ROMÂNIA
CURTEA DE APEL BACĂU
Str. Cuza Vodă nr. 1, cod 600274
Tel. 0234513296 Fax 0234514275
E – MAIL: ca-bacau@just.ro
http://portal.just.ro/32/
Operator de date cu caracter personal 3667

Nr. 4183/I/A/38/18.11.2019

POLITICA DE SECURITATE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL A CURȚII DE APEL BACĂU

CAPITOLUL 1. SCOP:

Scopul acestei politici este de a stabili măsurile necesare şi responsabilităţile angajaţilor Curții de Apel Bacău, pentru îndeplinirea obligaţiilor referitoare la garantarea şi protejarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la viaţa intimă, familială şi privată, cu privire la prelucrarea datelor cu caracter personal.

CAPITOLUL 2. DOMENIUL DE APLICARE:

Prezenta politică se aplică tuturor angajaţilor Curții de Apel Bacău cu atribuţii de prelucrare a datelor cu caracter personal şi/sau după caz persoanelor împuternicite.

CAPITOLUL 3. TERMENI ŞI DEFINIŢII:

ANSPDCP = Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal;

Codul numeric personal (CNP) = un număr semnificativ care individualizează în mod unic o persoană fizică, constituind un instrument de verificare a stării civile a acesteia şi de identificare în anumite sisteme informatice de către persoanele autorizate;

Date cu caracter personal = orice informaţii referitoare la o persoană fizică identificată sau identificabilă; o persoană identificabilă este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un număr de identificare ori la unul sau la mai mulţi factori specifici identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

Date cu caracter personal cu funcţie de identificare de aplicabilitate generala (date cu caracter special) = numere prin care se identifică o persoană fizică în anumite sisteme de evidenţă şi care au aplicabilitate generală, cum ar fi: codul numeric personal, seria şi numărul actului de identitate, numărul

pașaportului, al permisului de conducere, numărul de asigurare socială sau de sănătate;

Date anonime - date care, datorită originii sau modalității specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă

Operator - orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care stabilește scopul și mijloacele de prelucrare a datelor cu caracter personal; dacă scopul și mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoana fizică sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza acelui act normativ;

Persoană împuternicită de către operator - o persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care prelucrează date cu caracter personal pe seama operatorului;

Persoana responsabilă de politica de securitate a datelor cu caracter personal - persoana responsabilă de funcționarea corespunzătoare a sistemului complex de protecție a informației care conține date cu caracter personal, precum și de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a deținătorului de date cu caracter personal;

Prelucrarea datelor cu caracter personal - orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terți prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

Stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese;

Utilizator - orice persoană care acționează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

CAPITOLUL 4. DOCUMENTE DE REFERINȚĂ:

- Regulamentul (UE) 2016/679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- Ordinul Avocatului Poporului nr. 52 din 18/04/2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal;
- Decizia ANSPDCP nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video;
- Decizia ANSPDCP nr. 90 din 18/07/2006 privind stabilirea cazurilor în care nu este necesara notificarea prelucrării unor date cu caracter personal;
- Decizia ANSPDCP nr. 100 din 23/11/2007 privind stabilirea cazurilor în care nu este necesara notificarea prelucrării unor date cu caracter personal

- Decizia ANSPDCP nr. 132 din 20/12/2011 privind condiţiile prelucrării codului numeric personal şi a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală.

CAPITOLUL 5. PRECIZĂRI

5.1. REGULI GENERALE

Prin cerinţe minime de securitate este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice, proceduri şi politici de securitate prin care să se asigure nivelul minim de securitate prevăzut în Capitolul IV, Secţiunea I, art. 24 şi art. 25, respectiv, Secţiunea 4, art. 39 din Regulamentul (UE) 2016/679 din 27 aprilie 2016 (denumit în continuare Regulament UE), în conformitate cu cerinţele minime de securitate a prelucrărilor de date cu caracter personal, aprobate prin Ordinul 52 din 18 aprilie 2002 ale Avocatului Poporului.

Curtea de Apel Bacău a adoptat măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. În acest sens au fost desemnate, la nivelul Curţii de Apel Bacău, persoane responsabile cu respectarea dispoziţiilor Regulamentul (UE).

Curtea de Apel Bacău a luat măsuri de stocare în siguranţă a informaţiilor privind date cu caracter personal, astfel încât sa fie asigurat un nivel adecvat de protecţie şi securitate, în sensul Regulamentului (UE).

