GRUPUL DE LUCRU „ARTICOLUL 29” PRIVIND PROTECȚIA DATELOR

1021/00/RO
WP207

Avizul 06/2013 privind reutilizarea datelor deschise și a informațiilor din sectorul public („ISP”)

Adoptat la 5 iunie 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 articolul 29 și articolul 30 alineatul (1) litera (a) și alineatul (3) din această directivă,

având în vedere regulamentul său de procedură,

ADOPTĂ URMĂTORUL AVIZ:

I. Introducere

1.1. Modificarea Directivei „ISP"

La 26 iunie 2013, Uniunea Europeană a adoptat Directiva 2013/37/UE („Modificarea ISP") a Parlamentului European și a Consiliului de modificare a Directivei 2003/98/CE privind reutilizarea informațiilor din sectorul public („Directiva ISP"). [1]

Obiectivul Directivei ISP constă în facilitarea reutilizării informațiilor din sectorul public, prin armonizarea condițiilor de reutilizare pe întregul teritoriul Uniunii Europene și înlăturarea unor obstacole inutile din calea reutilizării informațiilor pe piața internă.

Textul inițial al Directivei ISP din 2003 a armonizat condițiile de reutilizare, însă nu a cerut organismelor din sectorul public punerea la dispoziție a datelor pentru reutilizare. Punerea datelor la dispoziție în scopul reutilizării a fost, în principiu, opțională: au fost lăsate să decidă statele membre și organismele din sectorul public în cauză. Drept rezultat, multe dintre organismele din sectorul public din Europa au refuzat pur și simplu să permită reutilizarea datelor pe care le dețineau.

În acest context, unul dintre obiectivele politice fundamentale ale Modificării ISP este introducerea principiului potrivit căruia toate informațiile publice (adică informațiile deținute de către sectorul public, accesibile publicului în conformitate cu legile naționale) sunt reutilizabile atât în scop comercial, cât și în scop necomercial. În anumite cazuri, se aplică excepții de la domeniul de aplicare al Directivei ISP modificate, inclusiv pe temeiul protecției datelor.[2]

Astfel, acum Directiva ISP modificată obligă organismele din sectorul public să permită reutilizarea tuturor informațiilor publice deținute. Cu toate acestea, după cum este indicat mai jos, aceasta nu impune organismelor din sectorul public obligația de a dezvălui publicului informațiile cu caracter personal. Aceasta dispune reutilizarea informațiilor numai dacă informațiile sunt deja accesibile publicului în conformitate cu legile naționale și numai în cazul în care reutilizarea nu aduce prejudicii legilor aplicabile privind protecția datelor.

Alte noi dispoziții relevante din Modificarea ISP extind domeniul de aplicare al Directivei ISP la biblioteci (inclusiv bibliotecile universitare), arhive și muzee.

Luând în considerare cele menționate, Directiva ISP modificată are potențialul de a crește în mod considerabil accesibilitatea informațiilor deținute de organismele publice.

1 JO L 175, 27.6.2013, p. 1.

2 Referitor la domeniul de aplicare al directivei ISP modificate și dispozițiile privind protecția datelor, a se vedea secțiunea V de mai jos.

1.2. Reutilizarea ISP și datele cu caracter personal

Inițiativele privind reutilizarea ISP vizează de regulă (i) punerea la dispoziție a unor întregi baze de date (ii) în format electronic standardizat (iii) oricărui solicitant, fără vreo procedură de selecție, (iv) gratuit (sau în schimbul unor onorarii limitate) și (v) în orice scop comercial sau necomercial, fără condiționare (sau potrivit unor condiții nerestrictive, pe bază de licență, după caz)[3].

Acest aspect ar putea aduce beneficii care să ducă la mai multă transparență și la reutilizarea inovativă a informațiilor din sectorul public. Cu toate acestea, accesibilitatea crescută a informațiilor care rezultă de aici nu este lipsită de riscuri.

În vederea minimalizării acestor riscuri, atunci când este vorba de date cu caracter personal, legile privind protecția datelor trebuie să contribuie la ghidarea procesului de selecție referitor la acele date cu caracter personal care pot fi puse la dispoziție pentru reutilizare și la identificarea măsurilor care trebuie luate în vederea protejării datelor cu caracter personal. Trebuie urmată o abordare echilibrată în toate cazurile în care este vorba de protecția vieții private și a datelor cu caracter personal. Pe de o parte, regulile privind protecția datelor cu caracter personal nu trebuie să constituie o barieră nejustificată în fața dezvoltării pieței reutilizării. Pe de altă parte, trebuie respectat dreptul la protecția datelor cu caracter personal și dreptul la viață privată. Este important de subliniat faptul că prin conceptul datelor deschise se pune accentul pe transparența și responsabilitatea organismelor din sectorul public și nu pe transparența cetățenilor individuali.

Când un organism din sectorul public aplică Directiva ISP și legea privind protecția datelor la reutilizarea datelor cu caracter personal, probabil că acest organism va lua una dintre următoarele trei tipuri de decizii:

1. decizia de a nu face disponibile pentru reutilizare informațiile cu caracter personal în temeiul Directivei ISP;
2. decizia de a transforma informațiile cu caracter personal în date anonimizate (de regulă, în date statistice agregate)[4] și de a face disponibile pentru reutilizare numai astfel de date anonimizate;
3. decizia de a face datele personale disponibile în vederea reutilizării (când este necesar, conform unor condiții și garanții adecvate).

II. <u>Obiectivul avizului</u>

2.1. Orientări și bune practici uniforme

Obiectivul acestui aviz este de a contribui la asigurarea unei interpretări uniforme în ceea ce privește cadrul legislativ aplicabil și de a oferi în mod consecvent orientare și exemple de bune practici privind punerea în aplicare a Directivei ISP (modificate) referitor la prelucrarea datelor personale.

Obiectivul acestui aviz nu este de a încerca armonizarea abordărilor naționale cu privire la nivelul de transparență, legislația națională privind accesul la documente și disponibilitatea informației în conformitate cu aceste legi naționale. Cu toate acestea, legislația națională de punere în aplicare cu

[3] De observat că, în temeiul modificării articolului 8 alineatul (1) din Directiva ISP, „condițiile respective (referitoare la licență) nu trebuie să limiteze în mod inutil posibilitățile de reutilizare și nu trebuie utilizate pentru restricționarea concurenței”.

[4] Cu privire la reutilizarea seturilor de date generale și anonimizate extrase din datele cu caracter personal, a se vedea secțiunea VI de mai jos.

privire la Directiva ISP și interpretările Directivei 95/46/CE[5] la nivel național diferă uneori în ceea ce privește reutilizarea ISP, în așa măsură încât se depășește ceea ce este necesar pentru a se ține seama de diversitatea privind regimurile naționale de acces și diferitele niveluri de transparență.

În această privință, recomandările de politică privind viața privată din septembrie 2012, pregătite de către rețeaua tematică LAPSI, arată clar disparitățile inutile dintre statele membre în ceea ce privește modalitatea de transpunere a Directivei ISP cu privire la protecția datelor cu caracter personal.[6] Însăși Directiva ISP avertizează că diferențele legislative și neclaritățile pot deveni mai pronunțate odată cu evoluția societății informaționale, ceea ce a dus deja la o intensificare semnificativă a exploatării transfrontaliere a informației.[7]

Lipsa unei abordări consistente ar putea slăbi poziția persoanelor vizate. De asemenea, aceasta ar putea crea probleme inutile de reglementare pentru afaceri și alte organizații care operează peste hotare, reprezentând astfel un obstacol în fața dezvoltării unei piețe europene comune pentru reutilizarea informațiilor. Pe de o parte, persoanele vizate trebuie asigurate că datele lor vor fi protejate în mod consecvent, chiar dacă sunt transferate în alt stat membru în vederea reutilizării. Pe de altă parte, trebuie evitate complexitatea și fragmentarea fără justificare pentru a permite libera circulație a datelor cu caracter personal în Europa, un alt obiectiv fundamental al Directivei 95/46/CE.

2.2. Necesitatea actualizării avizului 7/2003

Modificarea ISP vine la un deceniu după adoptarea Directivei ISP în 2003. La momentul respectiv, GL29 a adoptat un aviz referitor la problemele care țin de protecția datelor în legătură cu ISP („Avizul 7/2003”)[8]. În timp ce principiile fundamentale ale avizului 7/2003 rămân satisfăcătoare, progresul tehnologic și evoluțiile de altă natură din domeniul ISP și al protecției datelor, inclusiv propunerile legislative din ambele domenii, justifică eforturile curente de actualizare și completare a avizului din 2003.

În continuare, avizul poate lua în considerare acum alte eforturi recente și actuale de a oferi orientări suplimentare, mai precis:

- Avizul Autorității Europene pentru Protecția Datelor („AEPD”) referitor la pachetul de măsuri privind datele deschise al Comisiei Europene din 18 aprilie 2012[9],
- Avizul 3/2013 emis de GL29 privind limitarea scopului;[10]

---

[5] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24.10.1995 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).

[6] LAPSI este o rețea tematică europeană privind aspectele juridice referitoare la informațiile din sectorul public, finanțată de către Comisia Europeană, a se vedea http://www.lapsi-project.eu/. Recomandarea de politici este disponibilă la următoarea adresă: http://www.lapsi-project.eu/lapsifiles/lapsi_privacy_policy.pdf..

[7] A se vedea considerentul 7.

[8] A se vedea Avizul 7/2003 al grupului de lucru „Articolul 29” pentru protecția datelor privind reutilizarea informațiilor din sectorul public și protecția datelor cu caracter personal – Căutarea echilibrului – adoptat la 12 decembrie 2003 (WP83). A se vedea, de asemenea, două avize conexe mai recente ale GL29: avizul 3/1999 privind informațiile din sectorul public și protecția datelor personale, adoptat la 3 mai 1999 (WP20), precum și avizul 5/2001 privind raportul special al Ombudsmanului European, adoptat la 17 mai 2001.

[9] Avizul Autorității Europene pentru Protecția Datelor referitor la „pachetul de măsuri privind datele deschise” al Comisiei Europene, care include o propunere de directivă de modificare a Directivei 2003/98/CE privind reutilizarea informațiilor din sectorul public (ISP), o Comunicare privind datele deschise și Decizia 2011/833/UE a Comisiei privind reutilizarea documentelor. Acesta este disponibil aici: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:335:0008:01:RO:HTML .

[10] Avizul Grupului de lucru articolul 29 pentru protecția datelor din 3/2013 privind limitarea scopului adoptat la 2 aprilie 2013 (WP 203).

- lucrările în desfășurare ale sub-grupului tehnologie din cadrul GL29 referitoare la tehnicile de anonimizare[11];
- lucrările din unele state membre privind anonimizarea și evaluarea riscurilor[12] și
- jurisprudența și practicile existente în unele state membre, referitoare la echilibrul dintre reutilizarea și protecția datelor cu caracter personal.[13]

III. Conținutul și structura avizului

Avizul 7/2003 s-a bazat pe principiul limitării scopului[14], dar a abordat și alte subiecte, cum ar fi temeiurile legale pentru dezvăluirea publică și reutilizarea ISP, protecția specială acordată datelor sensibile, transferurile către țările terțe, calitatea datelor și drepturile persoanelor vizate. Aceste observații sunt încă valabile. Luând în considerare lucrările deja efectuate, prezentul aviz actualizează și completează doar concluziile avizului 7/2003, ținând cont, atunci când este necesar, de noile evoluții legislative și tehnologice.

În secțiunea IV se clarifică faptul că obligația de a reutiliza datele în conformitate cu Directiva ISP modificată nu prejudiciază cerințele privind protecția datelor și se subliniază importanța „protecției datelor începând cu momentul conceperii și a protecției implicite a datelor" și a „evaluării impactului protecției datelor" pentru a contribui la asigurarea faptului că problemele legate de protecția datelor sunt soluționate înainte ca datele cu caracter personal să fie făcute disponibile pentru reutilizare.

În secțiunea V se oferă orientări, prin exemple ilustrative, cu privire la tipurile de date cu caracter personal care ar putea intra în domeniul de aplicare a Directivei ISP.

Secțiunea VI se bazează pe situațiile care sunt în prezent cel mai frecvent întâlnite în inițiativele de reutilizare ISP: în cazul în care datele statistice agregate derivate din date cu caracter personal sunt făcute disponibile sub formă agregată și anonimizată. Printre exemple se pot menționa datele statistice agregate privind rata criminalității, cheltuielile bugetare sau privind nivelul de pregătire al elevilor din diferite regiuni geografice sau instituții de învățământ. Deoarece acesta este scenariul cel mai frecvent de reutilizare a informațiilor din sectorul public care conțin date cu caracter personal, o parte semnificativă a prezentului aviz va fi dedicată acestui scenariu. Problema fundamentală legată de protecția datelor în acest caz este asigurarea unei agregări și anonimizări eficiente, precum și reducerea riscului de reidentificare a oricăror date cu caracter personal din seturile de date agregate.

