. 21 GDPR. Când temeiul este consimțământul, îl puteți retrage oricând, fără să afecteze prelucrarea făcută până atunci (art. 7 alin. (3) GDPR).

EXEMPLU

Cererile persoanelor vizate

Scopul	Primirea cererilor privind drepturile din GDPR, răspunsul la ele și dovada răspunsului.
Datele	nume și prenume, date de contact, conținutul cererii și al răspunsului
Temeiul	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale), art. 12-22 GDPR
Durata de păstrare	3 ani de la răspuns. Temeiul termenului: art. 2517 din Codul civil

Mesajele primite prin formularul de contact și prin e-mail

Scopul	Răspunsul la întrebările vizitatorilor și ale clienților.
Datele	nume; adresă de e-mail; telefon, dacă este dat; conținutul mesajului
Temeiul	art. 6 alin. (1) lit. f) GDPR (interesul nostru legitim)
Durata de păstrare	12 luni de la ultimul mesaj, termen stabilit de noi

Comenzile și livrarea

Scopul	Preluarea comenzilor, confirmarea lor și livrarea produselor.

Datele	nume și prenume, adresa de livrare, telefon, adresă de e-mail, produsele comandate și valoarea comenzii
Temeiul	art. 6 alin. (1) lit. b) GDPR (executarea contractului)
Durata de păstrare	3 ani de la livrare. Temeiul termenului: art. 2517 din Codul civil

Facturarea

Scopul	Emiterea facturilor și transmiterea lor în sistemul RO e-Factura.
Datele	nume și prenume sau denumire; adresă; produsele facturate și valoarea; codul fiscal, doar pentru clienții care au unul
Temeiul	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale)
Durata de păstrare	5 ani de la 1 iulie a anului următor încheierii exercițiului financiar. Temeiul termenului: art. 25 din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare

Contul de client

Scopul	Crearea și administrarea contului, istoricul comenzilor și adresele salvate.
Datele	nume și prenume; adresă de e-mail; parola, stocată criptat; adresele salvate; istoricul comenzilor
Temeiul	art. 6 alin. (1) lit. b) GDPR (executarea contractului)
Durata de păstrare	până la ștergerea contului sau după 36 de luni de inactivitate, termen stabilit de noi

EXEMPLU

Retururile

Scopul	Primirea produselor returnate în termenul de retragere și rambursarea banilor.
Datele	nume și prenume, date de contact, comanda și produsele returnate, contul bancar pentru rambursare
Temeiul	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale); art. 6 alin. (1) lit. b) GDPR (executarea contractului)
Durata de păstrare	3 ani de la rambursare. Temeiul termenului: art. 2517 din Codul civil

Garanția și reclamațiile

Scopul	Soluționarea reclamațiilor privind neconformitatea produselor.
Datele	nume și prenume, date de contact, produsul și descrierea problemei, fotografiile trimise de client
Temeiul	art. 6 alin. (1) lit. c) GDPR (îndeplinirea unei obligații legale)
Durata de păstrare	durata garanției și 3 ani după încetarea ei. Temeiul termenului: art. 9 alin. (1) din Ordonanța de urgență a Guvernului nr. 140/2021 privind anumite aspecte referitoare la contractele de vânzare de bunuri; art. 2517 din Codul civil

Plățile online

Scopul	Încasarea plăților cu cardul sau în rate.
Datele	nume, valoarea plății, starea tranzacției, tokenul cardului sau ultimele 4 cifre
Temeiul	art. 6 alin. (1) lit. b) GDPR (executarea contractului)
Durata de păstrare	durata tranzacției și a eventualelor contestații, termen stabilit de noi

Prevenirea fraudei la plată

Scopul	Identificarea comenzilor și a plăților suspecte.
Datele	adresa IP, datele comenzii, rezultatul verificării făcute de procesatorul de plăți
Temeiul	art. 6 alin. (1) lit. f) GDPR (interesul nostru legitim)
Durata de păstrare	12 luni de la comandă, termen stabilit de noi

Jurnalele serverului și securitatea site-ului

Scopul	Funcționarea site-ului, depistarea erorilor și a atacurilor.
Datele	adresa IP, data și ora accesării, pagina accesată, browserul folosit
Temeiul	art. 6 alin. (1) lit. f) GDPR (interesul nostru legitim)
Durata de păstrare	90 de zile, termen stabilit de noi

EXEMPLU

Măsurarea audienței site-ului

Scopul	Statistici despre folosirea site-ului, cu acordul vizitatorului.
Datele	identificatorii din cookie-uri, paginile vizitate, dispozitivul și browserul, țara sau orașul aproximativ
Temeiul	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate), cerut de art. 4 alin. (5) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice
Durata de păstrare	durata fiecărui cookie, afișată în politica de cookie-uri sau în panoul „Setări cookie-uri”, termen stabilit de noi

Publicitatea online și măsurarea conversiilor

Scopul	Afișarea de reclame și măsurarea vânzărilor obținute din reclame.
Datele	identificatorii din cookie-uri, paginile vizitate, produsele adăugate în coș, comenzile finalizate
Temeiul	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate); operator asociat cu platforma de publicitate, conform art. 26 GDPR
Durata de păstrare	durata fiecărui cookie, afișată în politica de cookie-uri sau în panoul „Setări cookie-uri”, termen stabilit de noi

Newsletterul și ofertele prin e-mail

Scopul	Trimiterea de oferte și noutăți prin e-mail.

