GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL

00678/13/RO
WP205

Avizul 04/2013 privind modelul de evaluare a impactului asupra protecției datelor pentru rețelele inteligente și sistemele de contorizare inteligentă („modelul DPIA”), elaborat de grupul de experți 2 al grupului operativ al Comisiei pentru rețele inteligente

Adoptat la 22 aprilie 2013

GRUPUL DE LUCRU PENTRU PROTECȚIA PERSOANELOR ÎN CEEA CE PRIVEȘTE PRELUCRAREA DATELOR CU CARACTER PERSONAL,

instituit prin Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995,

având în vedere articolele 29 și 30 din directiva respectivă,

având în vedere regulamentul său de procedură,

ADOPTĂ PREZENTUL AVIZ:

1 Context

1.1 Introducere

Context

La 9 martie 2012, Comisia Europeană a formulat o recomandare privind pregătirea pentru introducerea sistemelor de contorizare inteligentă (denumită în continuare „recomandarea Comisiei”), cu scopul de a oferi orientări statelor membre cu privire la introducerea sistemelor de contorizare inteligentă pe piața energiei electrice și pe piața gazelor naturale. Recomandarea Comisiei urmărește să ofere orientări cu privire la anumite considerații în materie de protecție și securitate a datelor, la metodologia de evaluare economică a costurilor și a beneficiilor pe termen lung legate de introducerea sistemelor de contorizare inteligentă[1] și la cerințele funcționale minime comune aplicabile sistemelor de contorizare inteligentă a electricității.

În ceea ce privește protecția datelor și securitatea sistemelor de contorizare inteligentă și a rețelelor inteligente, recomandarea Comisiei oferă statelor membre orientări privind protecția datelor începând cu momentul conceperii și protecția implicită a datelor, precum și privind aplicarea anumitor principii de protecție a datelor prevăzute în Directiva 95/46/CE[2]. Recomandarea Comisiei prevede, de asemenea, faptul că statele membre ar trebui să adopte și să aplice un model de evaluare a impactului (asupra) protecției datelor („modelul DPIA”), care ar trebui să fie elaborat de Comisie și prezentat Grupului de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal (GL29) pentru a obține avizul acestuia în termen de 12 luni de la publicarea recomandării Comisiei. Statele membre trebuie să

---

1 Introducerea și analiza cost-beneficiu sunt obligatorii în temeiul (i) Directivei 2009/72/CE privind normele comune pentru piața internă a energiei electrice (JO L 211, 14.8.2009, p. 55) și (ii) al Directivei 2009/73/CE privind normele comune pentru piața internă în sectorul gazelor naturale (JO L 211, 14.8.2009, p. 94). Directiva 2012/27/UE privind eficiența energetică (JO L 315, 14.11.2012, p. 1) include dispoziții suplimentare referitoare la contorizarea inteligentă. În ceea ce privește piața energiei electrice, Directiva 2009/72/CE prevede că, în cazul în care introducerea sistemelor de contorizare inteligentă este evaluată pozitiv, până în 2020, cel puțin 80 % dintre consumatori trebuie să fie echipați cu un astfel de sistem. Nu se menționează un calendar precis pentru piața gazelor naturale.

2 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, JO L 281, 23.11.1995, p. 31-50.

se asigure că operatorii de rețele și operatorii de sisteme de contorizare inteligentă iau măsurile tehnice și organizatorice corespunzătoare pentru a asigura protecția datelor cu caracter personal în concordanță cu modelul DPIA, ținând seama de avizul GL29 cu privire la acesta[3].

Recomandarea Comisiei prevede, de asemenea, faptul că modelul DPIA ar trebui „*să cuprindă cel puțin o descriere a operațiunilor de prelucrare avute în vedere, o evaluare a riscurilor asupra drepturilor și libertăților persoanelor vizate, măsurile preconizate în vederea contracarării riscurilor, garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile Directivei 95/46/CE, ținând seama de drepturile și interesele legitime ale persoanelor vizate și ale celorlalte persoane interesate*".

Elaborare

În februarie 2012, Comisia a reînnoit mandatul grupului de experți 2 („GE2") al grupului operativ al Comisiei pentru rețele inteligente („SGTF"), cu scopul de a oferi un model DPIA pentru rețelele inteligente. În cursul anului 2012, GE2, alcătuit în principal din reprezentanți ai sectorului, a organizat patru ateliere de lucru. CNIL[4], AEPD[5] și ICO[6] au participat la aceste ateliere în calitate de observatori în numele GL29.

La 26 octombrie 2012, GL29 a trimis o scrisoare Direcției Generale Energie a Comisiei Europene („DG ENER") pentru a atrage atenția Comisiei asupra mai multor aspecte ale proiectului de model DPIA care, conform avizului GL29, necesită îmbunătățiri semnificative. Între altele, scrisoarea a recomandat ca modelul DPIA:

(i) să identifice în mod clar părțile interesate și responsabilitățile acestora,
(ii) să pună accentul pe riscurile legate de protecția datelor și a vieții private a persoanelor vizate,
(iii) să consilieze mai bine părțile interesate astfel încât să prevadă măsuri de control adecvate pentru fiecare tip de risc, și
(iv) să ofere recomandări mai specifice și mai practice referitoare la modalitățile de abordare a riscurilor în materie de protecție a datelor și a vieții private în contextul rețelelor inteligente.

Observațiile au fost făcute fără a aduce atingere evaluării finale a modelului DPIA efectuate de GL29.

---

[3] GE2 se bazează pe experiența dobândită în elaborarea și revizuirea, în urma observațiilor și a avizelor Grupului de lucru „articolul 29" („GL29"), a „Propunerii sectorului industrial referitoare la un cadru de evaluare a impactului aplicațiilor RFID asupra protecției vieții private și a datelor ".

[4] La Commission Nationale de l'Informatique et des Libertés (Comisia națională pentru tehnologia informației și libertățile civile), autoritatea națională franceză de supraveghere în domeniul protecției datelor cu caracter personal.

[5] Autoritatea Europeană pentru Protecția Datelor, autoritatea de supraveghere pentru protecția datelor cu caracter personal de către instituțiile și organismele UE.

