ARTIKEL 29-GRUPPEN VEDRØRENDE DATABESKYTTELSE

01189/09/DA
WP 163

Udtalelse nr. 5/2009 om internetbaserede sociale netværksaktiviteter

Vedtaget den 12. juni 2009

Arbejdsgruppen er nedsat på grundlag af artikel 29 i direktiv 95/46/EF. Den fungerer som en uafhængig europæisk rådgivningsinstans vedrørende databeskyttelse og beskyttelse af privatlivets fred. Dens opgaver er beskrevet i artikel 30 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF.

Sekretariatsfunktionen varetages af Direktorat D (Grundlæggende Rettigheder og EU-borgerskab) i Europa-Kommissionen, Generaldirektoratet for Retfærdighed, Frihed og Sikkerhed, B-1049 Bruxelles, Belgien, kontor LX-46 01/02.

Websted: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Indholdsfortegnelse

Resumé

Hovedsigtet med denne udtalelse er at anvise løsninger på, hvordan sociale netværkstjenester kan opfylde kravene i EU's lovgivning om beskyttelse af personoplysninger. Den er primært tænkt som en vejledning til sociale netværkstjenester om de forholdsregler, der skal tages for at sikre overholdelse af fællesskabslovgivningen.

Udtalelsen bemærker, at sociale netværkstjenester, og i mange tilfælde andre applikationsudbydere, er registeransvarlige med deraf følgende ansvar over for brugerne af de sociale netværk. I udtalelsen gøres der rede for, hvordan mange mennesker bruger de sociale netværk til rent personlige formål, idet de kontakter andre mennesker som led i deres personlige eller familiemæssige aktiviteter. I de tilfælde betragter udtalelsen "undtagelsen ved udøvelse af familiemæssige aktiviteter" som gældende, således at reglerne vedrørende dataregisteransvarlige ikke finder anvendelse. Samtidig gør udtalelsen også rede for omstændigheder, hvor en socialnetværksbrugers aktiviteter ikke er omfattet af "undtagelsen ved udøvelse af familiemæssige aktiviteter". Formidling og brug af de oplysninger, der ligger tilgængelige på sociale websteder til sekundære, utilsigtede formål, er et anliggende, der ligger artikel 29-arbejdsgruppen meget på sinde. Udtalelsen plæderer igen og igen for robuste, sikre og privatlivsvenlige standardindstillinger som ideelt afsæt for alle de tjenester, der udbydes. Adgang til oplysninger om personprofiler er et område, der især vækker bekymring. Udtalelsen beskæftiger sig også med spørgsmål omkring behandling af følsomme oplysninger og billeder, reklamer og direkte markedsføring på sociale netværk samt lagring af data.

De væsentligste henstillinger vedrører især de forpligtelser, som sociale netværkstjenester har med hensyn til at overholde direktivet om beskyttelse af personoplysninger og fastholde og styrke brugernes rettigheder. Det er af altafgørende betydning, at sociale netværkstjenester informerer brugerne om deres identitet lige fra begyndelsen og præciserer alle de forskellige formål, til hvilke de kan behandle personoplysninger. Især skal sociale netværkstjenester være ekstra påpasselige med hensyn til behandling af mindreåriges personoplysninger. Udtalelsen anbefaler, at brugerne kun uploader billeder eller oplysninger om andre personer med den pågældendes samtykke, og er af den opfattelse, at de sociale netværkstjenester også har pligt til at informere brugerne om andres ret til beskyttelse af deres privatliv.

Gruppen vedrørende beskyttelse af FYSISKE personer i forbindelse med behandling af personoplysninger,

som er nedsat ved Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995[1],

som henviser til artikel 29 og artikel 30, stk. 1, litra a), og artikel 30, stk. 3, i ovennævnte direktiv, og artikel 15, stk. 3, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002,

som henviser til EF-traktatens artikel 255 og til Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter,

som henviser til sin forretningsorden,

HAR VEDTAGET FØLGENDE DOKUMENT:

1. Indledning

Udviklingen af webportaler og hostede services, som f.eks. sociale netværkstjenester, er et relativt nyt fænomen, og antallet af brugere på disse websteder fortsætter med at stige eksponentielt.

