



INSTRUCȚIUNE PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

1. Dispoziții generale

1.1. Instrucțiunile privind prelucrarea datelor cu caracter personal sunt emise în conformitate cu obligațiile legale care îi revin Abonatului și Furnizorului în conformitate cu prevederile legale aferente domeniului protecției datelor cu caracter personal, care stabilesc că la prelucrarea datelor cu caracter personal trebuie asigurată confidențialitatea și operatorii sunt obligați să ia măsurile organizatorice și tehnice necesare pentru protecția datelor cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate.

1.2. Instrucțiunea completează celelalte cerințe prevăzute de contractul de furnizarea comunicațiilor electronice și de anexele la contract.

1.3. Instrucțiunea se va revizui cel puțin odată pe an, ca rezultat al modificărilor sau reevaluării componentelor acesteia.

2. Principiile de prelucrare a datelor cu caracter personal

2.1. Furnizorul și Abonatul vor lua în calcul toate măsurile de securitate și de conformitate stabilite de prezenta Instrucțiune în vederea prelucrării datelor cu caracter personal în limitele expres prevăzute de către acestea.

2.2. Furnizorul și Abonatul au implementat politici și reguli privind păstrarea datelor cu caracter personal, care să respecte principiile prevăzute de legislația privind protecția datelor cu caracter personal

2.3. Abonatul SCSV, în calitate de operator de date cu caracter personal, în conformitate cu prevederile legale aferente domeniului protecției datelor cu caracter personal, este responsabil de specificarea și documentarea scopurilor prelucrării datelor cu caracter personal prin mijloace de supraveghere video, delimitarea spațiilor supuse supravegherii prin mijloace video, informarea persoanelor vizate etc.

3. Prelucrarea datelor cu caracter personal

3.1. Prelucrarea datelor cu caracter personal în timpul supravegherii video trebuie să fie securizată corespunzător de către operatori și persoanele împuternicite de aceștia.

3.2. Personalul Furnizorului desemnat/autorizat de către acesta și care are acces/prelucrează datele personale în numele Abonatului (personal vânzări, personal suport, personal instalări etc.) are încheiat un Acord de confidențialitate, în care se stipulează aspecte legate de tipul de date confidențiale și obligații de procesare.

3.3. Pentru atenționarea persoanelor vizate cu privire la existența camerelor de supraveghere video, acestea se montează în locuri vizibile, iar prezența acestora este semnalată de către Abonat prin intermediul unei pictograme conform Anexei la Decizia Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova nr. 581/2015 cu privire la aprobarea formularului tipizat de informare privind efectuarea supravegherii prin mijloace video.

4. Conturi de acces în sistemul SCSV.

4.1. Pentru accesul la sistemul SCSV, Abonatul va indica datele de identificare ale utilizatorilor autorizați, inclusiv datele de contact ale acestora (număr de telefon și adresa de email) pentru crearea conturilor individuale de acces ale utilizatorilor vizați (cu nume utilizator și parolă). Abonatul este responsabil pentru autenticitatea datelor prezentate, pentru informarea privind suspendarea și/sau retragerea drepturilor de acces ale persoanelor vizate.

4.2. Este obligația utilizatorului fiecărui cont – Abonatului ca la prima logare, să se asigure de schimbarea parolei setată inițial. Formatul parolei acceptate de aplicație este de tipul alfanumeric (minim 8 caractere) și conține cifre, litere (scrise cu majuscule sau fără, cu restricția să conțină cel puțin un caracter cu majusculă sau un caracter numeric), precum și caractere speciale. Parolele vor fi schimbate la un interval de 90 zile, utilizatorii fiind notificați după trecerea perioadei de valabilitate, la momentul autentificării în sistemul SCSV, și obligați să schimbe parola curentă cu una nouă, diferită. Fiecare utilizator are posibilitatea de a-și schimba parola aferentă contului său. De asemenea în cazul în care utilizatorul a uitat parola contului său, are posibilitatea de resetare a parolei în mod automat, cu condiția să aibă o adresa de email validă setată pe cont. Dacă utilizatorul respectiv nu are setată o adresă validă pe cont resetarea parolei va putea fi realizată doar de către serviciul suport al Furnizorului.

4.3. În executarea contractului, Furnizorul prin angajații desemnați în condițiile pct. 3.2, accesează datele din conturile utilizatorilor Abonatului, atunci când este necesar pentru rezolvarea solicitărilor inițiate de către Abonat.

4.4. Responsabilitatea instruirii utilizatorilor proprii revine Abonatului, având posibilitatea să utilizeze materialele puse la dispoziție de Furnizor.