[6] Information Commissioner's Office (Biroului Comisarului pentru Informații), autoritatea națională de supraveghere în domeniul protecției datelor cu caracter personal din Regatul Unit.

Modelul DPIA

La 8 ianuarie 2013, Comisia a prezentat GL29 versiunea finală a modelului DPIA, elaborată de părțile interesate din cadrul GE2. În scrisoarea de însoțire a modelului DPIA, Comisia a menționat faptul că, sub rezerva observațiilor făcute de GL29 și a concilierii adecvate a acestora, poate lua în considerare adoptarea modelului DPIA elaborat de părțile interesate din cadrul GE2 sub forma unei recomandări a Comisiei[7]. Prezentul aviz prezintă observații cu privire la propunerea de model DPIA.

Structura prezentului aviz

Secțiunea 1.2 subliniază importanța protecției vieții private și a datelor pentru punerea în aplicare cu succes a rețelelor inteligente. Secțiunea 1.3 descrie obiectivele procesului DPIA. Secțiunea 2 conține evaluarea modelului DPIA efectuată de GL29. Secțiunea 3 formulează concluziile finale. Anexa I completează secțiunea 2, prin prezentarea unor observații și sugestii mai detaliate.

1.2 Rețelele inteligente și protecția datelor

GL29 reamintește avizul său anterior privind contorizarea inteligentă[8], precum și avizul Autorității Europene pentru Protecția Datelor („AEPD") din 8 iunie 2012 privind recomandarea Comisiei[9].

Ambele avize subliniază importanța protecției datelor în contextul rețelelor inteligente și al contorizării inteligente și oferă orientări și recomandări privind modalitatea de protecție a drepturilor în materie de protecție a datelor cu caracter personal în legătură cu desfășurarea sistemelor de contorizare inteligentă și a rețelelor inteligente în Europa. Prin urmare, această secțiune va descrie doar pe scurt contextul și principalele preocupări legate de protecția datelor.

Sistemele de contorizare inteligentă și rețelele inteligente au scopul de a permite producția, distribuția și utilizarea energiei într-o manieră inteligentă și raționalizată.

O caracteristică esențială a contoarelor inteligente de gaze și energie electrică este faptul că acestea pot furniza date prin intermediul comunicațiilor la distanță între contor și furnizorii de energie, operatorii de rețele și alte părți terțe. De asemenea, contoarele inteligente permit o comunicare mai frecventă. Prin intermediul contoarelor inteligente va fi posibilă citirea și înregistrarea consumului de energie la intervale foarte scurte de timp, de exemplu, la fiecare cincisprezece minute.

---

[7] La 17 ianuarie 2013, modelul DPIA a fost, de asemenea, prezentat Consiliului autorităților europene de reglementare în domeniul energetic (CEER). La 5 martie, președintele CEER a oferit un răspuns prin care a salutat activitatea desfășurată de GE2 și proiectul final de model DPIA. Scrisoarea a reiterat importanța securității, a protecției datelor, precum și necesitatea ca clienții să dețină controlul asupra datelor lor; a făcut referire la avizul anterior al CEER, publicat în 2011 și a solicitat finalizarea rapidă a modelului DPIA.

[8] Avizul nr. 12/2011 al Grupului de lucru „articolul 29" pentru protecția datelor privind contorizarea inteligentă , adoptat la 4 aprilie 2011 (WP183).

[9] Avizul furnizat de AEPD poate fi consultat pe site-ul de internet al AEPD, la adresa http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-06-08_Smart_metering_EN.pdf

Sistemele de contorizare inteligentă sunt elemente constitutive importante ale rețelelor inteligente, care sunt rețele electrice bidirecționale inteligente, ce combină informații provenite de la utilizatorii rețelelor respective pentru a permite, printre altele, planificarea furnizării de energie electrică într-un mod mai eficace și cu mai puține costuri.

Introducerea „sistemelor de contorizare inteligentă" la nivel european permite colectarea masivă de informații cu caracter personal de la gospodăriile europene, până în prezent fără precedent în ceea ce privește nivelul de detaliu și de acoperire: contorizarea inteligentă poate permite urmărirea activităților membrilor unei gospodării în intimitatea propriilor locuințe și, prin urmare, alcătuirea unor profiluri detaliate ale tuturor persoanelor pe baza activităților lor casnice.

Din datele detaliate privind consumul de energie colectate prin intermediul contoarelor inteligente se pot deduce numeroase informații referitoare la utilizarea de către consumatori a anumitor bunuri sau dispozitive, la programul zilnic, la condițiile de trai, la activitățile, stilurile de viață și comportamentele consumatorilor[10].

Astfel, utilizarea rețelelor inteligente și a sistemelor de contorizare inteligentă creează noi riscuri pentru persoanele vizate, care ar putea avea un impact în diferite domenii (de exemplu, discriminarea prin prețuri, crearea de profiluri pentru publicitatea comportamentală, impozitarea, accesul în scopul asigurării respectării aplicării legii, securitatea gospodăriilor) care nu erau prezente anterior în sectorul energetic, fiind mai tipice pentru alte medii și deja prezente numai în acestea (telecomunicații, comerțul electronic și Web 2.0).

De asemenea, contorizarea inteligentă se numără printre primele aplicații pe scară largă care prevestesc viitorul „internetului obiectelor". În viitor, probabil că riscurile legate de colectarea și disponibilitatea datelor detaliate privind consumul de energie vor crește, având în vedere disponibilitatea tot mai mare de date provenite din alte surse, cum ar fi datele de geolocalizare, datele disponibile prin urmărirea pe internet și crearea de profiluri prin intermediul internetului, datele provenite de la sistemele de supraveghere video și de la sistemele de identificare prin frecvențe radio(RFID), care pot fi combinate cu datele furnizate de sistemele de contorizare inteligentă[11].

1.3 Obiectivele modelului DPIA

Prin recomandarea formulată, Comisia Europeană își propune să încurajeze operatorii de date să efectueze evaluarea DPIA cu scopul de a obține următoarele avantaje:

- Evaluarea DPIA ar trebui să cuprindă o descriere a operațiunilor de prelucrare avute în vedere, o evaluare a riscurilor la adresa drepturilor și libertăților persoanelor vizate, măsurile preconizate în vederea contracarării riscurilor,

[10] De exemplu, prin utilizarea unui interval de citire de 2 secunde, s-a demonstrat faptul că este posibilă până și identificarea conținutului multimedia consumat în gospodărie: http://www.its.fh-muenster.de/greveler/pubs/preprint_online.pdf.