Datele	adresă de e-mail; nume, dacă este dat; data și sursa abonării; dezabonarea
Temeiul	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate), pentru abonați, cerut de art. 12 alin. (1) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice; pentru ofertele către clienții existenți, art. 6 alin. (1) lit. f) GDPR (interesul nostru legitim), în condițiile excepției din art. 12 alin. (2) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice
Durata de păstrare	până la dezabonare, termen stabilit de noi

Recenziile produselor

Scopul	Colectarea, verificarea și publicarea recenziilor.
Datele	numele afișat, adresă de e-mail, textul și nota recenziei, comanda verificată
Temeiul	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate), pentru publicare; art. 6 alin. (1) lit. f) GDPR (interesul nostru legitim), pentru verificarea recenziilor
Durata de păstrare	cât timp recenzia este publicată

Datele marcate ca obligatorii în formularul de comandă sunt necesare pentru încheierea și executarea contractului, iar datele de facturare sunt cerute de lege. Fără ele nu putem prelua și livra comanda. Celelalte date ni le dați doar dacă doriți.

EXEMPLU

Cui transmitem datele

Transmitem datele doar destinatarilor de care avem nevoie pentru activitățile de mai sus și doar datele necesare fiecăruia.

Furnizorii de servicii

Furnizorii care ne ajută să livrăm comenzile, să încasăm plățile, să emitem facturile și să ținem site-ul în funcțiune. Cei care prelucrează datele în numele nostru o fac pe bază de contract, potrivit art. 28 GDPR. Furnizorii al căror rol depinde de termenii lor (de exemplu curierii și procesatorii de plăți) pot prelucra unele date și în nume propriu, potrivit propriilor politici de confidențialitate.

- Agenția Exemplu Web SRL, administrarea tehnică a site-ului;
- Contabilitate Exemplu SRL, contabilitate externă, pentru ținerea contabilității;
- Delivery Solutions S.A., servicii de curierat (Sameday), pentru livrarea comenzilor;
- FAN Courier Express S.R.L., servicii de curierat (FAN Courier), pentru livrarea comenzilor;
- Google Cloud EMEA Limited, e-mail și stocare în cloud (Google Workspace), pentru e-mailul firmei și stocarea documentelor în cloud;
- Google Ireland Limited, Google Analytics 4, pentru măsurarea audienței site-ului;
- Hostico, găzduirea site-ului;
- Intelligent IT S.R.L., program de facturare online (SmartBill), pentru emiterea facturilor;
- NETOPIA Financial Services S.A., procesator de plăți online (NETOPIA Payments), pentru procesarea plăților cu cardul;
- The Rocket Science Group LLC, platformă de newsletter (Mailchimp), pentru trimiterea newsletterului.

Platformele de publicitate

Pentru pixelii publicitari suntem operatori asociați cu platformele de mai jos. Detaliile sunt în secțiunea despre publicitatea online.

- Meta Platforms Ireland Limited, Meta Pixel.

Autoritățile publice

- Agenția Națională de Administrare Fiscală (ANAF), pentru îndeplinirea obligațiilor fiscale;
- Instanțele și autoritățile publice, la cerere legală, pentru răspunsul la solicitările legale ale autorităților.

Transferurile în afara Spațiului Economic European

Transferăm date în afara Spațiului Economic European (SEE) către următorii destinatari: The Rocket Science Group LLC (Statele Unite ale Americii), pe baza Cadrului UE-SUA privind protecția datelor (DPF).

Potrivit termenilor publicați de ei, unii furnizori stabiliți în SEE transferă date mai departe, în afara SEE: Delivery Solutions S.A., pe baza clauzelor contractuale standard (art. 46 alin. (2) lit. c) GDPR); Google Cloud EMEA Limited, pe baza clauzelor contractuale standard (art. 46 alin. (2) lit. c) GDPR); Google Ireland Limited, pe baza Cadrului UE-SUA privind protecția datelor (DPF); NETOPIA Financial Services S.A., pe baza clauzelor contractuale standard (art. 46 alin. (2) lit. c) GDPR); Meta Platforms Ireland Limited, pe baza Cadrului UE-SUA privind protecția datelor (DPF).

Unii furnizori pot prelucra date în afara Spațiului Economic European; în acest caz folosim o decizie de adecvare (art. 45 GDPR) sau garanțiile prevăzute la art. 46 GDPR.

Ne puteți cere informații despre garanțiile folosite și o copie a lor, la datele de contact de mai sus.