În secțiunea VII sunt discutate – mai puțin detaliat – situațiile în care datele cu caracter personal sunt făcute publice și ar putea fi puse la dispoziție în scopul reutilizării. Deși în prezent acesta nu este un scenariu tipic pentru inițiativele de reutilizare a ISP, este important să se ia în considerare faptul că organismele din sectorul public pun din ce în ce mai frecvent la dispoziția publicului date cu caracter personal, adesea prin intermediul internetului. Aici este vorba despre date cu caracter personal direct identificabile, cum ar fi, de exemplu, informații din cartea funciară despre proprietarul unui anumit imobil, declarații privind dobânzile sau salariile anumitor funcționari de stat sau cheltuielile parlamentarilor. Întrebarea este în ce măsură, pentru ce scopuri, în ce condiții și în schimbul căror garanții pot fi puse la dispoziție aceste date pentru reutilizare. De asemenea, este important de clarificat dacă aceste date intră în domeniul de aplicare a Directivei ISP.

[11] Avizul privind acest subiect este anticipat pentru a doua jumătate a anului 2013.

[12] A se vedea, de exemplu, codul de bune practici privind anonimizarea „Anonimizarea: cod de bune practici pentru gestionarea riscurilor legate de protecția datelor" publicat de către biroul comisarului european pentru informații din Marea Britanie, în noiembrie 2012, precum și Ghidul pentru analiza de risc publicat de către autoritatea pentru protecția datelor din Franța în iunie 2012.

[13] A se vedea, de exemplu, Recomandarea de politică LAPSI din septembrie 2012 (pp. 4-14).

[14] A se vedea articolul 6 alineatul (1) litera (b) din Directiva 95/46/CE.

În acest context, este important de evidențiat faptul că orice informații legate de persoane fizice identificate sau identificabile, fie că sunt disponibile public sau nu, constituie date cu caracter personal. În consecință, accesarea și reutilizarea acelor date cu caracter personal care au fost făcute publice (de exemplu prin publicarea datelor pe internet) se supune în continuare legislației aplicabile privind protecția datelor.

Alte câteva scenarii specifice, cum ar fi cazul datelor de cercetare și situația arhivelor istorice – care în prezent intră în domeniul de aplicare al Directivei ISP – vor fi abordate pe scurt în cadrul secțiunilor VIII și IX.

În secțiunea X este prezentată problema acordării de licență ISP și nevoia de a integra clauza protecției datelor în textul licențelor, acolo unde este relevant.

În fine, secțiunea XI oferă un set de concluzii și recomandări.

IV. Nu toate datele cu caracter personal „accesibile publicului" trebuie puse la dispoziție pentru reutilizare

4.1. Obligația de a reutiliza datele conform Directivei ISP nu aduce prejudicii cerințelor legate de protecția acestora

În 2003, la momentul adoptării sale, Directiva ISP nu impunea organismelor din sectorul public obligația de a permite reutilizarea ISP. Decizia de a autoriza sau nu reutilizarea era lăsată la latitudinea statelor membre sau a organismului din sectorul public vizat (conform cadrelor de reglementare naționale referitoare la transparență și acces). Avizul 7/2003 a fost adoptat ținând cont de această „lipsă de obligativitate". Secțiunea 2 punctul (cc) din avizul 7/2003 prevede că „Este important de subliniat faptul că directiva privind reutilizarea nu poate fi invocată ca fiind o obligație juridică ce trebuie respectată, deoarece această directivă nu creează obligația de a dezvălui informații cu caracter personal".

Odată cu Modificarea ISP analiza a devenit mai complexă, însă concluziile au rămas aceleași.

Articolul 3 alineatul (1) din Directiva ISP modificată prevede că „Sub rezerva dispozițiilor alineatului (2), statele membre se asigură că documentele care intră sub incidența prezentei directive în conformitate cu articolul 1 sunt reutilizabile în scopuri comerciale sau necomerciale în conformitate cu condițiile stabilite în capitolele III și IV." Reutilizarea trebuie permisă, cu excepția cazului în care aceasta poate fi refuzată din motivele prevăzute la articolul 1 (motive legate de regimuri naționale de acces și, în mod specific, din motive de protecție a datelor cu caracter personal).

În același timp, considerentul 21 al Directivei ISP menționează că „Prezenta directivă trebuie transpusă în practică și aplicată cu respectarea deplină a principiilor privind protecția datelor personale". În plus, articolul 1 alineatul (4) prevede că Directiva ISP „lasă intact și nu aduce atingere în nici un fel nivelului de protecție al persoanelor prevăzut în legislația comunitară sau internă privind prelucrarea datelor personale".

Aceste prevederi, luate și interpretate împreună, înseamnă că „principiul reutilizării" nu este automat atunci când este vorba de dreptul de protecție a datelor cu caracter personal și nu aduce atingere dispozițiilor legale aplicabile referitor la protecția datelor. Atunci când documentele existente aflate în posesia organismelor din sectorul public conțin date cu caracter personal, reutilizarea acestora

intră sub incidența Directivei 95/46/CE și, astfel, se supune legislației aplicabile privind protecția datelor.

În consecință, dacă este vorba de reutilizarea unor date cu caracter personal, atunci organismul din sectorul public nu poate invoca necesitatea de a respecta Directiva ISP ca temei legal pentru punerea la dispoziție a datelor pentru reutilizare.[15]

4.2. Importanța evaluărilor de impact privind protecția datelor înainte de punerea la dispoziție a datelor pentru reutilizare

Luând în considerare riscul potențial al reutilizării ISP și în special faptul că, odată făcute publice în scopul reutilizării, folosirea acestor date cu caracter personal va fi foarte greu de controlat în mod eficient, GL29 subliniază necesitatea aderării la principiul „protecției datelor începând cu momentul conceperii și al protecției implicite a datelor", precum și necesitatea de a se asigura că problemele legate de protecția datelor sunt soluționate într-o fază timpurie. În special, GL29 recomandă cu tărie organismelor din sectorul public efectuarea unui studiu de impact privind protecția datelor înainte de punerea la dispoziție pentru reutilizare a datelor cu caracter personal. Statele membre trebuie aibă în vedere să facă obligatorie efectuarea unui astfel de studiu de impact prin legislația națională sau să promoveze studiul de impact drept cea mai bună practică. În orice caz, chiar dacă acest lucru nu este prevăzut în legislațiile naționale, înainte de a face publice informațiile și înainte de a decide dacă acestea vor fi disponibile în scopul reutilizării, organismele din sectorul public trebuie să efectueze studii aprofundate pentru a decide dacă datele cu caracter personal pot fi făcute disponibile în scopul reutilizării și, dacă da, în ce condiții și în schimbul căror garanții este permis acest lucru.

Evaluarea trebuie, printre altele, să stabilească o bază juridică pentru dezvăluirea datelor (și un potențial temei legal pentru reutilizarea acestora), să evalueze principiile limitării scopului, al proporționalității și al minimizării datelor și să ia în considerare protecția specială necesară în cazul datelor sensibile. În cursul efectuării acestui studiu trebuie luat în considerare cu mare atenție impactul asupra persoanelor vizate.

Acest studiu trebuie să contribuie la luarea unei decizii referitoare la acele date cu caracter personal care pot fi puse la dispoziție în scopul reutilizării, dacă este cazul, și în schimbul căror garanții.[16] Este de subliniat faptul că Regulamentul privind protecția datelor care a fost propus [17] încurajează și, în unele cazuri, impune efectuarea unor studii de impact privind protecția datelor, ca instrument menit să contribuie la asigurarea unei atitudini responsabile din partea operatorilor de date.[18]

---

[15] De asemenea, GL29 vrea să clarifice faptul că, din perspectiva reutilizatorului directiva ISP nu constituie temei legal pentru prelucrarea datelor. (Pentru temeiurile legale a se vedea Avizul 7/2003, precum și secțiunea 7.5 de mai jos.)

[16] În cazul în care se decide că datele cu caracter personal nu vor fi puse la dispoziție pentru reutilizare ca atare, ci mai degrabă vor fi puse la dispoziție sub forma unor seturi de date anonimizate, ar trebui efectuat un studiu de risc privind reidentificarea. A se vedea secțiunea VI referitoare la studiile de risc privind reidentificarea.

[17] La 25 ianuarie 2012, Comisia a adoptat un pachet legislativ 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].

[18] Pentru indicații suplimentare privind efectuarea unui studiu de impact privind protecția datelor a se vedea, de exemplu, site-ul proiectului PIAF (un cadru pentru studii de impact privind protecția datelor și dreptul la o viață privată) de la adresa http://www.piafproject.eu/Index.html. PIAF este un proiect co-finanțat de către Comisia Europeană al cărui obiectiv este încurajarea UE și a statelor sale membre să adopte o politică progresivă privind studiile de impact privind viața privată, ca metodă de abordare a nevoilor și problemelor legate de viața privată și de prelucrarea datelor cu caracter personal. Unele state membre oferă și ele orientări. A se vedea, de exemplu, manualul referitor la studiile de impact privind viața privată, publicat de către comisarul european pentru informații din Regatul Unit, la adresa http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment; orientările privind analiza de risc publicate de către autoritatea pentru protecția datelor din Franța, menționate deja la

Atunci când este posibil, analiza care precede decizia privind reutilizarea trebuie bazată pe o dezbatere documentată și pe reprezentarea diverselor părți interesate, inclusiv a operatorului de date care dorește să le publice, dar și a celor care vor să aibă datele și, deci, a celor care pot oferi contextul pentru dezbatere, precum și a reprezentanților persoanelor fizice ale căror date cu caracter personal sunt vizate (de exemplu, organizațiile de protecție a consumatorilor, organizațiile pentru drepturile pacienților, uniunile profesorilor). În cazul în care rezultatul este neclar, autoritatea competentă pentru protecția datelor și autoritățile naționale responsabile pentru libertatea informației ar putea oferi clarificările necesare.

De asemenea, statele membre trebuie să ia în considerare crearea unor rețele de cunoaștere/centre de excelență cărora să le ofere sprijin, astfel contribuind la schimbul de bune practici legate de anonimizare și date deschise. Acestea ar putea fi deosebit de importante pentru organismele mai mici din sectorul public, cărora le lipsește expertiza necesară pentru efectuarea anonimizării, a studiilor de impact privind protecția datelor și pentru a evalua și testa riscurile de reidentificare.[19]

În fine, studiul de impact este recomandat cu tărie și înainte de punerea în aplicare a noilor legi care impun dezvăluirea publică a datelor cu caracter personal.

V. Obiectivul Directivei ISP: excepții din motive de protecție a datelor cu caracter personal

Această secțiune oferă indicații privind obiectivul Directivei ISP și, în special, privind excepțiile din motive de protecție a datelor cu caracter personal.

5.1. Aplicabilitatea cadrului general privind protecția datelor în cazul reutilizării ISP

Considerentul 21 al Directivei ISP prevede că „prezenta directivă trebuie transpusă în practică și aplicată cu respectarea deplină a principiilor privind protecția datelor personale”. În plus, articolul 1 alineatul (4) prevede că Directiva ISP „lasă intact și nu aduce atingere în niciun fel nivelului de protecție al persoanelor prevăzut în legislația comunitară sau internă privind prelucrarea datelor personale”.

5.2. Excepții din motive de protecție a datelor cu caracter personal

Directiva ISP prevede că „prezenta directivă nu se aplică: „… documentelor la care accesul este exclus în temeiul regimurilor de acces din statele membre…”[20]

În plus, Directiva ISP modificată oferă excepții și din motive de protecție a datelor cu caracter personal. Articolul 1 alineatul (2) litera (cc) se referă la următoarele trei situații care nu fac obiectul Directivei ISP:

---

nota 12, și orientările oferite de către comisarul european pentru informații din Slovenia, în special cele referitoare la „Studiile de impact privind viața privată în proiectele de e-guvenare”, disponibile la adresele: https://webmail.europarl.europa.eu/exchweb/bin/redir.asp?URL=https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIASmernice__ENG_Lektorirano_10._6._2011.pdf

[19] Spre exemplu, în Regatul Unit, un consorțiu condus de Universitatea din Manchester, împreună cu Universitatea din Southhampton, Biroul național de statistică și noul Institut guvernamental pentru date deschise (ODI), operează Rețeaua de anonimizare din Regatul Unit (UKAN) pentru a contribui la schimbul de bune practici legate de anonimizare în sectorul public și privat. Rețeaua include un site internet, care poate fi accesat la următoarea adresă: https://webmail.europarl.europa.eu/exchweb/bin/redir.asp?URL=http://www.ukanon.net, studii de caz, ateliere și seminare.

[20] A se vedea Directiva ISP, Articolul 1(2)(c).