[11] Recomandarea CM/Rec(2010)13 din 23 noiembrie 2010 a Comitetului de Miniștri al Consiliului Europei către statele membre privind protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal în contextul creării unor tipologii pe baza unor criterii specifice („profiling").

garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile Directivei 95/46/CE.

- De asemenea, DPIA ar trebui să ajute autoritățile naționale pentru protecția datelor să evalueze dacă prelucrarea datelor s-a efectuat cu respectarea dispozițiilor Directivei 95/46/CE, în special, riscurile privind protecția datelor cu caracter personal ale persoanei vizate și garanțiile conexe, atunci când acestea sunt consultate de operatorii de date înainte de prelucrarea datelor, în conformitate cu recomandarea Comisiei[12]. Prin urmare, evaluările DPIA ar trebui, de asemenea, să ajute operatorul de date să demonstreze conformitatea cu Directiva 95/46/CE[13].

În plus, evaluările DPIA pot ajuta consumatorii, operatorii de date, autoritățile de protecție a datelor, autoritățile de reglementare din domeniul energiei, organizațiile de protecție a consumatorilor și alte părți interesate să înțeleagă mai bine aspectele specifice legate de protecția datelor ale sistemelor de contorizare inteligentă și ale aplicațiilor de rețea inteligente. Informațiile obținute în urma evaluărilor DPIA ar putea, de asemenea, să ajute autoritățile de protecție a datelor (APD) să identifice atât cele mai bune practici, cât și eventualele domenii cu un profil de risc ridicat, care ar trebui supuse auditurilor.

În statele membre în care este necesară efectuarea unei notificări/verificări prealabile pentru aplicațiile pentru contoarele și rețelele inteligente, DPIA ar putea simplifica procesul atât pentru APD, cât și pentru operatorii de date. Prin urmare, evaluările DPIA ar trebui, de asemenea, să ajute operatorii de date să demonstreze conformitatea cu Directiva 95/46/CE.

În fine, trebuie subliniat faptul că propunerea de regulament privind protecția datelor[14] ar crește importanța procesului DPIA, care este considerat un instrument esențial care contribuie la angajarea responsabilității operatorilor de date.

1.4 Rezumatul modelului DPIA propus

GE2 explică faptul că grupul se bazează pe experiența dobândită cu ocazia elaborării și a revizuirii, în urma observațiilor și a avizelor Grupului de lucru „articolul 29“ („GL29”), a „Propunerii sectorului industrial privind un cadru de evaluare a impactului aplicațiilor RFID asupra protecției vieții private și a datelor”.

---

[12] Recomandarea nu aduce atingere obligației legale de a efectua o verificare prealabilă în statele membre, în funcție de caracteristicile operațiunilor de prelucrare.

[13] 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 JO L 281, 23.11.1995, p. 31

[14] La 25 ianuarie 2012, Comisia a adoptat un pachet de măsuri pentru reformarea cadrului european privind protecția datelor. Pachetul include (i) o „Comunicare” [COM(2012)9 final], (ii) o „Propunere de regulament privind protecția datelor” [COM(2012)11 final], și (iii) o „Propunere de directivă privind protecția datelor” [COM(2012)10 final].

Modelul DPIA propus de GE2 explică, în primul rând, obiectivul, domeniul de aplicare, avantajele procesului, precum și părțile interesate în cadrul acestuia. Apoi, modelul definește o abordare care permite efectuarea unei DPIA în opt etape și oferă consiliere operatorului de date în fiecare etapă a procesului cu privire la modul de efectuare a DPIA.

2 Analiza modelului DPIA

GL29 recunoaște eforturile de anvergură depuse de părțile interesate în cadrul GE2 și salută obiectivele lor principale, evidențiate în secțiunile introductive ale modelului DPIA.

Deși — în general — abordarea bazată pe opt etape evidențiată în documentul propus este solidă, GL29 a identificat mai multe puncte nevralgice de ordin metodologic, precum și la conținutul modelului DPIA în sine, care sunt prezentate în detaliu în secțiunile următoare.

2.1 Lipsa de claritate privind tipul și obiectivele DPIA

Astfel cum este definită în secțiunea 3 litera (c) din recomandarea Comisiei, evaluarea impactului asupra protecției datelor „*înseamnă un proces sistematic de evaluare a impactului potențial al riscurilor, în cazul în care operațiunile de prelucrare sunt susceptibile să prezinte riscuri specifice pentru drepturile și libertățile persoanelor vizate, date fiind tipul, domeniul de aplicare și obiectivele acestor operațiuni”* care trebuie atinse de operatorul de date sau de persoana împuternicită de operator atunci când acționează în numele acestuia.

GL29 sprijină această definiție, prin urmare, obiectivul unei DPIA ar trebui să fie evaluarea impactului riscurilor asupra persoanelor vizate.

Cu toate acestea, GL29 regretă faptul că modelul DPIA prezentat nu abordează în mod direct impactul real asupra persoanelor vizate, cum ar fi, de exemplu, pierderile financiare rezultate ca urmare a unei facturări incorecte, discriminarea prin prețuri sau actele infracționale facilitate de crearea neautorizată de profiluri. Chiar dacă obiectivele privind protecția datelor și a vieții private enumerate în anexa I pot fi foarte utile pentru a facilita respectarea dispozițiilor, acestea nu sunt suficiente în contextul unei abordări bazate pe risc. Evaluarea impactului probabil asupra persoanelor vizate este un element indispensabil al unei astfel de abordări.

Prin urmare, GL29 consideră că modelul DPIA în forma sa actuală nu își poate atinge obiectivul impus de recomandarea Comisiei. DPIA nu oferă un instrument practic pentru evaluarea impactului asupra persoanelor vizate.

În cazul în care riscurile și impactul acestora asupra persoanelor vizate nu sunt analizate în integralitatea lor, nu este posibil să se identifice în mod corect și să se pună în aplicare controalele și garanțiile necesare.

