GRUPUL DE LUCRU „ARTICOLUL 29” PRIVIND PROTECȚIA DATELOR

2064/13/RO
WP 209

Avizul 07/2013 privind modelul de evaluare a impactului asupra protecției datelor pentru sistemele de rețele inteligente și de contorizare inteligentă („modelul DPIA”) pregătit de Grupul de experți nr. 2 al Grupului operativ pentru rețelele inteligente din cadrul Comisiei

Acest grup de lucru a fost instituit în temeiul articolul 29 din Directiva 95/46/CE și este un organism consultativ european independent privind protecția datelor și viața privată. Atribuțiile sale sunt prezentate la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de către Direcția C (Drepturi fundamentale și cetățenia Uniunii) a Comisiei Europene, Direcția Generală Justiție, B-1049 Bruxelles, Belgia, Biroul MO- 59 02/013.

Site internet: http://ec.europa.eu/justice/data-protection/index_ro.htm

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,

având în vedere regulamentul său de procedură,

ADOPTĂ PREZENTUL AVIZ:

1 Context

1.1 Introducere

Context

La 9 martie 2012, Comisia Europeană a emis Recomandarea 2012/148/UE privind pregătirile pentru introducerea sistemelor de contorizare inteligentă (denumită în continuare „recomandarea Comisiei”), în scopul de a oferi orientări statelor membre pentru introducerea sistemelor de contorizare inteligentă în sectorul energiei electrice și pe piețele gazelor. Recomandarea Comisiei își propune să ofere orientări privind chestiuni referitoare la protecția și securitatea datelor, privind o metodologie de evaluare economică a costurilor și beneficiilor pe termen lung legate de introducerea sistemelor de contorizare inteligentă[1], precum și privind cerințe funcționale minime comune aplicabile sistemelor de contorizare inteligentă a energiei electrice.

În ceea ce privește protecția datelor și securitatea pentru sistemele de contorizare inteligentă și rețelele inteligente, recomandarea Comisiei oferă statelor membre orientări privind protecția datelor începând cu momentul conceperii și protecția implicită a datelor și privind aplicarea unora dintre principiile de protecție a datelor prevăzute în Directiva 95/46/CE[2]. Recomandarea Comisiei prevede, de asemenea, că statele membre ar trebui să adopte și să aplice un model pentru evaluarea 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 (WP 29), în vederea emiterii unui aviz, în termen de 12 luni de la publicarea recomandării Comisiei. Ulterior, statele membre ar trebui să 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 conformitate cu raportul DPIA elaborat în

---

[1] Lansarea și analiza cost-beneficiu sunt prevăzute în (i) Directiva 2009/72/CE privind normele comune pentru piața internă a energiei electrice (JO L 211, 14.8.2009, p. 55) și (ii) Directiva 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) conține dispoziții suplimentare privind contorizarea inteligentă. Pentru piața energiei electrice, Directiva 2009/72/CE prevede că, în cazul în care introducerea contoarelor inteligente este evaluată pozitiv, cel puțin 80 % din consumatori trebuie să dețină astfel de contoare până în 2020. Nu s-a prevăzut 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.

urma aplicării modelului, ținând seama de avizul grupului de lucru WP 29 privind modelul[3].

De asemenea, recomandarea Comisiei prevede că DPIA ar trebui să conțină „*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*”.

Pregătirea

În februarie 2012, Comisia a reînnoit mandatul Grupului de experți nr. 2 („EG2”) al Grupului operativ pentru rețelele inteligente („SGTF”), pentru a oferi un model DPIA pentru rețelele inteligente. Ulterior, EG2, care este alcătuit în principal din reprezentanți ai sectorului, a organizat mai multe ateliere la care au participat reprezentanți ai WP 29, în calitate de observatori.

La 26 octombrie 2012, WP 29 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, în opinia WP29, necesită îmbunătățiri semnificative.

Prima emitere a modelului DPIA

La 8 ianuarie 2013, Comisia a transmis grupului de lucru WP 29 prima versiune a modelului DPIA elaborat de părțile interesate din cadrul EG2. În scrisoarea care însoțea modelul DPIA, Comisia a menționat că, sub rezerva observațiilor WP29 și a consensului său corespunzător, aceasta ar putea avea în vedere adoptarea modelului DPIA pregătit de părțile interesate din cadrul EG2 sub forma unei recomandări a Comisiei[4].

WP 29 a emis avizul 04/2013 la 22 aprilie 2013. Pe de o parte, avizul a recunoscut activitatea amplă a părților interesate din cadrul EG2 și a salutat obiectivele stabilite. Pe de altă parte, au fost identificate mai multe aspecte critice, care pot fi rezumate după cum urmează:

i. lipsa de claritate în ceea ce privește natura și obiectivele DPIA;

ii. deficiențe metodologice în modelul DPIA;

---

3 Grupul de experți EG2 a avut ca punct de plecare experiența dobândită în elaborarea și revizuirea „Propunerii sectorului privind un cadru de evaluare a impactului asupra vieții private și protecției datelor pentru aplicațiile RFID”, în urma observațiilor și avizelor emise de Grupul de lucru „articolul 29” („WP 29”).

4 La 17 ianuarie 2013, modelul DPIA a fost prezentat, de asemenea, Consiliului autorităților europene de reglementare în domeniul energetic (CEER). Președintele CEER a răspuns la 5 martie, salutând activitatea desfășurată de EG 2 și proiectul de model DPIA elaborat de acesta. Scrisoarea a reiterat importanța securității, a protecției datelor și a necesității ca clienții să aibă control asupra propriilor date, a făcut trimitere la recomandările anterioare ale CEER publicate în 2011 și a solicitat grăbirea procesului de finalizare a modelului DPIA.

iii. lipsa conținutului specific sectorului: riscurile specifice sectorului și controalele relevante pentru a face față riscurilor respective trebuie să fie identificate și corelate.