- documentele la care accesul este exclus în temeiul regimurilor de acces din motive de protecție a datelor cu caracter personal;
- documente la care accesul este limitat în temeiul regimurilor de acces din motive de protecție a datelor cu caracter personal, și
- „părților din documente accesibile în temeiul respectivelor regimuri care conțin date cu caracter personal a căror reutilizare a fost definită prin lege ca fiind incompatibilă cu legislația privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal."

5.3. Comentarii generale

GL29 subliniază faptul că, indiferent de „principiul reutilizării" formulat în Modificarea ISP, reutilizarea pentru orice scop comercial sau ne-comercial conform Directivei ISP nu este întotdeauna potrivită în cazurile în care ISP ce urmează a fi reutilizate conțin date cu caracter personal. Deciziile privind reutilizarea datelor cu caracter personal conform Directivei ISP trebuie luate în funcție de fiecare caz în parte și există nevoia de a pune în aplicare măsuri legale, tehnice sau organizatorice suplimentare pentru protecția persoanelor vizate.

Reutilizarea datelor cu caracter personal disponibile publicului este și trebuie limitată prin

- prevederi generale ale legilor aplicabile privind protecția datelor,
- (unde este cazul) constrângeri legale specifice suplimentare, și
- garanții tehnice și organizatorice create pentru protecția datelor cu caracter personal.

5.4. Documente la care accesul este exclus

Această prevedere exclude din domeniul de aplicare a Directivei ISP toate acele documente care sunt excluse conform regimurilor de acces ale statelor membre vizate, din motive de protecție a datelor cu caracter personal.

Spre deosebire de legile pentru protecția datelor, care sunt armonizate în mare măsură prin Directiva 95/46/CE, legile privind accesul la informații diferă în mod semnificativ de la un stat membru al UE la altul. De regulă, regimurile de acces necesită un test de echilibrare prin care se compară interesele protejate de regulile privind viața privată și protecția datelor cu beneficiile deschiderii și transparenței. Luând în considerare divergențele, rezultatul exercițiului de echilibrare poate fi diferit în diferitele state membre ale UE. De exemplu, autoritățile fiscale din unele state membre pot publica anumite părți din declarațiile fiscale ale contribuabililor (în conformitate cu măsurile legale, tehnice și organizatorice pentru reducerea riscului de abuz), în timp ce un alt stat membru ar considera acest tip de informație ca făcând parte din categoria excepțiilor care trebuie, în general, să nu fie divulgate.

Acestea fiind spuse, legislația națională trebuie să respecte articolul 8 din Convenția Europeană a drepturilor omului („CEDO") și articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene („Carta UE"). Acest fapt înseamnă că, în mod similar hotărârilor Curții Europene de Justiție din cauzele *Österreichischer Rundfunk* și *Schecke*[21], trebuie să se analizeze dacă dezvăluirea este necesară și proporțională cu scopul legitim urmărit conform legii.

[21] A se vedea hotărârea CEJ din 20 mai 2003, Rundfunk, cauzele conexate C-465/00, C-138/01 și C-139/01, și hotărârea CEJ 9 noiembrie 2010, Volker und Markus Schecke, cauzele conexate C-92/09 și C-93/09.

În orice caz, odată ce accesul la datele cu caracter personal dintr-un document nu mai este permis conform legilor din statul membru în cauză (inclusiv în cazul în care legislația națională privind transparența și deschiderea nu acoperă accesibilitatea generală a datelor cu caracter personal vizate), acestea nu vor intra nici sub incidența Directivei ISP.

Pentru a asigura securitatea și transparența juridică privind persoanele vizate, cea mai bună practică este abordarea proactivă, atunci când este posibil, și definirea prealabilă a datelor cu caracter personal care pot fi făcute publice. Astfel, persoanele vizate pot fi informate la momentul colectării acestora, dacă orice parte a datelor cu caracter personal oferite de aceștia sau care vor fi prelucrate ulterior, în cursul procedurilor administrative, va deveni disponibilă publicului ca urmare a legilor cu privire la libertatea informației.

5.5. Documente la care accesul este <u>limitat</u>

Această prevedere exclude din domeniul de aplicare a Directivei ISP toate acele documente la care accesul este limitat din motive de protecție a datelor cu caracter personal. Din nou, regimurile de acces din diferitele state membre pot varia în ceea ce privește datele cu acces limitat și tipurile de restricții existente. Iată câteva exemple:

- colecții ale arhivelor naționale care conțin date cu caracter personal accesibile numai în conformitate cu condiții specifice de acces și garanții suplimentare (a se vedea secțiunea IX mai jos);
- colecții de date de cercetare care conțin date cu caracter personal accesibile numai în conformitate cu condiții specifice de acces și garanții suplimentare (a se vedea secțiunea VIII mai jos);
- anumite informații conținute în registrele publice, dosare legale, sau alte documente administrative care conțin date cu caracter personal care pot fi accesate numai de persoane sau organizații care demonstrează un interes legitim, sau numai în conformitate cu condiții specifice de acces și garanții suplimentare.

5.6. Părți ale unor documente sunt <u>accesibile</u>, însă reutilizarea acestora este incompatibilă

Conform acestei prevederi, nu intră în domeniul de aplicare a Directivei ISP următoarele:

- părți ale documentelor
- care sunt accesibile conform regimurilor naționale de acces
- și care conțin date cu caracter personal „a căror reutilizare a fost definită prin lege ca fiind incompatibilă cu legislația privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal".

Această prevedere confirmă faptul că, chiar și în cazurile în care anumite documente ce conțin date cu caracter personal sunt pe deplin accesibile, reutilizarea acestora ar putea fi, totuși, restricționată din motive de protecție a datelor.

GL29 subliniază faptul că această prevedere a Directivei ISP trebuie interpretată în conformitate cu articolul 1 alineatul (4) al Directivei ISP conform căruia „prezenta directivă lasă intact și nu aduce atingere în nici un fel nivelului de protecție al persoanelor privind prelucrarea datelor personale".

GL29 ar aprecia ca fiind o bună practică adoptarea unor prevederi legale specifice în cadrul legislației naționale, care să descrie clar (i) care date sunt puse la dispoziția publicului, (ii) pentru ce scopuri, și care (iii) să specifice, după caz, în ce măsură și în ce condiții aceste date pot fi puse la

dispoziție pentru reutilizare. Cu toate acestea, atunci când nu există astfel de prevederi, acest fapt nu înseamnă că datele cu caracter personal disponibile public pot fi reutilizate oricând, în temeiul Directivei ISP.

În schimb, în aceste cazuri legea privind protecția datelor (aplicată împreună cu orice alte legi aplicabile, cum ar fi legislația privind accesul la documente) este cea care determină dacă într-un caz specific datele cu caracter personal pot fi puse la dispoziție, și dacă da, care sunt garanțiile suplimentare ce trebuie oferite. Dacă rezultatul acestei evaluări este pozitiv, atunci reutilizarea este autorizată în conformitate cu garanțiile specifice protecției datelor și cu alte condiții prevăzute de Directiva ISP (atâta timp cât nu aduc prejudicii legislației privind protecția datelor). Dacă rezultatul evaluării este negativ, atunci reutilizarea nu intră sub incidența Directivei ISP.

Exemplele următoare ilustrează când se aplică excepțiile de la Directiva ISP. În primul exemplu restricțiile privind reutilizarea sunt specificate în mod clar prin lege.

- Legile fiscale dintr-un anumit stat membru pot prevedea ca declarațiile fiscale ale tuturor rezidenților țării să fie făcute disponibile, prin cerere, oricărui alt rezident pentru a fi revizuite la sediul autorității fiscale, fără să fie nevoie să se demonstreze un interes legitim. De asemenea, legea specifică în mod clar că datele nu pot fi prelucrate ulterior, de exemplu, publicate pe internet, combinate cu alte date sau redactate. Un ONG solicită accesul și dreptul de a reutiliza baza de date conținând declarațiile fiscale pentru a le publica pe pagina sa de internet. În acest caz datele fiscale nu intră sub incidența Directivei ISP și organismul din sectorul public nu este obligat să facă seturile de date disponibile în scopul reutilizării conform Directivei ISP.

Însă în multe alte cazuri restricțiile legale sunt probabil mai puțin clar exprimate și mai puțin categorice în ceea ce privește reutilizarea datelor. De regulă, în cazul diverselor registre civile, comerciale și al registrelor de populație, precum și al altor baze de date, este permisă consultarea datelor cu caracter personal de către public din ce în ce mai des în formă digitală, pe internet. Accesibilitatea este deseori dictată de anumite garanții speciale, inclusiv restricții de ordin tehnic privind capacitatea de căutare și descărcările în masă. De asemenea, se poate solicita utilizatorilor să își dea acordul privind termenii și condițiile de acces.

- Legile unui stat membru pot prevedea ca numele acelor rezidenți care au avut arierate fiscale peste o anumită limită pentru o perioadă de timp îndelungată să fie publicate pe o pagină de internet special creată în acest scop, pentru o perioadă scurtă, cu condiția unor garanții tehnice suplimentare, inclusiv limitări privind descărcările în masă și capacitățile de căutare. Scopul acestei publicări este de a încuraja plata taxelor pe venit în timp util și de a servi drept sancționare suplimentară (a reputației) pentru cei care nu plătesc în timp util. Un consorțiu bancar cere permisiunea de a accesa datele în scopul reutilizării pentru a le introduce în sistemul de raportare a creditelor.
- Legile specifice din sectorul asistenței medicale dintr-un stat membru ar putea permite pacienților, ținând cont de anumite garanții, să verifice pe o pagină de internet special creată în acest scop dacă unui anumit doctor sau cadru medical i-a fost interzis să practice medicina. Se aplică garanțiile tehnice, inclusiv limitările privind descărcările în masă și capacitățile de căutare. O organizație pentru drepturile pacienților solicită accesul în vederea reutilizării pentru a crea o pagină de internet multilingvă și cu o interfață mai prietenoasă pentru a accesa aceleași date.
- Legile specifice unui stat membru ar putea impune publicarea numelor celor care fac donații unor partide politice peste o anumită limită. Informațiile care pot dezvălui opiniile politice ale

donatorului sunt publicate pe o pagină de internet special creată în acest scop. Se aplică garanțiile tehnice, inclusiv limitările privind descărcările în masă și capacitățile de căutare. Un grup de activiști solicită accesul la date în masă în vederea reutilizării în temeiul Directivei ISP pentru a crea o nouă pagină de internet cu caracteristici suplimentare și cu capacități de căutare mai bune.

- Numele și adresa unui anumit proprietar de imobil sunt făcute publice în cartea funciară a unui stat membru, însă căutarea în baza de date accesibilă publicului este limitată, astfel încât este posibilă numai căutarea unui anumit imobil și nu a unor persoane. Descărcările în masă sunt, de asemenea, limitate. O societate comercială solicită accesul la date în masă în vederea reutilizării pentru a crea o pagină de internet cu o interfață mai prietenoasă la un preț mai competitiv.
- Registrele comerțului dintr-un stat membru permit accesul public la o gamă largă de date cu caracter personal, inclusiv numele, adresele și specimenele de semnătură ale directorilor și informații privind forma de proprietate a unor diferite tipuri de societăți. Există anumite restricții cu privire la capacitățile de căutare și limitări privind numărul de fișiere care pot fi descărcate. Informațiile sunt disponibile prin intermediul unei pagini de internet create special în acest scop și contra cost. O societate comercială solicită accesul la date în masă în vederea reutilizării pentru a crea o pagină de internet care combină informațiile din câteva tipuri diferite de registre și pentru a oferi informații îmbunătățite la un preț competitiv.

În toate aceste cazuri, organismul vizat din sectorul public trebuie să efectueze un studiu de impact privind protecția datelor pentru a decide dacă datele pot fi făcute disponibile în vederea reutilizării în temeiul Directivei ISP, și în cazul unui răspuns pozitiv, dacă sunt necesare anumite condiții și garanții specifice în conformitate cu legea privind protecția datelor. „Principiul reutilizării" nu este automat și nu poate prevala asupra dispozițiilor aplicabile din legislația privind protecția datelor.

O asemenea evaluare atentă este importantă mai ales deoarece, conform Directivei ISP, organismul din sectorul public nu trebuie, în principiu, să țină cont de cine anume solicită accesul în vederea reutilizării datelor. În temeiul articolului 10 (Nediscriminarea), „nicio condiție aplicabilă în vederea reutilizării documentelor nu este discriminatorie pentru categorii comparabile de reutilizare. În plus, în temeiul articolului 11 (Interzicerea acordurilor de exclusivitate) „Reutilizarea documentelor este deschisă tuturor potențialilor actori de pe piață [….].Contractele sau alte acorduri încheiate între organismele din sectorul public care dețin documentele și părți terțe nu oferă drepturi exclusive."