De personoplysninger, som en person lægger ud på internettet, kombineret med oplysninger om brugerens aktioner og interaktioner med andre mennesker, kan skabe en risikoprofil af denne persons interesser og aktiviteter. Personoplysninger, der offentliggøres på sociale websteder kan bruges af andre til en lang række formål, bl.a. i kommercielt øjemed, og kan udgøre store risici, f.eks. identitetstyveri, økonomisk tab, tab af forretnings- eller beskæftigelsesmuligheder og fysiske overgreb**.**

International Working Group on Data Protection in Telecommunications ("Berlin-gruppen") vedtog i marts 2008 *Rome Memorandum*[2]. Memorandummet analyserer de risici, som sociale netværk udgør for privatlivets fred og for sikkerheden, og opstiller retningslinjer for regeludstedende myndigheder, tjenesteudbydere og brugere. Den netop vedtagne resolution om beskyttelse af privatlivets fred i sociale netværkstjenester (Privacy Protection in Social Network Services)[3] beskæftiger sig ligeledes med de ændringer, som sociale netværkstjenester er årsag til. Gruppen har ligeledes taget højde for holdningsdokumentet fra oktober 2007 offentliggjort af Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) med titlen "*Security Issues and Recommendations for Online Social Networks*"[4], som er rettet mod regeludstedende myndigheder og sociale netværkstjenester.

2. Definition af en "social netværkstjeneste" og forretningsmodel

Sociale netværkstjenester kan groft sagt defineres som internetbaserede kommunikationsplatforme, der gør det muligt for enkeltpersoner at tilmelde sig eller oprette

---

1 EFT L 281 af 23.11.1995, s. 31, kan findes på http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

3 Vedtaget på 30. International Conference of Data Protection and Privacy Commissioners i Strasbourg, 17.10.2008, http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf.

4 http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

netværk af ligesindede brugere. I juridisk forstand er sociale netværk tjenester i informationssamfundet, som defineret i artikel 1, stk. 2, i direktiv 98/34/EF som ændret ved direktiv 98/48/EF. Sociale netværkstjenester har visse fællestræk:

- brugerne opfordres til at udlevere personoplysninger med henblik på at generere en beskrivelse af dem selv, dvs. oprette en "profil"

- sociale netværkstjenester leverer ligeledes værktøjer, der sætter brugerne i stand til at lægge deres eget materiale op (brugergenereret indhold, såsom et billede eller en dagbogsoptegnelse, musik- eller videoklip eller links til andre websteder[5])

- ved sociale netværksaktiviteter anvendes der værktøjer, som genererer en liste over kontakter for hver enkelt bruger, og som den enkelte bruger kan kommunikere interaktivt med.

Størsteparten af de sociale netværkstjenesters indtjening kommer fra indtægter fra reklamer, der lægges op på de oprettede websider, og som brugerne kan klikke sig ind på. Brugere, der lægger store mængder oplysninger om deres interesser op på deres profil, giver annoncører, der ønsker at lave målrettet markedsføring på baggrund af disse oplysninger, en perfekt adgang til markedet.

Det er derfor vigtigt, at sociale netværkstjenester opererer på en måde, der respekterer de grundlæggende rettigheder og frihedsrettighederne for brugere, der har en legitim forventning om, at de personoplysninger, som de videregiver, vil blive behandlet i overensstemmelse med europæisk og national lovgivning om databeskyttelse og beskyttelse af privatlivets fred.