Pentru îndeplinirea prevederilor legale aferente şi în vederea satisfacerii cerinţelor păstrării în siguranţă a datelor şi informaţiilor, instituţia a elaborat şi implementat măsuri organizatorice şi tehnice orientate pe anumite direcţii de acţiune:

- Identificarea şi autentificarea utilizatorului
- Tipul de acces
- Colectarea datelor
- Execuţia copiilor de siguranţă
- Computerele şi terminalele de acces
- Fişierele de acces
- Instruirea personalului

5.2. PROCEDURI SPECIFICE

5.2.1 Identificarea si autentificarea utilizatorului

Pentru a primi acces la date cu caracter personal, utilizatorii trebuie să se autentifice în sistemele informatice ale Curţii de Apel Bacău. Autentificarea în cadrul sistemelor informatice ale Curţii de Apel Bacău se face prin introducerea parolelor de autentificare unice şi netransmisibile dobândite în urma procesului de înrolare şi management al identităţii electronice, guvernat de politicile de securitate în vigoare.

Fiecare utilizator are propriul său cod de identificare (nume de utilizator). Niciodată nu este alocat acelaşi cod de identificare mai multor utilizatori şi acesta nu poate fi partajat de către mai multe persoane.

Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată sunt dezactivate şi distruse după un control prealabil. Perioada după care codurile trebuie dezactivate şi distruse este stabilită prin politicile IT adoptate de Curtea de Apel Bacău.

Orice cont de utilizator este însoţit de o modalitate de autentificare, prin introducerea unei chei de autentificare, precum o parolă.

Parolele sunt şiruri de caractere, adecvate din punct de vedere al securităţii ca lungime şi compoziţie. La introducerea parolelor, acestea nu sunt afişate în clar pe monitor. Parolele sunt schimbate periodic conform politicilor de Securitate stabilite de Curtea de Apel Bacău (Politica de Securitate IT). Schimbarea periodică a parolelor se face numai de către utilizatori autorizaţi.

Sistemul informaţional blochează automat accesul unui utilizator după un număr fix de introduceri greşite ale cheii de autentificare.

Orice utilizator care primeşte un cod de identificare şi un mijloc de autentificare este obligat prin fişa postului să păstreze confidenţialitatea acestora şi să răspundă în acest sens în faţa operatorului.

Este stabilită o procedură proprie de administrare şi gestionare a conturilor de utilizator. Sunt autorizaţi anumiţi utilizatori pentru a revoca sau a suspenda un cod de identificare şi autentificare, dacă utilizatorul acestora şi-a dat demisia ori a fost concediat, şi-a încheiat contractul, a fost transferat la alt serviciu şi noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă va absenta o perioadă îndelungată stabilită de entitate.

5.2.2. Tipul de acces

Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuţiilor lor de serviciu. Pentru aceasta trebuie să fie stabilite tipurile de acces după funcţionalitate (administrare, introducere, prelucrare, salvare etc.) şi după acţiuni aplicate asupra datelor cu caracter personal (scriere, citire, ştergere), precum şi procedurile privind aceste tipuri de acces.

Compartimentul care asigură suportul tehnic poate avea acces la datele cu caracter personal pentru rezolvarea incidentelor şi a problemelor apărute în utilizarea sistemelor informatice.

Alte măsuri specifice implementate pentru controlul accesului, sunt:

- în spaţiile destinate desfăşurării activităţii instituţiei sunt instalate sisteme de alarmă antiefracţie;
- în spaţiul aferent intrării în cadrul instituţiei şi în holurile de acces la etajele superioare sunt instalate sisteme de supraveghere video;
- monitorizarea şi intervenţia în caz de alarmă este asigurată de JANDARMERIA ROMÂNĂ din cadrul Ministerul Afacerilor Interne.

5.2.3. Colectarea datelor

Curtea de Apel Bacău desemnează utilizatori autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal în sistemele informaţionale.

Orice modificare a datelor cu caracter personal trebuie să se poată face numai de către utilizatori autorizaţi desemnaţi.

Curtea de Apel Bacău va lua măsuri pentru ca sistemele informaţionale să înregistreze cine a făcut modificarea datelor cu caracter personal, data şi ora modificării. Pentru o mai bună administrare, vor fi implementate măsuri pentru ca sistemele informaţionale să menţină datele şterse sau modificate.

5.2.4. Execuţia copiilor de siguranţă

Curtea de Apel Bacău a stabilit intervalul de timp la care se vor executa copiile de siguranţă ale bazelor de date ce conţin date cu caracter personal, precum şi ale programelor folosite pentru prelucrările automatizate.

Utilizatorii care execută aceste copii de siguranţă sunt numiţi de Curtea de Apel Bacău, într-un număr restrâns.

