REGULAMENTE

REGULAMENTUL (UE) NR. 611/2013 AL COMISIEI

din 24 iunie 2013

privind măsurile aplicabile notificării încălcărilor securității datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European și a Consiliului privind confidențialitatea și comunicațiile electronice

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) ([1]), în special articolul 4 alineatul (5),

după consultarea Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (ENISA),

după consultarea Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, instituit prin articolul 29 din Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date ([2]) (Grupul de lucru instituit prin articolul 29),

după consultarea Autorității Europene pentru Protecția Datelor (AEPD),

întrucât:

(1) Directiva 2002/58/CE prevede armonizarea dispozițiilor naționale, lucru necesar în vederea asigurării unui nivel echivalent de protecție a drepturilor și libertăților fundamentale, în special a dreptului la confidențialitate și la respectarea vieții private, în domeniul prelucrării de date cu caracter personal în sectorul comunicațiilor electronice, precum și în vederea asigurării liberei circulații a acestor date și a serviciilor și echipamentelor de comunicații electronice în interiorul Uniunii.

(2) În temeiul articolului 4 din Directiva 2002/58/CE, prestatorii de servicii publice de comunicații electronice trebuie să informeze autoritățile naționale competente și, în anumite cazuri, de asemenea, abonații și persoanele în cauză cu privire la încălcarea securității datelor cu caracter personal. Încălcările privind securitatea datelor cu caracter personal sunt definite la articolul 2 litera (i) din Directiva 2002/58/CE ca încălcări ale securității având ca rezultat distrugerea accidentală sau ilegală, pierderea, alterarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod în legătură cu furnizarea de servicii de comunicații electronice destinate publicului în cadrul Uniunii.

(3) Pentru a asigura consecvența în punerea în aplicare a măsurilor la care se face referire la articolul 4 alineatele (2), (3) și (4) din Directiva 2002/58/CE, articolul 4 alineatul (5) din regulamentul respectiv permite Comisiei să adopte măsuri tehnice de punere în aplicare privind circumstanțele, formatul și procedurile aplicabile cerințelor de informare și notificare la care se face referire în articolul respectiv.

(4) Cerințe naționale diferite în aceste privințe ar putea genera incertitudine juridică, proceduri mai complexe și greoaie și costuri administrative semnificative pentru prestatorii care desfășoară activități transfrontaliere. Prin urmare, Comisia consideră că este necesar să se adopte astfel de măsuri tehnice de punere în aplicare.

(5) Prezentul regulament se limitează la notificarea încălcărilor securității datelor cu caracter personal și, prin urmare, nu prevede măsuri tehnice de punere în aplicare cu privire la articolul 4 alineatul (2) din Directiva 2002/58/CE în ceea ce privește informarea abonaților în cazul unui anumit risc de încălcare a securității rețelei.

(6) Din articolul 4 alineatul (3) primul paragraf din Directiva 2002/58/CE rezultă că prestatorii trebuie să notifice autorității naționale competente toate cazurile de încălcare a securității datelor cu caracter personal. Prin urmare, nu ar trebui lăsată la latitudinea prestatorului decizia de a notifica sau nu autoritatea națională competentă. Totuși, acest lucru nu ar trebui să împiedice autoritatea națională competentă în cauză să investigheze cu prioritate anumite încălcări ale securității în modul pe care îl consideră adecvat, în conformitate cu legislația aplicabilă, și să ia măsurile necesare pentru a evita supraraportarea sau subraportarea încălcărilor securității datelor cu caracter personal.

(7) Este necesar să se prevadă un sistem de notificare către autoritatea națională competentă a încălcărilor securității datelor cu caracter personal, un sistem alcătuit, în cazul în care sunt îndeplinite anumite condiții, din diferitele etape, fiecare etapă făcând obiectul unui anumit termen limită. Acest sistem este menit a garanta că autoritatea națională competentă este informată cât mai repede și cât mai complet posibil, fără însă a îngreuna în mod nejustificat eforturile prestatorului de a investiga încălcarea securității și de a lua măsurile necesare pentru a limita încălcarea și a remedia consecințele acesteia.

([1]) JO L 201, 31.7.2002, p. 37.
([2]) JO L 281, 23.11.1995, p. 31.