EXEMPLU

Deciziile automate

Nu luăm decizii bazate exclusiv pe prelucrare automată care să vă afecteze în mod semnificativ.

Publicitatea online și operatorii asociați

Dacă acceptați cookie-urile de marketing, pe site se încarcă pixelii unor platforme de publicitate. Pixelii transmit platformelor date despre navigarea pe site, de exemplu paginile vizitate, produsele adăugate în coș și comenzile finalizate. Pentru colectarea acestor date și transmiterea lor către platformă, noi și platforma suntem operatori asociați în sensul art. 26 GDPR (a se vedea Hotărârea Curții de Justiție a Uniunii Europene din 29 iulie 2019, cauza C-40/17, Fashion ID). Pentru ce face platforma ulterior cu datele, de exemplu crearea profilurilor de publicitate, platforma este singurul operator.

Noi răspundem de informarea dvs. și de obținerea acordului pe site. Vă puteți exercita drepturile atât față de noi, cât și față de platformă (art. 26 alin. (3) GDPR). Ce prevede înțelegerea cu fiecare platformă:

- Meta Platforms Ireland Limited, pentru Meta Pixel. Meta a publicat un acord de operator asociat (Controller Addendum). Potrivit acestuia, Meta răspunde la cererile privind drepturile de la art. 15–20 GDPR pentru datele pe care le stochează după transmitere. Politica de confidențialitate a platformei: https://www.facebook.com/privacy/policy/

Vă puteți retrage oricând acordul din panoul „Setări cookie-uri” de pe site.

Drepturile dvs.

În legătură cu datele dvs. personale aveți următoarele drepturi:

- dreptul de acces: să aflați dacă vă prelucrăm datele și să primiți o copie a lor (art. 15 GDPR);
- dreptul la rectificare: să corectăm datele greșite sau incomplete (art. 16 GDPR);
- dreptul la ștergere: să ștergem datele, în condițiile art. 17 GDPR, de exemplu când nu mai sunt necesare sau când vă retrageți consimțământul;
- dreptul la restricționarea prelucrării, în condițiile art. 18 GDPR;
- dreptul la portabilitate: să primiți datele pe care ni le-ați dat, într-un format structurat, sau să le transmitem altui operator, în condițiile art. 20 GDPR;
- dreptul de a vă opune, din motive legate de situația dvs. particulară, prelucrării bazate pe interesul nostru legitim (art. 21 alin. (1) GDPR);
- **dreptul de a vă opune oricând, fără să ne dați un motiv, prelucrării datelor în scop de marketing direct** (art. 21 alin. (2) GDPR);
- dreptul de a vă retrage consimțământul, oricând, pentru prelucrările bazate pe consimțământ (art. 7 alin. (3) GDPR).

Pentru a vă exercita drepturile, scrieți-ne la datele de contact din secțiunea „Cine suntem”. Răspundem gratuit, cu excepțiile de la art. 12 alin. (5) GDPR, fără întârziere și în cel mult o lună de la primirea cererii. Termenul se poate prelungi cu încă două luni pentru cereri complexe sau numeroase, caz în care vă anunțăm în prima lună (art. 12 alin. (3) GDPR). Înainte de a răspunde, putem cere informații care să ne confirme identitatea dvs.

Dacă considerați că vă prelucrăm datele cu încălcarea legii, puteți depune o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), www.dataprotection.ro, potrivit art. 77 GDPR, sau vă puteți adresa instanței, potrivit art. 79 GDPR.

EXEMPLU

Cookie-urile

Folosim cookie-uri și tehnologii asemănătoare. Ce cookie-uri folosim, pentru ce și cât timp, aflați din Politica de cookie-uri publicată pe site. Alegerile privind cookie-urile le puteți schimba oricând din panoul „Setări cookie-uri”.

Copiii

Nu ne adresăm minorilor sub 16 ani și nu le cerem date personale. Dacă aflați că un minor sub 16 ani ne-a trimis date, scrieți-ne, iar noi le vom șterge.

Modificarea politicii

Actualizăm această politică atunci când se schimbă datele pe care le prelucrăm, scopurile sau furnizorii. Versiunea în vigoare este cea publicată pe site.

Data ultimei actualizări: 16.11.2026.

Politica de cookie-uri

Această politică arată ce cookie-uri folosește site-ul magazin.example, operat de Exemplu Magazin Online SRL, CUI 00000000, și cum vă puteți alege sau schimba opțiunile.

Ce sunt cookie-urile

Cookie-urile sunt fișiere mici de text pe care un site le salvează în browserul dvs. când îl vizitați. La vizitele următoare, site-ul le citește din nou. Unele sunt necesare pentru ca site-ul să funcționeze, de exemplu ca să păstreze produsele din coș. Altele ajută la măsurarea folosirii site-ului sau la afișarea de reclame. Aceleași reguli se aplică tehnologiilor asemănătoare, precum pixelii sau stocarea locală din browser.