În consecință, atunci când se decide autorizarea reutilizării, organismele din sectorul public trebuie să ia în considerare compatibilitatea permisiunii de reutilizare conform unei licențe deschise nu doar cu solicitantul, ci cu oricine ar solicita aceste date. Astfel, este nevoie de un nivel ridicat de încredere că nici unul dintre potențialii reutilizatori nu vor putea abuza de datele cu caracter personal făcute publice.

Directiva ISP nu exclude autorizarea prelucrării numai pentru anumite scopuri specifice, conform unor termene și condiții. Problema cu care se confruntă organismul din sectorul public este dacă reutilizarea de către orice „potențial actor de pe piață" în aceste scopuri este compatibilă cu scopurile specificate de către organismul vizat din sectorul public. Potențiala reutilizare de către instituțiile financiare, de pildă, a informațiilor legate de plata taxelor în vederea raportărilor de credit este relevantă, deoarece aceste instituții rămân potențiali reutilizatori conform criteriului „orice persoană". În consecință, pentru a soluționa problemele legate de protecția datelor, în special, pentru a se asigura că este respectat principiul limitării scopului, trebuie să i se permită organismului din sectorul public (sau legiuitorului) să limiteze, acolo unde este cazul, scopurile reutilizării.

VI. Reutilizarea seturilor de date agregate și anonimizate derivate din date cu caracter personal

6.1. Care sunt beneficiile agregării și anonimizării ISP în vederea reutilizării?

Până în prezent, inițiativele de reutilizare ale ISP lansate de către organismele din sectorul public prin „portalurile de date deschise" sau alte platforme au avut, în general, scopul de a face disponibile în vederea reutilizării date agregate și anonimizate, și nu date cu caracter personal ca atare. Această abordare este, în mod cert, mai sigură și ar trebui încurajată.

În principiu, legile privind protecția datelor nu permit dezvăluirea publică de către organismele din sectorul public a datelor colectate în alt scop, de regulă în scop administrativ.[22]. Astfel, în aceste cazuri, reutilizarea datelor în cadrul unor inițiative de reutilizare a ISP nu este nici ea posibilă. De regulă sunt și ar trebui– în principiu – făcute publice în vederea reutilizării datelor statistice derivate din date cu caracter personal și nu datele cu caracter personal. Aceasta este soluția cea mai eficientă în vederea reducerii riscului de a dezvălui în mod necorespunzător datele cu caracter personal. Aceste seturi de date agregate și anonimizate nu trebuie să permită reidentificarea persoanelor și, deci, nu trebuie să conțină date cu caracter personal.

Este dificil să se decidă care este nivelul de agregare potrivit și ce tehnici de anonimizare specifice trebuie utilizate. Dacă agregarea și anonimizarea nu sunt realizate în mod eficient, acest fapt aduce după sine riscul de reidentificare a persoanelor vizate din aceste seturi de date. În consecință, legea privind protecția datelor are un rol important în determinarea pragului de „siguranță" pentru comunicarea datelor anonimizate și agregate în cadrul unei inițiative ISP.

Directiva 95/46/CE stabilește un prag înalt pentru anonimizare

Atunci când este folosit în prezentul document, termenul „anonimizare" se referă la datele care nu mai pot fi considerate date cu caracter personal conform articolului 2 litera (a) din Directiva 95/46/CE. Articolul 2 litera (a) definește „datele cu caracter personal" ca fiind orice informații referitoare la o persoană fizică identificată sau identificabilă („persoana vizată"). O persoană identificabilă este „o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale".[23]

Considerentul 26 din Directiva 95/46/CE este, de asemenea, relevant și prevede că „pentru a determina dacă o persoană este identificabilă este oportun să se ia în considerare toate mijloacele care pot fi utilizate în mod rezonabil fie de operator, fie de orice altă persoană pentru a identifica persoana vizată".

---

[22] Desigur, atunci când este cazul, legislația privind libertatea informației poate solicita dezvăluirea datelor cu caracter personal, iar interesul pentru transparența și disponibilitatea informațiilor în anumite situații poate prevala asupra problemelor legate de protecția datelor și dreptul la viața privată. Acesta este un domeniu care evoluează și care ar putea aduce schimbări pe viitor.

[23] În comunicatul din 27 februarie 2013 privind „discuțiile curente legate de pachetul de reforme privind protecția datelor", GL29 a subliniat faptul că „o persoană fizică poate fi considerată identificabilă atunci când, în cadrul unui grup de persoane, acesta/aceasta se distinge de ceilalți membri ai grupului și, drept consecință, poate fi tratată în mod diferit. Aceasta înseamnă că noțiunea identificabilității implică o referire la persoană". De asemenea, comunicatul clarifică faptul că „numerele de identificare, datele legate de locație, adresele IP, identificatorii online și alți factori specifici referitori la o persoană ar trebui considerate date cu caracter personal.

Trebuie subliniat faptul că aceste prevederi stabilesc un prag înalt, precum se va discuta mai departe în cadrul prezentului aviz. Dacă datele nu pot fi anonimizate în așa măsură încât să respecte acest prag, atunci se aplică în continuare legea privind protecția datelor. Aceasta înseamnă, printre altele, că dacă pragul nu este atins, punerea la dispoziția publicului (și orice altă utilizare ulterioară) a informațiilor trebuie să fie „compatibilă" cu scopul inițial pentru care datele au fost colectate, conform articolului 6 alineatul (1) litera (b) din Directiva 95/46/CE. În plus, trebuie să existe un temei legal pentru prelucrarea datelor conform articolului 7 literele (a) - (f) din Directiva 95/46/CE (spre exemplu, consimțământul sau nevoia de a respecta prevederile legale). În schimb, dacă datele au fost făcute anonime în sensul articolului 2 litera (a) și al considerentului 26 din Directiva 95/46/CE, atunci regulile privind protecția datelor nu se mai aplică, iar reutilizatorii pot reutiliza datele fără a ține cont de aceste restricții.

Din nou, trebuie subliniat faptul că „datele anonimizate" se referă, potrivit sensului din prezentul aviz, la datele care nu mai sunt considerate a avea un caracter personal. Datele anonimizate trebuie diferențiate în mod special de datele care au fost manipulate prin diverse tehnici de reducere a riscului de reidentificare a persoanelor vizate, dar care nu au atins pragul prevăzut de articolul 2 litera (a) și considerentul 26 din Directiva 95/46/CE.[24] În multe cazuri aceste tehnici sunt potrivite numai pentru o dezvăluire limitată în vederea reutilizării datelor de către persoane terțe verificate, dar nu pot fi făcute publice pe deplin și reutilizate prin licență deschisă.

De asemenea, este important de subliniat faptul că, odată făcute publice în vederea reutilizării, nu se va putea controla cine are acces la aceste date. Va crește în mod semnificativ probabilitatea ca „oricare alte persoane" să aibă mijloace de reidentificare a persoanelor vizate și să le utilizeze în acest scop. În consecință, indiferent de interpretările date considerentului 26 în alte contexte, atunci când este vorba de punerea datelor la dispoziție în vederea reutilizării în temeiul Directivei ISP, GL29 dorește să fie cât se poate de clar înțeles faptul că trebuie acordată mare atenție ca seturile de date ce vor fi dezvăluite să nu conțină date care pot fi reidentificate prin metode care, probabil, pot fi folosite de orice persoane, inclusiv de către potențialii reutilizatori, dar și de alte părți interesate să obțină datele, inclusiv de autoritățile de aplicare a legii.

Alte clarificări privind anonimizarea și conceptul de date cu caracter personal

Pentru mai multe clarificări privind anonimizarea și conceptual de date cu caracter personal, a se vedea Avizul 4/2007 al GL29 privind conceptul de date cu caracter personal adoptat la 20 iunie 2007 (GL 136). Probabil că GL29 va oferi clarificări ulterioare în ceea ce privește tehnicile de anonimizare într-un al doilea document separat, în a doua jumătate a anului 2013.

6.2. Care sunt provocările și limitările legate de anonimizare în cazul reutilizării ISP?

Anonimizarea este din ce în ce mai dificil de realizat odată cu evoluția tehnologiei computerizate moderne și disponibilitatea ubicuă a informației. Reidentificarea persoanelor este un pericol din ce în ce mai comun și mai prezent.[25] În practică, există o zonă gri foarte semnificativă, în care operatorii

[24] Comunicatul din 27 februarie 2013 subliniază faptul că „atunci când este posibilă regăsirea sau identificarea (indirectă) a unei persoane prin alte metode, normele privind protecția datelor continuă să fie aplicate."

[25] A se vedea, de exemplu, „Un guvern transparent, nu cetățeni transparenți", raport pregătit pentru biroul cabinetului Regatului Unit de către Kieron O'Hara de la Universitatea din Southampton în 2011, în care autorul a avertizat cu privire la posibilitatea de a identifica persoanele fizice din date anonimizate folosind, printre altele, „identificarea mozaicală" și spunând că nu există soluții tehnice complete pentru problema de-anonimizării. Disponibil la adresa: http://www.cabinetoffice.gov.uk/sites/default/files/resources/transparency-and-privacy-review-annex-b.pdf A se vedea, de asemenea, „Promisiuni nerespectate în ceea ce privește viața privată: răspuns la eșecul surprinzător de a

de date ar putea crede că un anumit set de date este anonimizat, însă o parte terță ar putea totuși identifica cel puțin unele dintre persoane pe baza datelor, spre exemplu prin folosirea unor alte date disponibile public sau a altor informații pe care le deține.

Un factor de risc major îl reprezintă numărul crescând de date online și offline, atât disponibile public cât și concentrate în mâinile organizațiilor comerciale, care apoi pot fi folosite în scopul profilării persoanelor pentru publicitate comportamentală și pentru o gamă din ce în ce mai largă de alte scopuri. Atunci când se adaugă realităților din „datele masive" deja disponibile acestor organizații, ISP derivate din datele cu caracter personal cresc probabilitatea ca persoanele să fie identificate sau ca profilurile acestora să fie și mai bine îmbogățite, deseori fără ca persoanele vizate să știe măcar că acest lucru se întâmplă.

6.3. Cine și când trebuie să efectueze agregarea și anonimizarea?

Agregarea și anonimizarea datelor trebuie efectuată din momentul în care acestea sunt disponibile, de către operatorul de date sau o parte terță de încredere care reprezintă operatorul sau mai mulți operatori (și care deține, de asemenea, cunoștințele specializate necesare). Anonimizarea nu trebuie lăsată la latitudinea reutilizatorului, de pildă prin acordarea unei licențe. În continuare, este important să se asigure că organizația terță care probabil va efectua agregarea și anonimizarea nu are un conflict de interese și răspunde fără echivoc de faptul că datele cu caracter personal vor fi folosite numai pentru efectuarea anonimizării și că au fost oferite toate garanțiile necesare în acest scop. Partea terță trebuie, de asemenea, să ofere garanție că datele cu caracter personal din care sunt derivate seturile de date agregate și anonimizate vor fi șterse în momentul în care nu mai sunt necesare pentru acel scop.

6.4. Studii de risc privind reidentificarea

Dacă datele nu pot fi anonimizate în sensul articolului 2 litera (a) și al considerentului 26 din Directiva 95/46/CE, atunci se aplică în continuare legea privind protecția datelor.

Operatorii trebuie să evalueze dacă persoanele individuale pot fi ușor identificate din seturile de date „anonimizate" menite să fie puse la dispoziție în vederea reutilizării. Cu alte cuvinte, dacă orice organizație sau persoană ar putea identifica orice persoană din datele făcute publice – doar din acestea sau în combinație cu alte informații disponibile.

După cum s-a explicat la secțiunea 6.1, prezentul aviz nu are obiectivul de a da clarificări cuprinzătoare și concludente privind studiile de risc privind reidentificarea. Acesta nu are drept obiectiv nici să dea o definiție concludentă pentru „anonimizare" sau „date anonimizate". Cu toate acestea, reiterează faptul că cititorul poate găsi mai multe clarificări în documentele existente (inclusiv cele menționate la secțiunea 6.1) și că se lucrează în prezent în cadrul sub-grupului tehnologie al GL29 pe tema tehnicilor de anonimizare, precum s-a observat la secțiunile 6.1 și 2.2.

Acestea fiind spuse și fără a acoperi subiectul în întregime, GL29 dorește să evidențieze anumiți factori/anumite concepte care sunt utili(e) pentru studiile de risc privind reidentificarea, inclusiv, în special:

---

face datele anonime", de Paul Ohm de la Școala de drept din cadrul Universității din Colorado, Legea UCLA 57 revizia 1701 (2010), disponibilă online la adresa http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

- ce alte informații sunt disponibile, fie publicului larg, fie anumitor persoane sau organizații, și dacă datele menite să fie publicate pot fi legate de alte seturi de date;
- probabilitatea încercării unei reidentificări (anumite tipuri de date vor fi mai atractive potențialilor intruși decât altele) și
- probabilitatea succesului unei încercări de reidentificare, ținând cont de eficacitatea tehnicilor de anonimizare propuse[26].