(8) Nici o simplă suspiciune că a avut loc o încălcare a securității datelor cu caracter personal, nici o simplă depistare a unui incident, în lipsa unor informații suficiente, în pofida tuturor eforturilor depuse de un prestator în acest sens, nu trebuie apreciate ca suficiente pentru a se considera că a fost depistată o încălcare a datelor cu caracter personal în scopul prezentului regulament. În acest sens, trebuie să se țină seama în special de disponibilitatea informațiilor menționate în anexa I.

(9) În contextul aplicării prezentului regulament, autoritățile naționale competente în cauză trebuie să coopereze atunci când încălcările securității datelor cu caracter personal au o dimensiune transfrontalieră.

(10) Prezentul regulament nu prevede detalii suplimentare referitoare la inventarul cazurilor de încălcare a securității datelor cu caracter personal pe care trebuie să îl țină prestatorii, deoarece articolul 4 din Directiva 2002/58/CE precizează în mod exhaustiv conținutul inventarului. Totuși, prestatorii pot face trimitere la prezentul regulament pentru a stabili formatul inventarului.

(11) Toate autoritățile naționale competente trebuie să pună la dispoziția prestatorilor un mijloc electronic sigur prin care să notifice încălcările securității datelor cu caracter personal într-un format comun, bazat pe un standard precum XML, care să conțină informațiile prevăzute în anexa I, în limbile relevante, astfel încât să toți prestatorii din Uniune să poată urma o procedură de notificare similară, indiferent de locul în care se află sau în care a avut loc încălcarea securității datelor cu caracter personal. În acest sens, Comisia trebuie să faciliteze implementarea mijloacelor electronice sigure, convocând reuniuni cu autoritățile naționale competente dacă este necesar.

(12) Atunci când se evaluează dacă o încălcare a securității datelor cu caracter personal ar putea afecta negativ datele cu caracter personal sau viața privată a unui abonat sau a unei persoane, ar trebui să se țină seama în special de natura și conținutul datelor cu caracter personal în cauză, în special în cazul în care este vorba despre informații financiare, cum ar fi datele privind cartea de credit și detaliile privind contul bancar, despre categoriile speciale de date menționate la articolul 8 alineatul (1) din Directiva 95/46/CE, precum și despre anumite date legate în mod specific de furnizarea de servicii de telefonie sau de internet, mai exact date legate de e-mail, date de localizare, fișiere jurnal, istorii de navigare pe internet și liste detaliate de apeluri.

(13) În circumstanțe excepționale, prestatorului trebuie să i se permită să întârzie notificarea abonatului sau persoanei, dacă notificarea abonatului sau a persoanei ar putea periclita investigarea adecvată a încălcării securității datelor cu caracter personal. În acest context, circumstanțele excepționale pot include cercetări penale, precum și alte încălcări ale securității datelor cu caracter personal care nu constituie o infracțiune gravă, dar pentru care poate fi adecvat să se amâne notificarea. În orice caz, autorității naționale competente trebuie să îi revină sarcina de a decide, în fiecare caz și în funcție de circumstanțe, dacă își dă acordul pentru amânare sau solicită notificarea.

(14) Prestatorii trebuie să dețină datele de contact ale abonaților lor, având în vedere relația contractuală directă dintre prestatori și abonați, însă este posibil ca astfel de informații să nu existe pentru alte persoane afectate negativ de încălcarea securității datelor cu caracter personal. Într-un astfel de caz, prestatorului trebuie să i se permită să notifice aceste persoane inițial prin anunțuri în mass-media națională sau regională de mare anvergură, de exemplu în ziare, acțiune urmată cât mai curând posibil de o notificare individuală, astfel cum se prevede în prezentul regulament. Prin urmare, prestatorul nu este obligat în mod specific să efectueze notificarea prin mass-media, ci mai degrabă este mandatat să acționeze în acest mod, dacă dorește, atunci când se află încă în procesul de identificare a tuturor persoanelor afectate.

(15) Informarea cu privire la încălcarea securității trebuie să fie limitată la încălcare și să nu fie asociată cu informații despre un alt subiect. De exemplu, includerea într-o factură obișnuită a unor informații despre o încălcare a securității datelor cu caracter personal nu trebuie considerată un mijloc adecvat de notificare a unei încălcări a securității datelor cu caracter personal.

