

CHECKLIST-URI OPERAȚIONALE privind protecția datelor cu caracter personal

Checklisturile sunt destinate verificării interne a conformității cu cerințele privind protecția datelor cu caracter personal. Pentru fiecare punct se marchează una dintre opțiunile: Da, Nu sau N/A.

Un răspuns „Nu” la o verificare de prioritate înaltă trebuie transformat într-o acțiune de remediere, cu indicarea persoanei responsabile și a termenului de executare.

CUM SE UTILIZEAZĂ PRIORITĂȚILE

Prioritate înaltă

Obligații esențiale sau zone cu risc sancționar direct: teme juridic, informare, drepturile persoanelor vizate, securitate, incidente, persoane împuternicite de operator, transferuri, DPIA, atunci când sunt aplicabile.

Prioritate medie

Măsuri necesare pentru organizarea și demonstrarea conformității: evidențe, proceduri, revizui, instrui și actualizări de documente.



Inventarierea prelucrărilor

Are loc atunci când datele sunt transmise către destinatari din alte state sau organizații internaționale.

Verificați transferurile realizate prin servicii cloud, CRM, newsletter, analiză, furnizori IT sau alte servicii externe care accesează ori stochează date în afara Republicii Moldova.

Pentru verificarea conformității, trebuie să:

Identificați toate activitățile de prelucrare care implică date cu caracter personal.	Prioritate: înaltă.
Stabiliți persoanele vizate și categoriile de date prelucrate pentru fiecare activitate.	Prioritate: înaltă.
Verificați dacă aveți obligația de a ține evidența activităților de prelucrare.	Prioritate: înaltă.
Completați evidențele cu scopurile, temeiurile juridice, categoriile de date, destinatarii, transferurile și termenele de stocare.	Prioritate: înaltă.
Includeți, după caz, măsurile generale de securitate aplicate.	Prioritate: medie.
Actualizați evidențele ori de câte ori se modifică scopul, destinatarii, sistemele utilizate, transferurile, termenele de stocare sau măsurile de securitate.	Prioritate: medie.



TEMEIUL JURIDIC AL PRELUCRĂRII

Pentru fiecare activitate de prelucrare, operatorul trebuie să stabilească scopul concret și temeiul juridic aplicabil. Datele nu pot fi colectate sau utilizate doar pentru că sunt „utile” companiei, ci numai dacă există un temei prevăzut de lege.

Pentru verificarea conformității, trebuie să:

Stabiliți temeiul juridic pentru fiecare scop de prelucrare, indicând baza legală aplicabilă (consimțământ, contract, obligație legală, interes legitim etc.).	Prioritate: înaltă.
Verificați dacă scopul prelucrării este determinat, explicit și legitim, evitând formulări generale sau neclare.	Prioritate: înaltă.
Aplicați principiul reducerii la minimum a datelor, colectând doar datele necesare scopului declarat.	Prioritate: înaltă.
Documentați analiza interesului legitim, atunci când acesta este utilizat ca temei juridic.	Prioritate: medie.
Identificați excepția aplicabilă pentru categoriile speciale de date și garanțiile necesare pentru protecția acestora.	Prioritate: înaltă.



INFORMAREA PERSOANEI VIZATE

Operatorul trebuie să furnizeze persoanei vizate informații clare despre prelucrarea datelor. Politica de confidențialitate nu trebuie să fie un text generic, ci trebuie să reflecte activitățile reale ale operatorului.

Pentru verificarea conformității, trebuie să:

Indicați identitatea și datele de contact ale operatorului, astfel încât persoana vizată să poată identifica responsabilul pentru prelucrarea datelor.	Prioritate: înaltă.
Indicați reprezentantul desemnat, dacă este cazul, și datele relevante de contact.	Prioritate: înaltă.
Prezentați scopurile prelucrării și temeiurile juridice aplicabile pentru fiecare categorie relevantă de date.	Prioritate: înaltă.
Stabiliți termenele de păstrare pentru fiecare categorie de date, pe baza unor criterii clare de ștergere sau arhivare.	Prioritate: înaltă.
Asigurați accesibilitatea informării la momentul colectării datelor, inclusiv prin site, formulare sau alte canale utilizate.	Prioritate: medie.



ASIGURAREA EXERCITĂRII DREPTURILOR

Operatorul trebuie să aibă un mecanism funcțional pentru primirea, înregistrarea, analizarea și soluționarea cererilor prin care persoanele vizate își exercită drepturile.