2.2 Deficiențe metodologice în modelul DPIA

În plus față de principala deficiență identificată mai sus și uneori legată de aceasta, GL29 consideră că modelul DPIA este afectat de o serie de deficiențe metodologice care pun în pericol aplicarea sa.

În primul rând, propunerea de model DPIA confundă adesea riscurile cu amenințările[15].

În al doilea rând, nu există o corespondență între riscurile care urmează să fie atenuate și lista controalelor posibile din anexa II. Chiar dacă fiecare scenariu de risc este specific și trebuie evaluat în funcție de particularitățile sale, adesea este posibil să se considere că anumite categorii de controale reușesc să atenueze anumite categorii de risc. Un exemplu tipic în acest sens este oferit de standardul în materie de securitate a informațiilor ISO/IEC 27002:2005, în care controalele sunt prezentate ca cele mai bune practici de atenuare a riscurilor în anumite zone. Măsurile de atenuare sugerate pot constitui o bază de referință pentru o abordare eficace și coerentă, fără a înlocui însă necesitatea unor proceduri bazate pe risc. De exemplu, riscul interceptării datelor privind consumul de energie al consumatorilor prin intermediul unui canal neprotejat poate fi atenuat, în general, prin tehnici de criptare. Evaluarea riscurilor specifice ar putea conduce la alegerea anumitor algoritmi de criptare și lungimi ale cheilor sau a unor măsuri de atenuare alternative sau complementare sau chiar la acceptarea riscurilor sau transferul riscurilor (prin urmare, fără luarea unor măsuri de atenuare).

În plus, modelul DPIA propus nu oferă nici suficiente detalii și orientări specifice privind conceptul de vulnerabilitate, privind modul de calculare și de stabilire a priorităților în materie de riscuri, precum și în ceea ce privește alegerea controalelor adecvate și evaluarea riscurilor reziduale existente care subzistă după efectuarea controalelor. Deși se face trimitere la un document extern, GL29 ar fi apreciat includerea unui număr mai mare de orientări și de explicații în modelul DPIA în sine, astfel încât acesta să ofere cititorilor un document de sine stătător. De asemenea, nu este clar modul în care trebuie completate formularele propuse.

În fine, modelul DPIA nu oferă suficientă consiliere privind modalitatea de determinare a rolurilor și a responsabilităților diferitelor părți interesate în ceea ce privește protecția datelor. Există doar o singură trimitere la un alt document al GE2. Viitoarele aplicații pentru rețelele inteligente vor fi variate și vor fi puse la dispoziție de numeroase părți interesate. Prin urmare, este esențial să se ofere acestui sector orientări care să permită identificarea operatorilor de date și a persoanelor

[15] A se vedea definiția riscului în domeniul securității informațiilor din standardul ISO/IEC 27005:2008: „probabilitatea ca o anumită amenințare să exploateze vulnerabilitățile unui activ sau grup de active și, în consecință, să cauzeze un prejudiciu organizației”. Amenințările nu sunt definite direct, însă se poate deduce o definiție operațională din standardul ISO/IEC 27001:2005. În consecință, amenințările se referă la capacitatea de a exploata vulnerabilitățile cu privire la activele care urmează să fie protejate. Acest lucru va avea impact asupra activelor în ceea ce privește pierderea proprietăților de securitate. Anexa C la ISO/IEC 27005:2008 conține exemple tipice de amenințări legate de securitate.
A se vedea, de asemenea, metodologia elaborată de CNIL: http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf și peisajul amenințărilor descris de ENISA: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport).

împuternicite de operatori. De exemplu, în a treia etapă a modelului DPIA ar putea fi inclusă o a patra secțiune care să vizeze determinarea diferitelor responsabilități ale diverselor entități implicate în prelucrarea datelor.

Mai multe detalii privind aceste deficiențe și alte deficiențe metodologice sunt prezentate în anexa 1.

2.3 Modelul DPIA nu este adaptat specificităților sectoriale: ar trebui să se identifice și să se stabilească o corespondență între riscurile specifice sectorului și controalele destinate contracarării riscurilor respective

Modelul DPIA nu este adaptat specificităților sectoriale. Atât riscurile, cât și controalele enumerate în model au un caracter generic și conțin numai ocazional orientări cu caracter sectorial specific— cele mai bune practici care ar putea fi cu adevărat utile. În esență, riscurile și controalele nu reflectă experiența din diferitele sectoare legate de care sunt principalele preocupări și cele mai bune practici .

GL29 înțelege faptul că GE2 lucrează în prezent la o colecție cu „cele mai bune tehnici disponibile" (BAT), care ar permite unei organizații care efectuează o DPIA să aleagă măsurile corespunzătoare, dacă este cazul, răspunzând, prin urmare, unora dintre criticile formulate în secțiunea precedentă. GL29 insistă asupra importanței unui astfel de document, care este complementar modelului DPIA.

Cu toate acestea, documentul BAT nu poate înlocui identificarea celor mai frecvente riscuri specifice unui anumit sector și a controalelor posibile aferente riscurilor respective din modelul DPIA. Acest lucru este cu atât mai adevărat cu cât — spre deosebire de modelul DPIA— documentul BAT nu va fi prezentat GL29 în vederea unei evaluări suplimentare și a unor orientări suplimentare și nu urmează să fie adoptat de către Comisie. Date fiind deficiențele identificate ale modelului DPIA, Comisia ar trebui să ia în considerare posibilitatea integrării BAT în model și prezentarea documentului integrat GL29 în vederea obținerii unui aviz.

În plus, noțiunea de model DPIA este diferită de noțiunea de cadru DPIA. Un cadru ar trebui să identifice obiectivele, să descrie o metodologie și să definească domeniul de aplicare a evaluării în ceea ce privește limitele sistemului/procesului analizat. Un model ar trebui să meargă și mai departe și să ofere un instrument operațional pentru gestionarea riscurilor legate de sistemul/procesul specific și cazurile de utilizare ale acestuia, să sugereze controalele posibile și cele mai bune tehnici disponibile pentru atenuarea riscurilor respective și să ofere orientări specifice. Acest lucru este îndeosebi necesar în cazurile care nu este disponibilă niciun fel de expertiză specifică (de exemplu, IMM-urile, sau în cazul rețelelor inteligente, într-un sector care s-a confruntat anterior cu un număr relativ mic de probleme legate de protecția vieții private și a datelor).