WP 29 a concluzionat că modelul DPIA nu era suficient de matur și de bine dezvoltat și a invitat Comisia să facă demersurile necesare pentru continuarea lucrului la modelul DPIA cu scopul de a asigura, în final, orientări practice suficient de specifice, utile și clare pentru operatorii de date.

De asemenea, WP 29 a invitat Comisia să aibă în vedere posibilitatea integrării în modelul DPIA a celor mai bune tehnici disponibile (BAT, astfel cum sunt definite la punctul 3.f din recomandare) și să transmită documentul integrat grupului de lucru WP29 în vederea emiterii unui aviz. De asemenea, se recomandă Comisiei să treacă în revistă activitățile din trecut și din prezent în domeniul DPIA și să ia în considerare posibilitatea de a defini o metodologie generică privind DPIA, de pe urma căreia să beneficieze activitatea din domenii specifice.

A doua emitere a modelului DPIA

Comisia a răspuns la avizul WP 29 din 27 mai 2013. Scrisoarea acesteia a făcut trimitere la o cerere din partea Comisiei către EG2 de revizuire a modelului și a recunoscut disponibilitatea WP 29 de a susține, într-o anumită măsură, activitatea GE2, păstrându-și, în același timp, rolul specific. În plus, Comisia a preferat să nu integreze BAT în model, din cauza domeniului lor de aplicare limitat la cerințele minime de funcționare comune pentru contorizarea inteligentă și a caracterului evolutiv al acestora[5]. În ceea ce privește propunerea de a defini o metodologie generică privind DPIA, de pe urma căreia ar putea beneficia inițiative specifice unui anumit domeniu, scrisoarea a indicat un alt departament competent al Comisiei, de la care nu s-a primit niciun răspuns până în prezent.

EG2 a creat o echipă de redactare pentru cel de-al doilea proiect al modelului, care s-a întrunit la 4 iunie și 3 iulie 2013. O serie de reprezentanți ai WP 29 au participat la prima reuniune în calitate de observatori și au răspuns întrebărilor din partea reprezentanților EG2 referitoare la diferitele aspecte legate de model.

La 20 august 2013, Comisia a prezentat grupului de lucru WP29 versiunea finală a modelului DPIA revizuit elaborat de membrii EG2.

Structura prezentului aviz

Secțiunea 1 prezintă evenimentele care au condus la revizuirea modelului DPIA și face referire la secțiunile din avizul 04/2013 cu privire la aspectul protecției datelor în cadrul rețelelor inteligente și la obiectivele DPIA în acest context.

---

[5] *„Consider că acest lucru nu ar fi atât de benefic pe cât intenționați din următoarele motive: (i) în conformitate cu Recomandarea 2012/148/UE a Comisiei, BAT se concentrează numai pe cerințele funcționale minime comune pentru contorizarea inteligentă, în timp ce domeniul de aplicare a modelului DPIA depășește porțiunea finală a rețelei, incluzând întregul spectru ale rețelei inteligente; și (ii) în cazul în care BAT ar fi incluse în modelul DPIA, caracterul evolutiv și ilustrativ al acestora ar determina, prin însuși acest fapt, efemeritatea modelului și, posibil, necesitatea nepractică ca acesta să fie suspus în mod frecvent revizuirii .”*
(scrisoarea ener.b.3 VL/CV (2013) 1506536 adresată dlui Kohnstamm, 27 mai 2013)

Secțiunea 2 conține evaluarea modelului DPIA revizuit efectuată de către WP29.

În secțiunea 3 sunt prezentate concluziile finale.

1.2 Protecția datelor în rețelele inteligente și obiectivele DPIA în acest context

Secțiunile 1.2 și 1.3 din avizul 04/2013 au abordat deja aspectele legate de protecția datelor în rețelele inteligente și obiectivele DPIA în acest context. WP 29 nu are de adăugat niciun element nou cu privire la chestiunile respective.

2 Analiza modelului DPIA

WP 29 consideră binevenite activitățile desfășurate de membrii EG2 în încercarea de a găsi răspunsuri la observațiile WP29 și disponibilitatea acestora de a ține seama de recomandările WP 29 considerându-le un sprijin prețios.

Prezenta analiză urmărește în principal observațiile formulate în avizul 04/2013. Aceasta include, de asemenea, îmbunătățiri și optimizări care ar trebui luate în considerare pentru finalizarea modelului. Secțiunile de mai jos țin seama de ambele aspecte.

Pentru o înțelegere cuprinzătoare și clară, analiza trebuie citită având în vedere conținutul și terminologia din avizul 04/2013.

2.1 Modelul DPIA și Recomandarea 2012/148/UE

WP 29 a utilizat acest prilej pentru a reexamina îndeaproape cel de-al doilea aspect al modelului DPIA pentru rețelele inteligente având în vedere recomandarea Comisiei, care prevede scopul, domeniul de aplicare și aplicabilitatea acestuia.

2.1.1 Considerații privind natura discreționară a elaborării unei DPIA pentru rețelele inteligente

Deși existența unei recomandări a Comisiei nu impune, pe de o parte, o obligație legală, pe de altă parte, aceasta implică faptul că anumite măsuri sunt recomandate cu insistență. Recomandarea 2012/148/UE prevede că operațiunile de prelucrare a datelor cu caracter personal în cadrul contoarelor inteligente/rețelelor inteligente necesită un „*proces sistematic de evaluare a impactului potențial al riscurilor,... drepturile și libertățile persoanelor vizate prin însăși natura, domeniul de aplicare sau scopurile lor”.* WP 29 dorește să reitereze că necesitatea unui astfel de proces, stabilită deja în Avizul 12/2011 al WP 29 privind contorizarea inteligentă în contextul unei abordări de tipul „luarea în considerare a vieții private începând cu momentul conceperii”, este justificată în mare măsură de complexitatea infrastructurii tehnice și administrative a rețelelor inteligente, de potențiala scară de aplicare și evoluție a acesteia și de riscurile specifice pentru drepturile și libertățile fundamentale ale omului, inclusiv, printre altele, dreptul la viață (de exemplu, întreruperea aprovizionării cu energie electrică în cazul în care anumite mașini alimentate cu energie electrică susțin funcții vitale).

