Asociaţia Naţională a Evaluatorilor Autorizaţi din România

HOTĂRÂRE

pentru aprobarea Politicii de răspuns la incidentele și breșele de securitate referitoare la datele cu caracter personal

În temeiul art. 5 alin. (2) şi al art.8 alin. (8) lit. j) din Ordonanţa Guvernului nr. 24/2011 privind unele măsuri în domeniul evaluării bunurilor, aprobată cu modificări prin Legea nr. 99/2013, cu modificările şi completările ulterioare

În vederea aducerii la îndeplinire a prevederilor Regulamentului (UE) 2016/679 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date, pus în aplicare în România prin Legea 190/2018 (RGPD);

Consiliul director al Asociaţiei Naţionale a Evaluatorilor Autorizaţi din România adoptă prezenta hotărâre.

Art. 1. – Se aprobă Politica de răspuns la incidentele și breșele de securitate referitoare la datele cu caracter personal, prevăzuta in anexa care face parte integrantă din prezenta hotărâre.

Art. 2. – Prezenta hotărâre se publică în Buletinul informativ şi pe pagina web a Asociației și intră în vigoare la data publicării pe pagina web.

Preşedintele Asociaţiei Naţionale a Evaluatorilor Autorizaţi din România

Sorin Adrian Petre

ASOCIAȚIA NAȚIONALĂ A EVALUATORILOR AUTORIZAȚI DIN ROMÂNIA
ANEVAR

Bucureşti, 25 noiembrie 2020

Nr. 86

Anexa la HCD nr. 86/2020

Politica de răspuns la incidentele și breșele de securitate referitoare la datele cu caracter personal

I. Cadrul general

(1) Asociația Națională a Evaluatorilor Autorizați din România, numită în continuare „Asociația" are obligația, conform RGPD, de a lua măsuri pentru ca datele cu caracter personal pe care le prelucrează să fie păstrate în condiții de siguranță.

(2) Această politică detaliază modul în care Asociația va păstra evidența incidentelor de securitate și modul de răspuns în eventualitatea unor breșe de securitate.

(3) Indiferent de toate precauțiile și măsurile aplicate de Asociație pentru stocarea și utilizarea în siguranță a datelor, va exista întotdeauna un potențial de producere a unui incident sau a unei breșe de securitate cu impact asupra datelor cu caracter personal. Din acest motiv este necesară implementarea unui sistem care să permită depistarea momentului producerii incidentelor sau breșelor, limitarea efectelor negative și contracararea rapidă și eficientă a acestora.

(4) Această politică se aplică tuturor angajaților, prestatorilor de servicii precum și membrilor Consiliului director, ai Consiliilor filialelor și ai grupurilor de lucru care au acces la informațiile deținute de Asociație.

(5) Această politică se completează cu următoarele documente:

- Regulamentul European 2016/679 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date, pus în aplicare în România prin Legea 190/2018 (RGPD);
- Politica de securitate a datelor cu caracter personal (care definește noțiunile de incident și breșă de securitate și conține prevederi specifice privind măsurile de precauție și prevenire);
- Politica de confidențialitate cu privire la prelucrarea datelor cu caracter personal.

II. Scop şi obiective

(6) Această politică stabileşte modalitatea de înregistrare a incidentelor de securitate şi de tratare a oricăror breşe de securitate care ar putea surveni, concentrându-se asupra etapelor de urmat în momentul în care este descoperită o breşă şi a măsurilor pe care angajaţii le vor aplica în această situaţie.

(7) Situaţiile de pierdere sau corupere a datelor cu caracter personal de către Asociaţie sunt rare; cu toate acestea, consecinţele asupra imaginii Asociaţiei şi impactul potenţial asupra persoanelor vizate şi asupra disponibilităţii datelor impun existenţa unui plan de acţiuni rapide şi adecvate în eventualitatea producerii unui incident.