Potrivit art. 4 alin. (5) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, salvarea informațiilor în echipamentul dvs. și accesul la ele se fac numai cu acordul dvs., după ce ați fost informat. Cookie-urile necesare funcționării site-ului nu cer acordul, pentru că fără ele site-ul nu vă poate furniza serviciul pe care l-ați cerut. Pe celelalte le folosim doar dacă le acceptați.

Categoriile de cookie-uri

Panoul „Setări cookie-uri” împarte cookie-urile în patru categorii:

- Necesare: asigură navigarea, coșul de cumpărături, securitatea site-ului și memorarea alegerii dvs. privind cookie-urile. Sunt mereu active.
- Preferințe: rețin setări precum limba sau regiunea, ca să nu le alegeți la fiecare vizită.
- Statistici: arată cum este folosit site-ul, de exemplu paginile vizitate și timpul petrecut pe ele.
- Marketing: permit afișarea de reclame și măsurarea rezultatelor lor, inclusiv pe alte site-uri și rețele sociale.

EXEMPLU

Cookie-urile de preferințe, de statistici și de marketing se activează doar după ce le acceptați.

Cookie-urile folosite pe site

Tabelul de mai jos arată cookie-urile găsite pe site la ultima verificare. Unele cookie-uri aparțin altor firme, trecute în coloana Furnizor, care le folosesc și potrivit propriilor politici de confidențialitate.

Nume	Furnizor	Scop	Durată	Categorie
woocommerce_cart_hash	WooCommerce	Păstrează conținutul coșului.	sesiune	Necesare
_ga	Google	Deosebește vizitatorii.	2 ani	Statistici
_fbp	Meta	Măsoară conversiile din reclame.	3 luni	Marketing

Cookie-urile, pe categorii, le puteți vedea și în panoul „Setări cookie-uri” de pe site.

Cum vă dați sau vă retrageți acordul

La prima vizită, bannerul de cookie-uri vă lasă să acceptați toate cookie-urile, să le refuzați pe cele care nu sunt necesare sau să alegeți pe categorii. Refuzul este la fel de simplu ca acceptarea.

Vă puteți schimba alegerea oricând, din panoul „Setări cookie-uri”: debifați categoriile pe care nu le mai acceptați și salvați. Retragerea acordului este la fel de simplă ca exprimarea lui și nu afectează folosirea cookie-urilor de până atunci.

Setările browserului

Puteți șterge cookie-urile deja salvate și puteți bloca cookie-urile din setările browserului, de obicei în secțiunea despre confidențialitate sau securitate. Browserele principale (Chrome, Firefox, Safari, Edge) au această opțiune. Dacă blocați toate cookie-urile, inclusiv pe cele necesare, unele părți ale site-ului, precum coșul sau finalizarea comenzii, pot să nu funcționeze.

Google Consent Mode

Folosim Google Consent Mode: etichetele Google de pe site primesc alegerea pe care ați făcut-o în bannerul de cookie-uri și o respectă. Fără acordul dvs., etichetele Google nu salvează cookie-uri de statistici sau de marketing. În funcție de configurare, ele pot transmite către Google semnale fără cookie-uri, de exemplu că o pagină a fost încărcată și ce alegere ați făcut privind cookie-urile.

Mai multe informații

Ce date personale prelucrăm, cui le transmitem și ce drepturi aveți aflați din Politica de confidențialitate publicată pe site. Pentru întrebări ne puteți scrie la adresa gdpr@magazin.example.

Data ultimei actualizări: 16.11.2026.

EXEMPLU

Texte pentru site și formulare

Textele din casete sunt gata de copiat pe site, magazin.example. Fiecare trimite la Politica de confidențialitate sau la Politica de cookie-uri, care se publică pe site ca pagini separate, cu link în subsolul fiecărei pagini. Deasupra fiecărei casete scrie unde se pune textul.

Bannerul de cookie-uri

Primul strat al bannerului, adică mesajul afișat la prima vizită:

> **Folosim cookie-uri**
>
> Folosim cookie-uri necesare pentru funcționarea site-ului și, cu acordul dvs., cookie-uri de statistici și de marketing. Puteți accepta toate cookie-urile, le puteți refuza pe cele care nu sunt necesare sau puteți alege din setări. Vă puteți schimba alegerea oricând, din „Setări cookie-uri”. Detalii în Politica de cookie-uri.
>
> Butoanele: „Accept toate”, „Refuz toate”, „Setări”.

Butonul „Refuz toate” stă pe primul strat, la fel de vizibil ca „Accept toate”. Cookie-urile care nu sunt necesare pornesc doar după acord, iar linkul „Setări cookie-uri” rămâne disponibil pe fiecare pagină, pentru schimbarea alegerii.

EXEMPLU

Formularul de comandă

Lângă butonul de finalizare a comenzii:

> Folosim datele din acest formular pentru a prelua, a livra și a factura comanda. Le transmitem doar furnizorilor care ne ajută să livrăm comanda și să încasăm plata. Detalii în Politica de confidențialitate.