În plus, WP29 a salutat propunerea Comisia cu privire la un regulament general privind protecția datelor, care ar introduce obligativitatea, în anumite condiții, a evaluării impactului asupra protecției datelor. Ar trebui să fie clar pentru părțile interesate de modelul DPIA pentru rețelele inteligente, și anume, operatorii de date și persoanele împuternicite de către operatori, că utilizarea modelului ar trebui privită ca o modalitate de respectare a unei obligații legale în viitor. Având în vedere investițiile enorme și orizontul îndepărtat de planificare pentru rețelele de utilități, ar trebui să se înțeleagă că este în interesul real al părților interesate să dobândească deja experiență în ceea ce privește abordarea DPIA și să o aplice încă de la început în proiectarea sistemelor proprii, astfel încât să nu se confrunte cu probleme de conformitate atunci când legislația care este în prezent în curs de adoptare va intra în vigoare. În cazul în care limbajul utilizat în prezentul model, în special în secțiunea 2.1, ar putea fi interpretat ca lăsând o marjă considerabilă pentru o abordare discreționară din partea întreprinderii, Comisia ar trebui să clarifice faptul că marja trebuie să fie interpretată în mod strict, asigurându-se că se efectuează o DPIA reală în modul cel mai exhaustiv cu putință, de exemplu, prin explicarea abordării într-o recomandare a Comisiei care ar putea însoți și susține modelul. WP 29 privește evaluarea prealabilă ca având un rol funcțional, pentru a lua în considerare toate situațiile posibile cu care s-ar putea confrunta potențialii operatori și persoanele împuternicite de către operator, pe baza informațiilor prelucrate, al domeniului de aplicare a (sub)sistemului aflat în curs de analizare, al statutului proiectului etc., și nu ca o etapă din metodologie care scade importanța obiectivelor recomandării Comisiei.

2.1.2 DPIA și autoritățile de protecție a datelor

Punctul 8 din recomandarea Comisiei prevede că statele membre ar trebui să se asigure că entitatea responsabilă cu prelucrarea datelor cu caracter personal consultă APD cu privire la evaluarea impactului asupra protecției datelor, înainte de prelucrare. WP 29 remarcă faptul că, în multe locuri, modelul nu reflectă în totalitate această abordare. Câteva citate: „în caz de dubiu” (secțiunea 2.1.4) sau a se consulta numai responsabilul cu protecția datelor (nu APD), „atunci când sunt disponibile” (secțiunea 2.6.2) sau care urmează să fie prezentate APD „în cazul în care este necesar” după adoptarea raportului final (secțiunea 2.7). Deși ar fi preferabil ca modelul să clarifice în mod consecvent faptul că, exceptând cazul în care legislația în domeniul protecției datelor și/sau politica națională a APD prevăd explicit o derogare, autoritățile naționale pentru protecția datelor trebuie să fie consultate înainte de prelucrare, în conformitate cu recomandarea Comisiei. Comisia ar trebui să se asigure în mod corespunzător că părțile interesate înțeleg clar că modelul DPIA adoptat în conformitate cu recomandarea acesteia nu poate modifica principiile adoptate în recomandare ca atare. Pasajele la care se face trimitere pot fi înțelese numai ca recomandând posibilități suplimentare de a obține consiliere, care sunt complementare consultării APD, astfel cum recomandă Comisia.

2.2 Claritate cu privire la natura și obiectivele DPIA

2.2.1 Luarea în considerare a impactului final asupra drepturilor și libertăților persoanelor

WP 29 consideră binevenit faptul că etapa evaluării riscurilor din cadrul metodologiei prevăzute în model (secțiunea 2.5) urmărește să analizeze efectele reale asupra persoanelor vizate cu privire la drepturile, libertățile fundamentale și libertățile civile ale acestora (cum ar fi, de exemplu, pierderi financiare sau discriminarea prin prețuri

sau infracțiuni facilitate prin crearea de profiluri neautorizate) ca fiind efecte ale „evenimentelor nedorite" ce au drept cauză prelucrarea neloială și ilegală a datelor cu caracter personal, și nu impactul asupra obiectivelor în materie de viață privată ca atare.

Cu toate acestea, pare să existe încă un anumit grad de confuzie în textul care explică metodologia de evaluare a riscurilor (a se vedea secțiunea relevantă din prezentul aviz), în special, la punctul 2.5.1.1 din model, care descrie modul de evaluare a impactului evenimentelor nedorite. În special, teza care încearcă să identifice elementele utilizate pentru evaluarea „*impactului și gravității unei anumite amenințări identificate*" nu este deloc clară. Aceasta menționează obiectivele privind viața privată ca elemente componente ale evaluării (a se vedea punctul 2.2.2 din prezentul aviz) fără a detalia și a explica modul în care acestea se integrează, scoate în evidență „*riscurile legate de activitatea infracțională*" fără motive declarate și enumeră separat elemente precum „*dreptul la liberă circulație, pierderea independenței, pierderea egalității"*, numindu-le „*alte principii privind viața privată*"[6].

WP 29 dorește să sublinieze că DPIA evaluează, întotdeauna și în mod consecvent, impactul asupra „*drepturilor și libertăților persoanei vizate*", astfel cum s-a amintit la punctul 2.1 din avizul 04/2013 și astfel cum s-a precizat în mod corect în mai multe locuri în cadrul formularului. În cazul în care modelul utilizează o terminologie diferită, de exemplu, care se referă numai la dreptul la viață privată, acest lucru trebuie interpretat ca făcând referire la conceptul mai larg. Acest aspect ar trebui abordat în cadrul revizuirilor viitoare ale modelului.