Ce „alte" informații există?

Atunci când se determină dacă o persoană poate fi identificată indirect trebuie avut în vedere dacă identificarea este posibilă prin datele vizate (în cazul nostru setul de date „anonimizat") sau prin acele date și *alte informații* deținute de organizațiile sau persoanele care încearcă reidentificarea sau prin informații care urmează să intre în posesia acestor organizații sau persoane.

Aceste „alte informații" necesare pentru efectuarea reidentificării pot fi informații disponibile anumitor societăți sau organizații, inclusiv autorităților de aplicare a legii sau altor organisme din sectorul public, anumitor persoane sau tuturor, deoarece au fost, de pildă, publicate pe internet. Un exemplu evident este când datele disponibile publicului – cum ar fi listele electorale, cartea de telefon sau alte date ușor de obținut printr-o căutare pe internet – pot fi combinate cu datele „anonimizate" în mod nepotrivit, permițând identificarea unei persoane (de exemplu, folosind data de naștere și codul poștal al acesteia).

Riscul de reidentificare poate crește atunci când o persoană sau un grup cunosc deja multe detalii despre o altă persoană, de exemplu un membru al familiei, un coleg, o persoană de contact pe o pagină de socializare, un doctor, un profesor/profesoară, un agent al organului de aplicare a legii, sau altă persoană care exercită o profesie.

Însă ceea ce contează aici nu este pur și simplu dacă persoana care cunoaște deja anumite lucruri poate identifica persoana vizată, ci dacă el/ea va afla ceva nou din informațiile obținute prin reidentificare. Cele două exemple de mai jos ilustrează importanța acestei distincții.

Primul exemplu: statisticile privind incidența rujeolei. Într-un caz, statisticile anonimizate pot arăta că în orașul A, în anul 2012, un număr de X persoane au contractat rujeola. Nu se oferă mai multe detalii sau informații. Doctorul care a contribuit la statistică prin oferirea unor informații despre proprii pacienți autorităților relevante din domeniul îngrijirii medicale, are dosare mai complete referitor la acești pacienți în cabinetul său, care sunt protejate prin principiul confidențialității medicale. Doctorul poate identifica cu ușurință mai mulți dintre pacienți din seturile de date statistice. În mod similar, o mamă care știe că copilul său a contractat rujeola în acel an ar putea să-și reidentifice cu ușurință copilul din acel set de date. Cu toate acestea, nici doctorul și nici mama nu ar afla nimic necunoscut lor înainte ca setul de date anonimizat să fi fost făcut public.

Al doilea exemplu: abuzul de droguri și de alcool, abuzul sexual și performanța școlară. Acest exemplu poate fi comparat cu ceea ce urmează. Se efectuează o cercetare privind legăturile dintre abuzul de droguri și de alcool al părinților, abuzul sexual al copiilor și performanța școlară. Sunt publicate datele de cercetare presupus „anonimizate" cu bune intenții, însă fără un studiu atent de risc privind reidentificarea.

[26] În ceea ce privește tehnicile de anonimizare, a se vedea următorul aviz al GL29 dedicat acestui subiect.

Printre altele, statisticile arată că la școala A, unde sunt înscriși în total un număr de 500 elevi, în anul 2012, 20 % dintre elevi (100 elevi) au trăit într-o casă în care cel puțin un părinte este alcoolic sau dependent de droguri. Dintre aceștia, în 8 % din cazuri (8 elevi) copilul a fost abuzat sexual. Raportul specifică și faptul că nici unul dintre ceilalți elevi din școala A nu au fost abuzați sexual.

Cifrele arată, de asemenea, că în 96 % dintre cazuri (96 elevi) copii ai căror părinți erau alcoolici sau dependenți de droguri, se străduiau mult pentru a da randament la școală (definiți ca fiind „elevi cu randament slab" conform standardului academic potrivit), însă la această școală numai 50 % dintre cei abuzați sexual (4 elevi) au avut dificultăți majore cu activitățile școlare.

La școală este un lucru bine știut că elevul AA, un băiat deștept și muncitor, are un context familial dificil, iar mama sa este alcoolică. Este deseori brutalizat de către unii dintre colegii de clasă. Aceeași colegi de clasă pot acum afla din statisticile republicate în ziarul școlii că AA trebuie să intre în categoria celor 50 % dintre copii abuzați sexual care nu au probleme cu învățatul („elevii cu randament bun"). Astfel, au aflat informații noi (și în acest caz foarte sensibile) dintr-un set de date anonimizate în mod ineficient.

Riscul de a combina informații pentru a obține date cu caracter personal este în creștere odată cu evoluția tehnicilor de legătură și a puterii computaționale și deoarece din ce în ce mai multe informații „comparabile" devin accesibile publicului. Într-adevăr, puterea computațională se dublează în fiecare an, iar stocarea datelor, datorită și disponibilității serviciilor de informatică dematerializată, va deveni probabil marfă de consum. Astfel, riscul reidentificării prin conectarea datelor este imprevizibil, deoarece nu se poate evalua cu certitudine ce date sunt deja disponibile sau ce date vor putea fi comunicate pe viitor.

În ciuda tuturor nesiguranțelor, riscurile de reidentificare pot fi, cel puțin într-o anumită măsură, reduse prin aderarea la principiul minimizării datelor, adică, prin asigurarea faptului că sunt comunicate numai datele necesare pentru un anumit scop.

Probabilitatea ca reidentificarea să fie realizată cu succes: testul „intrusului motivat"

„Testul intrusului motivat" este un concept în formare, care încă nu a fost pe deplin încercat. S-ar putea să fie util să se determine dacă:

- există cineva care ar avea motivația să efectueze reidentificarea, și
- reidentificarea poate avea succes/există probabilitatea unei reidentificări cu succes.

În cadrul acestui test al „intrusului motivat", de fapt, se are în vedere măsura în care un „intrus" ar putea reidentifica pe cineva cu succes *dacă* ar fi motivat să încerce. „Intrusul motivat" este o persoană (un individ sau o organizație) care vrea să identifice persoana din datele personale ale căreia s-au derivat datele anonimizate. Testul este menit să evalueze dacă intrusul motivat ar avea succes. Abordarea presupune că „intrusul motivat" este competent și are acces la resursele potrivite pentru motivația pe care ar putea să o aibă pentru a reidentifica.

Anumite tipuri de date vor fi mai atractive pentru un „intrus motivat" decât altele. De exemplu, un intrus – în general – ar putea fi mai motivat să reidentifice datele cu caracter personal dacă aceste date:

- au o valoare comercială semnificativă (inclusiv pe piața neagră din afara Uniunii Europene) și, astfel, pot fi vândute și cumpărate pentru câștiguri financiare[27];
- pot fi folosite în scopuri legate de aplicarea legii sau de către serviciile de informații;
- dezvăluie informații demne de știri despre personalități;
- pot fi folosite în scopuri politice sau activiste (de exemplu, ca parte a unei campanii împotriva unei anume organizații sau persoane);
- ar putea fi folosite în scopuri personale cu intenții rele (de exemplu, urmărire, hărțuire, intimidare sau pur și simplu pentru a pune într-o situație neplăcută alte persoane);
- ar putea stârni curiozitate (de exemplu, dorința unei persoane locale de a afla cine a fost implicat într-un anume incident ilustrat pe o hartă a criminalității).

Deși este util să ne gândim la motivațiile potențiale ale intrușilor, GL29 subliniază faptul că această abordare are și limitări importante:

- exercițiul poate fi speculativ într-o anumită măsură;
- în absența unor „factori motivanți" evidenți, cum ar fi cei descriși anterior, exercițiul ar putea duce la reasigurări false și sugera că datele cu caracter personal relativ nevătămătoare pot fi făcute publice în vederea reutilizării fără o anonimizare efectivă;
- intrușii pot fi inventivi și sofisticați, și pot „avea unele avantaje", găsind soluții pentru folosirea datelor de-identificate la care alții nici nu s-au gândit;
- odată cu tendințele tot mai accentuate de a analiza cantități mari de date, crește și riscul ca, odată identificate, datele aparent nevătămătoare, combinate cu alte date, să reprezinte de fapt riscuri mult mai severe.

6.5. Testul de reidentificare

În anumite cazuri, riscul reidentificării este dificil de stabilit, mai ales acolo unde sunt folosite metode statistice complexe de către o parte terță pentru a combina diverse elemente de date anonimizate. În consecință, este o bună practică să se efectueze un test de reidentificare, ca parte a studiilor de risc generale privind reidentificarea, pentru a detecta și a soluționa punctele vulnerabile privind reidentificarea. Acesta constă în încercarea de a reidentifica persoanele vizate din seturile de date care vor fi emise.

Prima fază a procesului de testare a reidentificării trebuie să fie analiza situației seturilor de date pe care organismul din sectorul public le-a publicat sau pe care intenționează să le publice. Următoarea fază trebuie să fie încercarea de a determina ce alte date – date cu caracter personal sau nu – sunt disponibile, care ar putea fi conectate cu aceste date și care ar putea duce la reidentificare. În special, „testele de penetrare" vizate trebuie să contribuie la studiul riscurilor existente privind identificarea mozaicală, adică punerea laolaltă a unor fragmente de informații în vederea creării unei imagini de ansamblu despre cineva.

Desigur, testul de reidentificare nu trebuie considerat un panaceu și nu trebuie să creeze un sentiment fals de securitate. În primul rând, testul ar putea fi dificil de efectuat, deoarece necesită deseori o

[27] Acestea pot include, spre exemplu, date legate de tranzacții sau alte date comportamentale din care se pot sustrage profiluri individuale de consumatori, care apoi pot fi folosite în scop publicitar sau în vederea discriminării prin preț, informații financiare sau alte informații care pot contribui la furt de identitate, informații sensibile care pot fi folosite pentru a șantaja anumite persoane sau pentru a le discrimina, informații medicale care ar putea fi folosite de către companiile de asigurări, de exemplu, pentru a refuza să acopere o asigurare invocând drept motiv o afecțiune medicală preexistentă, informații care permit concluzii despre bonitate care ar putea fi folosite în vederea evaluării riscului legat de credite etc.

expertiză tehnică avansată și instrumentele potrivite, precum și cunoașterea existenței unor alte date care ar putea fi disponibile. În al doilea rând, operatorii de date trebuie să fie conștienți de faptul că riscul de reidentificare se poate schimba de-a lungul timpului. De exemplu, în prezent sunt disponibile tehnici de analiză a datelor din ce în ce mai puternice și ieftine, iar corelarea cu alte seturi de date devine din ce în ce mai ușoară și sunt generate din ce în ce mai multe date. În consecință, organizațiile trebuie să efectueze revizii periodice ale politicilor privind punerea la dispoziție a datelor și a tehnicilor folosite pentru anonimizarea datelor. În plus, deciziile nu trebuie niciodată bazate numai pe amenințările curente – ci și pe amenințările viitoare ce pot fi prevăzute.

Odată ce s-a efectuat un studiu de risc privind reidentificarea conform secțiunii 6.4 și – după caz – în urma testului de reidentificare, organismul din sectorul public poate decide dacă setul de date poate fi considerat anonimizat sau nu, cu alte cuvinte, dacă acesta conține sau nu date cu caracter personal în sensul articolului 2 litera (a) și al considerentului 26 din Directiva 95/46/CE. Dacă da, atunci setul de date poate fi comunicat fără restricții legate de protecția datelor.[28] Pe de altă parte, dacă testul se soldează cu succes, atunci aceste date nu pot (sau nu mai pot) fi făcute disponibile sub formă de date anonimizate, ci trebuie considerate date cu caracter personal (și deci publicarea acestora nu mai este posibilă, sau poate fi posibilă numai în temeiul cerințelor discutate în secțiunea VII).

6.6. Eliminarea seturilor de date compromise

În cazul unei reidentificări dovedite a datelor dintr-un set de date deschis, organismul din sectorul public care oferă setul de date trebuie să poată închide informația sau să îndepărteze setul de date de pe pagina de internet cu date deschise. În cazul în care setul de date este îndepărtat de pe pagina de internet, organismul din sectorul public trebuie să informeze, de asemenea, reutilizatorii și să le ceară să nu mai prelucreze datele și să șteargă toate datele provenite din setul de date compromis. Deoarece va fi dificil să informeze toți reutilizatorii datorită regimului de acordare a licențelor deschis impus de către Directiva ISP, organismul din sectorul public va trebui să pună în aplicare măsuri eficiente, în mod rezonabil, pentru a soluționa această problemă. Deși deseori o solicitare de eliminare poate veni prea târziu pentru a evita prejudiciul, acesta este un pas necesar pentru a contribui la reducerea impactului advers asupra persoanelor vizate.