3. Anvendelse af direktivet om beskyttelse af personoplysninger

Bestemmelserne i direktivet om beskyttelse af personoplysninger finder anvendelse på sociale netværkstjenester i de fleste tilfælde, også selv om deres hovedsæde er beliggende uden for EØS. Artikel 29-gruppen henviser til sin tidligere udtalelse om søgemaskiner for yderligere vejledning om etablering og brug af udstyr som afgørende faktorer for anvendelsen af direktivet om beskyttelse af personoplysninger og de regler, der efterfølgende udløses af behandlingen af IP-adresser og brugen af cookies.[6]

3.1 Hvem er den dataregisteransvarlige?

Udbydere af sociale netværkstjenester

Udbydere af sociale netværkstjenester er dataregisteransvarlige i henhold til direktivet om beskyttelse af personoplysninger. De leverer midlerne til behandling af brugerdata og yder alle de "basale" tjenester i forbindelse med brugerstyringen (f.eks. registrering og sletning af konti). Udbydere af sociale netværkstjenester bestemmer ligeledes, i hvor stort omfang brugerdata kan benyttes til reklame- og markedsføringsformål – herunder reklame tilvejebragt af tredjepart.

Applikationsudbydere

[5] I de tilfælde, hvor sociale netværk leverer elektroniske kommunikationstjenester, finder bestemmelserne i direktiv 2002/58 om databeskyttelse inden for elektronisk kommunikation ligeledes anvendelse.

[6] WP148, "Udtalelse nr. 1/2008 om databeskyttelsesproblemer i forbindelse med søgemaskiner".

Også applikationsudbydere kan være dataregisteransvarlige, hvis de udvikler applikationer, der supplerer dem, der kommer fra sociale netværkstjenester, og hvis brugerne beslutter at bruge en sådan applikation.

Brugere

I de fleste tilfælde betragtes brugerne som registrerede. Direktivet pålægger ikke fysiske personer, der behandler persondata, pligter som dataregisteransvarlig, for så vidt behandlingen foretages *"med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter"* – den såkaldte "undtagelse ved udøvelse af familiemæssige aktiviteter". I nogle tilfælde kan det være, at aktiviteterne for en bruger af sociale netværkstjenester ikke er omfattet af en sådan undtagelse, og brugeren kan antages at have påtaget sig en del af det ansvar, som en dataregisteransvarlig har. Nogle af disse typer aktiviteter behandles neden for:

3.1.1. Formål og art

En tendens, der bliver mere og mere fremherskende ved sociale netværkstjenester, er, at Web 2.0 er begyndt at udvikle sig væk fra ikke-kommerciel brug til at blive brugt kommercielt og til udnyttelse at tjenester[7], således at nogle af brugernes aktiviteter kan gå længere end udøvelse af rent personlige eller familiemæssige aktiviteter, f.eks. når det sociale netværk bruges som samarbejdsplatform for en sammenslutning eller en virksomhed. Hvis en bruger af sociale netværkstjenester optræder på en virksomheds eller sammenslutnings vegne, eller primært bruger sociale netværkstjenester som en platform til fremme af kommercielle, politiske eller velgørende formål, finder undtagelsen ikke anvendelse. Her påtager brugeren sig det fulde ansvar som dataregisteransvarlig, der videregiver personoplysninger til en anden dataregisteransvarlig (den sociale netværkstjeneste) og til tredjeparter (andre brugere af sociale netværk eller potentielt endog andre dataregisteransvarlige med adgang til oplysningerne). Her skal brugeren sørge for at indhente de berørte personers samtykke eller have et andet legitimt grundlag i medfør af direktivet om beskyttelse af personoplysninger.

Typisk er adgang til oplysninger (profiloplysninger, indslag, historier…), som leveres af en bruger, begrænset til kontakter, den pågældende selv har valgt. Men i nogle tilfælde kan brugerne erhverve et stort antal tredjepartskontakter, hvoraf der er nogle, han rent faktisk ikke kender. Et stort antal kontakter kunne være en indikation af, at undtagelsen ved udøvelse af familiemæssige aktiviteter ikke finder anvendelse, og at brugeren derfor ville blive anset for at være dataregisteransvarlig.

3.1.2. Adgang til profiloplysninger

Sociale websteder skal sikre privatlivets fred og tilbyde gratis standardopsætninger, således at der kun er adgang til kontakter, som brugeren selv har valgt.