(16) Prezentul regulament nu stabilește măsuri tehnologice de protecție specifice care să justifice o derogare de la obligația de notificare a abonaților sau a persoanelor cu privire la încălcările securității datelor cu caracter personal, deoarece aceste măsuri se pot modifica pe parcursul timpului, pe măsură ce progresează tehnologia. Totuși, Comisia ar trebui să fie în măsură să publice o listă orientativă a unor astfel de măsuri tehnologice de protecție specifice conforme cu practicile actuale.

(17) Aplicarea criptării sau a *hashing*-ului nu trebuie considerată suficientă în sine pentru a le permite prestatorilor să pretindă, în termeni mai generali, că s-au conformat obligației generale de securitate stabilite la articolul 17 din Directiva 95/46/CE. În această privință, prestatorii trebuie, de asemenea, să pună în aplicare măsuri organizaționale și tehnice adecvate pentru a preveni, a depista și a bloca încălcarea securității datelor cu caracter personal. Prestatorii trebuie să ia în considerare orice risc rezidual care ar putea exista după implementarea controalelor, pentru a înțelege unde ar putea apărea încălcări ale securității datelor cu caracter personal.

(18) Dacă prestatorul utilizează un alt prestator pentru a furniza o parte din serviciu, de exemplu în ceea ce privește facturarea sau funcțiile de gestionare, respectivul alt prestator, care nu are relații contractuale directe cu

utilizatorul final, nu trebuie să fie obligat să emită notificări în cazul unei încălcări a securității datelor cu caracter personal. În schimb, partea terță trebuie să alerteze și să informeze prestatorul cu care are o relație contractuală directă. Această dispoziție trebuie aplicată, de asemenea, în contextul furnizării angro de servicii de comunicații electronice, context în care, în mod normal, prestatorul angro nu are o relație contractuală directă cu utilizatorul final.

(19) Directiva 95/46/CE definește un cadru general pentru protecția datelor cu caracter personal în Uniunea Europeană. Comisia a prezentat o propunere de regulament al Parlamentului European și al Consiliului care să înlocuiască Directiva 95/46/CE (Regulamentul privind protecția datelor). Având la bază articolul 4 alineatul (3) din Directiva 2002/58/CE, propunerea de regulament privind protecția datelor ar introduce obligația de notificare a încălcărilor securității datelor cu caracter personal pentru toți controlorii de date. Prezentul regulament al Comisiei este pe deplin coerent cu această măsură propusă.

(20) Propunerea de regulament privind protecția datelor cuprinde, de asemenea, un număr limitat de modificări tehnice ale Directivei 2002/58/CE, pentru a se ține cont de transformarea în regulament a Directivei 95/46/CE. Consecințele juridice semnificative ale noului regulament în ceea ce privește Directiva 2002/58/CE vor face obiectul unei analize a Comisiei.

(21) Aplicarea prezentului regulament trebuie analizată la trei ani de la intrarea în vigoare, iar conținutul prezentului regulament trebuie revizuit prin prisma cadrului juridic aflat în vigoare la momentul respectiv, aceleași acțiuni fiind prevăzute în ceea ce privește propunerea de regulament privind protecția datelor. Revizuirea prezentului regulament trebuie să fie legată, atât cât este posibil, de orice viitoare revizuire a Directivei 2002/58/CE.

(22) Aplicarea prezentului regulament poate fi evaluată, printre altele, pe baza oricărui tip de statistici realizate de autoritățile naționale competente privind încălcările securității datelor cu caracter personal care le sunt notificate. Aceste statistici pot include, de exemplu, informații privind numărul cazurilor de încălcare a securității datelor personale notificate autorității naționale competente, numărul cazurilor de încălcare a securității datelor cu caracter personal notificate abonatului sau persoanei, durata necesară pentru a soluționa încălcarea securității datelor cu caracter personal și eventualele măsuri tehnologice de protecție luate. Aceste statistici trebuie să furnizeze Comisiei și statelor membre informații statistice coerente și comparabile și nu trebuie să dezvăluie nici identitatea prestatorului care a efectuat notificarea, nici identitatea abonaților sau a persoanelor în cauză. De asemenea, Comisia poate organiza, în acest scop, întruniri periodice cu autoritățile naționale competente și cu alte părți interesate.