De asemenea, dacă este adevărat că același eveniment nedorit ar putea conduce la numeroase efecte asupra persoanelor vizate, ar putea fi util, în vederea unei sensibilizări sporite și a calibrării impactului, să se enumere cele mai relevante impacturi asupra persoanelor vizate cu privire la evenimentele nedorite în cadrul exemplelor citate la punctul 3.4.1. Legătura dintre evenimentul nedorit și impactul asupra drepturilor și libertăților fundamentale ale omului caracterizează acest efort, în contextul protecției persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, spre deosebire, de exemplu, de o simplă evaluare a riscurilor privind securitatea informațiilor.

2.2.2 Gestionarea obiectivelor privind viața privată

Modul de gestionare a obiectivelor privind viața privată este unul dintre cele mai importante aspecte din cadrul evaluării impactului asupra vieții private. Într-adevăr, scopul său este de a se asigura că obiectivele privind viața privată au fost corect luate în considerare.

---

[6] O soluție ar putea fi completarea ultimei teze a primului alineat de la punctul 2.5.1.1. „Impactul evenimentelor nedorite" cu alte elemente; aceasta ar putea fi formulată astfel: „Impactul potențial se definește prin consecințele pe care fiecare eveniment nedorit le-ar putea avea asupra vieții private și asupra altor drepturi și libertăți fundamentale ale persoanelor vizate, inclusiv, de exemplu, riscurile legate de activitatea infracțională, cum ar fi furtul de identitate și frauda, sau dreptul la liberă circulație, independența, egalitatea de tratament, relațiile sociale, interesele financiare etc. din cauza, de exemplu, creării de profiluri, a comercializării neautorizate, a discriminării sau a deciziilor individuale pe baza unor informații eronate..."

În prezent, obiectivele privind viața privată sunt:

- menționate la punctul „2.5.1.1 Impactul evenimentelor nedorite” ca elemente care trebuie luate în considerare atunci când se evaluează impactul și gravitatea unei anumite amenințări identificate;
- menționate la punctul „2.6.3. Riscuri reziduale și acceptarea riscului” ca scopuri care trebuie atinse;
- enumerate și descrise în „Anexa 1. Obiective privind protecția vieții private și a datelor”.

Directiva 95/46/CE[7] stabilește, în cadrul majorității dispozițiilor sale, condiții specifice pentru prelucrarea datelor cu caracter personal și o serie de obligații care trebuie respectate de către operatorii de date și persoanele împuternicite de către operatori. Directiva nu prevede o marjă de apreciere sau niveluri acceptabile de nerespectare a dispozițiilor. Deși asigurarea securității prelucrării este una dintre obligații, pentru punerea sa în aplicare directiva prevede la articolul 17 o metodă de gestionare a riscurilor, menționând că „având în vedere stadiul actual al tehnologiei și costurile punerii lor în aplicare, aceste măsuri trebuie să asigure un nivel de securitate corespunzător riscurilor reprezentate de prelucrarea și de natura datelor care trebuie protejate”. În contextul unui model de evaluare a impactului, este important să se conștientizeze faptul că strategiile de gestionare a riscurilor, cum sunt cele elaborate în domeniul securității, pot fi aplicate pentru protecția datelor, dar numai cu privire la aspectele de securitate, și că, pentru majoritatea obligațiilor, respectarea în totalitate a legislației este necesară. Modelul utilizează termenul „obiective privind viața privată” pentru a desemna obligațiile de conformitate și clarifică la punctul 2.6.3 că noțiunile de riscuri reziduale și acceptare a riscului nu se aplică obiectivelor în materie de viață privată care „trebuie să fie atinse” (p. 33).

WP 29 consideră binevenit faptul că distincția între gestionarea riscurilor și conformitate este recunoscută în model, dar ar fi dorit o prezentare mai clară și mai vizibilă.

În consecință, ar trebui să existe întotdeauna două acțiuni complementare și distincte pentru a aborda constatările DPIA. Prima acțiune se referă la riscurile asupra datelor cu caracter personal. Acestea ar trebui să facă obiectul gestionării riscurilor (evaluare, prelucrare etc.). Cea de-a doua acțiune se referă la conformitatea cu obiectivele privind viața privată ca atare, ca obligații legale. Acest lucru trebuie considerat drept probleme de conformitate (măsurile puse în aplicare sau planificate pentru a atinge obiectivele privind viața privată, justificarea în cazul în care acest lucru nu este realizat, riscurile juridice într-un astfel de caz, controale planificate pentru a verifica dacă și în ce mod se realizează...).

În ceea ce privește analiza riscurilor, ar trebui să se sublinieze că evenimentele nedorite descrise la punctul „2.4.1. Introducere” ar trebui să fie evaluate în mod sistematic. Impactul lor potențial asupra persoanelor vizate ar trebui să fie identificat,

[7] 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.

iar estimarea prejudiciului rezultat ar trebui să se bazeze pe impactul potențial. Cu toate acestea, Comisia ar putea dori să verifice care este distincția dintre ultimul eveniment nedorit (devierea datelor cu caracter personal... către persoane care nu au nevoie de acestea) și cel de-al treilea (accesul ilegitim la datele cu caracter personal... de către persoanele neautorizate).

WP 29 dorește să propună o serie de instrumente pentru a completa metodologia propusă în model, pentru a facilita aplicabilitatea acesteia. Acesta invită Comisia să aducă sugestiile la cunoștința potențialilor utilizatori ai modelului, de exemplu, prin punerea la dispoziție a prezentului aviz împreună cu modelul sau efectuarea de trimiteri la acesta în orice instrument de însoțire. Instrumentele complementare sunt descrise în anexa la prezentul aviz.