Copiile de siguranţă se stochează într-un safe box cu acces restricţionat la personal IT, aflat într-o altă locaţie fata de cea în care se efectuează copia de siguranţă.

Accesul la copiile de siguranţă trebuie sa fie monitorizat.

Sistemele care gestionează date cu caracter personal trebuie sa fie protejate prin procesul de back-up periodic împotriva pierderii, sau distrugerii datelor sau a sistemului informatic.

5.2.5. Computerele şi terminalele de acces

Computerele şi alte terminale de acces la date cu caracter personal aflate în sediul Curţii de Apel Bacău vor fi instalate în încăperi cu acces restricţionat.

Unde nu pot fi asigurate aceste condiţii, computerele vor fi instalate în încăperi care se pot încuia. Dacă pe ecran apar date cu caracter personal asupra cărora nu se acţionează o perioadă dată, stabilită de către Curtea de Apel Bacău, sesiunea de lucru se va închide automat. Mărimea acestei perioade se determină în funcţie de operaţiile care trebuie executate.

Terminalele de acces folosite în relaţia cu publicul, pe care apar date cu caracter personal, vor fi poziţionate astfel încât să nu poată fi văzute de public şi după o perioadă scurtă, stabilită de Curtea de Apel Bacău, în care nu se acţionează asupra lor, acestea vor fi ascunse sau sesiunea de lucru va fi închisă.

Servere-le care găzduiesc date cu caracter personal pot fi accesate doar în mod controlat, pe baza de drepturi de acces, conform politicilor de securitate ale grupului si adoptate de Curtea de Apel Bacău .

5.2.6. Fişierele de acces

Curtea de Apel Bacău ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată.

Pentru prelucrările automate, aceste informaţii sunt stocate într-un fişier de acces general sau în fişiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată.

Curtea de Apel Bacău păstrează fişierele de acces cel puţin 2 ani, pentru a fi folosite ca probe în cazul unor investigaţii. Dacă investigaţiile se prelungesc, aceste fişiere se vor păstra atât timp cât se va considera necesar.

Fişierele de acces fac posibilă identificarea de către Curtea de Apel Bacău sau de către persoana împuternicită, a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancţiuni sau a sesizării organelor competente.

5.2.7. Sistemele de telecomunicaţii

Curtea de Apel Bacău face periodic revizuirea conturilor de utilizatori şi a privilegiilor acordate pentru detectarea unor disfuncţionalităţi în ceea ce priveşte sistemelor informaţionale.

Sistemele informaţionale vor fi concepute astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde.

Prin sistemele de telecomunicaţii datele cu caracter personal vor fi transmise printr-un canal sigur. Datele cu caracter personal transferate in zonele de securitate externă sau nesigură vor fi criptate. Toate prevederile documentului Politica de Securitate a Informaţiei - Reţea şi Firewall sunt aplicabile.

5.2.8. Instruirea personalului

Personalul Curţii de Apel Bacău este informat cu privire la prevederile Regulamentului (UE) pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, la cerinţele minime de securitate a prelucrărilor de date cu caracter personal, precum şi cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal.

Utilizatorii care au acces la date cu caracter personal vor fi instruiţi asupra confidenţialităţii acestora şi vor fi avertizaţi prin mesaje care vor apărea pe monitoare în timpul activităţii.

Utilizatorii sunt obligaţi să îşi închidă sesiunea de lucru atunci când părăsesc locul de muncă.

Toate prevederile documentului Politica de Securitate a Informaţiei - Utilizarea Adecvata a Sistemelor IT sunt aplicabile.

5.2.9. Folosirea computerelor

Pentru menţinerea securităţii prelucrării datelor cu caracter personal (în special împotriva virusilor informatici) trebuie luate măsuri privind:

- interzicerea folosirii de către utilizatori a programelor software care provin din surse neverificate;
- informarea utilizatorilor în privinţa pericolului privind virusii informatici;

- implementarea unor sisteme automate de tip antivirus şi protective malware şi de securitate a sistemelor informatice;

- dezactivarea posibilităţii de copiere sau imprimare a datelor cu caracter personal afişate pe ecran în afara fluxurilor normale de lucru.

5.2.10. Imprimarea datelor

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizaţi de către Curtea de Apel Bacău pentru această operaţiune.

5.2.11. Prelucrarea manuala de date cu caracter personal

Documentele care conţin date cu caracter personal vor fi ţinute în fişete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare. Documentele care conţin date cu caracter personal, folosite pentru realizarea anumitor operaţiuni se vor preda persoanelor abilitate sau se vor închide imediat după terminarea acestora şi se vor păstra în spaţii de arhivare special amenajate.