(23) Măsurile prevăzute de prezentul regulament sunt conforme cu avizul Comitetului pentru comunicații,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Domeniu de aplicare

Prezentul regulament se aplică notificării de către prestatorii de servicii de comunicații electronice disponibile publicului („prestatorul") a încălcării securității datelor cu caracter personal.

Articolul 2

Notificarea autorității naționale competente

(1) Prestatorul notifică autorității naționale competente toate încălcările securității datelor cu caracter personal.

(2) Prestatorul notifică autorității naționale competente încălcarea datelor cu caracter personal nu mai târziu de 24 de ore după detectarea încălcării securității datelor cu caracter personal, atunci când acest lucru este fezabil.

În notificarea adresată autorității naționale competente, prestatorul trebuie să includă informațiile prevăzute în anexa I.

Se consideră că a fost depistată o încălcare a securității datelor cu caracter personal atunci când prestatorul de suficiente elemente care să arate că a avut loc un incident de securitate care a dus la compromiterea datelor cu caracter personal, pentru a efectua o notificare clară, în conformitate cu prezentul regulament.

(3) În cazul în care nu sunt disponibile toate informațiile prevăzute în anexa I și este necesară investigarea mai amănunțită a încălcării securității datelor cu caracter personal, prestatorului i se permite să efectueze o notificare inițială către autoritatea națională competentă nu mai târziu de 24 de ore după detectarea încălcării securității datelor cu caracter personal. Această notificare inițială a autorității naționale competente trebuie să cuprindă informațiile prevăzute în secțiunea 1 din anexa I. Prestatorul efectuează o a doua notificare către autoritatea națională competentă cât mai curând posibil și cel mai târziu în termen de trei zile de la notificarea inițială. Această a doua notificare include informațiile prevăzute în secțiunea 2 din anexa I și, dacă este necesar, actualizează informațiile deja furnizate.

În cazul în care, în ciuda investigațiilor sale, nu poate furniza toate informațiile în termen de trei zile de la notificarea inițială, prestatorul notifică toate informațiile de care dispune în acest interval de timp și prezintă autorității naționale competente o justificare argumentată pentru notificarea tardivă a informațiilor rămase. Cât mai curând posibil, prestatorul notifică autorității naționale competente informațiile rămase și, dacă este necesar, actualizează informațiile deja furnizate.

(4) Autoritatea națională competentă pune la dispoziția tuturor prestatorilor stabiliți în statul membru în cauză un mijloc electronic sigur de notificare a încălcării securității datelor cu caracter personal și informații privind procedurile de acces și de utilizare. Atunci când este necesar, Comisia convoacă reuniuni cu autoritățile naționale competente pentru a facilita aplicarea acestei dispoziții.

(5) Dacă încălcarea securității datelor cu caracter personal afectează abonați sau persoane din alte state membre decât cel al autorității naționale competente căreia i-a fost notificată încălcarea securității datelor cu caracter personal, autoritatea națională competentă informează celelalte autorități naționale în cauză.

Pentru a facilita aplicarea acestei dispoziții, Comisia creează și menține o listă cu autoritățile naționale competente și punctele de contact corespunzătoare.

Articolul 3

Notificarea abonatului sau a persoanei

(1) Atunci când încălcarea securității datelor cu caracter personal ar putea afecta negativ datele cu caracter personal sau viața privată a unui abonat sau a unei persoane, prestatorul trebuie să emită notificarea menționată la articolul 2 și, în plus, să notifice respectiva încălcare abonatului sau persoanei în cauză.