Modelul DPIA ar trebui să urmărească elaborarea de orientări sectoriale mai numeroase și mai ușor de utilizat. În special, este necesar să se definească mai bine impactul probabil asupra persoanelor vizate în contextul rețelelor inteligente și să se ofere orientări mai precise în ceea ce privește tipurile de controale care pot fi puse în aplicare.

Comisia ar fi putut oferi GE2 o metodologie generică privind evaluarea riscurilor legate de protecția vieții private și a datelor[16]. La rândul său, GE2 ar fi putut aplica o astfel de metodologie și, pe baza acesteia, ar fi putut crea un model DPIA mai adaptat specificităților sectoriale. O astfel de abordare ar fi permis GE2 să se axeze pe aspectele pertinente, cum ar fi riscurile și controalele specifice rețelelor inteligente, bazându-se, în același timp, pe cadrul de referință pentru aspectele metodologice fundamentale. GL29 recomandă ca GE2 și Comisia să adopte o astfel de abordare pentru elaborarea viitoare a modelului DPIA și pentru orice alte modele DPIA sectoriale.

3 Concluzii și recomandări

GL29 recunoaște progresele realizate comparativ cu versiunile anterioare, precum și elementele utile pe care modelul DPIA le conține deja. Cu toate acestea, Grupul este de părere că modelul DPIA în forma sa actuală nu este suficient de matur și de bine dezvoltat.

Prin urmare, GL29 recomandă Comisiei să ia măsurile necesare pentru a se asigura că se continuă lucrul la modelul DPIA și că forma sa finală va oferi orientări practice suficient de specifice, utile și clare pentru operatorii de date.

Pentru a facilita eforturile de îmbunătățire a modelului, GL29 oferă mai multe recomandări specifice în anexa 1 la prezentul aviz. Cu toate acestea, având în vedere deficiențele metodologice ale documentului și lipsa de adaptare a acestuia la contextul rețelelor inteligente, în acest stadiu, GL29 nu este în măsură să aibă o contribuție suplimentară mai detaliată și mai concludentă.

Date fiind deficiențele identificate ale modelului DPIA, GL29 recomandă, în plus, Comisiei să ia în considerare posibilitatea integrării BAT în modelul DPIA și prezentarea documentului integrat GL29 în vederea obținerii unui aviz[17].

În plus și la un nivel mai general, GL29 recomandă Comisiei să ia în considerare realizarea unui bilanț al activităților anterioare și a celor în derulare în domeniul DPIA[18] și, de asemenea, să ia în considerare posibilitatea de a defini o metodologie generică DPIA care s-ar putea dovedi benefică pentru eforturile specifice realizate în diferitele domenii.

În fine, în ceea ce privește necesitatea unei evaluări obligatorii a impactului, GL29 face referire la experiența dobândită cu ocazia derulării proiectului PIAF pentru aplicațiile RFID și subliniază faptul că statisticile disponibile în statele membre arată că recurgerea la evaluări ale impactului în sectorul RFID a fost extrem de scăzută. Deși motivele care stau la baza acestor statistici pot fi multiple, unul dintre factorii principali care au avut o contribuție în această privință pare a fi, în mod evident, lipsa actuală a unei cerințe obligatorii privind efectuarea unei astfel de evaluări a impactului.

---

16 A se vedea, de exemplu, metodologia elaborată de CNIL, citată deja mai sus.

17 Acest lucru nu exclude posibilitatea ca documentul BAT să fie actualizat periodic în viitor pentru a reflecta schimbările tehnologice și tehnologia de vârf.

18 A se vedea, de exemplu, proiectul PIAF: http://www.piafproject.eu/Index.html, precum și metodologiile existente la care s-a făcut referire mai sus.

Adoptat la Bruxelles, la 22 aprilie 2013

Pentru grupul de lucru
Președintele
Jacob KOHNSTAMM

Anexa 1: Observații specifice privind modelul DPIA

Prezenta anexă completează secțiunea 2 din aviz. Structura observațiilor respectă structura modelului DPIA.

→ Domeniul de aplicare a DPIA

- Modelul nu oferă o definiție precisă și o descriere a tipurilor de prelucrare a datelor care fac obiectul unei DPIA. În plus, domeniul de aplicare a DPIA nu este definit precis în secțiunea 1.2 din modelul DPIA. Recomandarea Comisiei definește în mod clar DPIA ca „un proces sistematic de evaluare a impactului potențial al riscurilor, în cazul în care operațiunile de prelucrare sunt susceptibile să prezinte riscuri specifice pentru drepturile și libertățile persoanelor vizate, date fiind tipul, domeniul de aplicare și obiectivele acestor operațiuni". Definiția include drepturile fundamentale definite la articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta"), și anume dreptul la viața privată și dreptul la protecția datelor cu caracter personal. Ar trebui să se țină seama de faptul că modelul este legat de protecția datelor cu caracter personal, astfel cum este definită în Directiva 95/46/CE[19].
- Astfel cum s-a subliniat în observațiile generale, modelul DPIA ar trebui să se axeze pe impactul asupra persoanei vizate. Deși este necesară îndeplinirea dispozițiilor în materie de protecție a vieții private și a datelor, astfel cum se indică în anexa I, precum și respectarea legislației în materie de protecție a datelor, respectarea legislației în materie de protecție a datelor nu reprezintă un scop în sine. Astfel, obiectivul final al procesului DPIA este de a identifica controalele care reduc la minimum orice impact negativ asupra drepturilor și libertăților persoanelor vizate.
- Următoarele exemple pot ilustra diferența între o abordare redusă la o simplă verificare a conformității și una care se bazează pe evaluarea riscurilor reale și a impactului real al acestora asupra persoanelor vizate.
    - riscuri legate de infracționalitate: dacă măsurile tehnice și organizatorice luate pentru a garanta securitatea datelor privind consumul de energie nu sunt adecvate, datele privind consumul de energie provenite de la o gospodărie individuală pot fi accesate în mod ilegal. Acest lucru poate determina creșterea riscului ca respectivul consumator să devină victimă a infracțiunii. De exemplu, cunoașterea obișnuințelor de ordin comportamental ale acestuia, care pot fi deduse din datele privind consumul de energie, în special momentele în care o anumită casă este goală, ar putea conduce la creșterea riscului de spargeri și furturi.
    - posibila facturare eronată a persoanelor fizice în cazul în care datele privind consumul lor de energie sunt modificate[20].

