CENTRUL NAŢIONAL DE RĂSPUNS LA INCIDENTE DE SECURITATE CIBERNETICĂ

CERT-RO

PROCEDURĂ PENTRU GESTIONAREA DATELOR CU CARACTER PERSONAL

Versiunea 1.0

APROB

DIRECTOR GENERAL CERT-RO

Augustin Jianu

Pagină albă

TERMENI SPECIFICI

Prin **operator** se înțelege orice instituție publică sau privată care are dreptul de a lucra cu date considerate a fi cu caracter personal, conform legii aflate în vigoare în acest sens.

Prin **utilizator** se înţelege orice persoană care acţionează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.

Prin **alertă de securitate cibernetică** se înțelege orice semnalare ce conține o adresă IP sau un domeniu web (URL), referitoare la un posibil incident sau eveniment de securitate cibernetică, ce implică sau poate implica sisteme informatice din spațiul cibernetic național deținute/administrate de persoane fizice sau juridice.

Prin **incident de securitate cibernetică** se înțelege orice eveniment survenit în spaţiul cibernetic a cărui consecinţe afectează securitatea cibernetică sau orice acțiune, contrară oricăror reglementări în vigoare, în legătură cu un sistem informatic, a cărei consecință poate afecta sau a afectat securitatea cibernetică a acestuia, sau a dus la compromiterea informațiilor procesate de acesta.

Activitatea de răspuns (rezolvare) la alerte de securitate cibernetică - acțiunile desfășurate în scopul apărării cibernetice, investigării alertei de securitate sau restabilirii stării normale de funcționare a unui sistem informatic, în urma unui incident/eveniment de securitate, precum și în scopul identificării cauzelor incidentului/evenimentului.

PRINCIPII de BAZĂ

Principiile care stau la baza protecţiei datelor cu caracter personal sunt:

- **Prelucrate cu buna-credinţă şi în conformitate cu dispoziţiile legale în vigoare**;

  Prelucrarea datelor include colectarea, înregistrarea, organizarea, stocarea, consultarea, utilizarea, transferul, combinarea, blocarea, ştergerea sau distrugerea lor.

  Datele obţinute se vor prelucra numai în scopurile permise de lege. Legea impune condiţii suplimentare când este vorba de date sensibile, referitoare la originea rasială sau etnică, convingerile politice, religioase, apartenenţa sindicală, starea de sănătate sau viaţa sexuală. CERT-RO nu colectează date considerate sensibile, coform legii.

- **Datele sunt colectate în scopuri determinate, explicite şi legitime**;

  Prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice sau de cercetare nu va fi considerată incompatibilă cu scopul colectării, dacă se efectuează cu respectarea dispoziţiilor legilor în vigoare, precum şi cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele care reglementează activitatea statistica ori cercetarea;

- **Datele sunt adecvate, pertinente şi neexcesive prin raportare la scopul în care sunt colectate şi ulterior prelucrate**;
- **Datele sunt exacte şi, dacã este cazul, actualizate**;

  În acest scop se vor lua măsurile necesare pentru ca datele inexacte sau incomplete din punct de vedere al scopului pentru care sunt colectate şi pentru care vor fi ulterior prelucrate, să fie şterse sau rectificate;

- **Datele sunt stocate într-o formă care să permită identificarea persoanelor vizate strict pe durata necesară realizării scopurilor în care datele sunt colectate şi în care vor fi ulterior prelucrate**;

  Stocarea datelor pe o durata mai mare decât cea menţionată, în scopuri statistice sau de cercetare se va face cu respectarea garanţiilor privind prelucrarea datelor cu caracter personal, prevăzute în normele care reglementează aceste domenii, şi numai pentru perioada necesară realizării acestor scopuri.

REGULI PENTRU SECURITATEA DATELOR CU CARACTER PERSONAL

- Operatorul desemnează utilizatori autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional. Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori autorizaţi desemnaţi de operator.
- Operatorul va lua măsuri pentru ca sistemul informaţional să înregistreze cine a făcut modificarea, data şi ora modificării. Pentru o mai bună administrare operatorul va lua măsuri ca sistemul informaţional să menţină datele şterse sau modificate.
- Operatorul stabileşte intervalul de timp la care se vor executa copiile de siguranţă ale bazelor de date cu caracter personal, precum şi ale programelor folosite pentru prelucrările automatizate. Utilizatorii care execută aceste copii de siguranţă vor fi numiţi de operator, într-un număr restrâns. Operatorul trebuie să ia măsuri ca accesul la copiile de siguranţă să fie monitorizat.
- Computerele şi alte terminale de acces pot fi instalate în încăperi cu acces restricţionat. Dacă nu pot fi asigurate aceste condiţii, computerele se vor instala în încăperi care se pot încuia sau se vor lua măsuri ca accesul la computere să se facă cu ajutorul unor chei ori cartele magnetice. Dacă pe ecran apar date cu caracter personal asupra cărora nu se acţionează o perioadă dată, stabilită de operator, sesiunea de lucru trebuie închisă 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 operator, în care nu se acţionează asupra lor, acestea trebuie ascunse.
- Operatorul este obligat să ia măsuri ca orice accesare a bazei de date cu caracter personal să fie înregistrată într-un fişier de acces (numit log la prelucrările automate) sau într-un registru pentru prelucrările manuale de date cu caracter personal, stabilit de operator.
- Pentru prelucrările automate aceste informaţii vor fi stocate într-un fişier de acces general sau în fişiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată. Operatorul este obligat să păstreze