(8) Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P.) are atribuţia legală de a impune amenzi semnificative în cazul unor încălcări serioase ale prevederilor RGPD de către operatorii de date cu caracter personal. Totodată, Autoritatea poate impune măsuri corective constând în remedierea, într-un anumit termen, a încălcărilor constatate. Există însă şi posibilitatea ca operatorii să primească atât amenda cât şi măsuri corective.

(9) Prin urmare, această politică urmăreşte să ofere o abordare a situaţiilor nedorite în care pot avea loc incidente cu impact asupra datelor cu caracter personal. Totuşi, managementul incidentelor şi breşelor de securitate este un proces complex, cu multe variabile potenţiale, astfel încât este necesară o analiză echilibrată, de la caz la caz.

(10) RGPD impune obligaţia notificării autorităţii de supraveghere în cazul încălcării securităţii datelor cu caracter personal, fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data la care operatorul a luat act de producerea acesteia. În plus, operatorul trebuie să păstreze documente referitoare la toate cazurile de încălcare a securităţii datelor cu caracter personal. Aceste înregistrări trebuie să cuprindă o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor cu caracter personal, a efectelor acesteia şi a măsurilor de remediere întreprinse. Această documentaţie permite autorităţii de supraveghere să verifice conformitatea cu prevederile Regulamentului.

(11) Pentru motivele enunţate anterior, este esenţial ca întregul staff al Asociaţiei să fie pregătit să identifice o breşă de securitate şi să raporteze toate incidentele cât mai curând posibil de la producerea acestora.

III. Cum recunoaştem un incident / o breşă de securitate?

(12) Un incident de securitate este un eveniment care aduce sau are potențialul de a aduce atingere datelor cu caracter personal, în mod accidental sau intenționat, a datelor cu caracter personal, în timp ce o breșă de securitate apare ca efect al unui incident de securitate și poate duce la pierderea, dezvăluirea, alterarea sau distrugerea datelor. Diferența dintre cele două constă în aceea că cele mai multe dintre incidentele de securitate nu produc întotdeauna o breșă. Tipurile de incidente sunt descrise pe larg în Politica de securitate a datelor cu caracter personal.

(13) În multe cazuri, detectarea unui incident de securitate are loc după mult timp de la producerea acestuia. Din acest motiv este importantă înțelegerea cauzelor care determină problemele de securitate.

(14) Cauzele incidentelor de securitate pot fi externe (terţe părţi – hackeri, persoane neautorizate care pătrund în sediu sau dobândesc acces la sistemele informatice, atacuri de tip ransomware, malware sau phishing, prestatori care nu respectă bunele practici de securitate) sau interne (spre exemplu, angajaţi neinstruiţi în privinţa procedurilor de securitate, neglijenţă sau eroare umană care duce la divulgări de informaţii din interior etc.). Conform studiilor recente, 70% din incidentele legate de încălcarea securităţii datelor sunt datorate vulnerabilităţilor interne şi doar 30% au cauze externe.

(15) Recunoașterea primelor semnale de alarmă este foarte importantă în detectarea incidentelor de securitate. De cele mai multe ori nu soluțiile tehnologice implementate ci vigilența umană este cea care grăbește timpul necesar pentru depistarea breșelor de securitate. Deşi **indiciile** privind compromiterea datelor depind de tipul atacului, există totuși câteva semnale de alarmă care ridică suspiciuni:

- durate de login neobișnuit de mari; login-uri multiple eșuate sau neobișnuite;
- prezența unui IP-uri necunoscute sau neautorizate în rețelele wireless;
- activitate suspectă în rețea după orele de program;
- reducerea vitezei de operare a calculatoarelor și serverelor;
- trafic neobișnuit în rețea; restartări sau închideri pe neașteptate ale calculatoarelor;
- proasta funcționare sau blocarea programelor antivirus sau de securitate informatică;
- erori ale aplicațiilor sau aplicații configurate să ruleze automat fără autorizare;

- porturi nou deschise în sistemele firewall etc.