---

[19] Orice trimitere la conceptul de „confidențialitate a datelor" sau orice încercare de definire *ad hoc* a „protecției vieții private" în secțiunea 1.2 sau în glosar este nenecesară și ar putea crea confuzii. Terminologia din Directiva 95/46 ar trebui să fie utilizată ori de câte ori este posibil. Articolele 7 și 8 din Cartă pot fi citate și menționate în scopul unor orientări suplimentare.

[20] De asemenea, proprietarii de panouri solare sau de unități de microcogenerare se pot confrunta cu riscuri similare legate de facturare.

- crearea de profiluri, excluderea, discriminarea, publicitatea nesolicitată: disponibilitatea tot mai mare a datelor privind consumatorii din cadrul rețelelor inteligente poate conduce la intensificarea activității de creare de profiluri, care, la rândul său, ar putea conduce la discriminare prin prețuri și la excludere (de exemplu, punerea pe o listă neagră, aplicarea unor tarife mai mari), la publicitate comportamentală direcționată nesolicitată, precum și la un dezechilibru global în situația economică a consumatorilor în raport cu furnizorii de servicii/operatorii de date de care se poate ulterior profita în mod abuziv.
- riscurile legate de o utilizare incompatibilă și ilegală de către autoritățile de aplicare a legii sau de către alți terți, riscul de supraveghere crescută din partea autorităților (care ar putea fi atenuat, de exemplu, prin reducerea la minimum a datelor cu caracter personal prelucrate).

- Exemplele de riscuri enumerate mai sus, precum și alte exemple de riscuri și de impacturi posibile asupra persoanelor vizate ar trebui să fie luate în considerare și incluse în evaluarea impactului.

→ Părțile interesate

- Modelul DPIA nu ia în considerare rolurile și funcțiile diferitelor părți interesate din cadrul ecosistemului rețelelor inteligente și, în consecință, nu face distincție între responsabilitățile lor. Cu toate acestea, rețelele inteligente își pot atinge obiectivele numai printr-o cooperare organizată și prin schimbul de date între diferitele organizații participante. Va fi nevoie de cooperare din partea participanților pentru a produce un model DPIA pertinent. Modelul DPIA propus nu oferă suficiente orientări privind modul de efectuare a unei DPIA în cazul în care sunt implicați mai mulți operatori care desfășoară activități conexe de prelucrare a datelor.
- În secțiunea 1.3.3, termenul de „operator de rețea inteligentă” este unul foarte generic și nu ia în considerare faptul că diverse părți interesate pot îndeplini diferite funcții în cadrul rețelelor inteligente, aspect care influențează puternic limitele și domeniul de aplicare ale DPIA efectuate[21]. Aceste funcții ar trebui să fie descrise, acordându-se o atenție specială rolului lor în schimbul de informații cu caracter personal necesar pentru desfășurarea proceselor în cadrul rețelelor inteligente. Modelul DPIA ar trebui să includă o definiție concisă și actualizată a rolurilor părților implicate în procesul DPIA (a se vedea, de exemplu, raportul GE2 din 16 februarie 2011[22]).
- Ar trebui să fie reamintită necesitatea de a respecta legislația în vigoare.
- De asemenea, în modelul DPIA ar trebui să fie menționați în calitate de părți interesate (i) destinatarii datelor și (ii) responsabilii cu protecția datelor (în cazul în care există) din cadrul organizației.

[21] A se vedea, de exemplu, http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGConceptualModel#Smart_Grid_Conceptual_Model_Doma.

[22] A se vedea http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2.pdf.

→ **Etapa 1**

- Trebuie reconsiderate criteriile de evaluare prealabilă. În consecință, chestionarul din secțiunea 3.1 trebuie, de asemenea, revizuit. Acest lucru este necesar, de asemenea, pentru a se asigura coerența cu secțiunea 2.1.
- Ordinea criteriilor ar trebui să fie modificată astfel încât să se respecte ordinea logică în care acestea ar trebui să fie examinate:
    1. Se prelucrează date cu caracter personal?
    2. Operatorul de date este chiar organizația în cauza?
    3. Prelucrarea datelor are vreun impact asupra drepturilor și libertăților?
    4. Când va fi momentul potrivit și care va fi motivația?
- Printre tipurile de date enumerate în modelul DPIA care pot fi considerate date cu caracter personal, există unele tipuri care nu sunt în mod evident date cu caracter personal (previziunile privind cererea de construcții, campusuri și organizații). În schimb, unele date care pot constitui date cu caracter personal nu sunt enumerate sau sunt enumerate în mod eronat (temperatura din interiorul unei case poate face parte din datele cu caracter personal, deoarece poate indica dacă în casa respectivă se află sau nu cineva; locațiile succesive în care s-a încărcat cu energie o mașină electrică sunt date cu caracter personal întrucât acestea indică localizarea utilizatorului etc.). Este necesar să se furnizeze un număr mai mare de orientări pentru a sprijini organizația să identifice datele cu caracter personal care vor fi prelucrate.
- În plus, și cu privire la criteriul 1, ar trebui să se efectueze o DPIA inclusiv în cazul sistemelor existente care nu au fost construite ținând seama de „protecția datelor începând cu momentul conceperii” și pentru care nu a fost efectuată anterior nicio DPIA. Acest lucru ar trebui subliniat în text, de exemplu, prin introducerea unui punct suplimentar în lista elementelor declanșatoare care figurează la rubrica „Momentul oportun” sau într-un alineat separat după lista de puncte.