2.3 Metodologia utilizată în modelul DPIA

În general, metodologia descrisă în model a fost clarificată și este mai concretă. Cu toate acestea, numeroase elemente rămân neclare și confuze, inclusiv în lista amenințărilor generice prevăzute la punctul 3.4.1, în formularele modelului și în chestionarul furnizat.

Unele dintre elemente au fost abordate la punctul 2.1, atunci când s-a discutat aspectul clarității privind natura și obiectivele DPIA. Celelalte vor fi abordate aici.

2.3.1 Metodologia evaluării (gestionării) riscurilor

Majoritatea elementelor din metodologia gestionării riscurilor sunt, se pare, bazate în principal pe metodologia ISO 31 000, EBIOS și pe sinteza elaborată de către CNIL[8].

Identificarea activelor

Există o definiție a activelor primare și de sprijin, ca obiective ale evaluării globale a riscurilor.

Identificarea și evaluarea amenințărilor și a punctelor vulnerabile

Distincția dintre amenințări și riscuri este stabilită în prezent. Există mai multe orientări cu privire la conceptul de vulnerabilitate.

Cu toate acestea, WP 29 este preocupat de faptul că prezentarea obiectivelor neîndeplinite privind viața privată ca amenințări generice enumerate la punctul 3.4.1, în special la subpunctul 3.4.1.4, ar putea conduce la interpretarea greșită potrivit căreia modelul ar „defini un obiectiv neîndeplinit privind viața privată drept o amenințare”, în concordanță cu evaluarea obiectivelor privind viața privată în contextul metodologiei evaluării riscurilor. Aspectul a fost deja discutat la punctul 2.2.2 din prezentul aviz.

WP 29 recunoaște, cu toate acestea, că exemplele relevante și orientările furnizate (în ceea ce privește datele din tabelele de la punctul 3.4.1, care descriu obiectivele neîndeplinite privind viața privată) în celelalte coloane sunt încă utile, odată îmbunătățite, în vederea îndeplinirii obiectivelor privind viața privată. WP29

[8] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf.

sugerează ca informațiile respective să fie utilizate în contextul unei abordări mai largi și mai precise a obiectivelor privind viața privată (a se vedea, de asemenea, considerațiile de la sfârșitul secțiunii 2.2.2 din prezentul aviz), pentru a oferi orientări cu privire la modul de îndeplinire a acestora. Aceasta ar putea lua forma unui tabel sau, probabil mai bine, a unei secțiuni speciale în cadrul căreia s-ar putea oferi, de asemenea, orientări în contextul unor operațiuni riscante de prelucrare a datelor (cum ar fi crearea de profiluri sau adoptarea de decizii asupra unor persoane pe baza operațiunilor de prelucrare automată).

Calcularea riscurilor/stabilirea priorităților în materie de riscuri

Există orientări mai clare referitoare la modalitatea de calculare a riscurilor și de stabilire a priorităților în materie de riscuri. Sunt necesare o mai bună formulare și mai multă claritate în secțiunea privind calcularea riscurilor (2.5.1.3).

Regimul riscurilor

„Punctul 2.6.1. Modificarea riscurilor: controale planificate și puse în aplicare” ar trebui să fie integrat în „2.5. Etapa 5 – Evaluarea riscurilor în materie de protecție a datelor” și să fie luat în considerare în prima estimare a riscurilor. Cu toate acestea, titlul nu ar trebui să menționeze „modificarea riscurilor”, care reprezintă una dintre opțiunile de abordare a riscurilor. Acesta ar putea să fie pur și simplu „Controale planificate și puse în aplicare”. În plus, la punctul „2.6. Etapa 6 – Identificarea și recomandarea de controale și riscuri reziduale”, în special, la punctul „2.6.2. Regimul riscurilor”, sunt stabilite controale suplimentare și riscurile sunt estimate din nou ca riscuri reziduale.

În avizul 04/2013, WP 29 a remarcat că, în prima versiune a modelului, nu existau corespondențe între riscurile care trebuiau să fie diminuate și lista controalele posibile din anexa II. WP 29 salută faptul că, în noua versiune a modelului, descrierea obiectivului controalelor posibile include, adesea, tipul de riscuri a căror diminuare este urmărită. În plus, lista neexhaustivă a amenințărilor generice de la punctul 3.4.1 stabilește legături între amenințări și controalele posibile din anexa II.

Riscuri reziduale

Este necesară o ponderare a riscurilor reziduale, deoarece la sfârșitul procesului de gestionare a riscurilor este la fel de important să se identifice toate interesele aflate în joc într-un stadiu incipient. Acestea pot fi preluate din procesul global de gestionare a riscurilor al întreprinderii, în cazul în care acesta există. Pot fi reprezentate nu numai interesele economice sau alte interese legitime, ci și alte mize, cum ar fi, de exemplu, responsabilitatea socială sau respectarea celorlalte cerințe juridice.

WP 29 sugerează adăugarea unei noi secțiuni în scopul de a identifica mizele prelucrării. Secțiunea ar putea fi introdusă între 2.3.1 și 2.3.2 și denumită „2.3.2. Mize ale prelucrării”. Aceasta ar putea cuprinde o descriere a oportunităților de creare a prelucrării în cadrul rețelei inteligente (comerciale/economice, societale, de conformitate juridică etc.).

S-ar putea adăuga o evaluare a riscurilor reziduale, dată fiind miza, după primul alineat de la punctul „2.6.4. Rezoluție”. Alineatul respectiv ar putea explica faptul că

rezoluția constă în luarea deciziei de a accepta sau nu riscurile reziduale, dată fiind miza identificată la punctul 2.3.

2.3.2 Roluri și responsabilități

WP29 salută integrarea (secțiunea 1.4.2) unei liste cu diferitele tipuri de operatori de rețele inteligente, inclusiv o descriere generică a scopurilor pentru care aceștia ar putea prelucra date cu caracter personal.