Når adgangen til profiloplysninger udvides til kontakter, som brugeren ikke selv har valgt, f.eks. når der gives adgang til en profil til samtlige medlemmer af det sociale netværk[8], eller når dataene kan indekseres af søgemaskiner, går adgangen ud over de personlige og familiemæssige aktiviteter. Tilsvarende gælder, at hvis en bruger træffer en informeret beslutning om at tillade adgang til ikke-selvvalgte "venner", træder ansvaret som dataregisteransvarlig i kraft. Rent faktisk vil der så gælde samme regler, som når en person bruger andre teknologiplatforme til at offentliggøre personoplysninger på internettet[9]. I flere medlemsstater betyder de manglende adgangsbegrænsninger (deraf den offentlige karakter), at direktivet om beskyttelse af personoplysninger finder anvendelse i relation til en internetbruger, der erhverver ansvar som dataregisteransvarlig[10].

Det skal erindres, at selv om undtagelsen ved udøvelse af familiemæssige aktiviteter ikke finder anvendelse, kan brugeren af den sociale netværkstjeneste være omfattet af andre undtagelser, f.eks. hvis behandlingen finder sted i journalistisk øjemed eller med henblik på

---

7 "Internet of the future: Europe must be a key player" tale holdt af Viviane Reding, EU-kommissær for Informationssamfundet og Medier, på mødet i "Lisbon Council" om initiativet "Future of the Internet", Bruxelles, den 2. februar 2009

8 eller når det kan argumenteres, at der ikke foretages nogen faktisk selektering med hensyn til godkendelse af kontakter, dvs. brugerne accepterer "kontakter" uanset, hvilken relation de har

9 Som det f.eks. gælder for offentliggørelse på platforme, der ikke er sociale netværk, eller med self-hosted software.

10 I Domstolens dom (Satamedia) hedder det omvendt i præmis 44: "Det følger heraf, at den anden undtagelse skal fortolkes således, at den udelukkende vedrører de aktiviteter, der indgår i den enkelte borgers privatliv eller familieliv (jf. Lindqvist-dommen, præmis 47). Dette er åbenbart ikke tilfældet hvad angår Markkinapörssis og Satamedias behandling af personoplysninger, som består i at gøre de indsamlede oplysninger offentligt tilgængelige for et ubestemt antal personer."

kunstnerisk eller litterær virksomhed. I disse tilfælde skal der findes en balance mellem reglerne for ytringsfrihed og retten til privatlivets fred.

3.1.3 Brugeres behandling af tredjepartsoplysninger

Anvendelsen af undtagelsen ved udøvelse af familiemæssige aktiviteter er ligeledes begrænset af behovet for at garantere tredjeparters rettigheder, navnlig med hensyn til følsomme oplysninger. Derudover skal det bemærkes, at selv om undtagelsen ved udøvelse af familiemæssige aktiviteter finder anvendelse, kan en bruger være ansvarlig efter de almindelige nationale civil- eller strafferetlige bestemmelser (f.eks. bagvaskelse, personlighedskrænkende overgreb, strafferetligt ansvar).

3.2 Sikkerhedsindstillinger og privatlivsvenlige standardindstillinger

Sikker behandling af oplysninger er et afgørende element for tilliden til sociale netværkstjenester. Dataregisteransvarlige skal træffe de fornødne tekniske og organisatoriske foranstaltninger "både under selve udformningen og under iværksættelsen af en behandling", navnlig for at varetage sikkerheden og derved forhindre enhver form for ubeføjet handling, i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, der skal beskyttes[11].

Et vigtigt element i indstillingerne for personlige oplysninger (privacy settings) er adgangen til personoplysninger, der offentliggøres i en profil. Hvis der ikke er nogen begrænsninger for en sådan adgang, kan tredjeparter hente alle mulige slags intime detaljer om brugerne, enten som medlem af det sociale netværk eller via søgemaskiner. Det er imidlertid kun et fåtal af de brugere, der tilmelder sig denne service, som rent faktisk vil foretage ændringer i standardindstillingerne. Sociale netværkstjenester bør derfor tilbyde privatlivsvenlige standardindstillinger, som giver brugerne mulighed for frit og specifikt at godkende enhver adgang til indholdet af deres profil, der går ud over de kontakter, de selv har valgt, således at risikoen for, at tredjeparter behandler oplysningerne ulovligt, reduceres. Begrænsede adgangsprofiler skal ikke kunne registreres af interne søgemaskiner, herunder muligheden for søgning på parametre som alder eller sted. Beslutninger om at udvide adgangen kan ikke være underforstået[12], f.eks. med en "opt-out"-klausul fastsat af den sociale netværkstjeneste.