5.3. Principiile care stau la baza prelucrării datelor cu caracter personal

Prelucrarea datelor cu caracter personal se realizează cu respectarea cerinţelor legale şi în condiţii care să asigure securitatea, confidenţialitatea şi respectarea drepturilor persoanelor vizate.

Prelucrarea datelor cu caracter personal se face cu respectarea următoarelor principii:

- Notificarea: Curtea de Apel Bacău este înregistrată ca operator în Registrul general de evidenţă a prelucrărilor de date cu caracter personal :

- cu numărul 3666, având ca scop administrarea justiţiei, pentru colectarea, prelucrarea şi stocarea datelor cu caracter personal ale angajaţilor instituţiei şi ale tuturor participanţilor în cauzele de pe rolul instanţei (părţi, inculpaţi, participanţi, avocaţi, procurori, etc.);

- cu numărul 3667 având ca scop prevenirea, cercetarea, reprimarea infracţiunilor, menţinerea ordinii publice;

- cu numărul 27284 având ca scop monitorizarea/securitatea persoanelor, spaţiilor şi/sau bunurilor publice/private.

- Legalitatea : Prelucrarea datelor cu caracter personal se face în temeiul şi în conformitate cu prevederile legale;

- Scopul bine-determinat: Orice prelucrare de date cu caracter personal se face în scopuri bine determinate, explicite şi legitime, adecvate, pertinente şi neexcesive prin raportare la scopul în care sunt colectate şi ulterior prelucrate;

- Confidenţialitatea: Persoanele care prelucrează, în numele Curţii de Apel Bacău, date cu caracter personal au prevăzute, în fişa postului, clauzele de confidenţialitate;

- Consimţământul persoanei vizate: Orice prelucrare de date cu caracter personal, cu excepţia prelucrărilor care vizează date din categoriile strict

menţionate în Regulamentul (UE), poate fi efectuată numai dacă persoana vizată şi-a dat consimţământul în mod expres şi neechivoc pentru acea prelucrare;

- Informarea: Persoanele vizate iau cunoştinţă despre faptul că li se vor prelucra date cu caracter personal;

- Protejarea persoanelor vizate: Drepturile persoanelor vizate sunt prezentate la punctul 5.6.

- Securitatea: Masurile de securitate a datelor cu caracter personal sunt stabilite astfel încât să asigure un nivel adecvat de securitate a datelor cu caracter personal procesate.

5.4. Prelucrarea datelor cu caracter personal având o funcţie de identificare de aplicabilitate generală,

inclusiv dezvăluirea acestora către terţi, se face numai în următoarele condiţii:

a) persoana vizată şi-a dat în mod expres consimţământul; sau

b) prelucrarea este prevăzută în mod expres de o dispoziţie legală; sau

c) în alte cazuri, cu avizul Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal şi numai cu condiţia instituirii unor garanţii adecvate pentru respectarea drepturilor persoanelor vizate.

Curtea de Apel Bacău respectă principiul caracterului adecvat, pertinent şi neexcesiv, precum şi măsurile de confidenţialitate şi de securitate a prelucrărilor. În cazul prevăzut la punctul c) de mai sus, se au în vedere următoarele aspecte:

- scopul prelucrării să fie determinat, explicit şi legitim;
- stabilirea şi aplicarea unor măsuri prin care să se asigure exercitarea drepturilor persoanelor vizate;
- durata de stocare a datelor să fie pe perioada strict necesară îndeplinirii scopului, după care datele vor fi şterse sau distruse, după caz;
- stabilirea modalităţilor de acces la sistemele de evidenţă în vederea colectării datelor, în funcţie de care se vor stabili şi respecta măsuri tehnice şi organizatorice adecvate pentru protejarea datelor;
- utilizarea datelor numai în limitele scopului stabilit;
- dezvăluirea către alţi destinatari este interzisă, cu excepţia situaţiei în care există consimţământul persoanei vizate sau o prevedere legală expresă;
- desemnarea, în scris, a persoanei/persoanelor care va/vor prelucra datele şi care trebuie să îşi asume răspunderea păstrării confidenţialităţii acestora, lista conţinând evidenţa acestor persoane fiind actualizată ori de câte ori se impune;
- numirea, în scris, a unei persoane specializate în securitatea informaţiei care să vegheze la prelucrarea datelor, inclusiv la buna funcţionare a sistemelor informatice utilizate în această activitate;
- stabilirea unui plan de securitate a informaţiilor care să cuprindă, în principal, securitatea tehnică pe plan informatic şi securitatea spaţiilor în care se prelucrează datele, ţinând cont de cerinţele minime de securitate;

- stabilirea, în scris, a drepturilor şi obligaţiilor operatorului care transmite datele şi ale operatorului care le primeşte.