Existența subpunctului specific 2.1.2 subliniază mai bine în prezent necesitatea alocării clare a responsabilităților operatorului și ale persoanei împuternicite de către operator. Exemplul din text privind responsabilitățile operatorului și ale persoanei împuternicite de către operator ar trebui să fie completat cu alte exemple care abordează situații mai complexe. Un alt exemplu este raportat în text (micro-operatorul de rețea și societatea de asigurări implicată), unde este prezentată problema, dar nu este prevăzută nicio recomandare.

De asemenea, astfel cum se recomandă deja în avizul 04/2013, modelul DPIA ar putea include, în a treia etapă, o a patra secțiune vizând determinarea diferitelor responsabilități ale diferitelor entități implicate în prelucrarea datelor (în cazul în care există deja un formular corespunzător în secțiunea 3).

2.3.3 Formularele modelului

Pe lângă considerentele din celelalte secțiuni ale prezentului aviz, WP 29 dorește să sublinieze o serie de alte deficiențe în secțiunile care descriu unele formulare utilizate pentru implementarea DPIA.

De exemplu, la punctul 3.3, relația dintre diferitele modele utilizate pentru identificarea, caracterizarea și descrierea sistemelor de rețele inteligente, ordinea utilizării modelelor și modul exact în care acestea ar trebui să fie utilizate nu sunt clare. Există o trimitere la un document extern fără nicio observație cu privire la ce se face astfel trimitere. Dar se pare că nu există nicio mențiune în metodologie cu privire la situația în care trebuie să fie utilizat formularul din secțiunea 3.3.5.

Pe de altă parte, un tabel cu active primare și active de sprijin corespunzătoare este important în evaluarea riscurilor.

În general, este necesară furnizarea unor orientări suplimentare privind utilizarea formularelor. Prezentarea unuia sau a mai multor exemple într-o anexă ar fi foarte utilă.

2.4 Conținutul specific sectorului al modelului DPIA

Unul dintre principalele aspecte din avizul 04/2013 a fost că riscurile și controalele prevăzute în prima versiune a modelului nu reflectau experiența din cadrul sectorului în ceea ce privește principalele preocupări și cele mai bune practici.

WP 29 constată și salută faptul că unele aspecte specifice au fost adăugate în lista neexhaustivă a amenințărilor generice raportate în secțiunea 3.4.1.1, în special, în coloana cu titlul „Exemple specifice din industria energetică privind punctele vulnerabile ale activelor de sprijin”. Cu toate acestea, WP29 consideră că sunt

necesare în continuare îmbunătățiri și orientări, atât în ceea ce privește textul, cât și în ceea ce privește modelul, în special, în vederea îndeplinirii obiectivelor în materie de viață privată (a se vedea, de asemenea, punctul 2.2.2).

Astfel cum s-a amintit la punctul 1.1, Comisia a respins propunerea WP29 de a integra în model cele mai bune tehnici disponibile (BAT), la care lucrează EG2, din cauza domeniului lor de aplicare limitat la contoarele inteligente și a naturii evolutive a acestora.

WP 29 confirmă faptul că, în opinia sa, luarea în considerare a BAT ca rezultat legat în mod inerent de model va permite unei organizații care efectuează o DPIA să aleagă măsurile adecvate atunci când este necesar. Natura evolutivă a BAT nu contravine rolului său complementar pentru modelul DPIA. În plus, modelul în sine va avea nevoie de un ciclu de revizuire pentru a menține și a perfecționa metodologia după o primă fază de aplicare și, în orice caz, periodic. Faptul că domeniul de aplicare a BAT este limitat la contoarele inteligente și, prin urmare, nu este exhaustiv nu este un motiv pentru a exclude utilizarea sa în cadrul unui exercițiu DPIA. Contoarele inteligente reprezintă subsistemele în care datele cu caracter personal sunt colectate și prelucrate în principal și, în orice caz, este mai bine să existe câteva orientări decât niciuna. În plus, WP29 profită de această ocazie pentru a propune ca sectorul și Comisia să exploreze posibilitatea de a extinde activitatea valoroasă din domeniul BAT și la domeniul mai larg al rețelelor inteligente.

În avizul 04/2013, în special, în anexa II, WP 29 recomandă ca cel puțin cele mai comune tehnologii de protecție a vieții private („PET”) și alte „cele mai bune tehnici disponibile” pentru reducerea la minim a datelor să fie descrise pe scurt și într-un mod neutru din punct de vedere tehnologic în modelul DPIA, iar ulterior să fie detaliate suplimentar în documentul de însoțire privind BAT. Acest lucru nu s-a întâmplat. WP29 consideră în continuare că acest lucru ar fi foarte util pentru sector, pentru a avea un portofoliu de măsuri pregătite pentru a fi puse în aplicare și pentru a cunoaște tehnologiile de protecție a vieții private în vederea conceperii de noi controale adecvate.

2.5 Necesitatea testării/validării modelului DPIA

WP 29 sugerează efectuarea unei testări/validări adecvate a modelului DPIA pe teren, pe baza versiunii existente și ținând seama într-o măsură cât mai mare de observațiile de mai sus. WP 29 sugerează că, în urma testelor, modelul și metodologia sa ar trebui să fie revizuite și consolidate, ținând cont de experiențele și de observațiile menționate anterior. Astfel de teste, cu privire la care WP 29 ar trebui să fie informat și pentru care APD ar putea să ofere sprijin, pot fi utile, de asemenea, pentru oferirea de exemple valoroase care urmează să fie incluse în anexele la model, pentru o mai bună înțelegere a metodologiei propuse.

2.6 Alte considerații

2.6.1 Conceptul de date cu caracter personal

Secțiunea 2.1 descrie modul în care se determină dacă datele cu caracter personal sunt prelucrate în subsistemul rețelei inteligente aflate în curs de analizare. WP 29 ia act de faptul că, în exemplele enumerate, clasificarea ca date cu caracter personal pare a fi

corectă, chiar dacă justificarea oferită pentru a identifica o informație ca date cu caracter personal nu aplică întotdeauna strict terminologia juridică.