3.3 Oplysninger, som skal tilvejebringes af sociale netværkstjenester

Udbydere af sociale netværkstjenester skal i henhold til artikel 10 i direktivet om beskyttelse af personoplysninger informere brugerne om deres identitet og formålene med den behandling, hvortil oplysningerne er bestemt, herunder, men ikke begrænset til:

- brug af oplysninger med henblik på direkte markedsføring
- eventuel deling af oplysningerne med nærmere angivne kategorier af tredjeparter
- en oversigt over profiler: deres oprettelse og vigtigste datakilder
- brug af følsomme oplysninger.

---

[11] Artikel 17 og betragtning 46 i direktivet om beskyttelse af personoplysninger.

[12] I "Report and Guidance on Privacy in Social Network Services ("Rome Memorandum")" angives forskellige risici, såsom den vildledende opfattelse af samfund ("The misleading notion of community"), side 2, og afgivelse af flere personoplysninger, end man tror man gør ("Giving away more personal information than you think you do"), side 3. Et computersikkerhedsfirma advarer en vigtig social netværkstjeneste om standardindstillinger for adgang til medlemmer inden for det samme geografiske område: http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html.

Arbejdsgruppen anbefaler, at:

- udbyderne af de sociale netværkstjenester, i det omfang det er relevant, advarer brugerne om de risici, de selv udsættes for med hensyn til beskyttelsen af personoplysninger, og om de risici, som andre udsættes for, når de uploader oplysninger på det sociale websted

- brugerne af den sociale netværkstjeneste også bør mindes om, at de ved at uploade oplysninger om andre personer kan overtræde disses ret til privatlivets fred og databeskyttelse

- den sociale netværkstjeneste adviserer brugerne om, at hvis de ønsker at uploade billeder eller oplysninger om andre enkeltpersoner, skal dette ske med den pågældendes samtykke[13].

3.4 Følsomme oplysninger

Oplysninger, der afslører race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger, medlemskab af fagforeninger eller oplysninger om helbred eller seksualliv, betragtes som følsomme. Følsomme personoplysninger kan kun offentliggøres på internettet med den registreredes udtrykkelige samtykke, eller hvis den registrerede klart har offentliggjort oplysningerne.[14]

I nogle medlemsstater betragtes billeder af registrerede som en særlig kategori af personoplysninger, fordi de kan bruges til at skelne mellem race/etnisk oprindelse eller måske bruges til at udlede religiøse overbevisninger eller helbred. Arbejdsgruppen finder ikke, at billeder på internettet generelt udgør følsomme data[15], med mindre billederne klart bruges til at afsløre følsomme data om enkeltpersoner.

Sociale netværkstjenester kan som registeransvarlige ikke behandle følsomme data om medlemmer eller ikke-medlemmer uden disses udtrykkelige samtykke[16]. Såfremt en social netværkstjeneste i brugernes profilformularer modtager spørgsmål, der vedrører følsomme oplysninger, skal netværkstjenesten klart anføre, at besvarelsen af sådanne spørgsmål er helt frivillig.

3.5 Ikke-medlemmers behandling af oplysninger

Mange brugere af sociale netværkstjenester bidrager med oplysninger om andre mennesker, f.eks. ved at føje et navn til et billede, give en person karakter, opliste de "mennesker jeg har mødt/kunne tænke mig at møde" til arrangementer. Denne mærkning (tagging) kan ligeledes identificere ikke-medlemmer. De sociale netværkstjenesters behandling af sådanne oplysninger om ikke-medlemmer kan imidlertid kun ske, såfremt et af kriterierne i artikel 7 i direktivet om beskyttelse af personoplysninger er opfyldt.