Colectarea şi prelucrarea datelor cu caracter personal având o funcţie de identificare de aplicabilitate generală, inclusiv dezvăluirea acestora, prin efectuarea şi reţinerea de copii de pe cartea de identitate sau de pe documente care le conţin, sunt interzise, cu excepţia situaţiilor prevăzute la punctele a), b) si c) de mai sus.

5.5. Prelucrarea datelor cu caracter personal prin utilizarea sistemelor de supraveghere video

Prelucrarea datelor cu caracter personal prin utilizarea sistemelor de supraveghere video se efectuează cu respectarea regulilor generale prevăzute Regulamentul (UE).

Camerele de supraveghere video sunt montate în locuri vizibile.

Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se face pentru realizarea unor interese legitime, fără a se prejudicia drepturile şi libertăţile fundamentale sau interesul persoanelor vizate. Nu este permisă prelucrarea datelor cu caracter personal ale angajaţilor prin mijloace de supraveghere video în interiorul spatiilor/birourilor unde aceştia îşi desfăşoară activitatea la locul de muncă, cu excepţia situaţiilor prevăzute expres de lege sau a avizului ANSPDCP.

Curtea de Apel Bacău, în calitate de operator care prelucrează date cu caracter personal prin mijloace de supraveghere video, este obligată să furnizeze informaţiile inclusiv cu privire la:

a) existenţa sistemului de supraveghere video şi scopul prelucrării datelor prin astfel de mijloace;

b) identitatea operatorului;

c) existenţa înregistrării imaginilor şi categoriile de destinatari ai acestora;

d) drepturile persoanelor vizate şi modul de exercitare a acestora.

Informaţiile menţionate mai sus trebuie aduse la cunoştinţa persoanelor vizate, în mod clar şi permanent.

Existenţa sistemului de supraveghere video este semnalată prin intermediul unei pictograme care conţine o imagine reprezentativă cu vizibilitate suficientă şi poziţionată la o distanţă rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere video.

Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se poate realiza numai de persoanele autorizate de către Curtea de Apel Bacău (personal propriu sau persoane împuternicite de către operator), instruite cu privire la legislaţia referitoare la protecţia datelor cu caracter personal şi obligate să se supună acesteia.

Durata de stocare a datelor obţinute prin intermediul sistemului de supraveghere video este proporţională cu scopul pentru care se prelucrează datele, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.

La expirarea termenului stabilit, înregistrările se distrug sau se şterg, după caz, în funcţie de suportul pe care s-au stocat.

5.6. Drepturile persoanelor ale căror date personale sunt colectate şi/sau prelucrate

5.6.1. Dreptul de a fi informat

(1) În cazul în care datele cu caracter personal sunt obţinute direct de la persoana vizată, Curtea de Apel Bacău este obligat să furnizeze persoanei vizate cel puţin următoarele informaţii, cu excepţia cazului în care această persoană posedă deja informaţiile respective:

a) scopul în care se face prelucrarea datelor;

b) informaţii suplimentare, precum: destinatarii sau categoriile de destinatari ai datelor; dacă furnizarea tuturor datelor cerute este obligatorie şi consecinţele refuzului de a le furniza;

c) existenţa drepturilor prevăzute de lege pentru persoana vizată, în special a dreptului de acces, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care pot fi exercitate;

d) orice alte informaţii a căror furnizare este impusă prin dispoziţie a autorităţii de supraveghere, ţinând seama de specificul prelucrării.

(2) Pe pagina de internet a Curţii de Apel Bacău **http://portal.just.ro/32/** este postată politica privind Protecţia datelor cu caracter personal;

(3) Înainte de completarea datelor cu caracter personal se solicită consimţământul persoanelor vizate, pentru prelucrarea acestora;

(4) Numărul de înregistrare a notificării comunicat de Autoritatea Naţională de Supraveghere se menţionează în orice document prin care se colectează, stochează sau dezvăluie date cu caracter personal;

(5) Clădirile care sunt supravegheate video vor avea, la intrare, afişat în loc vizibil, informarea privind preluarea şi stocarea de imagini.

5.6.2. Dreptul de acces la date

Orice persoană vizată are dreptul de a obţine de la Curtea de Apel Bacău (în calitate de operator), la cerere şi în mod gratuit pentru o solicitare pe an, confirmarea faptului că datele care o privesc sunt sau nu sunt prelucrate de aceasta.