(16) Din punct de vedere al securității datelor, pot fi identificate trei categorii de breșe:

- ***breșe care afectează disponibilitatea datelor*** – acestea corespund distrugerii accidentale sau intenționate sau pierderii datelor cu caracter personal;
- ***breșe de integritate*** – care se referă la alterarea (modificarea) datelor;
- ***breșe de confidențialitate*** – care se referă la accesul neautorizat sau la dezvăluirea de date cu caracter personal.

IV. Raportarea incidentelor

(17) De îndată ce un incident de securitate a fost detectat, acesta va fi raportat superiorului ierarhic.

(18) În cazul unor incidente legate de securitatea echipamentelor și sistemelor informatice ale asociației (inclusiv furtul sau pierderea unor laptopuri, tablete, telefoane mobile) va fi informat departamentul IT și administratorul rețelei IT în cel mai scurt timp posibil.

(19) Responsabilul cu protecția datelor va fi informat imediat dacă incidentele de securitate implică date cu caracter personal.

(20) Membrii Consiliului director, ai Consiliilor filialelor și ai grupurilor de lucru vor notifica Directorul general în cazul producerii unor incidente legate de activitatea acestora în cadrul Asociației.

(21) Directorul general, în urma analizării situației și a consultării cu responsabilul cu protecția datelor și cu administratorul rețelei IT, va stabili dacă în urma unui incident s-a produs sau nu o breșă de securitate.

(22) În cazul producerii unei breșe asupra datelor cu caracter personal în situațiile în care Asociația acționează ca operator asociat sau ca împuternicit, părțile implicate vor fi notificate imediat. În mod similar, dacă o organizație parteneră se confruntă cu o breșă de securitate asupra datelor cu caracter personal, efectele acesteia asupra Asociației vor fi evaluate cu atenție astfel încât să fie protejate interesele Asociației și ale membrilor acesteia.

(23) Atunci când e suspectată producerea unui incident, pentru a putea estima gravitatea potențialei breșe de securitate sunt necesare următoarele informații:

- tipul datelor implicate

- gradul de sensibilitate a datelor
- dacă datele au fost pierdute sau sustrase, dacă există protecţii (criptare, parolare)
- ce s-a întâmplat cu datele
- ce informaţii ar putea afla o terţă parte despre o persoană, pe baza acestor date
- numărul persoanelor afectate de breşa de securitate
- identitatea persoanelor ale căror date au fost compromise
- efectele negative asupra persoanelor ale căror date au fost afectate, atât directe cât şi indirecte (secundare)
- implicaţiile mai largi pe care le poate avea asupra Asociaţiei o astfel de breşă (pierderea încrederii, publicitate negativă, consecinţe financiare – amenzi, despăgubiri sau juridice – procese intentate de părţile afectate)

(24) Dacă după evaluarea impactului unui incident a fost identificată cu certitudine o breşă de securitate, va fi formată o echipă de răspuns la incidente, coordonată de responsabilul cu protecţia datelor. Această echipă va fi formată din personalul cheie din cadrul departamentelor afectate de breşă.

(25) În funcţie de severitatea breşei, echipa poate fi formată, după caz, din unul sau mai mulţi angajaţi ai departamentului afectat, şeful de departament, reprezentanţii departamentului IT, administratorul reţelei IT, responsabilul cu protecţia datelor, departamentul juridic, directorul general.