De exemplu, așa-numitele date „de utilizare" sunt considerate date cu caracter personal deoarece „oferă o perspectivă asupra vieții cotidiene personale", în timp ce acestea sunt date cu caracter personal doar pentru că se referă la persoana care deține contractul și la familia sa potențială. Faptul că acestea oferă o perspectivă asupra vieții de zi cu zi constituie un impact asupra vieții private. Acest aspect este valabil, de asemenea, pentru celelalte elemente enumerate în anexa respectivă. În timp ce lista de exemple este, cu siguranță, utilă pentru potențialii utilizatori ai modelului, se creează impresia că un impact atât de semnificativ asupra vieții private este necesar pentru ca datele să fie considerate ca având caracter personal. În plus, ar trebui să fie clar că lista de exemple nu este exhaustivă.

2.6.2 Alte observații privind terminologia referitoare la protecția datelor

În anumite secțiuni, modelul utilizează termeni precum „deținătorul sistemului", care are semnificație în domeniul de aplicare, însă nu clarifică întotdeauna relația cu terminologia referitoare la protecția datelor care ar putea fi aplicabilă (precum operator de date,...) (p. 14, 18, 32,...) sau „persoana", „consumatorul", „clientul", fără o legătură clară cu persoana vizată (p. 10, 15, ...)

În plus, anumite formulări utilizate precum „a fost convenit cu clientul" (p 10), „clienții trebuie să aibă posibilitatea de a alege" (p 11) ar putea fi corelate cu necesitatea de a obține „consimțământul", astfel cum este definit la articolul 2 litera (h) din directivă.

WP 29 recomandă să se aibă în vedere indicarea, de asemenea, a terminologiei relevante privind protecția datelor, și să se explice nivelul de interoperabilitate a termenilor, dacă este cazul.

2.7 Concluzii și recomandări

WP 29 recunoaște activitatea desfășurată de grupul de experți EG2 și este conștient de faptul că a doua versiune a modelului aduce îmbunătățiri considerabile comparativ cu versiunea anterioară, metodologia fiind mai bine definită și ușor de urmărit. Cu toate acestea, există încă o serie de elemente neclare și este necesară o mai mare claritate în anumite locuri, aspecte care, dacă vor fi soluționate astfel cum s-a indicat, vor contribui în mod determinant la aplicarea și utilizarea cu succes a modelului.

WP 29 înțelege că versiunea evaluată ar putea fi supusă în continuare editării lingvistice și juridice.

WP 29 este conștientă de necesitatea urgentă a unei DPIA în sectorul industrial și consideră binevenită elaborarea promptă a unei versiuni finale a modelului, a cărei eficacitate, după o anumită perioadă de utilizare, va trebui, cu siguranță, să fie verificată și îmbunătățită. Prin urmare, se recomandă să se organizeze o fază de testare utilizând o serie de cazuri reale, cu privire la care WP 29 ar trebui să fie informată și în cadrul căreia APD-uri individuale ar putea oferi sprijin și care ar trebui, de asemenea, să ofere asigurări că modelul asigură persoanelor o mai bună protecție a datelor în contextul implementării rețelelor inteligente. În testarea

modelului, astfel cum se prevede în acesta, sectorul este încurajat să acorde atenție conceptelor cheie ale reformei în materie de protecție a datelor, cum ar fi protecția datelor începând cu momentul conceperii și protecția implicită a datelor, reducerea la minim a datelor, dreptul de a fi uitat și portabilitatea datelor.

De asemenea, WP 29 recomandă în continuare să se aibă în vedere posibilitatea de a defini o metodologie generică privind DPIA, de pe urma căreia vor putea beneficia eforturile în acest sens din domenii specifice.

Adoptat la Bruxelles, 4 decembrie 2013

Pentru grupul de lucru
Președintele
Jacob KOHNSTAMM

Anexă: Instrumente metodologice suplimentare

La punctul „3.5. Etapa 5 – Evaluarea riscurilor în materie de protecție a datelor”, următorul tabel ar putea fi utilizat pentru a evalua evenimentele nedorite:

Procesul și datele cu caracter personal	Nivelul de identificare (NI)	Evenimente nedorite	Efecte potențiale	Prejudicii (P)	Gravitate (NI + P)
[lista datelor cu caracter personal în cauză]	[nivelul cel mai adecvat în scara NI, pe baza datelor cu caracter personal]	[eveniment nedorit]	[lista potențialelor consecințe asupra persoanelor vizate în cazul în care evenimentul nedorit se produce]	[nivelul cel mai adecvat pe scara prejudiciilor, pe baza efectelor potențiale]	[sumă]

În cazul în care datele cu caracter personal nu sunt evaluate la nivel global, rubricile trebuie repetate (de exemplu, pentru fiecare proces).

Același tabel ar putea fi extins prin adăugarea altor coloane privind amenințările, astfel încât să se poată prezenta toate riscurile:

Procesul și datele cu caracter personal	Nivelul de identificare (NI)	Evenimente nedorite	Efecte potențiale	Prejudicii (P)	Gravitate (NI + P)	Amenințările principale	Puncte vulnerabile (VUL.)	Surse de risc	Capacități (CAP)	Probabilitate (VUL + CAP)

O nouă secțiune ar trebui să fie adăugată pentru a demonstra conformitatea cu obiectivele privind viața privată. Secțiunea ar putea fi introdusă între 2.6.2 și 2.6.3 și denumită „2.6.3. Conformitatea cu obiectivele privind viața privată”. Deoarece obiectivele privind viața privată sunt obligatorii și nu sunt negociabile, în secțiunea respectivă ar trebui să se descrie pentru fiecare obiectiv privind viața privată modul în care acesta este pus în aplicare sau ar trebui să se justifice nepunerea sa în aplicare[9].