(2) Riscul ca o încălcare a securității datelor cu caracter personal să afecteze negativ datele cu caracter personal sau viața privată a unui abonat sau a unei persoane trebuie evaluat luând în considerare, în special, următoarele circumstanțe:

(a) natura și conținutul datelor cu caracter personal în cauză, în special în cazul în care este vorba despre informații financiare, despre categoriile speciale de date menționate la articolul 8 alineatul (1) din Directiva 95/46/CE, precum și despre date de localizare, fișiere jurnal, istorii de navigare pe internet, date legate de e-mail și liste detaliate de apeluri;

(b) consecințele probabile ale încălcării securității datelor cu caracter personal pentru abonatul sau persoana în cauză, în special în cazul în care încălcarea ar putea duce la furtul sau fraudarea identității, vătămare corporală, stres psihologic, umilire sau compromiterea reputației; precum și

(c) circumstanțele încălcării securității datelor cu caracter personal, în special dacă datele au fost furate sau dacă prestatorul știe că datele sunt în posesia unei părți terțe neautorizate.

(3) Notificarea abonatului sau a persoanei în cauză se face cât mai repede posibil după detectarea încălcării securității datelor cu caracter personal, în conformitate cu articolul 2 alineatul (2) al treilea paragraf. Acest lucru nu depinde de notificarea încălcării securității datelor cu caracter personal către autoritatea națională competentă, menționată la articolul 2.

(4) În notificarea adresată abonatului sau persoanei, prestatorul trebuie să includă informațiile prevăzute în anexa II. Notificarea adresată abonatului sau persoanei trebuie formulată într-un limbaj clar și ușor de înțeles. Prestatorul nu utilizează notificarea ca pe o oportunitate de a promova servicii noi sau suplimentare sau pentru a le face reclamă acestora.

(5) În cazuri excepționale, dacă notificarea abonatului sau a persoanei ar putea periclita investigarea adecvată a încălcării securității datelor cu caracter personal, prestatorului i se permite, după obținerea acordului autorității naționale competente, să amâne notificarea abonatului sau a persoanei până când autoritatea națională competentă consideră că este posibilă notificarea încălcării securității datelor cu caracter personal în conformitate cu prezentul articol.

(6) Notificarea de către prestator a abonatului sau a persoanei privind încălcarea securității datelor cu caracter personal se face printr-un mijloc de comunicare care asigură primirea rapidă a informațiilor și care este securizat în mod corespunzător, conform celor mai recente standarde tehnologice. Informarea cu privire la încălcarea securității trebuie să fie limitată la încălcare și să nu fie asociată cu informații despre un alt subiect.

(7) Dacă, în ciuda faptului că a depus eforturi rezonabile, prestatorul care are o relație contractuală directă cu utilizatorul final nu poate identifica, în intervalul de timp menționat la alineatul (3), toate persoanele care riscă să fie afectate negativ de încălcarea securității datelor cu caracter personal, prestatorul poate notifica persoanele respective, în acest interval de timp, prin anunțuri în mass-media regională sau națională de mare anvergură din statul membru în cauză. Aceste anunțuri trebuie să conțină informațiile prevăzute în anexa II, în mod succint dacă este necesar. În acest caz, prestatorul continuă să depună toate eforturile rezonabile pentru a identifica persoanele respective și pentru a le notifica, în cel mai scurt timp posibil, informațiile prevăzute în anexa II.

Articolul 4

Măsuri tehnologice de protecție

(1) Prin derogare de la articolul 3 alineatul (1), notificarea încălcării securității datelor cu caracter personal către abonatul sau persoana în cauză nu este necesară dacă prestatorul a demonstrat autorității naționale competente, într-un mod pe care aceasta îl consideră satisfăcător, că a aplicat măsuri tehnologice de protecție adecvate și că respectivele măsuri au fost aplicate datelor afectate de încălcarea securității. Astfel de măsuri tehnologice de protecție asigură faptul că datele devin neinteligibile pentru persoanele care nu sunt autorizate să le acceseze.

(2) Datele sunt considerate neinteligibile dacă:

(a) au fost criptate în mod sigur cu un algoritm standardizat, iar cheia folosită pentru decriptarea datelor nu a fost compromisă prin nicio încălcare a securității și a fost generată în așa fel încât să nu poată fi identificată prin mijloacele tehnologice disponibile de nicio persoană care nu este autorizată să o acceseze; sau

(b) au fost înlocuite cu valoarea algoritmului de criptare (*hash*) calculată cu o funcție *hash* standardizată cu cheie criptografică, cheia folosită pentru criptarea (*hashing*-ul) datelor nu a fost compromisă prin nicio încălcare a securității și a fost generată în așa fel încât să nu poată fi identificată prin mijloacele tehnologice disponibile de nicio persoană care nu este autorizată să o acceseze.