Curtea de Apel Bacău este obligată, în situaţia în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea, cel puţin următoarele:

a) informaţii referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;

b) comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării, precum şi a oricărei informaţii disponibile cu privire la originea datelor;

c) informaţii asupra principiilor de funcţionare a mecanismului prin care se efectuează orice prelucrare automată a datelor care vizează persoana respectivă;

d) informaţii privind existenţa dreptului de intervenţie asupra datelor şi a dreptului de opoziţie, precum şi condiţiile în care pot fi exercitate;

e) informaţii asupra posibilităţii de a înainta plângere către autoritatea de supraveghere, precum şi de a se adresa instanţei pentru atacarea deciziilor operatorului, în conformitate cu dispoziţiile legii.

Notă:

(1) Persoana vizată poate solicita de la Curtea de Apel Bacău informaţiile prevăzute de lege, printr-o cerere întocmită în formă scrisă, semnată şi înregistrată la registratura sau la secretariatul instanţei. În cerere solicitantul poate arăta dacă doreşte ca informaţiile să îi fie comunicate la o anumită adresă, care poate fi şi de poştă electronică, sau printr-un serviciu de corespondenţă care să asigure că predarea i se va face numai personal.

(2) Curtea de Apel Bacău este obligată să comunice informaţiile solicitate, în termen de 15 zile de la data primirii cererii, cu respectarea eventualei opţiuni a solicitantului.

5.6.3. Dreptul de intervenţie asupra datelor

Orice persoană vizată are dreptul de a obţine de la operator, la cerere şi în mod gratuit:

a) după caz, rectificarea, actualizarea, blocarea sau ştergerea datelor a căror prelucrare nu este conformă legii, în special a datelor incomplete sau inexacte;

b) după caz, transformarea în date anonime a datelor a căror prelucrare nu este conformă legii.

5.6.4. Dreptul de opoziţie

Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate şi legitime legate de situaţia sa particulară, ce date care o vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care există dispoziţii legale contrare. În caz de opoziţie justificată prelucrarea nu mai poate viza datele în cauză.

5.6.5. Dreptul de a nu fi supus unei decizii individuale

(1) Orice persoană are dreptul de a cere şi de a obţine retragerea/ anularea/ reevaluarea oricărei decizii care produce efecte juridice în privinţa sa, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate, destinată să evalueze unele aspecte ale personalităţii sale, precum competenţa profesională, credibilitatea, comportamentul său ori alte asemenea aspecte.

(2) Respectându-se celelalte garanţii prevăzute de lege, o persoană poate fi supusă unei decizii de natura celei vizate la alin.(1), numai în următoarele situaţii:

a) decizia este luată în cadrul încheierii sau executării unui contract, cu condiţia ca cererea de încheiere sau de executare a contractului, introdusă de persoana vizată, să fi fost satisfăcută sau ca unele măsuri adecvate, precum posibilitatea de a-şi susţine punctul de vedere, să garanteze apărarea propriului interes legitim;

b) decizia este autorizată de o lege care precizează măsurile ce garantează apărarea interesului legitim al persoanei vizate.

5.6.6. Dreptul de a se adresa justiţiei

(1) Fără a se aduce atingere posibilităţii de a se adresa cu plângere autorităţii de supraveghere, persoanele vizate au dreptul de a se adresa justiţiei pentru apărarea oricăror drepturi garantate de lege, care le-au fost încălcate.

(2) Orice persoană care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal, efectuată ilegal, se poate adresa instanţei competente pentru repararea acestuia.

5.7. Comunicarea datelor cu caracter personal

(1) Datele cu caracter personal se pot comunica între Curtea de Apel Bacău și instanţele din circumscripţia acesteia sau între Curtea de Apel Bacău sau alte instanțe și alte instituţii ori organisme publice sau entităţi de drept public sau privat în una dintre următoarele situaţii:

a) dacă persoana vizată şi-a dat consimţământul expres şi neechivoc pentru comunicarea datelor sale;

b) fără consimţământul persoanei vizate în cazurile prevăzute de lege.