Crearea contului

Pe pagina de înregistrare, lângă butonul de creare a contului:

> Contul păstrează datele dvs. de livrare și istoricul comenzilor, ca să comandați mai ușor data viitoare. Îl puteți șterge oricând din pagina contului sau printr-o cerere către noi. Dacă nu vă conectați la cont timp de 36 de luni, îl ștergem. Detalii în Politica de confidențialitate.

Abonarea la newsletter și ofertele prin e-mail către clienții existenți

În formularul de abonare și, dacă doriți, în formularul de comandă. Căsuța rămâne nebifată: abonarea pornește doar după ce vizitatorul o bifează (art. 12 alin. (1) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice). Data și sursa abonării se păstrează ca dovadă a acordului.

> ☐ Vreau să primesc pe e-mail newsletterul Exemplu Magazin Online SRL, cu oferte și noutăți.

> Mă pot dezabona oricând, din linkul din fiecare mesaj. Detalii în Politica de confidențialitate.

În formularul de comandă, pentru ofertele prin e-mail către clienții existenți. Excepția din art. 12 alin. (2) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice cere ca clientul să se poată opune simplu și gratuit chiar la colectarea adresei, iar fiecare mesaj să aibă link de dezabonare. Căsuța rămâne nebifată; clientul o bifează doar dacă nu dorește ofertele:

> ☐ Nu vreau să primesc pe e-mail oferte pentru produse similare celor cumpărate.

Dacă în formularul de comandă apar ambele căsuțe, nu le puneți una lângă alta fără explicație: prima cere acordul pentru newsletter, a doua permite refuzul ofertelor pentru clienții existenți. Puneți fiecare căsuță sub un titlu scurt, de exemplu „Newsletter” și „Oferte pentru clienți”.

Formularul de contact

Sub formularul de contact:

> Folosim datele din acest formular doar pentru a vă răspunde la mesaj. Detalii în Politica de confidențialitate.

Clauza de date personale pentru termeni și condiții

Clauza se adaugă ca secțiune separată în termenii și condițiile magazinului:

> **Datele personale**
>
> Exemplu Magazin Online SRL prelucrează datele personale ale clienților pentru încheierea și executarea contractului și pentru obligațiile legale, de exemplu facturarea, în conformitate cu Regulamentul (UE) 2016/679. Ofertele prin e-mail se trimit doar cu acordul clientului sau, pentru clienții existenți, în condițiile permise de lege, cu posibilitatea de a refuza oricând. Ce date prelucrăm, în ce scop, cât timp le păstrăm, cui le transmitem și ce drepturi aveți este descris în Politica de confidențialitate, publicată pe site. Pentru întrebări și pentru exercitarea drepturilor ne puteți scrie la adresa gdpr@magazin.example.

Termenii și condițiile, formularul de retragere și politica de retur nu fac parte din acest dosar; pentru ele recomandăm consultanță.

Linkurile de afișat pe site

- ☐ Politica de confidențialitate și Politica de cookie-uri, cu link în subsolul fiecărei pagini, în banner și lângă formularele care colectează date (art. 13 GDPR și art. 4 alin. (5) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice).
- ☐ Pictograma SAL, de 250 x 50 pixeli, pe prima pagină a site-ului, cu link către https://reclamatiisal.anpc.ro, potrivit art. 2 din Ordinul președintelui Autorității Naționale pentru Protecția Consumatorilor nr. 449/2022 privind unele măsuri de informare a consumatorilor cu privire la soluționarea alternativă a litigiilor, modificat prin Ordinul nr. 270/2026. Ordinul nu stabilește locul exact pe pagină; o puteți pune, de exemplu, în subsol.

EXEMPLU

- ☐ Recomandăm și un link către site-ul ANPC, https://anpc.ro, lângă pictograma SAL. Ordinul de mai sus cere doar pictograma SAL.
- Linkul către platforma europeană de soluționare online a litigiilor (SOL) nu se mai cere: platforma a fost desființată (Regulamentul (UE) 2024/3228 al Parlamentului European și al Consiliului din 19 decembrie 2024 de abrogare a Regulamentului (UE) nr. 524/2013). Dacă îl aveți încă pe site, îl puteți scoate.

Minimizarea datelor la checkout

Formularul de comandă cere doar datele necesare comenzii:

- ☐ Nu cereți obligatoriu un titlu de politețe (Dl., Dna.).
- ☐ Nu cereți data nașterii dacă nu aveți nevoie de ea pentru comandă.
- ☐ Nu cereți CNP-ul. Pentru factura unei persoane fizice fără cod fiscal se folosește codul format din 13 cifre de zero, potrivit art. 10^{1} alin. (3) din Ordonanța de urgență a Guvernului nr. 120/2021 privind administrarea, funcționarea și implementarea sistemului național privind factura electronică RO e-Factura și factura electronică în România.
- ☐ Telefonul se cere pentru curier și se folosește doar pentru livrare și pentru întrebări despre comandă.
- ☐ Câmpurile pentru firmă (denumirea și codul fiscal) apar doar când clientul cere factură pe firmă.
- ☐ Căsuțele pentru newsletter și pentru alte mesaje comerciale sunt nebifate implicit.