Pentru verificarea conformității, trebuie să:

Puneți la dispoziție un canal clar pentru exercitarea drepturilor, prin e-mail, formular sau adresă poștală	Prioritate: înaltă.
Înregistrați cererile primite și asigurați evidența soluționării acestora.	Prioritate: înaltă.
Verificați identitatea solicitantului în mod proporțional cu riscul, atunci când este necesar.	Prioritate: medie.
Respectați termenul legal de răspuns și documentați comunicarea cu persoana vizată.	Prioritate: înaltă.
Asigurați exercitarea dreptului de acces prin furnizarea informațiilor relevante și, după caz, a copiei datelor.	Prioritate: înaltă.
Gestionați cererile privind rectificarea, ștergerea, restricționarea, portabilitatea și opoziția, documentând măsurile aplicate.	Prioritate: înaltă.



GESTIONAREA INCIDENTELOR DE SECURITATE

Operatorul trebuie să poată identifica, documenta și gestiona rapid orice incident care afectează securitatea datelor cu caracter personal. Nu orice incident se notifică Centrului, însă fiecare incident trebuie analizat și documentat.

Pentru verificarea conformității, trebuie să:

Instituiți o procedură internă de raportare a incidentelor de securitate, cu responsabilități și fluxuri clare de comunicare.	Prioritate: înaltă.
Stabiliți termene interne pentru soluționarea rapidă a incidentelor și evaluarea necesității notificării.	Prioritate: înaltă.
Documentați fiecare incident de securitate, inclusiv cele care nu sunt supuse notificării, indicând situația, datele afectate, efectele și măsurile aplicate.	Prioritate: înaltă.
Evaluați riscul generat de incident și documentați decizia privind notificarea sau ne-notificarea acestuia.	Prioritate: înaltă.
Notificați CNPDCP atunci când incidentul poate genera un risc pentru drepturile și libertățile persoanelor vizate.	Prioritate: înaltă.
Verificați obligațiile prestatorilor privind raportarea incidentelor și asigurați stabilirea clară a termenelor, canalelor și conținutului notificărilor.	Prioritate: înaltă.



EVALUAREA IMPACTULUI / DPIA

Evaluarea impactului asupra protecției datelor cu caracter personal se verifică înainte de lansarea unei prelucrări care poate genera risc ridicat pentru drepturile și libertățile persoanelor fizice.

Pentru verificarea conformității, trebuie să:

Verificați dacă prelucrarea poate genera un risc ridicat pentru drepturile și libertățile persoanelor vizate.	Prioritate: înaltă.
Identificați situațiile care impun realizarea evaluării impactului (ex. profilare, decizii automatizate, prelucrare pe scară largă a datelor speciale).	Prioritate: înaltă.
Descrieți operațiunile de prelucrare și scopurile urmărite, inclusiv fluxurile de date, persoanele vizate și sistemele utilizate.	Prioritate: înaltă.
Analizați necesitatea, proporționalitatea și riscurile prelucrării în cadrul evaluării impactului.	Prioritate: înaltă.
Solicitați avizul responsabilului cu protecția datelor, dacă acesta este desemnat.	Prioritate: medie.
Consultați CNPDCP înainte de prelucrare, dacă riscul ridicat nu poate fi redus suficient.	Prioritate: înaltă.



TRANSFERUL INTERNAȚIONAL DE DATE

Operatorul verifică dacă orice transfer de date către state din afara Republicii Moldova sau organizații internaționale are un temei legal și respectă condițiile aplicabile. Operatorul verifică dacă transferul se bazează pe o decizie de adecvare emisă de CNPDCP sau pe emiterea de garanții adecvate.

Pentru verificarea conformității, trebuie să:

Identificați dacă transmiteți date către state din afara Republicii Moldova sau organizații internaționale.	Prioritate: înaltă.
Verificați baza legală a transferului (decizie de adecvare, garanții adecvate sau excepție legală).	Prioritate: înaltă.
Asigurați că transferul oferă un nivel adecvat de protecție a datelor (ex. decizie privind caracterul adecvat, clauze standard de protecție a datelor, reguli corporatiste obligatorii sau alte garanții aprobate).	Prioritate: înaltă.
Documentați transferurile, inclusiv țara, destinatarul, datele transmise și garanțiile aplicate.	Prioritate: înaltă.
Informați persoanele vizate despre transferurile internaționale de date, indicând țara sau organizația internațională, scopul transferului, destinatarii, garanțiile aplicabile și, după caz, riscurile asociate transferului.	Prioritate: înaltă.