(26) Incidentele nu vor necesita doar un răspuns iniţial constând în investigarea şi ţinerea sub control a situaţiei ci şi un **plan de redresare** care va include, după caz:

- limitarea daunelor – prevenirea unor daune suplimentare şi izolarea sistemelor afectate;
- stabilirea celor care trebuie informaţi cu privire la producerea incidentului şi a măsurilor necesare (de exemplu, izolarea sau închiderea zonelor compromise ale reţelei, găsirea unui echipament pierdut, schimbarea parolelor şi a codurilor de acces, ştergerea de la distanţă a datelor de pe telefoanele inteligente, actualizarea programelor antivirus etc.);
- eradicarea cauzei – identificarea cauzei producerii incidentului, soluţionarea problemelor cauzate de aceasta şi monitorizarea periodică pentru a preveni repetarea ameninţărilor;
- posibilitatea de a recupera datele pierdute sau de a limita impactul negativ;

- evaluarea riscului producerii unor consecinţe negative asupra persoanelor vizate (cât de serioase sunt efectele negative, care este probabilitatea lor de a se produce şi ce măsuri pot fi luate pentru a-i proteja pe cei afectaţi de incident);
- restaurarea sistemelor / datelor.

(27) Acţiunile care vor fi luate în eventualitatea producerii unor breşe vor avea ca obiectiv:

- limitarea şi stoparea efectelor negative
- protejarea intereselor persoanelor afectate
- protejarea intereselor Asociaţiei
- îndeplinirea cerinţelor prevăzute de RGPD în privinţa notificării Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P.)

V. Notificarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P.)

(28) RGDP impune operatorilor de date obligaţia de a raporta anumite tipuri de breşe de securitate către Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P.)

(29) O breşă de securitate susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor fizice trebuie raportată autorităţii de supraveghere fără întârzieri nejustificate şi, dacă este posibil, în termen de cel mult 72 de ore de la data constatării producerii acesteia. În cazul depăşirii acestui termen, notificarea va fi însoţită de o motivaţie a întârzierii.

(30) Riscurile pentru drepturile şi libertăţile persoanelor se referă la discriminare, afectarea reputaţiei, pierderi financiare, pierderea confidenţialităţii şi orice alt dezavantaj semnificativ de natură economică sau socială.

(31) Analiza cu privire la aceste riscuri se va face de la caz la caz. În cazul în care nu sunt identificate riscuri care pot afecta drepturile şi libertăţile fundamentale ale persoanelor vizate, nu este obligatorie notificarea Autorităţii.

(32) Notificarea trebuie să conţină:

a) descrierea caracterului breşei de securitate care afectează datele cu caracter personal;

b) categoriile și numărul aproximativ al persoanelor vizate, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
c) numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
d) descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
e) măsurile luate sau propuse pentru a remedia breșa, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

(33) Atunci când nu este posibil să fie furnizate informațiile în același timp, acestea pot fi transmise în mai multe etape, fără întârzieri nejustificate.

(34) Notificarea va fi transmisă prin intermediul formularului online disponibil pe site-ul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal - dataprotection.ro.

(35) Asociația va păstra documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal care cuprind o descriere a situației de fapt în care s-a produs breșa, efectele acesteia și măsurile de remediere întreprinse.

VI. Informarea persoanelor vizate cu privire la încălcarea securității datelor cu caracter personal

(36) Atunci când o breșă de securitate este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, Asociația va comunica fără întârziere producerea acestei încălcări a securității datelor către persoanele vizate, după detectarea acesteia. Informarea nu este condiționată de notificarea Autorității de supraveghere sau de un anumit număr al persoanelor afectate.

(37) Riscurile există atunci când breșa de securitate poate conduce la efecte negative și vulnerabilitate (în mod direct sau indirect), respectiv la daune fizice, materiale sau non-materiale pentru persoanele ale căror date au fost afectate (discriminare, furt de identitate sau fraudă, pierderi financiare, afectarea renumelui profesional, a reputației etc.).

(38) În cazurile în care breșele de securitate implică date care dezvăluie originea etnică sau rasială, opiniile politice, credințele religioase sau filosofice, apartenența la sindicate, date genetice, date privind starea de sănătate, orientarea sexuală sau condamnările penale, este foarte probabil să survină astfel de daune.