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.

- Operatorii sunt obligaţi să conceapă sistemul de telecomunicaţii astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde. Dacă sistemul de telecomunicaţii nu poate fi astfel securizat, operatorul este obligat să impună folosirea metodei de criptare pentru transmisia datelor cu caracter personal. Prin sistemele de telecomunicaţii se vor transmite numai datele cu caracter personal strict necesare.
- În cadrul cursurilor de pregătire a utilizatorilor operatorul este obligat să facă informarea acestora cu privire la prevederile Legii nr. 677/2001 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, în funcţie de specificul activităţii utilizatorului. Utilizatorii care au acces la date cu caracter personal vor fi instruiţi de către operator asupra confidenţialităţii acestora. Utilizatorii sunt obligaţi să îşi închidă sesiunea de lucru atunci când părăsesc locul de muncă.
- Pentru menţinerea securităţii prelucrării datelor cu caracter personal (în special împotriva viruşilor informatici) operatorul va lua măsuri care vor consta în: a) interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase; b) informarea utilizatorilor în privinţa pericolului privind viruşii informatici; c) implementarea unor sisteme automate de devirusare şi de securitate a sistemelor informatice; d) dezactivarea, pe cât posibil, a tastei “Print screen”, atunci când sunt afişate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora.
- Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de utilizatori autorizaţi pentru această operaţiune de către operator. Operatorii sunt obligaţi să aprobe proceduri interne specifice privind folosirea şi distrugerea acestor materiale. Fiecare entitate îşi va aproba propriul sistem de securitate, ţinând seama de aceste cerinţe minime de securitate a prelucrărilor de date cu caracter personal,

iar în funcţie de importanţa datelor cu caracter personal prelucrate, îşi va impune măsuri de securitate suplimentare.

OBLIGAȚII SPECIFICE ALE UTLIZATORILOR

- Să cunoască şi să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal precum şi ale prezentei proceduri;
- Să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condiţiile legii, cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute şi consecinţele refuzului de a le pune la dispoziţie, drepturile prevăzute de lege, în special drepturile de acces, de intervenţie asupra datelor şi de opoziţie, condiţiile în care pot fi exercitate aceste drepturi;
- Să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuţiilor de serviciu şi să acorde sprijin conducătorului operatorului pentru realizarea activităţilor specifice ale acestuia; d) să păstreze confidenţialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal; e) să respecte măsurile de securitate, precum şi celelalte reguli stabilite de operator; f) să informeze de îndată conducerea instituţiei despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situaţie în care au fost accesate/ prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoştinţă.

ETAPELE GESTIONĂRII DATELOR CU CARACTER PERSONAL

1. COLECTARE

Activitatea de răspuns la incidente de securitate cibernetică se bazează pe primirea de alerte de către CERT-RO, respectiv semnalări asupra identificării unor incidente sau evenimente de securitate cibernetică. Acestea pot fi transmise prin orice mijloc, de către orice entitate (persoană fizică sau juridică), atât timp cât se asigură confidențialitatea comunicării, iar datele transmise sunt coerente și complete.

Prin **alertă de securitate cibernetică** înțelegem orice semnalare ce conține o adresă IP sau un domeniu web (URL), referitoare la un posibil incident sau eveniment de securitate cibernetică, ce implică sau poate implica sisteme informatice din spațiul cibernetic național deținute/administrate de persoane fizice sau juridice.

SURSE DE COLECTARE A DATELOR

1.1. Alerte colectate și transmise prin intermediul unor sisteme automate

Aceste alerte sunt transmise de către organizații specializate, ce dețin sisteme de detecție a incidentelor de securitate cibernetică. Marea majoritate a acestor alerte (99%) sunt procesate automat de către CERT-RO și transmise către furnizorii de servicii Internet ce dețin/administrează infrastructurile vizate de alerte (IP, domeniu/URL etc.).

În cazul acestui tip de alerte, CERT-RO nu deține date exacte despre utilizatorul adresei IP, identificarea acestuia putând fi făcută numai de către furnizorul de servicii internet (ISP), care de altfel ar trebui să retransmită și alerta către client.