EXEMPLU

Marketing direct prin e-mail

> Regulile de mai jos se aplică oricărui mesaj comercial trimis de Exemplu Magazin Online SRL prin e-mail: newsletter, oferte, reduceri sau anunțuri de produse noi. Mesajele strict legate de o comandă (confirmarea, factura, livrarea) nu sunt mesaje comerciale și nu intră aici.

Scopul	Trimiterea de oferte și noutăți prin e-mail.
Persoanele vizate	abonați la newsletter; clienți care au cumpărat produse similare
Datele	adresă de e-mail; nume, dacă este dat; data și sursa abonării; dezabonarea
Temeiul	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate), pentru abonați, cerut de art. 12 alin. (1) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice; pentru ofertele către clienții existenți, art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului), în condițiile excepției din art. 12 alin. (2) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice
Durata de păstrare	până la dezabonare, termen stabilit de operator

EXEMPLU

1. Cui trimitem mesaje comerciale

Abonații la newsletter

Mesajele comerciale prin e-mail se trimit doar persoanelor care și-au dat acordul expres în prealabil, potrivit art. 12 alin. (1) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice. Acordul se cere cu o căsuță nebifată, separată de acceptarea termenilor și condițiilor, cu textul din DP-M3.

Recomandăm abonarea cu dublă confirmare: după abonare, platforma trimite un e-mail cu un link de confirmare, iar adresa intră în listă doar după ce persoana deschide linkul. Dubla confirmare arată că adresa aparține celui care s-a abonat și împiedică abonarea unei persoane de către altcineva.

Clienții existenți (excepția pentru produse similare)

Fără abonare separată, societatea poate trimite oferte clienților care au cumpărat deja, numai în condițiile excepției din art. 12 alin. (2) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice:

- adresa de e-mail a fost primită direct de la client, cu ocazia unei vânzări;
- ofertele privesc produse sau servicii similare celor cumpărate, vândute de Exemplu Magazin Online SRL;
- clientul a putut refuza simplu și gratuit chiar la colectarea adresei, prin căsuța de refuz din formularul de comandă (DP-M3);
- fiecare mesaj îi permite clientului să refuze, simplu și gratuit, mesajele următoare.

Dacă una dintre condiții lipsește, de exemplu adresa vine de la un marketplace sau ofertele privesc alte tipuri de produse, mesajul se trimite doar cu acordul expres al persoanei. Evaluarea interesului legitim pentru aceste oferte este fișa 4 din DP-16.

Societatea nu cumpără și nu închiriază liste de adrese și nu trimite mesaje comerciale la adrese găsite pe internet sau primite de la parteneri.

2. Dezabonarea

- Fiecare mesaj comercial are, la vedere, un link de dezabonare care funcționează fără autentificare și fără alte date cerute persoanei.
- Platforma de trimitere aplică dezabonarea din link imediat. O cerere de dezabonare primită pe altă cale (răspuns la mesaj, e-mail, telefon) se aplică în cel mult 2 zile lucrătoare, termen stabilit de societate.
- Adresa dezabonată rămâne doar în lista de excludere a platformei, ca să nu primească din nou mesaje. Lista de excludere nu se folosește în alt scop.
- Opoziția față de marketingul direct se respectă întotdeauna, fără justificare (art. 21 alin. (2) și (3) GDPR), iar retragerea acordului este la fel de simplă ca acordarea lui (art. 7 alin. (3) GDPR).

3. Dovada consimțământului

Societatea trebuie să poată demonstra că persoana și-a dat acordul (art. 7 alin. (1) GDPR). Pentru fiecare abonat se păstrează:

- adresa de e-mail;
- data și ora abonării și, pentru abonarea cu dublă confirmare, data și ora confirmării;
- sursa abonării: formularul și pagina din care s-a abonat persoana;
- textul căsuței de acord din momentul abonării, cu versiunea lui;
- data dezabonării, când este cazul.

EXEMPLU

Majoritatea platformelor de newsletter înregistrează automat aceste date. Responsabilul intern verifică o dată pe an că exportul listei le cuprinde și păstrează o copie a textelor de acord folosite. După dezabonare, dovada se păstrează doar cât este necesar pentru apărarea societății în cazul unei plângeri, cel mult în termenul general de prescripție din art. 2517 din Codul civil.

Pentru ofertele către clienții existenți se păstrează data comenzii din care provine adresa, textul căsuței de refuz din formularul de comandă și data refuzului, când clientul a refuzat ofertele la comandă sau ulterior.

4. Pixelii de urmărire din e-mailuri

Un pixel de urmărire sau un link cu identificator personal arată dacă și când persoana a deschis mesajul sau a accesat un link. Ghidul EDPB 2/2023 privind domeniul tehnic de aplicare a art. 5 alin. (3) din Directiva 2002/58/CE, versiunea 2.0, adoptată la 7 octombrie 2024 arată că această tehnică intră sub regula accesului la informațiile din echipamentul utilizatorului, deci cere acordul persoanei.