(2) Comunicarea datelor cu caracter personal în situaţiile prevăzute la alin. (1) se poate face dacă este îndeplinită una dintre următoarele condiţii:

a) comunicarea se efectuează pe baza unui contract sau, după caz, a unui document de cooperare care trebuie să cuprindă cel puţin: numărul de înregistrare a notificării, temeiul legal al prelucrării şi scopul acesteia, termenul maxim de prelucrare, drepturile şi obligaţiile părţilor, modalităţile de asigurare a securităţii prelucrărilor şi de respectare a drepturilor persoanei vizate, precum şi menţiunea că datele pot fi utilizate doar de structura beneficiară şi numai în scopul pentru care au fost solicitate;

b) comunicarea se efectuează în baza unei solicitări scrise, care trebuie să cuprindă temeiul legal, scopul prelucrării şi datele solicitate, precum şi, dacă este cazul, numărul atribuit beneficiarului de Autoritatea Naţională de Supraveghere.

(3) Comunicarea datelor cu caracter personal se poate face şi on-line, cu respectarea dispoziţiilor alin. (1) şi (2) şi asigurarea securităţii sistemelor de comunicaţii a datelor cu caracter personal.

(4) Datele cu caracter personal asupra cărora persoanele vizate au exercitat şi li s-a recunoscut dreptul de opoziţie nu pot face obiectul prelucrării.

(5) Cererile pentru comunicarea datelor cu caracter personal adresate Curţii de Apel Bacău trebuie să conţină datele de identificare ale solicitantului, precum şi motivarea şi scopul cererii, conform prevederilor legale.

(6) Cererile care nu conţin aceste elementele se restituie pentru completare, iar cele care nu se încadrează în condiţiile prevăzute de lege se resping, menţionându-se motivele pentru care comunicarea datelor cu caracter personal nu este posibilă.

(7) Înainte de comunicarea datelor cu caracter personal, Curtea de Apel Bacău verifică dacă acestea sunt exacte şi, dacă este cazul, actualizate.

(8) În situaţia în care se constată că au fost transmise date incorecte sau neactualizate, Curtea de Apel Bacău are obligaţia de a informa destinatarii respectivelor date asupra neconformităţii acestora, cu menţionarea datelor care au fost modificate.

(9) La comunicarea datelor cu caracter personal Curtea de Apel Bacău atenţionează destinatarii asupra interdicţiei de a prelucra datele pentru alte scopuri decât cele specificate în cererea de comunicare.

5.8. Măsuri tehnice privind prelucrarea datelor cu caracter personal

Toate documentele care conţin date cu caracter personal se înregistrează şi urmează regulile de păstrare, procesare, multiplicare, transport, transmitere, distrugere şi arhivare stabilite prin Legea Arhivelor naţionale şi prin proceduri interne.

Principalele proceduri și politici de securitate aplicate sunt:

a) Accesul autentificat la utilizatorilor

La nivelul Curții de Apel Bacău, fiecare utilizator la baza de date cu caracter personal este autentificat în mod unic de un user și o parolă gestionate de către responsabilul cu protecția datelor care are și funcția de administrator de sistem.

Pentru o securitate sporită, utilizatorii care nu-și desfășoară activitatea o perioadă mai îndelungată, din diferite motive, (pensionare, demisie, transfer,...) sunt scoși din sistem, cei care încearcă să intre fraudulos în rețea prin autentificare cu o altă parolă decât cea desemnată, sunt restricționați automat.

Există o procedură de actualizare a conturilor de utilizatori ce se aplică lunar.

b) Protecție antivirus și antispam

Calculatoarele din rețeaua cu date cu caracter personal sunt protejate prin instalarea pe fiecare ca și pe server a unui program antivirus (ESET Security) cu licență și permanentă actualizare, ce asigură o protecție adecvată.

Ca o măsură suplimentară de protecție, rețeaua este configurată să acționeze un server suplimentar (proxy) al Ministerului Justiției care restricționează prin mai multe porturi desemnate atacurile nedorite.

c) Protecție antiefracție și video

La nivelul Curții de Apel Bacău, în spațiile unde se desfășoară activitatea, sunt instalate sisteme antiefracție și cu senzori de fum, iar intrarea se face pe bază de cod unic.

De asemenea, există un sistem propriu de 8 camere video care împreună cu cele ale unității de jandarmi ce asigură paza pot ajuta la identificarea video a eventualelor pătrunderi neautorizate.

d) Prelucrarea datelor cu caracter personal

Responsabilul cu protecția datelor cu caracter personal, în cadrul rețelei existente, stabilește utilizatorii desemnați pentru introducerea, modificarea sau actualizarea datelor în sistemul informatic.

Numai utilizatorii autorizați au dreptul și obligația de accesare a datelor cu caracter personal.

Sistemul realizat permite vizualizarea de către administratorul de sistem în orice moment numele și locația utilizatorului desemnat și operațiunea efectuată.