---

[13] Dette kunne man gøre simplere ved at indføre værktøjer til kategoristyring (tagging) i sociale netværk, f.eks. ved at gøre områder i en personlig profil tilgængelige for at angive tilstedeværelsen af en brugers navn i mærkede (taggede) billeder eller videoer, der afventer godkendelse, eller ved at fastlægge udløbsfrister for tags, der ikke er blevet godkendt af den taggede person.

[14] Medlemsstaterne kan fastsætte undtagelser fra denne regel, jf. artikel 8, stk. 2, litra a), andet punktum, og artikel 8, stk. 4, i direktivet om beskyttelse af personoplysninger.

[15] Offentliggørelsen af billeder på Internettet giver imidlertid anledning til stigende bekymring omkring privatlivsbeskyttelse i takt med, at teknologierne til ansigtsgenkendelse bliver stadig bedre.

[16] samtykket skal være frit, informeret og specifikt

Desuden er der ikke noget retsgrundlag for oprettelse af pre-built profiler af ikke-medlemmer gennem aggregering af data, som brugerne af det sociale websted leverer uafhængigt, herunder kontaktoplysninger, der hentes fra uploadede adressebøger.[17]

Også selv om de sociale netværkstjenester skulle have midlerne til at kontakte ikke-brugeren og underrette denne om, at der foreligger personoplysninger om ham/hende, ville en eventuel e-mailinvitation til at blive medlem af den sociale netværkstjeneste med henblik på at få adgang til disse personoplysninger udgøre en overtrædelse af forbuddet i artikel 13, stk. 4, i e-datadirektivet, mod udsendelse af uopfordret elektronisk post som led i direkte markedsføring.

3.6 Tredjepartsadgang

3.6.1 Tredjepartsadgang formidlet af sociale netværkstjenester

Ud over den grundlæggende sociale netværksservice tilbyder de fleste sociale netværkstjenester brugerne yderligere applikationer leveret af andre udbydere, som også behandler personoplysninger.

Sociale netværkstjenester bør have de midler, der er nødvendige for at sikre, at tredjepartsapplikationer overholder bestemmelserne i direktivet om beskyttelse af personoplysninger og e-datadirektivet. Det indebærer især, at de leverer klar og specifik information til brugerne om behandling af deres personoplysninger, og at de kun har adgang til de personoplysninger, der er nødvendige. Derfor bør de sociale netværkstjenester tilbyde applikationsudbydere en flerdelt adgang, således at de kan vælge en adgangsmåde, der i sig selv er mere begrænset. Sociale netværkstjenester bør derudover sikre, at brugerne let kan indberette deres klager over applikationer.

3.6.2 Tredjepartsadgang formidlet af brugere

Sociale netværkstjenester tillader til tider brugerne at få adgang til og opdatere deres oplysninger med andre applikationer. F.eks. kan brugerne være i stand til at:

- læse og sende meddelelser til netværket fra deres mobiltelefon
- synkronisere deres venners kontaktoplysninger i det sociale websted med deres adressebog på en bærbar computer
- opdatere deres status eller position i det sociale websted automatisk ved at bruge et andet websted.

Den sociale netværkstjeneste offentliggør den måde, denne software kan skrives på i form af en "Application Programming Interface" ("API") (programmeringsinterface for applikationer). Det sætter tredjeparter i stand til at skrive software for at udføre disse opgaver, og tillade brugerne frit at vælge mellem flere forskellige tredjepartsleverandører[18]. Når en social netværkstjeneste tilbyder en API, der giver adgang til kontaktoplysninger, bør den:

---

[17] I betragtning 38 i direktivet om beskyttelse af personoplysninger hedder det: "en rimelig behandling af oplysninger forudsætter, at de registrerede kan få kendskab til en behandlings eksistens og, når der indsamles oplysninger hos dem, kan få nøjagtige og fyldestgørende oplysninger med hensyn til de nærmere omstændigheder ved indsamlingen." For nogle sociale netværks vedkommende synes offentliggørelse af profiler på ikke-medlemmer at være blevet en vigtig metode til markedsføring af deres "tjenester".

[18] Hvor "API" normalt er et bredt teknisk begreb, refererer API her til adgang på vegne af en bruger, dvs. brugerne vil skulle afgive deres login credentials til softwaren, således at den kan optræde på deres vegne.