VII. Deschiderea datelor cu caracter personal în vederea reutilizării

7.1. Exemple de date cu caracter personal emise de către organismele din sectorul public

Deși în mod tipic organismele din sectorul public comunică seturi de date anonimizate conform inițiativelor de reutilizare a ISP, în anumite cazuri acestea pot face publice în vederea reutilizării și date cu caracter personal.

Multe registre disponibile public, cum ar fi registrele funciare sau registrele comerciale conțin cantități mari de date cu caracter personal și sunt, datorită inițiativelor de e-guvernare, din ce în ce mai disponibile online. Sunt multe alte exemple în care legiuitorii din anumite state membre au stabilit un temei legal pentru a face datele cu caracter personal disponibile pe internet sau printr-o cerere de a accesa documente. Acestea pot include, de exemplu[29]:

- cheltuieli, salarii, sau declarații privind conflictul de interese al anumitor funcționari publici, sau beneficiari de ajutoare de stat (de exemplu subvenții agricole);

[28] A se vedea, însă, secțiunea 10.3 referitoare la „Condițiile de acordare a licenței pentru seturile de date compromise”, în special privind nevoia de a institui garanții care să asigure că persoanele nu vor fi reidentificate.

[29] A se vedea, de asemenea, exemplele date la secțiunea V, unde s-a discutat obiectivul Directivei ISP.

- numele organizațiilor sau persoanelor care fac donații către partidele politice;
- declarațiile fiscale ale persoanelor fizice[30];
- hotărâri judecătorești (cu numele părților sau al altor persoane uneori șterse sau înlocuite cu inițiale pentru a se reduce riscul de reidentificare);
- liste electorale;
- liste judecătorești (adică orarul cauzelor care vor fi prezentate în fața curții în anumite zile).

În fiecare din aceste cazuri organismele din sectorul public sau legiuitorii pot analiza dacă vor să facă aceste date disponibile în vederea reutilizării (de exemplu, pentru a îmbunătăți serviciile publice, cum ar fi obținerea accesului la registrele comerciale sau funciare). Potențialii reutilizatori pot, de asemenea, contacta organismele din sectorul public pentru a solicita reutilizarea datelor. În unele cazuri este posibil, de asemenea, ca reutilizatorii potențiali să ia, pur și simplu, datele cu caracter personal care sunt deja disponibile online și să le folosească fără a contacta neapărat organismul din sectorul public care a emis informația. Desigur, în toate cele trei cazuri reutilizatorii trebuie să respecte legea privind protecția datelor, dat fiind că au de-a face cu date cu caracter personal.

7.2. Diferențele dintre regimurile naționale de acces la informații

Obligațiile legale privitoare la accesibilitatea publică a anumitor date cu caracter personal variază în mare măsură de la un stat membru la altul, datorită diferitelor tradiții juridice și culturale. În unele state membre există un temei juridic pentru a face anumite date cu caracter personal disponibile, în timp ce alte state membre ar interzice dezvăluirea acelorași date cu caracter personal în aceeași situație. Directiva ISP recunoaște și precizează în mod foarte clar faptul că pornește de la regimurile existente privind accesul din statele membre și nu schimbă normele naționale referitoare la accesul la documente.[31]

7.3. Nevoia unor studii de impact privind protecția datelor și a unor garanții adecvate

Atunci când se are în vedere ca datele cu caracter personal să fie făcute publice în vederea reutilizării – ca regulă generală – o abordare atentă este absolut necesară. GL29 recomandă în special efectuarea unui studiu de impact exhaustiv privind protecția datelor înainte de a se publica setul de date (sau înainte de a adopta o lege care prevede publicarea acestora), care să evalueze și posibilitățile legate de potențiala reutilizare a acestora și impactul reutilizării. În general, trebuie evitată deschiderea datelor cu caracter personal în vederea reutilizării în baza unei licențe deschise fără restricții tehnice și legale privind reutilizarea acestora.

7.4. Importanța regimului de acordare a licențelor

În plus, GL29 recomandă instituirea unui regim riguros de acordare a licențelor, care să fie pus în aplicare corect, pentru a se asigura că datele cu caracter personal nu vor fi utilizate în scopuri incompatibile – de exemplu, pentru trimiterea unor mesaje publicitare nesolicitate sau, altfel, într-un mod în care persoanele vizate să găsească gestul neașteptat, impropriu sau neplăcut.

[30] A se vedea, de exemplu, hotărârea Curții Europene de Justiție din 16 decembrie 2008 în cauza C-73/07 Tietosuojavaltuutettu /Satakunnan Markkinapörssi Oy en Satamedia Oy.

[31] Acestea fiind spuse, după cum s-a explicat deja la secțiunea 5.4, legislația națională trebuie să respecte în continuare articolul 8 din ECHR și articolele 7 și 8 din Carta UE, așa cum au fost interpretate în jurisprudența aplicabilă.

7.5. Importanța unui temei juridic solid pentru publicare și pentru reutilizare

GL29 reiterează importanța stabilirii unei baze legale solide pentru a face publice datele cu caracter personal, ținând seama de normele relevante privind protecția datelor, inclusiv de principiul proporționalității, al minimizării datelor și al limitării scopului.

GL29 recomandă ca orice legislație care solicită accesul public la date să specifice clar scopul pentru care vor fi dezvăluite datele cu caracter personal. Dacă nu se face aceasta, sau se face doar în termeni vagi și generali, va suferi siguranța și predictibilitatea legilor. În special, va fi foarte dificil pentru organismul din sectorul public și pentru potențialii reutilizatori să determine, în ceea ce privește orice cerere de reutilizare, care au fost scopurile publicării inițiale și, implicit, ce alte scopuri ar fi compatibile cu aceste scopuri inițiale. După cum s-a menționat deja, chiar dacă datele cu caracter personal sunt publicate pe internet, nu trebuie să se presupună că acestea pot fi prelucrate ulterior în orice scop posibil.

Orice reutilizare va trebui, în aceste cazuri, să aibă un temei juridic adecvat (de exemplu, consimțământ sau prevedere legală) conform articolului 7 literele (a) - (f) din Directiva 95/46/CE și să respecte toate celelalte principii privind protecția datelor.

7.6. Limitarea scopului

Aplicarea principiului limitării scopului în cazul reutilizării ISP reprezintă o provocare. Pe de o parte, însăși ideea și motorul pentru inovare, care se află în spatele conceptului de „date deschise" și al reutilizării ISP, sunt că informația trebuie să fie disponibilă în vederea reutilizării pentru produse și servicii noi inovatoare și, astfel, pentru scopuri care nu pot fi definite în prealabil și nu pot fi clar prevăzute. Directiva ISP cere, de asemenea, ca licența să nu fie excesiv de restrictivă în ceea ce privește reutilizarea datelor.

Pe de altă parte, limitarea scopului este un principiu fundamental pentru protecția datelor și presupune ca datele cu caracter personal care au fost colectate cu un anume scop să nu fie folosite pentru alt scop incompatibil cu cel dintâi.[32] Acest principiu se aplică în mod egal și datelor cu caracter personal care sunt disponibile public. Simplul fapt că datele cu caracter personal sunt disponibile public nu înseamnă că aceste date cu caracter personal pot fi folosite în mod deschis în orice alt scop.

Spre exemplu – cheltuielile oficialilor publici seniori sunt făcute publice pe internet în vederea oferirii unei transparențe, însă a permite reutilizarea în alte scopuri de către orice alt membru al publicului nu ar fi compatibilă.

După cum s-a discutat în detaliu în cadrul Avizului 3/2013 al GL29 privind limitarea scopului (a se vedea secțiunea III și Anexa 1), stabilirea incompatibilității prelucrării datelor cu caracter personal cu scopurile pentru care acele date au fost colectate necesită o evaluare multifactorială. Se va lua în considerare în special:

(a) raportul dintre scopul pentru care datele cu caracter personal au fost colectate și scopurile prelucrării;
(b) contextul în care datele cu caracter personal au fost colectate și așteptările rezonabile ale persoanelor vizate în ceea ce privește reutilizarea acestora pe viitor;

[32] Datele pot fi utilizate într-un mod incompatibil cu scopurile specificate în momentul colectării numai în cazuri excepționale – conform garanțiilor stricte prevăzute la articolul 13 din Directiva 95/46/CE. A se vedea secțiunea III.3 din avizul 3/2013 al GL29 în ceea ce privește limitarea scopului.

(c) caracterul datelor personale și impactul reutilizării asupra persoanelor vizate;
(d) garanțiile oferite de către operatorul de date pentru a asigura prelucrarea corectă a acestora și pentru a preveni orice impact nedorit asupra persoanelor vizate.

Acești factori fundamentali trebuie evaluați atunci când se decide publicarea datelor cu caracter personal, precum și de fiecare dată când datele cu caracter personal sunt reutilizate. În continuare prezentăm câteva exemple în acest sens.

- Un organism din sectorul public a publicat informații de contact, inclusiv numele, funcția, adresa de lucru și numărul de telefon de la locul de muncă al funcționarilor săi publici într-un registru. Scopul evident – deși nu specificat în mod direct – al acestui registru este de a ajuta publicul să identifice persoana care trebuie contactată pentru întrebări și alte chestiuni oficiale. Un reutilizator vrea să „adune" conținutul acestui registru, să îl combine cu adresa de acasă și cu numărul de telefon de acasă al angajatului vizat (dacă acestea sunt disponibile public, de pildă într-o carte de telefon) și să pună ambele adrese, de la locul de muncă și de acasă, pe o hartă interactivă ca să arate unde locuiesc și unde lucrează funcționarii civili. Această combinare și reutilizare de date trebuie să fie considerate incompatibile cu scopul inițial. Funcționarul public al cărui număr de telefon și adresă sunt dezvăluite astfel încât să poată fi contactat de către public, nu s-ar fi așteptat, în mod rezonabil, ca această informație să fie ulterior corelată cu alte date pe care le-a făcut publice în alte scopuri, fără a avea legătură cu locul de muncă.
- În unele state membre, conform legii naționale, anunțurile privind căsătoriile planificate sunt publice și pot fi consultate de către oricine. Astfel de anunțuri sunt menite să arate intenția cuplului logodit de a se căsători și să permită persoanelor interesate să se opună căsătoriei. Însă, faptul că datele cu caracter personal conținute de anunțul de căsătorie sunt disponibile pentru toată lumea nu îngăduie părților terțe să folosească informația pentru a trimite mesaje comerciale cuplului. Această utilizare suplimentară ar fi incompatibilă cu scopul anunțurilor de căsătorie publice, adică să permită trimiterea de obiecțiuni privind căsătoria, în conformitate cu legea.

7.7. Scopuri comerciale vs. scopuri necomerciale

Avizul 7/2003 evidențiază faptul că activitățile comerciale sunt stimulentul principal pentru reutilizarea ISP, spre deosebire de accesul la informații, unde scopul legislației privind libertatea informației este de a asigura transparența, deschiderea și responsabilitatea în fața cetățenilor.

Avizul 7/2003 subliniază și faptul că „în mod normal [cetățenii] folosesc informația în scop propriu, necomercial". Afirmația de mai sus trebuie actualizată în lumina experienței câștigate între timp privind reutilizarea ISP. Experiența cu inițiativele privind datele deschise a arătat că reutilizarea ISP poate contribui la îmbunătățirea transparenței și a responsabilității, și poate, de asemenea, conduce la o mai bună utilizare a serviciilor publice. Diferența dintre reutilizarea în scopuri comerciale și cea în scopuri necomerciale nu ar trebui să fie decisivă atunci când este vorba de compatibilitatea utilizării datelor cu caracter personal. Evaluarea compatibilității nu trebuie bazată în primul rând pe importanța dată profitului în modelul economic al unui reutilizator potențial.

Ceea ce trebuie evaluat cu atenție este compatibilitatea scopurilor și a modului în care datele sunt prelucrate ulterior cu scopurile inițiale, conform criteriilor menționate la secțiunea 7.6. În cazul reutilizării ISP aceasta va însemna, inevitabil, că trebuie luate în considerare o gamă largă de scenarii de prelucrare nu doar unul.

7.8. Proporționalitatea și alte probleme

Proporționalitatea este un alt principiu fundamental formulat în Directiva 95/46/CE [33]. Există multe metode și modalități de a face publice datele cu caracter personal. Unele pot fi mai inoportune decât altele și pot reprezenta un risc mai ridicat. În consecință, unele pot fi considerate proporționale, iar altele nu.

La fel ca în cazul scopului, sunt probleme legate de controlul prelucrării ulterioare a datelor și de asigurarea respectării altor principii ale legilor privind protecția datelor, inclusiv, dar nu numai, problema proporționalității. Odată ce datele sunt făcute publice, mai ales pe internet, este foarte dificil să se limiteze efectiv utilizarea acestora și să se asigure că sunt respectate legile privind protecția datelor.