Potrivit răspunsurilor, societatea nu măsoară deschiderea e-mailurilor. Multe platforme activează implicit măsurarea deschiderilor și a clicurilor: dezactivați-o din setările contului. Dacă doriți să o folosiți, cereți mai întâi acordul separat al abonaților și actualizați acest dosar.

5. Platforma de trimitere

Mesajele se trimit prin The Rocket Science Group LLC. Platforma este persoană împuternicită (art. 28 GDPR); acordul ei de prelucrare și garanția transferului sunt în lista destinatarilor (DP-14).

Lista de abonați se folosește doar pentru mesajele Exemplu Magazin Online SRL. Ea nu se transmite altor firme și nu se combină cu date din alte surse fără o informare prealabilă a abonaților.

Versiunea 2026.1 din 16.11.2026.

EXEMPLU

Pixeli publicitari

> Pixelii publicitari sunt scripturi ale platformelor de publicitate, puse pe site ca să măsoare vânzările obținute din reclame și să arate reclame vizitatorilor. Documentul arată cum împart Exemplu Magazin Online SRL și fiecare platformă răspunderea pentru datele colectate, ce acord se acceptă cu fiecare platformă și cum se încarcă pixelii.

Scopul	Afișarea de reclame și măsurarea vânzărilor obținute din reclame.
Persoanele vizate	vizitatori ai site-ului care acceptă cookie-urile de marketing
Datele	identificatorii din cookie-uri, paginile vizitate, produsele adăugate în coș, comenzile finalizate
Temeiul	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate); operator asociat cu platforma de publicitate, conform art. 26 GDPR
Durata de păstrare	durata fiecărui cookie, afișată în politica de cookie-uri sau în panoul „Setări cookie-uri”, termen stabilit de operator

Pixelii de pe site

- Meta Platforms Ireland Limited: Meta Pixel.

EXEMPLU

Operatorii asociați

Pentru colectarea datelor prin pixel și transmiterea lor către platformă, societatea și platforma stabilesc împreună scopurile și mijloacele prelucrării, deci sunt operatori asociați în sensul art. 26 GDPR. Așa a decis Curtea de Justiție pentru un modul inserat pe site de un magazin online (Hotărârea Curții de Justiție a Uniunii Europene din 29 iulie 2019, cauza C-40/17, Fashion ID). Pentru ce face platforma ulterior cu datele, de exemplu crearea profilurilor de publicitate, platforma este singurul operator.

Ce revine societății:

- să obțină acordul vizitatorului înainte ca pixelul să se încarce, potrivit art. 4 alin. (5) din Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice;
- să informeze vizitatorii despre pixeli și despre platforme, în politica de confidențialitate și în politica de cookie-uri;
- să pună la dispoziția vizitatorilor esența înțelegerii cu fiecare platformă (art. 26 alin. (2) GDPR);
- să răspundă cererilor primite de la vizitatori și, pentru datele aflate deja la platformă, să le arate cum se pot adresa platformei. Persoanele își pot exercita drepturile față de oricare dintre operatorii asociați (art. 26 alin. (3) GDPR).

Acordurile de operator asociat

Platformele de mai jos au publicat un acord de operator asociat. Acordul se acceptă din contul de publicitate al societății, înainte de folosirea pixelului. Păstrați la dosar o copie a acordului sau o captură de ecran cu data acceptării.

- Meta Platforms Ireland Limited (Meta Pixel). Meta a publicat un acord de operator asociat (Controller Addendum). Potrivit acestuia, Meta răspunde la cererile privind drepturile de la art. 15–20 GDPR pentru datele pe care le stochează după transmitere. Acordul: https://www.facebook.com/legal/controller_addendum

Încărcarea pixelilor doar după acord

- Pixelii se încarcă doar după ce vizitatorul acceptă cookie-urile de marketing în banner. Până atunci, bannerul blochează scripturile lor.
- Dacă vizitatorul își retrage acordul din panoul „Setări cookie-uri”, pixelii nu se mai încarcă la paginile următoare.
- Verificați funcționarea într-o fereastră privată a browserului, la instalarea bannerului și la fiecare pixel nou: înainte de acord, în lista cookie-urilor din browser nu trebuie să apară cookie-uri de marketing.