- sørge for en grad af granularitet, der lader brugeren vælge et niveau for tredjepartens adgang, der lige netop er tilstrækkeligt til, at denne kan udføre en given opgave.

Når tredjepartstjenester skaffer sig adgang til personoplysninger via tredjepartens API på en brugers vegne, bør de:

- ikke behandle og lagre oplysninger i længere tid, end hvad der er nødvendigt for at udføre en given opgave;

- ikke udføre handlinger vedrørende importerede brugeres kontaktoplysninger til andet end den bidragende brugers personlige brug.

3.7 Lovgrundlag for direkte markedsføring

Direkte markedsføring er et væsentligt element i den sociale netværkstjenestes forretningsmodel; netværkstjenesten kan anvende forskellige markedsføringsmodeller. Imidlertid skal markedsføring, hvor der gøres brug af brugernes personoplysninger, overholde de relevante bestemmelser i både direktivet om beskyttelse af personoplysninger og e-datadirektivet[19].

Kontekstbaseret markedsføring er specifikt rettet mod indholdet, der ses eller tilgås af brugeren.[20]

Segmenteret markedsføring består i at levere reklamer til målrettede grupper af brugere[21]; en bruger indplaceres i en gruppe afhængigt af de oplysninger, han har kommunikeret direkte til den sociale netværkstjeneste[22].

Endelig vælges der ved *adfærdsbaseret markedsføring* de reklamer, der er baseret på observation og analyse af brugernes aktivitet over tid. Disse teknikker kan være underlagt forskellige retskrav, afhængigt af de forskellige lovgrundlag og de anvendte teknikkers karakteristika. Arbejdsgruppen anbefaler, at der ikke bruges følsomme oplysninger i adfærdsbaserede markedsføringsmodeller, med mindre alle lovgivningskrav er opfyldt.

Uanset hvilken model eller kombination af modeller, der anvendes, kan reklamer enten leveres direkte af den sociale netværkstjeneste (udbyderen af den sociale netværkstjeneste fungerer her som formidler) eller af en anden annoncør. I det første tilfælde behøver brugernes personoplysninger ikke at blive videregivet til tredjeparter. I det andet tilfælde kan den anden annoncør behandle personoplysninger om brugerne, f.eks. hvis den behandler brugerens IP- adresse og en cookie, der placeres på brugerens computer.

3.8 Lagring af data

Sociale netværkstjenester falder uden for definitionen af elektroniske kommunikationstjenester, som anført i artikel 2, litra c), i rammedirektivet (2002/21/EF). Udbydere af sociale netværkstjenester kan tilbyde yderligere tjenester, der falder ind under en elektronisk kommunikationstjeneste, såsom en offentligt tilgængelig e-mailtjeneste. En sådan tjeneste vil være omfattet af bestemmelserne i e-datadirektivet og direktivet om lagring af data.

---

[19] Arbejdsgruppen agter inden for den nærmeste fremtid at tage de forskellige aspekter af internetbaserede reklamer op i et separat dokument.

[20] f.eks. hvis den viste side omtaler ordet "Paris", kan reklamen vedrøre en restaurant i denne by

[21] hver enkelt gruppe defineres ved et sæt kriterier

[22] f.eks. da han blev registreret hos tjenesten

Nogle sociale netværkstjenester tillader deres brugere at sende invitationer ud til tredjeparter. Forbuddet mod brug af elektronisk post med henblik på direkte markedsføring finder ikke anvendelse på personkommunikation. For at være i overensstemmelse med undtagelsen for personkommunikation skal en social netværkstjeneste overholde følgende kriterier:

- der må ikke gives hverken afsender eller modtager nogen tilskyndelse
- udbyderen må ikke vælge modtagerne af meddelelsen[23]
- den afsendende brugers identitet skal være klart angivet
- den afsendende bruger skal kende det fulde indhold af meddelelsen, der vil blive sendt på hans vegne.