Printre problemele legate de asigurarea respectării legilor privind protecția datelor putem menționa:

- cum să ne asigurăm că datele care sunt deconectate de sursa primară sunt actualizate și exacte;
- cum să ne asigurăm că utilizarea datelor cu caracter personal se limitează la funcțiile prevăzute în scopul inițial al publicării;
- cum să ne asigurăm că datele cu caracter personal sunt șterse în timp util dacă publicarea acestora a fost prevăzută doar pentru o perioadă de timp limitată[34];
- cum să își exercite persoana vizată drepturile cu privire la datele cu caracter personal făcute publice în vederea reutilizării (inclusiv dreptul de a cere corectarea, actualizarea sau ștergerea datelor).

7.9. Restricții legale și/sau tehnice privind reutilizarea

Uneori, legislația sau proiectarea tehnică a sistemului limitează anumite operațiuni de prelucrare sau stabilesc alte precauții care restricționează utilizarea registrelor publice (de exemplu, restricționarea posibilității de a descărca întregul conținut al registrului sau restricții privind căutarea, de exemplu, pe baza numelui de familie sau a numelui unei persoane). În acest caz reutilizarea trebuie permisă, în principiu, numai în conformitate cu aceste condiții și restricții specifice.

În acest context, este importat să se analizeze cu atenție ce măsuri – atât măsuri legale cât și tehnice – ar putea fi puse în aplicare pentru a se asigura că problemele legate de protecția datelor, inclusiv cele descrise la secțiunea 7.8, vor fi soluționate. Este deosebit de important să se analizeze modul în care vor accesa reutilizatorii aceste date – de exemplu, prin funcția de descărcare în masă sau printr-o interfață personalizată cu acces limitat permis în anumite condiții. În acest sens este foarte important ce măsuri de securitate suplimentare vor fi create, cum ar fi, de exemplu, un sistem de verificare de tip „captcha[35]" pentru a preveni accesul automat și a minimiza riscul de obținere a unor baze de date întregi. Folosirea unor măsuri tehnice speciale poate contribui la reducerea utilizării în mod necorespunzător a datelor cu caracter personal și a impactului negativ asupra persoanelor

[33] A se vedea articolul 6 alineatul (1) litera (c) din Directiva 95/46/CE.

[34] A se vedea, de exemplu, cauza Curții Europene de Justiție Volker und Markus Schecke GbR vs. Land Hessen (cauzele conexate C 92/09 și C 93/09), punctul 31: „Nu este posibilă retragerea datelor de pe internet după expirarea perioadei de doi ani prevăzută la articolul 3 alineatul (3) din Regulamentul nr. 259/2008".

[35] CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart)* este o metodă automată utilizată pentru a determina dacă utilizatorul este o persoană sau un program de calculator. CAPTCHA distinge între o persoană și un calculator prin propunerea unei probleme care este ușor de rezolvat pentru o persoană umană, dar mai dificil de rezolvat pentru programele de calculator existente.

vizate, ceea ce altminteri ar fi posibil datorită accesului nelimitat și necondiționat la seturi de date întregi acordat reutilizatorilor.

În mod semnificativ, în multe cazuri este necesar să ne asigurăm că reutilizatorii vor putea să facă numai căutări specifice prin tehnologii menite să prevină descărcările în masă a registrelor de date, cum ar fi prin interfețele de programe de aplicare (API-uri) personalizate. Acest fapt ar putea contribui la asigurarea proporționalității utilizării și la reducerea riscului de abuz al unor baze de date întregi. În plus, asemenea interfețe personalizate pot contribui și la asigurarea faptului că datele sunt întotdeauna actualizate și că, de asemenea, datele nu mai vor fi disponibile prin API odată ce s-a luat decizia în acest sens de către organismul vizat din sectorul public. Pe de altă parte, vor fi limitate modalitățile prin care un reutilizator va putea reutiliza datele.

7.10. Acuratețea, actualizarea și ștergerea

O altă chestiune este ce se întâmplă dacă datele cu caracter personal sunt publicate sau făcute publice prin alte metode pentru o perioadă de timp limitat. Articolul 6 alineatul (1) litera (e) din Directiva 95/46/CE prevede că datele cu caracter personal trebuie păstrate într-o formă care permite identificarea persoanelor vizate o perioadă care să nu fie mai lungă decât este necesar pentru îndeplinirea scopurilor pentru care au fost colectate sau pentru care vor fi prelucrate ulterior. De asemenea, considerentul 18 din Directiva ISP prevede că, în cazul în care „decide să nu mai permită reutilizarea unor documente sau să nu mai actualizeze documentele, autoritatea competentă trebuie să facă publice respectivele decizii cât mai curând posibil, ori de câte ori este posibil prin mijloace electronice”.

Însă este dificil sau uneori imposibil să ne asigurăm că datele sunt șterse sau îndepărtate odată ce acestea au fost publicate și făcute disponibile în vederea reutilizării.

În această privință, soluția – deși nu completă – este de a nu face datele disponibile în format descărcabil, ci doar printr-un API personalizat și guvernat de anumite restricții și măsuri de securitate, după cum s-a menționat mai sus.

VIII. Datele de cercetare

În acest caz este important să facem diferența dintre publicarea datelor anonimizate, pe de o parte (a se vedea secțiunea VI) și accesul limitat, pe de altă parte. În mod clar, proiectul privind datele deschise se bazează pe disponibilitatea publică a datelor. Însă, de cele mai multe ori proiectele de cercetare (în mod special cercetările științifice în scop comercial cât și necomercial, dar și alte tipuri de cercetare) comunică datele în cadrul unor comunități închise, adică unui număr finit de cercetători sau instituții care au acces la date, iar cercetarea este efectuată în spații în care este posibilă restricționarea dezvăluirii sau utilizării ulterioare a datelor, și siguranța acestora poate fi garantată.

Accesul limitat este important mai ales în cazul gestionării datelor cu caracter personal (deseori sub formă de pseudonim[36]) derivate din surse sensibile sau dacă există un risc major de reidentificare. Pot exista alte riscuri asociate cu dezvăluirile limitate – dar acestea sunt mai reduse și pot fi mai ușor soluționate dacă datele sunt dezvăluite în cadrul unor comunități închise care funcționează în conformitate cu reguli stabilite.

[36] A se vedea, din nou, Avizul 4/2007 privind conceptul de date cu caracter personal adoptat la 20.6.2007 (WP 136), în special paginile 12-21 (privind „datele sub formă de pseudonim”, „datele codificate” și „datele anonime”, paginile 18-21). Problema informației „legate de” persoane este discutată la paginile 9-12. De asemenea, după cum s-a observat la pagina 3, este important că GL29 se străduiește în prezent să ofere mai multe clarificări în ceea ce privește tehnicile de anonimizare.

O problemă des întâlnită de cei care folosesc date în scopul cercetării este că, pe de o parte, aceste persoane vor date bogate, detaliate, și destul de utile pentru scopul dorit; pe de altă parte, vor să se asigure că persoanele vizate nu pot fi reidentificate. La un capăt al spectrului datele sub formă de pseudonim la nivel individual (de exemplu, datele pur și simplu codificate) pot fi extrem de valoroase pentru cercetători, din cauza detaliilor la nivel individual și pentru că registrele cu date sub formă de pseudonim din diferite surse pot fi combinate relativ ușor. Însă, aceasta înseamnă că există și un risc ridicat de reidentificare: posibilitatea de a lega câteva seturi de date (sub formă de pseudonim sau nu) de aceeași persoană poate fi precursoarea identificării sau poate permite o identificare directă.

În consecință, este nevoie de un nivel înalt de examinare și de mare atenție înainte de orice publicare sau înainte de a face disponibile în vederea reutilizării seturile de date sub formă de pseudonim. De regulă, cu cât datele sunt mai detaliate, conectabile și individualizate, cu atât mai limitat și controlat trebuie să fie accesul la aceste date. Cu cât sunt mai agregate și mai puțin conectabile, cu atât este mai probabil că aceste date pot fi publicate și făcute disponibile în vederea reutilizării fără riscuri majore.

Acesta este un domeniu complex și în schimbare, și nu ar fi corect să se excludă în mod categoric publicarea și reutilizarea tuturor seturilor de date care nu respectă întru totul pragul ridicat de „anonimizare” descris la secțiunea IV. Acestea fiind spuse, și ținând cont de faptul că este întotdeauna nevoie de o analiză de la caz la caz și de o evaluare atentă, GL29 este de părere că, în general, punerea la dispoziție în condițiile Directivei ISP a seturilor de date la nivel individual sau a altor seturi de date cu un nivel semnificativ de risc al reidentificării va fi deseori neadecvată.

În plus, este important de subliniat faptul că, în cazul în care asemenea seturi de date sunt totuși publicate și făcute disponibile, după o evaluare atentă a riscurilor și beneficiilor, orice dezvăluire și reutilizare ulterioară va trebui să fie în deplină conformitate cu legile privind protecția datelor (a se vedea secțiunea VII). Aceasta pentru că datele vizate, în ciuda unor măsuri (uneori foarte importante) de reducere a riscului de reidentificare, continuă să fie considerate date cu caracter personal.

IX. Arhivele istorice

Arhivele istorice și muzeele au, de asemenea, caracteristici specifice care necesită garanții specifice. În multe cazuri și în funcție de factori precum vechimea și sensibilitatea datelor și contextul colectării, alte opțiuni – cum ar fi permisiunea la acces limitat numai în condițiile existenței unor obligații de confidențialitate – ar putea fi mai adecvate decât digitalizarea și publicarea pe internet în vederea reutilizării nerestricționate.

În ceea ce privește arhivele este, de asemenea, important de subliniat faptul că, deși datele devin din ce în ce mai puțin sensibile cu trecerea timpului, publicarea neadecvată a unor documente vechi de câteva decenii ar putea avea încă un efect negativ sever asupra persoanei direct vizate sau asupra altor persoane, cum ar fi membrii familiei sau urmașii acestuia/acesteia. Acest fapt este valabil mai ales în cazul unor date extrem de sensibile. De exemplu, publicarea cazierului judiciar ar continua să stigmatizeze persoana vizată și să împiedice reabilitarea acesteia. În plus, informația conform căreia o persoană decedată fusese agent secret sau colaborator al unui regim opresiv, pedofil, autorul unor crime, a suferit de o boală mentală care stigmatizează, sau a suferit de o boală ereditară, ar putea de asemenea avea un efect negativ asupra familiei (de exemplu, a soției/soțului supraviețuitoare/supraviețuitor, a copiilor sau altor descendenți) persoanei decedate. Din motive similare ar trebui protejate și mostrele de ADN prelevate de la persoane decedate, uneori reținute în arhivele spitalelor publice. În consecință, asemenea informații, chiar dacă au legătură cu persoane

decedate, ar avea nevoie de protecție în temeiul legilor privind protecția datelor și/sau al legilor privind drepturile fundamentale, după caz.

Deseori, în statele membre există legi care guvernează accesul la arhivele naționale, arhivele perioadelor istorice recente ce reprezintă un interes special (cum ar fi arhivele care dețin dovezile colaborărilor cu regimuri opresive) și la dosarele deținute de instanțe judecătorești.[37] Aceste legi cer deseori aplicarea unor măsuri de securitate și restricții adecvate în legătură cu accesul, precum și alte garanții menite să echilibreze interesele vizate și să asigure accesibilitatea anumitor date cu caracter personal în scopul cercetării istorice, pentru a asigura transparența, și pentru anchete jurnalistice, dar în același timp, să asigure că dezvăluirea datelor, după caz, este limitată astfel încât să nu se aducă prejudicii vieții private, vieții de familie și demnității părților vizate.

În ceea ce privește „limitarea scopului", trebuie observat că, de regulă, arhivele istorice stochează informații în scopul cercetării istorice. Aceste scopuri sunt diferite de scopurile inițiale pentru care datele au fost colectate. Materialele care ajung în final în posesia arhivelor istorice au fost create în scopuri administrative specifice de către diverse organisme din sectorul public. În mod tipic, după o anumită perioadă de timp, când documentul nu mai este necesar pentru scopul administrativ inițial, se va efectua un proces de selecție, iar documentele care sunt considerate a avea o valoare „istorică" sunt transferate la arhivele istorice. Problema care se pune în acest caz este pentru ce scopuri să fie disponibile în vederea reutilizării datele cu caracter personal stocate în arhivele istorice. În acest context este important să se facă o evaluare atentă - ținând cont de valoarea potențială a disponibilității materialului de arhivă în vederea reutilizării, dar și de potențialul impact asupra drepturilor, libertăților și a demnității persoanelor vizate.