Textul pentru politica de confidențialitate și pentru registru

Politica de confidențialitate (DP-M1) și registrul activităților de prelucrare (DP-04) cuprind deja descrierea pixelilor și a operatorilor asociați. Dacă folosiți altă politică de confidențialitate decât DP-M1, includeți în ea textul de mai jos:

> Dacă acceptați cookie-urile de marketing, pe site se încarcă pixelii unor platforme de publicitate. Pixelii transmit platformelor date despre navigarea pe site, de exemplu paginile vizitate, produsele adăugate în coș și comenzile finalizate. Pentru colectarea acestor date și transmiterea lor către platformă, noi și platforma suntem operatori asociați în sensul art. 26 GDPR (a se vedea Hotărârea Curții de Justiție a Uniunii Europene din 29 iulie 2019, cauza C-40/17, Fashion ID). Pentru ce face platforma ulterior cu datele, de exemplu crearea profilurilor de publicitate, platforma este singurul operator.
>
> Noi răspundem de informarea dvs. și de obținerea acordului pe site. Vă puteți exercita drepturile atât față de noi, cât și față de platformă (art. 26 alin. (3) GDPR). Ce prevede înțelegerea cu fiecare platformă:
>
> - Meta Platforms Ireland Limited, pentru Meta Pixel. Meta a publicat un acord de operator asociat (Controller Addendum). Potrivit acestuia, Meta răspunde la cererile privind drepturile de la art. 15–20 GDPR pentru datele pe care le stochează după transmitere. Politica de confidențialitate a platformei: https://www.facebook.com/privacy/policy/
>
> Vă puteți retrage oricând acordul din panoul „Setări cookie-uri” de pe site.

La fiecare pixel nou sau la schimbarea unei platforme, actualizați acest document, politica de confidențialitate, politica de cookie-uri și lista destinatarilor (DP-14).

Versiunea 2026.1 din 16.11.2026.

EXEMPLU

Recenzii

> Recenziile produselor se colectează pe site, cu sistemul propriu al magazinului. Documentul arată ce află autorul recenziei despre datele lui, cum se afișează numele și ce spune societatea despre verificarea recenziilor.

Scopul	Colectarea, verificarea și publicarea recenziilor.
Persoanele vizate	clienți care scriu recenzii
Datele	numele afișat, adresă de e-mail, textul și nota recenziei, comanda verificată
Temeiul	art. 6 alin. (1) lit. a) GDPR (consimțământul persoanei vizate), pentru publicare; art. 6 alin. (1) lit. f) GDPR (interesul legitim al operatorului), pentru verificarea recenziilor
Durata de păstrare	cât timp recenzia este publicată

1. Informarea autorului

Lângă formularul de recenzie se afișează textul:

> Recenzia dvs. se publică pe site cu numele prescurtat, de exemplu „Maria I.”, împreună cu nota și textul scris. Adresa de e-mail nu se publică; o folosim doar ca să verificăm că ați cumpărat produsul. Puteți cere oricând ștergerea recenziei, scriindu-ne la adresa gdpr@magazin.example. Detalii în Politica de confidențialitate.

EXEMPLU

2. Afișarea numelui

- Pe site apare doar prenumele și inițiala numelui, de exemplu „Maria I.”, sau pseudonimul ales de autor.
- Adresa de e-mail, adresa de livrare, telefonul și detaliile comenzii nu se publică.
- Recenziile nu se folosesc în reclame sau în alte materiale cu numele întreg al autorului fără acordul lui separat.

3. Verificarea recenziilor

Potrivit art. 7 alin. (6) și anexa nr. 1 pct. 26 și 27 din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor, modificată prin Ordonanța de urgență a Guvernului nr. 58/2022, un magazin care afișează recenzii trebuie să spună dacă și cum verifică faptul că recenziile provin de la consumatori care au cumpărat sau au folosit produsul. Sunt practici interzise afirmația că recenziile provin de la cumpărători, fără măsuri rezonabile de verificare, publicarea sau comandarea de recenzii false și denaturarea recenziilor.

Societatea verifică recenziile. Recenzia se publică doar dacă adresa de e-mail a autorului corespunde unei comenzi livrate pentru acel produs; sistemul compară adresa cu comenzile, iar recenziile care nu corespund unei comenzi nu se publică. Lângă recenzii, pe pagina produsului, se

afișează textul de mai jos, doar după ce ați confirmat că verificarea se face exact așa. Dacă verificarea se face altfel, adaptați textul ca să descrie metoda reală.

> Recenziile sunt publicate doar de clienți care au cumpărat produsul. Verificăm acest lucru comparând adresa de e-mail a autorului cu comenzile livrate. Publicăm toate recenziile care respectă regulile site-ului, pozitive și negative.

Verificarea se face pe temeiul interesului legitim; evaluarea este fișa 5 din DP-16.

Recenziile negative nu se ascund și nu se șterg pentru că sunt negative. O recenzie se poate refuza doar după reguli publicate pe site, aplicate la fel tuturor, de exemplu limbaj jignitor, date personale ale altor persoane sau conținut fără legătură cu produsul.

E-mailurile prin care se cer recenzii pot fi comunicări comerciale, mai ales dacă au și oferte sau reduceri. Trimiteți-le după regulile pentru marketingul prin e-mail din DP-M4 sau cereți părerea consultantului.

4. Cererile autorilor

Cererea de ștergere sau de corectare a unei recenzii se tratează după procedura DP-07. Recenzia ștearsă dispare de pe site.

Versiunea 2026.1 din 16.11.2026.

EXEMPLU