5. Accesarea datelor din aplicația sistemul SCSV

5.1. Utilizarea datelor colectate din SCSV se realizează pe terminalele Abonatului, prin accesarea pe conexiune securizată HTTPS a unui portal web (securizare realizată cu ajutorul unor certificate digitale SSL). Ca și recomandare la regulile de utilizare a terminalelor din cadrul Abonatului, ar trebui inclusă blocarea sesiunii de lucru pe terminal după o perioadă de inactivitate de 10 minute. Sistemul SCSV dispune de măsura închiderii sesiunii de lucru pe portalul web al aplicației și obligă la re-autentificare după 15 minute de inactivitate a utilizatorului.

6. Colectare, loguri, stocare date

6.1. Colectarea datelor prin sistemul SCSV se va realiza automatizat, cu utilizarea echipamentului indicat în Anexa privind Serviciile de supraveghere video (SCSV) semnată la contractul privind furnizarea serviciilor de comunicații electronice.

6.2. Orice operațiune cu privire la extragerea, stocarea sau copierea acestor date se poate face numai de către utilizatori desemnați de către Abonat sau de către utilizatorii Furnizorului la cererea scrisă a Abonatului.

6.3. Sistemul SCSV dispune de posibilitatea de înregistrare a operațiunilor principale, realizatori ai acestora, data și ora operațiunii. Aplicația are un modul de loguri care permite auditarea operațiunilor principale derulate, informațiile pot fi furnizate la cerere și unui reprezentant împuternicit din partea Abonatului.

6.4. Sistemul SCSV menține datele de audit ca disponibile pentru Abonat pentru ultimele 24 luni din perioada contractuală de furnizare a serviciului, cu excepția altor înțelegeri referitoare la păstrarea datelor, stabilite contractual.

6.5. Datele sunt stocate pe serverele Furnizorului, în perimetrul de securitate în Republica Moldova.

6.6. Datele cu caracter personal colectate prin mijloacele de supraveghere video sunt stocate în conformitate cu cerințele și în funcție de capacitatea de stocare, după care se șterg prin procedură automată în ordinea în care au fost înregistrate. În cazul producerii unui incident de securitate sau a înregistrării unei solicitări întemeiate a unei persoane vizate, durata de stocare a imaginilor pentru intervalul de timp relevant poate depăși limitele normale în funcție de timpul necesar investigării suplimentare a incidentului de securitate sau de soluționare a solicitării primite.

6.7. Mediile de stocare sunt păstrate în spații securizate, protejate de măsuri de securitate fizică și organizatorică.

7. Alte măsuri de securitate

7.1. În toate cazurile de colectare a datelor cu caracter personal acestea sunt prelucrate de către Furnizor în perimetrul de securitate, fiind realizate măsuri organizatorice și tehnice necesare pentru asigurarea unui nivel adecvat de protecție a datelor cu caracter personal, în conformitate cu legislația națională și europeană în vigoare.

7.2. Modul în care se realizează accesul fizic și accesul logic al angajaților este descris prin Politica de securitate a datelor cu caracter personal, cum ar fi: modul de gestionare al conturilor utilizatorilor, managementul parolilor, măsuri de securitate pentru lucrul la distanță (ex: VPN). Se acordă o importanță deosebită securității fizice a centrului de date (camera de servere), fiind asigurat un control riguros al accesului din punct de vedere fizic și logic (ex: utilizare de firewall-uri, criptare date, semnalizare anti-incendiară, măsuri de control acces etc.)

8. Modul și condițiile de informare a operatorului de date cu caracter personal

8.1. Furnizorul la cerere, informează Abonatul asupra măsurilor pe care le-a adoptat în vederea respectării cerințelor prevăzute de prezenta Instrucțiune.

8.2. În cazul producerii unui incident de securitate care s-a soldat cu scurgerea unor date cu caracter personal sau prelucrarea ilegală a acestora, Furnizorul informează Abonatul imediat, dar nu mai târziu decât 24 de ore din momentul producerii acestuia. Informațiile furnizate, vor fi complete, corecte și exacte.

8.3. Nota de informare privind producerea unui incident de securitate va conține cel puțin:

- a) data, ora, locația producerii sau suspectării de producere a unui incident de securitate;
- b) cauza sau presupusa cauză de scurgere a informației;
- c) consecințele cunoscute sau care ar putea urma;
- d) măsurile deja luate și soluțiile de remediere a situației create.

8.4. Atât Furnizorul, cât și Abonatul vor întreprinde toate măsurile necesare în vederea conlucrării cu Autoritatea de protecție a datelor cu caracter personal.

9. Cerințele de securitate la prelucrarea datelor cu caracter personal

9.1. Furnizorul va lua măsuri organizatorice și tehnice necesare împotriva pierderii sau a oricărei forme de prelucrare ilegală (cum ar fi divulgarea, deteriorarea, modificarea sau prelucrarea neautorizată a datelor cu caracter personal) în mărimea măsurilor de control disponibile.

9.2. Utilizatorii autorizați ai abonatului, cu drept de acces la sistemul de supraveghere video, au obligația de a asigura confidențialitatea datelor cu caracter personal în vederea respectării prevederilor legale aferente domeniului protecției datelor cu caracter personal.