(3) După consultarea autorităților naționale competente prin intermediul Grupului de lucru instituit prin articolul 29, a Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor și a Autorității Europene pentru Protecția Datelor, Comisia poate publica o listă orientativă a măsurilor tehnologice de protecție adecvate menționate la alineatul (1), în conformitate cu practicile actuale.

Articolul 5

Utilizarea unui alt prestator

Dacă un alt prestator este contractat pentru a furniza o parte a serviciului de comunicații electronice fără a avea o relație contractuală directă cu abonații, acest alt prestator informează imediat prestatorul care l-a contractat în cazul în care are loc o încălcare a securității datelor cu caracter personal.

Articolul 6

Raportare și revizuire

În termen de trei ani de la intrarea în vigoare a prezentului regulament, Comisia prezintă un raport privind punerea în aplicare a prezentului regulament, precum și privind eficacitatea și impactul acestuia asupra prestatorilor, a abonaților și a persoanelor fizice. Pe baza acestui raport, Comisia revizuiește prezentul regulament.

Articolul 7

Intrare în vigoare

Prezentul regulament intră în vigoare la 25 august 2013.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 24 iunie 2013.

Pentru Comisie

Președintele

José Manuel BARROSO

ANEXA I

Conținutul notificării adresate autorității naționale competente

Secțiunea 1

Identificarea prestatorului

1. Denumirea prestatorului

2. Identitatea și datele de contact ale responsabilului cu protecția datelor sau ale unui alt punct de contact de unde se pot obține mai multe informații

3. Se specifică dacă este vorba despre o primă sau o a doua notificare

Informații inițiale privind încălcarea securității datelor cu caracter personal (de completat în notificările ulterioare, dacă este cazul)

4. Data și ora incidentului (dacă se cunosc; dacă este necesar, se poate face o estimare) și ale depistării incidentului

5. Circumstanțele încălcării securității datelor cu caracter personal (de exemplu, pierdere, furt, copiere)

6. Natura și conținutul datelor cu caracter personal în cauză

7. Măsurile tehnice și organizatorice aplicate (sau care urmează a fi aplicate) de prestator datelor cu caracter personal afectate

8. Utilizarea relevantă a altor prestatori (dacă este cazul)

Secțiunea 2

Informații suplimentare privind încălcarea securității datelor cu caracter personal

9. Rezumatul incidentului care a generat încălcarea securității datelor cu caracter personal (inclusiv localizarea fizică a încălcării și suporturile de stocare implicate)

10. Numărul abonaților sau al persoanelor în cauză

11. Eventualele consecințe și efecte adverse pentru abonați sau persoane

12. Măsurile tehnice și organizatorice luate de prestator în scopul atenuării eventualelor efecte negative

Eventuale notificări suplimentare către abonați sau persoane

13. Conținutul notificării

14. Mijloace de comunicare utilizate

15. Numărul abonaților sau al persoanelor notificate

Eventuale aspecte transfrontaliere

16. Încălcare a securității datelor cu caracter personal care implică abonați sau persoane din alte state membre

17. Notificarea altor autorități naționale competente

ANEXA II

Conținutul notificării adresate abonatului sau persoanei

1. Denumirea prestatorului

2. Identitatea și datele de contact ale responsabilului cu protecția datelor sau ale unui alt punct de contact de unde se pot obține mai multe informații

3. Rezumatul incidentului care a generat încălcarea securității datelor cu caracter personal

4. Data estimată a incidentului

5. Natura și conținutul datelor cu caracter personal în cauză, astfel cum se menționează la articolul 3 alineatul (2)

6. Consecințele probabile ale încălcării securității datelor cu caracter personal pentru abonatul sau persoana în cauză, astfel cum se menționează la articolul 3 alineatul (2)

7. Circumstanțele încălcării securității datelor cu caracter personal, astfel cum se menționează la articolul 3 alineatul (2)

8. Măsurile luate de prestator pentru a rezolva problema generată de încălcarea securității datelor cu caracter personal

9. Măsurile recomandate de prestator pentru atenuarea eventualelor efecte negative