→ **Etapa 2**

- Atunci când resursele organizației permit acest lucru, este important să se garanteze faptul că echipa care efectuează DPIA este independentă de echipa care lucrează la aplicația propriu-zisă pentru rețelele inteligente. Acest aspect va contribui la corectitudinea și obiectivitatea DPIA: o astfel de cerință nu este inclusă în document.

→ **Etapa 3**

- În descrierea sistemului nu este prevăzută o descriere clară a activelor pe care se bazează prelucrarea datelor cu caracter personal (de exemplu, o bază de date care să aibă rol de antrepozit pentru datele colectate dintr-o anumită zonă). Acest lucru ar fi important având în vedere că unele amenințări vor viza, de asemenea, activele respective. De asemenea, trebuie să fie identificate în mod exhaustiv diferitele tipuri de date cu caracter personal prelucrate, precum și scopul și modul în care acestea sunt prelucrate. Trebuie să se indice, de asemenea, perioadele propuse de păstrare a datelor.

→ **Etapa 4**

- Această etapă se bazează în cea mai mare parte pe lista de amenințări enumerată în chestionarele modelului DPIA. Se pare că există o confuzie între amenințări și riscuri (a se vedea secțiunea 2.2 din prezentul aviz). În plus, unele dintre elementele enumerate se referă mai degrabă la o „lipsă de măsuri” (de exemplu, mecanismul insuficient de înregistrare, lipsa de unificare în mecanismul solicitărilor de acces ale persoanelor vizate”) decât la amenințări.

→ **Etapa 5**

- Impactul amenințărilor la adresa protecției datelor este calculat ca impact asupra obiectivelor privind protecția datelor și a vieții private identificate în anexa I, și nu ca impact asupra persoanelor fizice (persoanele vizate) în cauză. În plus, modelul DPIA în sine nu conține orientări adecvate privind tipul de impact și privind metodologia aplicabilă.
- Probabilitatea materializării riscului este descrisă ca o combinație între nivelul de vulnerabilitate și ușurința cu care poate fi exploatată această vulnerabilitate. Cu toate acestea, având în vedere că activele pe care se bazează datele cu caracter personal nu au fost identificate în etapa 3, nu există nicio indicație privind semnificația/definiția vulnerabilității.

→ **Etapa 6**

- De asemenea, este esențial ca modelul DPIA să prevadă pentru fiecare risc unul sau mai multe controale adecvate în vederea atenuării riscurilor (explicând, în același timp, că în cazurile în care este relevant și se justifică în mod corespunzător, unele riscuri pot fi, de asemenea, transferate sau acceptate). Această relație ar trebui să devină un element central al documentului. Structura actuală a modelului nu permite o astfel de abordare integrată, astfel cum a subliniat deja GL29 în scrisoarea din octombrie 2012.
- Cu privire la riscurile reziduale (secțiunea 6), astfel cum a menționat deja GL29 în observațiile sale din octombrie 2012, dreptul la protecția datelor cu caracter personal este un drept fundamental, iar conformitatea cu acesta este o cerință juridică clară și de nivel înalt. Acest lucru ar trebui să fie evidențiat mai clar atunci când se face referire la posibilitatea de a accepta un anumit grad de riscuri reziduale: ar putea fi explicat faptul că, indiferent de rezultatul evaluării riscurilor, trebuie îndeplinite obiectivele de protecție a datelor și a vieții private: de exemplu, persoanele vizate trebuie să fie notificate corespunzător în toate cazurile și, de asemenea, trebuie să existe un motiv legal pentru prelucrarea datelor (de exemplu, o obligație legală sau consimțământul persoanei vizate). Este esențial să se precizeze foarte clar faptul că legislația privind protecția datelor trebuie să fie respectată în toate cazurile. Evaluarea riscurilor poate contribui la identificarea celor mai bune modalități de a respecta legislația privind protecția datelor. De exemplu, tipul de criptare care trebuie utilizat pentru a se asigura un nivel corespunzător de securitate a datelor, intervalul de timp care poate fi considerat o perioadă de păstrare adecvată sau cea mai bună modalitate de a reduce la minimum cantitatea de date colectate și prelucrate ulterior. Cu toate acestea, evaluarea riscurilor nu ar trebui să fie utilizată drept scuză pentru nerespectarea cerințelor legale în

cazurile în care riscurile sunt percepute a fi mai reduse. Dintr-un punct de vedere general, referitor la acest aspect, nu există nicio recomandare cu privire la modul de determinare a nivelul de risc rezidual care poate fi acceptat.

Anexa II Lista controalelor posibile

Controalele enumerate în anexa II nu sunt suficient de specifice încât să ofere orientări utile operatorilor. De asemenea, cea mai mare parte a acestora nu sunt adaptate particularităților contextului rețelelor inteligente și nu reflectă experiența actorilor din acest sector privind principalele preocupări și cele mai bune practici în acest domeniu.

Pentru a ilustra așteptările noastre în ceea ce privește nivelul de detaliu și exemplele practice care considerăm că ar trebui incluse în model, dorim să evidențiem unele dintre cele mai importante aspecte pe care, în opinia noastră, modelul ar trebui să le trateze amănunțit.

Temeiul juridic și alegerea instrumentului

GL29 ar dori ca modelul să conțină mai multe orientări privind temeiul juridic care trebuie ales pentru prelucrarea datelor și privind plaja de opțiuni care ar trebui pusă la dispoziția persoanelor vizate. În special, ar trebui să existe orientări clare cu privire la ceea ce poate fi realizat fără acordul utilizatorului și la ceea ce necesită acordul utilizatorului. Ar trebui acordată o atenție deosebită punerii în aplicare a dezactivării la distanță și a citirilor detaliate[23].

În majoritatea cazurilor, ar fi necesar un consimțământ acordat din proprie voință, specific, avizat și explicit al persoanei vizate pentru toate prelucrările care nu se limitează la prelucrarea necesară pentru (i) furnizarea de energie, (ii) facturarea aferentă, (iii) detectarea fraudelor legate de utilizarea energiei furnizate fără efectuarea plății corespunzătoare[24] și (iv) pregătirea datelor agregate necesare pentru menținerea eficienței energetice a rețelei (realizarea de previziuni și efectuarea plăților)[25]. Urmărirea și crearea de profiluri în vederea publicității direcționate sunt exemple în care ar fi necesar acordul.