(39) Informarea transmisă persoanei vizate se va face în scris (prin email, scrisoare sau prin intermediul paginii personale) şi va include o descriere într-un limbaj clar şi simplu a naturii breşei de securitate, precum şi informaţiile şi recomandările menţionate în cadrul paragrafului (32), lit. b), c) şi d).

(40) Informarea persoanei vizate nu este necesară în următoarele situaţii:

- Asociaţia a adoptat măsuri de protecţie tehnice şi organizatorice adecvate, aplicate în cazul datelor cu caracter personal afectate de încălcarea securităţii, în special măsuri prin care datele devin neinteligibile persoanelor neautorizate să le acceseze (de exemplu, criptarea);
- Asociaţia a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile şi libertăţile persoanelor nu mai este susceptibil să se materializeze;
- ar necesita un efort disproporţionat. În această situaţie, se va efectua o informare publică, prin intermediul site-ului, al newsletter-ului sau al unui ziar cu circulaţie naţională.

(41) Rolul informării este acela de a oferi persoanelor vizate informaţiile necesare pentru a reduce efectele negative care decurg din circumstanţele producerii breşei. Atunci când Asociaţia nu are certitudinea producerii unor efecte negative, va alege calea prudenţei şi va notifica persoanele vizate.

(42) În cazul unor date cu caracter personal care sunt publice (de exemplu, Tabloul Asociaţiei), ori de câte ori este afectat nivelul de disponibilitate sau de publicitate ca urmare a producerii unui incident, se va considera că s-a produs o breşă de confidenţialitate iar dacă aceasta este probabil să producă efecte negative, va fi adusă la cunoştinţa persoanelor vizate.

VII. Evaluarea ulterioară a breşelor de securitate

(43) După finalizarea acţiunilor de răspuns imediat la producerea unei breşe de securitate, este importantă atât investigarea cauzelor apariţiei breşei cât şi evaluarea eficacităţii planului de răspuns.

(44) Dacă s-a constatat că breşa de securitate s-a produs datorită unor erori de aplicare a procedurilor sau a alocării deficitare a responsabilităţilor, a continua activitatea ca şi când nimic nu s-ar fi întâmplat este nerecomandabil. În astfel de situaţii, vor fi luate măsuri de îmbunătăţire în cel mai scurt timp posibil iar acestea vor fi comunicate angajaţilor în scris, astfel încât Asociaţia să poată demonstra că a acţionat într-o manieră responsabilă. În plus, vor fi

organizate acţiuni suplimentare de instruire a personalului cu privire la protecţia datelor cu caracter personal.

(45) Dacă breşa s-a produs datorită unor atacuri informatice sau a vulnerabilităţii sistemelor IT ale Asociaţiei, vor fi luate măsuri tehnice pentru a preveni atacuri recurente viitoare.

VIII. Măsuri de prevenire şi reducere a riscurilor

(46) Pentru a preveni breşele de disponibilitate şi integritate a datelor, Asociaţia va face back-up-uri periodice ale datelor cu caracter personal şi le va stoca pe un server dedicat, în condiţii de siguranţă.

(47) Pentru a preveni breşele de confidenţialitate şi a reduce efectele negative asociate, vor fi luate următoarele măsuri:

- aplicarea recomandărilor descrise în Politica de securitate a datelor şi în Politica de confidenţialitate cu privire la prelucrarea datelor cu caracter personal;
- monitorizarea continuă a vulnerabilităţilor potenţiale ale tehnologiilor utilizate (scanarea website-ului din punct de vedere al vulnerabilităţilor, actualizarea programelor antivirus, filtrarea emailurilor de tip spam etc.)
- securizarea conturilor de membru de pe site-ul Asociaţiei şi pagina personală şi recomandarea schimbării parolei odată cu lansarea noii aplicaţii de evidenţă a membrilor şi a noului portal extern.

IX. Validitatea politicii (versiunea 1 – 2020)

Această politică a intrat în vigoare la data de …….. şi va fi verificată şi actualizată periodic de responsabilul cu protecţia datelor.