Datele actualizate sunt stocate în fișiere separate pentru fiecare utilizator cel puțin 2 ani, pentru a fi folosite ca probe în cazul investigațiilor. La nevoie, dacă se prelungesc cercetările, datele sunt păstrate cât timp este necesar.

e) Realizarea salvărilor de siguranță

La Curtea de Apel Bacău se fac copii de siguranță ale documentelor ce conțin date cu caracter personal la intervale stabilite.

Utilizatorii desemnați de responsabilul cu protecția datelor cu realizarea copiilor de siguranță cu rol și de administratori de sistem, sunt specialiștii IT.

Acest back-up se face periodic pe alt server protejat de utilizator și parolă într-o încăpere izolată și cu acces prin cod.

f) Sistemul informatic folosit

La Curtea de Apel Bacău sistemul informatic utilizat pentru protecția datelor cu caracter personal cuprinde:

- **Calculatoare** din cadrul instanței cu acces restricționat prin user și parolă, protejate de atacurile cibernetice, și prin reintroducerea parolei la deblocarea ecranului odată cu reluarea activității;
- **Servere de date** ce stochează informațiile cu caracter personal beneficiază de aceeași protecție controlată precum calculatoarele și în plus sunt situate într-o cameră a cărui temperatură constantă de 20 de grade este asigurată de unitățile de aer condiționat cu funcționare permanentă;
- **Sursele neinteruptibile (UPS)** contribuie în mare măsură la protejarea documentelor cu caracter personal oferind timpul necesar salvării în bune condițiuni a datelor înainte de închidere în cazul apariției penelor de curent;
- **Switch-uri** de rețea ce asigură interconectarea la rețeaua LAN protejată între diferitele calculatoare, imprimante și servere;
- **Rețeaua LAN** folosită este protejată printr-un server (proxy) de posibilele atacuri din exterior;
- **Imprimante de rețea** cu acces restricționat pentru imprimarea la nevoie și numai cu aprobarea prealabilă a conducerii instanței a documentelor solicitate;

- **Terminale de acces** folosite în relația cu publicul și care conțin date cu caracter personal, vor fi astfel montate ca să nu poată fi văzute de public, ele după o perioadă scurtă de inactivitate stabilită de operator își vor termina sesiunea și va necesita o nouă conectare sau se vor închide.

  La Curtea de Apel Bacău, din motive de maximă securitate, este interzisă folosirea rețelelor de tip wireless sau bluetooth între diferitele echipamente și pentru a nu introduce din exterior vulnerabilități prin posibila accesare.

g) Instruirea personalului

Utilizatorii Curții de Apel Bacău ce prelucrează date cu caracter personal sunt informați cu privire la prevederile Legii nr. 677/2001 pentru protecția datelor cu caracter personal și libera circulație a acestor date împreună cu actualizările ulterioare, precum și de cerințele esențiale de securitate și de confidențialitate a prelucrărilor de date cu caracter personal dar și asupra riscurilor pe care le implică nerespectarea acestora.

La terminarea lucrului cu datele cu caracter personal, utilizatorii sunt obligați să-și închidă sesiunea de lucru, iar documentele prelucrate sunt ținute în fișiere și dulapuri încuiate situate în încăperi cu acces restricționat.

Toate documentele care conțin date cu caracter personal se înregistrează și urmează regulile de păstrare, procesare, multiplicare, transport, transmitere, distrugere și arhivare stabilite prin Legea Arhivelor naționale și prin proceduri interne.

h) Controlul protecției datelor cu caracter personal la elaborarea documentelor de către utilizatori

Responsabilul cu monitorizarea aplicării legislației privind protecția datelor personale, specialist IT la Curtea de Apel Bacău, verifică săptămânal modul de introducere a datelor de către utilizatorii instanței.

Astfel, prin intermediul unui program denumit script se extrage și verifică într-un tabel toate câmpurile cu „Soluția pe scurt", și se salvează fișierele cu neregulile constatate, ulterior atrăgând atenția utilizatorilor în cauză în vederea anonimizării soluțiilor cu probleme și salvează datele.

Se constată, printr-o verificare mai atentă, o micșorare a numărului utilizatorilor cu probleme, ceea ce denotă faptul că și-au însușit temeinic, în urma instruirii făcute, importanța și modalitățile de protecție a datelor cu caracter personal.

Rezultatele verificărilor săptămânale sunt cumulate lunar într-un referat și aduse la cunoștința conducerii.

De asemenea, toate comunicările emanate de la instanță au prevăzut în antet precizarea: " *Operator de date cu caracter personal nr. 3666*"

PREȘEDINTE,
LOREDANA LENUȚA ALBESCU