Pentru ca acest consimțământ să fie valabil, consumatorii trebuie să înțeleagă ceea ce se întâmplă cu datele lor cu caracter personal. Un aspect foarte important este faptul că, în cazul creării de profiluri, aceștia ar trebui să aibă dreptul de a-și cunoaște profilurile individuale și logica algoritmilor utilizați în scopul extragerii de date. De asemenea, în aceeași măsură sunt importante informațiile privind funcționalitatea de activare/dezactivare la distanță: consumatorii trebuie să cunoască evenimentele care pot declanșa dezactivarea.

---

[23] A se vedea, de exemplu, punctul 48 din avizul AEPD din 8 iunie 2012, menționat la nota de subsol 3 de mai sus.

[24] Desigur, prelucrarea datelor în scopul detecției fraudelor trebuie să respecte în continuare toate garanțiile relevante privind protecția datelor, inclusiv cerința de proporționalitate și principiul reducerii la minimum a datelor.

[25] După caz, aceste scopuri, pentru care nu este necesar consimțământul persoanei vizate, coincid de regulă cu sarcinile reglementate ale operatorilor de date.

Reducerea la minimum a prelucrării datelor și tehnologiile de protecție a vieții private (PET)

Modelul DPIA ar trebui, de asemenea, să încurajeze întreprinderile în cauză să se asigure că datele cu caracter personal sunt colectate și prelucrate doar în măsura în care acest lucru este absolut necesar. Pentru a realiza acest lucru, pot fi avute în vedere o serie de metode și se recomandă ca cel puțin cele mai comune tehnologii de protecție a vieții private („PET") și alte „cele mai bune tehnici disponibile" pentru reducerea la minimum a prelucrării datelor să fie descrise pe scurt și într-o manieră neutră din punct de vedere tehnologic în modelul DPIA, iar ulterior să fie detaliate suplimentar, în documentul de însoțire BAT care urmează să fie elaborat de către GE2, cu scopul de a contribui la promovarea tehnologiilor de contorizare inteligentă și a celor din domeniul rețelelor inteligente într-o manieră favorabilă protecției datelor.

Mai concret, în prezent, există PET inovatoare, aflate în diferite etape de cercetare și dezvoltare, care pot face posibilă atingerea obiectivelor fundamentale ale sistemului de contorizare inteligentă [facturare, menținerea eficienței energetice a rețelei (realizarea de previziuni și efectuarea plăților) și de asigurare a securității (inclusiv de prevenire a fraudelor)], astfel încât să poată fi complet evitate — cel puțin pentru astfel de scopuri de bază — situațiile în care citirile deosebit de detaliate ale contoarelor ar trebui să nu se aplice contoarelor inteligente sau gospodăriilor în care sunt instalate contoare inteligente. În plus, ar putea fi discutate următoarele aspecte:

- frecvența citirii contoarelor: gradul de intruziune în viața privată crește semnificativ pe măsură ce citirea contoarelor devine mai frecventă. GL29 ar saluta includerea în modelul DPIA a unor orientări suplimentare, inclusiv unele trimiteri[26] și exemple referitoare la acest aspect.
- eșantionarea: utilizarea eșantionării (și anume, colectarea de date numai de la un procent semnificativ din totalul gospodăriilor) ar putea contribui la eliminarea colectării și prelucrării datelor din toate gospodăriile pentru anumite scopuri (de exemplu, realizarea de previziuni). Exemple în acest sens ar trebui, de asemenea, să fie incluse în modelul DPIA.
- agregarea combinată cu ștergerea: pentru anumite scopuri, inclusiv realizarea de previziuni, ar trebui să fie suficientă păstrarea citirilor deosebit de detaliate ale contoarelor numai până în momentul în care se calculează agregarea. În astfel de cazuri, datele pot fi șterse definitiv de îndată ce agregarea este finalizată. Din nou, ar trebui să fie furnizate exemple.
- colectarea de date deja agregate (în loc de colectarea datelor individuale și agregarea ulterioară a acestora): pentru anumite scopuri (inclusiv unele scopuri legate de realizarea de previziuni, întreținerea rețelei și detectarea fraudelor), ar trebui să fie suficient ca operatorul rețelei de distribuție a energiei electrice sau a gazelor naturale să colecteze datele de la contoare care nu măsoară consumul gospodăriilor individuale, ci mai degrabă de la contoare amplasate în locații din cadrul rețelei de distribuție în care se poate măsura numai consumul agregat de la un număr de gospodării (de exemplu, un bloc de

[26] A se vedea GE2.P.1 în "Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection" („Cerințe esențiale de reglementare și recomandări pentru prelucrarea datelor, siguranța datelor și protecția consumatorului") (http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/expert_group2_deliverable.pdf)

apartamente mare, o stradă sau un cartier). În aceste cazuri, pentru astfel de scopuri, se poate evita în totalitate colectarea datelor deosebit de detaliate din gospodăriile individuale. Din nou, ar fi utilă introducerea în modelul DPIA a unor exemple ilustrative din viața reală pentru a încuraja respectarea legislației privind protecția datelor și bunele practici.

- pentru a contribui atât la reducerea la minimum a volumului de date colectate, cât și la minimizarea perioadei de timp pentru care datele vor fi păstrate, modelul DPIA ar trebui, de asemenea, să ofere un număr mai mare de orientări privind perioadele de păstrare a datelor. În opinia noastră, în principiu, stocarea datelor de consum deosebit de detaliate ale gospodăriilor individuale colectate în vederea facturării ar trebui să fie permisă doar până la sfârșitul perioadei în care factura poate fi contestată în mod legal sau pot fi făcute demersuri pentru efectuarea plății. (Desigur, aceasta nu aduce atingere dreptului consumatorului la o perioadă de păstrare mai lungă pe baza consimțământului său, de exemplu, pentru a obține recomandări specifice în materie de energie și pentru alte scopuri legale posibile.)

Glosar

GL29 recomandă ca glosarul să fie revizuit cu atenție astfel încât terminologia să fie conformă cu formularea actuală din Directiva 95/46/CE, precum și compatibilă cu noul cadru de protecție a datelor propus.