Tabelul următor ar putea fi utilizat în acest scop:

[9] Aceasta este comparabilă cu noțiunea de „declarație privind aplicabilitatea” din ISO/IEC 27001.

Obiective privind viața privată	Explicații	Descriere/justificare
Protejarea calității datelor cu caracter personal	Evitarea și reducerea la minim a utilizării datelor, specificarea și limitarea domeniului de aplicare, calitatea datelor și transparența sunt obiective esențiale a căror îndeplinire trebuie asigurată.	[descrierea modului în care obiectivul privind viața privată a fost realizat SAU justificarea în cazul în care acesta nu a fost realizat]
Legitimitatea prelucrării datelor cu caracter personal	Legitimitatea prelucrării datelor cu caracter personal trebuie asigurată prin prelucrarea datelor pe baza consimțământului explicit, a unui contract, a obligației legale etc.	[descrierea modului în care obiectivul privind viața privată a fost realizat sau justificarea în cazul în care nu a fost realizat]
Legitimitatea prelucrării datelor sensibile cu caracter personal	Legitimitatea prelucrării datelor sensibile cu caracter personal trebuie asigurată prin prelucrarea datelor pe baza consimțământului explicit, a unui temei juridic special etc.	[descrierea modului în care obiectivul privind viața privată a fost realizat SAU justificarea în cazul în care acesta nu a fost realizat]
Respectarea dreptului persoanei vizate de a fi informată	Trebuie să se asigure informarea persoanei vizate cu privire la colectarea datelor acesteia în timp util.	[descrierea modului în care obiectivul privind viața privată a fost realizat SAU justificarea în cazul în care acesta nu a fost realizat]
Respectarea dreptului persoanei vizate de a avea acces la date, de a rectifica și a șterge datele	Trebuie să se garanteze că dorința persoanei vizate de a accesa, a rectifica, a șterge și a bloca datele sale este respectată în timp util. Punerea în aplicare a dreptului de a fi uitat și a dreptului la portabilitatea datelor ar trebui să fie încurajată.	[descrierea modului în care obiectivul privind viața privată a fost realizat SAU justificarea în cazul în care acesta nu a fost realizat]
Respectarea dreptului de opoziție al persoanei vizate	Trebuie să se asigure că datele persoanei vizate nu mai sunt prelucrate dacă aceasta se opune. Transparența deciziilor automate privind persoanele fizice trebuie să fie asigurată, în special, în cazul creării de profile.	[descrierea modului în care obiectivul privind viața privată a fost realizat SAU justificarea în cazul în care acesta nu a fost realizat]
Protejarea confidențialității și a securității prelucrării	Împiedicarea accesului neautorizat, înregistrarea prelucrării datelor, securitatea rețelei și a transportului și prevenirea pierderii accidentale a datelor sunt obiective esențiale a căror respectare trebuie să fie asigurată. Ar trebui promovată procedura de notificare a încălcărilor.	[descrierea modului în care obiectivul privind viața privată a fost realizat SAU justificarea în cazul în care acesta nu a fost realizat]
Respectarea cerințelor în materie de notificare	Notificarea privind prelucrarea datelor, verificarea anterioară a conformității și documentarea sunt obiective esențiale a căror respectare trebuie să fie asigurată. DPIA trebuie să fie considerat un instrument determinant pentru acest obiectiv.	[descrierea modului în care obiectivul privind viața privată a fost realizat SAU justificarea în cazul în care acesta nu a fost realizat]
Respectarea cerințelor în materie de păstrare a datelor	Păstrarea datelor ar trebui să se efectueze pe perioada minimă de timp corespunzătoare scopului păstrării sau altor cerințe juridice.	[descrierea modului în care obiectivul privind viața privată a fost realizat SAU justificarea în cazul în care acesta nu a fost realizate]

Obiective privind viața privată	Explicații	Descriere/justificare
Respectarea vieții private încă din stadiul conceperii	Având în vedere stadiul actual al tehnicii și costurile de punere în aplicare, măsurile tehnice și organizatorice și procedurile trebuie concepute atât în momentul stabilirii mijloacelor pentru prelucrare, cât și în cel al prelucrării în sine, astfel încât să respecte pe deplin drepturile persoanei vizate în materie de protecție a datelor și a vieții private.	[descrierea modului în care obiectivul privind viața privată a fost realizat SAU justificarea în cazul în care acesta nu a fost realizat]
Respectarea implicită a vieții private	Trebuie puse în aplicare mecanisme care garantează că, implicit, se prelucrează numai datele cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării și că datele respective nu sunt colectate sau păstrate mai mult decât minimul necesar pentru îndeplinirea acestor scopuri, în ceea ce privește atât volumul datelor, cât și perioada de stocare a acestora.	[descrierea modului în care obiectivul privind viața privată a fost realizat SAU justificarea în cazul în care acesta nu a fost realizat]

Desigur, fiecare dintre rubricile de mai sus poate fi multiplicată pentru defalcarea fiecăruia dintre obiectivele privind viața privată, în cazul în care se consideră util. De exemplu, „calitatea datelor” cuprinde multe alte principii precum reducerea la minim și evitarea datelor, necesitatea și proporționalitatea cu privire la scopuri etc. În plus, controale diferite utilizate pentru a îndeplini același obiectiv privind viața privată pot necesita rubrici diferite pentru a fi puse în evidență.

În acest mod, în concluzie, riscurile privind protecția datelor sunt gestionate (evaluate și abordate) și acțiunile întreprinse pentru îndeplinirea obiectivelor privind viața privată sunt descrise (și pot fi controlate).

De asemenea, este posibilă o abordare mixtă prin studierea, în egală măsură, a riscurilor de a nu îndeplini anumite obiective privind viața privată (nu numai securitatea, ci și, de exemplu, limitarea scopului, necesitatea și proporționalitatea, păstrarea datelor, respectarea drepturilor persoanelor vizate etc.).