1.2. Alerte colectate prin intermediul serviciului de e-mail

CERT-RO colectează aceste alerte prin intermediul adresei de e-mail alerts@cert.ro, adresă unde orice utilizator/organizație afectată de un incident de securitate cibernetică poate notifica problema pentru analiză și rezolvare către CERT-RO.

Aceste alerte sunt considerabil mai puține decât cele automate, dar conțin informații mult mai complete și mai relevante despre incident și despre organizația afectată, precum sursa atacului și metoda de atac. În majoritatea cazurilor datele sunt colectate de la entitățile afectate (persoane fizice sau juridice din țară sau străinătate), de către analiștii CERT-RO, odată cu raportarea incidentului.

1.3. Alerte colectate prin intermediul apelurilor telefonice

Pe lângă alertele colectate și transmise automatizat, CERT-RO primește totodată sesizări transmise telefonic de către persoane fizice sau juridice din țară sau străinătate, cu privire la incidente de securitate cibernetică. Datele colectate depind de natura incidentului de securitate cibernetică notificat și de acordul telefonic al interlocutorului de a furniza aceste date.

1.4. Alerte colectate prin intermediul corespondenței scrise

O altă modalitatea de sesizare a CERT-RO cu privire la incidente de securitate cibernetică o reprezintă corespondeța scrisă. Sesizarea poate fi depusă sau transmisă în scris de către persoane fizice sau juridice, din țară sau străinătate.

1.5. Date colectate despre vizitatorii site-ului web www.cert.ro

Site-ul web www.cert.ro folosește un instrument de monitorizare a traficului denumit *Google Analytics*. Acesată platformă colectează și interpretează, în scop statistic, informații cu privire la:

- *HTTP Referrer* - informații transmise unei pagini web de destinație, cu privire la ultima pagină pe care a accesat-o browserul web;

- *Adresa IP* - Fiecare echipament conectat la Internet primește o astfel de adresă, care este unică. Deoarece adresele IP sunt alocate pe grupe, pot fi utilizate la poziționarea geografică a echipamentului folosit;

- *Identificatorul unic al dispozitivului* - denumit și UUID;

- *Date legate de browser* - denumire și versiune;

- *Date legate de sistemul de operare* - denumire și versiune;

- *Identificatori de timp* - data și ora la care au fost realizate conexiunile, precum și durata acestora.

1.6. Asigurarea suportului tehnic în cadrul investigațiilor derulate de organele competente

Există cazuri în care CERT-RO este solicitată să analizeze diferite echipamente, pentru derularea investigațiilor organelor competente.

Personalul CERT-RO care realizează acest proces este format din specialiști în securitate cibernetică cu pregătire tehnică necesară pentru activitatea de *forensic*. Datele colectate în aceste cazuri pot varia și depind de conținutul instrumentelor vizate (dispozitive electronice, capturi de memorie, capturi de hard-disk, capturi de trafic sau orice alt tip de fișiere în format electronic). Colectarea datelor ce pot conține date cu caracter personal se face după semnarea în prealabil a unui acord legal/proces verbal între proprietarul datelor sau reprezentantul său legal și CERT-RO sau în urma solicitărilor legale ale instituțiilor statului cu competențe în domeniu.

2. PRELUCRARE

În cazul prelucrării datelor cu caracter personal, operatorul este obligat să aplice măsurile tehnice şi organizatorice adecvate pentru protejarea datelor împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei reţele, precum şi împotriva oricărei alte forme de prelucrare ilegală.

Personalul responsabil cu activitatea de răspuns la alertele de securitate are obligația de a lua în considerare toate datele transmise și în orice format. Acesta va verifica

corectitudinea datelor transmise și se va asigura că acestea sunt complete și se pot folosi în rezolvarea alertei.

De regulă orice alertă trebuie să conțină cel puțin următoarele date: date de identificare ale petentului; adrese IP, adrese de email, timestamp și servicii afectate ale victimei; adrese IP, adrese de email sau surse generatoare ale atacului; fișiere de tip log care să demonstreze existența și identificarea incidentului/evenimentului sau orice alte fișiere ce pot constitui probe.

Pe baza informațiilor complete și corecte referitoare la alertă, personalul responsabil poate trece la identificarea entităților reale ce reprezintă sursa precum și victima incidentului/evenimentului. Ulterior, se vor identifica persoanelor fizice sau juridice ce trebuie contactate pentru rezolvarea incidentului (furnizor de serviciide internet - ISP, deținători domenii .ro sau clase de adrese IP, persoane fizice juridice etc.)