În general, se poate concluziona că, dacă digitalizarea anumitor documente care conțin date cu caracter personal și faptul de a le face disponibile în vederea reutilizării pot fi adecvate în anumite situații, iar anumite date pot fi făcute publice și în formă anonimizată, în alte cazuri sunt extrem de importante limitările publicării și reutilizării datelor cu caracter personal precum și luarea unor măsuri de securitate adecvate în vederea protejării acestora. Trebuie să se asigure, printr-un studiu atent de impact privind protecția datelor, că nicio colecție de arhivă nu este făcută disponibilă în scopul reutilizării, decât dacă s-a asigurat excluderea oricărui impact negativ potențial asupra persoanelor vizate sau dacă orice asemenea riscuri sunt reduse la un minim acceptabil. Sectorul arhivelor trebuie să ia în considerare crearea unor coduri de procedură sau modificarea codurilor existente în vederea explicării bunelor practici.

X. Acordarea de licențe pentru datele cu caracter personal în vederea reutilizării

10.1. Prevederi relevante din Directiva ISP

Considerentul 15 din directiva ISP prevede că „asigurarea clarității și disponibilității publice a documentelor din sectorul public reprezintă o cerință preliminară a dezvoltării unei piețe comunitare a informației. În consecință, toate condițiile aplicabile pentru reutilizarea documentelor trebuie prezentate în mod clar potențialilor reutilizatori. Statele membre trebuie să încurajeze, după caz, crearea de indexuri accesibile online, care să cuprindă documentele disponibile în vederea promovării și facilitării cererilor de reutilizare".

[37] Alte exemple pot include arhivele registrului de stare civilă care conțin, în unele state membre, printre altele și cauza decesului, schimbările de sex, numele partenerului (din care poate reieși orientarea sexuală) sau faptul că o anumită persoană a fost adoptată. Accesul la arhive este permis conform anumitor condiții.

Considerentul 26 din Modificarea ISP prevede în continuare că „în ceea ce privește orice reutilizare a documentului, organismele din sectorul public pot impune o serie de condiții, după caz prin intermediul unei licențe…" iar „statele membre trebuie, după caz, să încurajeze utilizarea în formate deschise, care pot fi citite automat".

În continuare, articolul 8 alineatul (1) prevede că „Organismele din sectorul public pot acorda permisiunea reutilizării necondiționate sau pot impune o serie de condiții, dacă este cazul prin intermediul unei licențe. Condițiile respective nu trebuie să limiteze în mod inutil posibilitățile de reutilizare și nu trebuie utilizate pentru restricționarea concurenței.."

10.2. Acordarea de licențe și protecția datelor

Licențele sunt o parte esențială a regimului ISP. De asemenea, ele pot afecta modul în care sunt prelucrate datele cu caracter personal și ar trebui să constituie una dintre garanțiile aplicate atunci când datele cu caracter personal (sau datele anonimizate derivate din date cu caracter personal) sunt făcute disponibile în vederea reutilizării. Licențele nu elimină necesitatea respectării legilor privind protecția datelor, dar o clauză privind protecția datelor în condițiile de acordare a licențelor ar putea contribui la asigurarea respectării acestor legi printr-un plus de „forță executorie". O astfel de clauză poate contribui, de asemenea, la sensibilizare, amintindu-le reutilizatorilor de obligațiile lor în calitate de operatori de date.

În ceea ce privește conținutul licențelor, este util să distingem între două scenarii diferite.

10.3. Termenele de licență pentru seturile de date anonimizate

În primul rând, în ceea ce privește datele anonimizate (adică, seturile de date care nu mai conțin date cu caracter personal), condițiile de licență trebuie

- să reitereze faptul că seturile de date au fost anonimizate;
- să interzică deținătorilor de licență reidentificarea oricărei persoane[38];
- să interzică deținătorilor de licență luarea oricăror măsuri sau decizii în ceea ce privește persoanele vizate; și
- de asemenea, să conțină obligația ca deținătorul de licență să anunțe entitatea care acordă licența în cazul în care anumite persoane pot fi sau au fost reidentificate.

Ca alternativă la condițiile de licență s-ar putea da un mesaj de atenționare a reutilizatorilor, evidențiat, pe portalul de date deschise. Însă, ar trebui promovată acordarea de licențe, deoarece ar avea beneficiul adăugat al forței executorii contractuale.

Eliminarea seturilor de date compromise

Toți utilizatorii pe web, inclusiv persoanele vizate, trebuie să aibă posibilitatea de a atenționa entitatea care acordă licența asupra unei reidentificări sau a posibilității reidentificării. Dacă entitatea care acordă licența constată un risc ridicat de reidentificare, trebuie prevăzută o procedură în licență, conform căreia entitatea care acordă licența să poată elimina datele „compromise". Cu alte cuvinte,

[38] Există excepții limitate, de pildă, în cazuri de testări ale re-identificării *bona fide*. Însă, chiar și în aceste cazuri rezultatele testelor trebuie aduse la cunoștința operatorului și a organismului vizat din sectorul public, iar datele re-identificate nu trebuie publicate sau diseminate mai pe larg.

clauza privind protecția datelor trebuie să dea entității care acordă licența dreptul de a suspenda sau înceta accesibilitatea datelor (de exemplu, dreptul de a închide API-ul sau de a înlătura fișierul de pe platformă). Entitatea care acordă licența trebuie să depună toate eforturile posibile pentru a cere reutilizatorilor să șteargă toate seturile de date sau acele părți care au fost compromise (adică au devenit reidentificabile). Aceasta înseamnă anunțuri clare pe paginile de web, cum ar fi pe portalurile de date deschise, și forumuri/liste de emailuri/rețele sociale accesate de grupuri sau persoane susceptibile să reutilizeze datele. Cerința de înregistrare ar fi cea mai eficientă metodă de rechemare a seturilor de date, dar aceasta nu ar trebui încurajată dacă necesită agregarea unor noi date cu caracter personal din partea reutilizatorilor și ar avea efectul general de a descuraja folosirea paginilor web ISP și a altor servicii.

10.4. Condiții de licență pentru datele cu caracter personal

Atunci când se acordă licență pentru date cu caracter personal, este nevoie să se definească limitele utilizării acestor date. Aici problema principală este să ne asigurăm că orice reutilizare este limitată la ceea ce „este compatibil cu scopurile pentru care datele au fost inițial colectate”.[39] Pentru a face acest lucru, condițiile de licență trebuie să clarifice cel puțin care au fost scopurile pentru care datele au fost în primul rând publicate și să dea indicații referitoare la ce este o utilizare compatibilă a datelor cu caracter personal și ce nu.

Însă trebuie observat că acest fapt nu trebuie „să limiteze în mod inutil posibilitățile de reutilizare” [articolul 8 alineatul (1) din Modificarea ISP]. Aceasta înseamnă deseori că termenii generici ai licențelor deschise standard nu sunt potriviți și este necesară dezvoltarea unor licențe specifice pentru anumite date cu caracter personal sau pot fi folosite anumite modele care se pot adapta.

În momentul de față unele licențe deschise standardizate (cum ar fi licența guvernamentală în Regatul Unit) exclud datele cu caracter personal – pentru acestea nu se acordă licență în baza unor condiții.

10.5. Reidentificarea sau utilizarea incompatibilă trebuie urmate de o aplicare judicioasă a normelor

Odată ce datele sunt publicate prin licență – cum ar fi licența deschisă guvernamentală – acestea vor fi dificil de protejat de utilizări incompatibile ulterioare sau dezvăluire, iar siguranța lor va fi greu de asigurat. În acest context este foarte important ca entitatea care acordă licența să monitorizeze reutilizările și să pedepsească orice abuzuri care constau fie în forma reidentificării persoanelor vizate, fie în reutilizarea datelor în scopuri incompatibile.

În timp ce GL29 reiterează rolul important jucat de către organismele din sectorul public, acesta vrea să sublinieze, de asemenea, că atunci când un reutilizator adună date cu caracter personal printr-un proces de reidentificare, se va considera cel mai probabil că reutilizatorul prelucrează date cu caracter personal în mod ilegal și autoritățile de protecție a datelor vor lua măsurile legale necesare împotriva acestuia. Printre aceste măsuri sunt incluse amenzi severe în temeiul Regulamentului pentru protecția datelor care a fost propus.

[39] A se vedea din nou Avizul 3/2013 al GL29 privind limitarea scopului.

XI. Concluzii

În concluzie, GL29 reiterează faptul că reutilizarea ISP poate aduce beneficii care să ducă la mai multă transparență și la reutilizarea inovativă a informațiilor din sectorul public. Însă accesibilitatea mai mare a informațiilor care rezultă nu este lipsită de riscuri. Pentru a asigura protecția vieții private și a datelor cu caracter personal, este nevoie să se urmeze o abordare echilibrată, iar legile privind protecția datelor trebuie să contribuie la clarificarea procedurii de selecție a datelor care pot fi făcute disponibile în vederea reutilizării și a celor care nu pot fi făcute disponibile, și să precizeze ce măsuri trebuie luate pentru a garanta protecția datelor cu caracter personal.

Indiferent de „principiul reutilizării" formulat în Modificarea ISP, reutilizarea în orice scop comercial sau necomercial în temeiul Directivei ISP nu este întotdeauna adecvată în cazurile în care ISP conțin date cu caracter personal. De regulă sunt și trebuie făcute publice în vederea reutilizării datele statistice derivate din date cu caracter personal, și nu datele cu caracter personal.

Cu toate acestea, este posibil, în anumite situații, ca și datele cu caracter personal să fie considerate ca fiind disponibile în vederea reutilizării conform Directivei ISP, după caz, în temeiul unor măsuri legale, tehnice și organizaționale suplimentare pentru protejarea persoanelor vizate. Pentru aceste cazuri GL29 reiterează importanța stabilirii unui temei juridic solid pentru publicarea datelor cu caracter personal, luând în considerare normele relevante de protecție a datelor, inclusiv principiile proporționalității, minimizării datelor și limitării scopului. În acest context este, de asemenea, important de subliniat din nou faptul că orice informații legate de persoane fizice identificate sau identificabile, fie că sunt disponibile public sau nu, constituie date cu caracter personal. În consecință, accesarea și reutilizarea acelor date cu caracter personal care au fost făcute publice se supune în continuare legii aplicabile pentru protecția datelor.

Luând în considerare aceste observații GL29 recomandă:

- să se ia în considerare faptul că unele ISP pot conține date cu caracter personal cu prima ocazie când se decide publicarea ISP, conform principiului „protecției datelor începând cu momentul conceperii și al protecției implicite a datelor";
- având în vedere acest fapt, organismul vizat din sectorul public (sau, după caz, legiuitorul) trebuie să efectueze un studiu de impact privind protecția datelor înainte de a face disponibile în vederea reutilizării orice ISP care conțin date cu caracter personal (sau înainte de adoptarea unei legi care să permită publicarea datelor cu caracter personal astfel făcându-le potențial disponibile în vederea reutilizării); un studiu de impact privind protecția datelor trebuie efectuat și în situațiile în care se vor face disponibile în vederea reutilizării seturi de date anonimizate derivate din date cu caracter personal;
- când seturile de date sunt anonimizate, este esențial să se efectueze un studiu de risc privind reidentificarea, iar testele de reidentificare sunt considerate bună practică;
- rezultatul studiului ar putea contribui la identificarea măsurilor de precauție necesare pentru reducerea riscului inclusiv, dar nu numai, măsuri tehnice, juridice și organizaționale, cum ar fi termene de licență adecvate și măsuri tehnice pentru evitarea descărcărilor în masă a datelor, precum și tehnici adecvate de anonimizare; de asemenea, ar putea conduce la decizia de a nu publica și/sau a face datele disponibile în vederea reutilizării;
- termenele de licență pentru reutilizarea ISP trebuie să includă o clauză privind protecția datelor, de fiecare dată când sunt prelucrate date cu caracter personal, inclusiv în situațiile când se vor face disponibile în vederea reutilizării seturi de date anonimizate derivate din date cu caracter personal;

- dacă studiul de impact privind protecția datelor conclude că o licență deschisă nu este suficientă pentru a soluționa riscul legat de protecția datelor, organismele din sectorul public nu vor face aceste date publice în temeiul Directivei ISP. (Însă, organismul din sectorul public poate decide încă dacă va lua în considerare reutilizarea în afara condițiilor și domeniului de aplicare ale Directivei ISP și poate, de asemenea, cere solicitanților să demonstreze că toate riscurile privind protecția datelor cu caracter personal sunt soluționate în mod adecvat și că solicitantul va prelucra datele în conformitate cu legile aplicabile privind protecția datelor);
- organismele din sectorul public trebuie să se asigure, după caz, că datele cu caracter personal sunt anonimizate, iar condițiile de acordare a licenței interzic reidentificarea persoanelor și reutilizarea datelor cu caracter personal în scopuri care ar putea afecta persoanele vizate;
- în fine, statele membre trebuie să ia în considerare stabilirea și sprijinirea unor rețele de cunoaștere/centre de excelență, contribuind astfel la schimbul de bune practici privind anonimizarea și datele deschise.

Adoptat la Bruxelles, la 5 iunie 2013

Pentru grupul de lucru
Președintele
Jacob KOHNSTAMM