3. VALORIFICARE

3.1. Alertarea urgentă a entităților afectate precum și a instituțiilor cu responsabilități

În momentul în care sunt colectate date suficiente despre victimă, sursa atacului, entitățile implicate, instituțiile publice responsabile, tipul de incident precum și date care să confirme existența acestuia, personalul responsabil trebuie să transmită urgent alerte de notificare către toate părțile implicate.

În cadrul activității de notificare se vor aplica principiile enumerate mai sus, entitatea afectată fiind prima alertată despre existența incidentului/evenimentului. În cazul în care responsabilitatea rezolvării incidentului/evenimentului cade în sarcina altei instituții/autorități, iar acea instituție/autoritate consideră necesar ca alerta să nu fie transmisă către părțile afectate, pentru a nu perturba activitățile post-incident/eveniment, atunci personalul responsabil va respecta întocmai decizia instituției/autorității.

Alertele transmise către părțile implicate trebuie să conțină următoarele:

- Date relevante despre CERT-RO și baza legală în urma căreia se transmit alertele.

- Date despre resursele tehnice ce fac parte din incident/eveniment (resurse afectate sau resursele ce produc atacul).
- Fișiere log, sau orice alte probe ce pot susține existența atacului.
- Măsurile exprese ce trebuie luate de către destinatarul alertei.
- Date de contact pentru comunicări ulterioare asupra incidentului/evenimentului.
- Solicitare de răspuns cu privire la măsurile luate de părțile afectate.
- Detalii despre cum au fost obținute datele despre incident/eveniment (doar în cazul în care este neapărat necesar; dezvăluirea sursei nu reprezintă un obiectiv al activității de alertare).

Datele cu caracter personal se pot comunica între operatori şi împuterniciţii acestora sau între operatori sau împuterniciţi ai acestora şi alte instituţii ori organisme publice sau entităţi de drept public sau privat în una dintre următoarele situaţii:

1. dacă persoana vizată şi-a dat consimţământul expres şi neechivoc pentru comunicarea datelor sale;
2. fără consimţământul persoanei vizate, în cazurile prevăzute de lege.

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.

Comunicarea datelor cu caracter personal de către operatori şi împuterniciţii acestora se poate face şi on-line, cu respectarea dispoziţiilor specificate anterior şi asigurarea securităţii sistemelor de comunicaţii a datelor cu caracter personal.

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

3.2. Lansarea investigației detaliate (dacă este cazul)

În cazul în care o parte afectată solicită date suplimentare despre incidentul/evenimentul de securitate, personalul responsabil va contacta părțile ce pot oferi aceste informații, solicitându-le în scopul finalizării investigației.

În acest caz investigații suplimentare pot fi demarate, putând fi folosite orice surse disponibile.

3.3. Publicarea de documente tehnice și rapoarte asupra incidentului / evenimentului fără a menționa date cu caracter personal

Pentru restrângerea numărului posibilelor victime ale amenințării ce a generat incidentul de securitate, personalul responsabil va transmite alerte de atenționare către toți partenerii vizați, sau chiar către publicul larg în caz că se impune.

Alertele vor fi transmise prin email, notificări oficiale sau vor fi publicate pe pagina de Internet a CERT-RO. Alertele trebuie să conțină date relevante despre tipul amenințării, modalități de detecție precum și modalități de protecție.

3.4. Închiderea/clasarea alertei de securitate

Alerta de securitate este considerată închisă/clasată în momentul în care au fost alertate toate părțile responsabile precum și cele afectate (sursă și victimă), acestea confirmând primirea mesajelor și demararea activităților de remediere a problemelor. Pentru ca alerta să poată fi considerată închisă/clasată trebuie ca toate posibilitățile de acțiune ale CERT-RO să fie epuizate.

În cazul în care părțile notificate nu vor da curs solicitării CERT-RO timp de o săptămână, incidentul/evenimentul este considerat închis/clasat.

4. DISTRUGEREA/ANONIMIZAREA DATELOR

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 nationale şi prin proceduri interne.

Datele cu caracter personal sunt păstrate cel putin 2 ani, pentru a fi puse la dispoziție în cazul solicitării legale a organelor competente ori pentru considerente statistice. Dacă investigaţiile se prelungesc, aceste fișiere se vor păstra atât timp cât se va considera necesar.

Accesul în scop statistic la datele cu caracter personal este permis, după încheierea perioadei necesare realizării scopurilor în care datele sunt colectate, doar în cazul în care acestea au fost transformate în date anonime.

Atribuția monitorizării datelor cu caracter personal după închiderea/clasare incidentelor de securitate cibernetică va fi a Comisiei de distrugere/anonimizare a datelor cu caracter personal. Comisia se va reuni o dată pe lună pentru a analiza volumul de date ieșit din termenul acordat pentru rezolvarea incidentului pentru a lua o decizie referitoare la stocarea datelor sau, în alte cazuri, cu privire la înapoierea lor.