Nogle sociale netværkstjenester lagrer ligeledes identifikationsdata for brugere, der er blevet forment adgang til tjenesten, for at sikre at de ikke kan tilmelde sig igen. I det tilfælde skal disse brugere være informeret om, at en sådan behandling finder sted. Derudover er de eneste oplysninger, der må lagres, identifikationsoplysninger og ikke oplysninger om grunden til, at de er blevet forment adgang. Disse oplysninger bør ikke lagres i mere end et år.

Personoplysninger, der meddeles en bruger, når han tilmelder sig en social netværkstjeneste, bør slettes, så snart enten brugeren eller udbyderen af den sociale netværkstjeneste beslutter at slette kontoen[24]. Tilsvarende bør der ikke lagres oplysninger, der slettes af en bruger, når han opdaterer sin konto. Sociale netværkstjenester bør advisere brugerne, før de tager sådanne skridt med de midler, de har til deres rådighed for at informere brugerne om disse opbevaringsperioder. Af sikkerhedsmæssige og juridiske årsager kan det i særlige tilfælde være berettiget at gemme opdaterede eller slettede data og konti i et nærmere defineret tidsrum med det formål at forhindre misbrug som følge af identitetstyveri og andre lovovertrædelser eller kriminelle handlinger.

Når en bruger ikke bruger tjenesten i en nærmere angivet periode, bør profilen sættes som inaktiv, dvs. at den ikke længere er synlig for andre brugere eller for omverdenen, og efter yderligere et tidsrum bør dataene i den inaktive konto slettes. Sociale netværkstjenester bør advisere brugerne, inden de tager disse skridt med de midler, de måtte have til deres rådighed.

3.9 Brugerrettigheder

Sociale netværkstjenester bør overholde de pågældende personers rettigheder ved behandling i overensstemmelse med bestemmelserne i artikel 12 og artikel 14 i direktivet om beskyttelse af personoplysninger.

Brugernes rettigheder med hensyn til at få adgang til og korrigere oplysninger er ikke begrænset til brugere af tjenesten, men i det hele taget til alle fysiske personer, hvis oplysninger behandles[25]. Medlemmer og ikke-medlemmer af sociale netværkstjenester skal have midlerne til at udøve deres ret til at få adgang til at korrigere og slette oplysninger. Der skal på de sociale websteder være en tydelig reference til eksistensen af en

---

[23] dvs. nogle udbyderes praksis med at sende invitationer vilkårligt ud til hele en brugers adressebog er ikke tilladt

[24] I henhold til artikel 6, stk. 1, litra e) i direktivet om beskyttelse af personoplysninger må personoplysninger "ikke opbevares på en måde, der giver mulighed for at identificere de registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de indsamles, eller i forbindelse med hvilke de behandles på et senere tidspunkt."

[25] f.eks. er det tilfældet, hvis denne persons e-mailadresse er blevet brugt af den sociale webtjeneste til at sende ham en invitation

"klagebehandlingsinstans" oprettet af udbyderen af sociale netværkstjenester, der skal beskæftige sig med spørgsmål og klager fra både medlemmer og ikke-medlemmer om databeskyttelse og privatlivets fred.

I henhold til artikel 6, stk. 1, litra c), i direktivet om beskyttelse af personoplysninger skal personoplysninger være *"relevante og tilstrækkelige og ikke omfatte mere end, hvad der kræves til opfyldelse af de formål, hvortil de indsamles, og til de formål, hvortil de senere behandles"*. I den forbindelse kan det bemærkes, at sociale netværkstjenester kan have behov for at registrere visse identifikationsoplysninger om medlemmerne, men ikke behøver at offentliggøre medlemmernes rigtige navne på internettet. Derfor bør disse netværkstjenester nøje overveje, om de kan retfærdiggøre at tvinge deres medlemmer til at optræde under deres virkelige identitet og ikke under et pseudonym. Der er stærke argumenter for at give brugerne valget i denne henseende, og i mindst én medlemsstat har brugerne juridisk krav på at få valgmuligheden. Disse argumenter har særlig vægt for sociale netværk med et bredt medlemsgrundlag.

I henhold til artikel 17 i direktivet om beskyttelse af personoplysninger skal den registeransvarlige iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger. Især omfatter sådanne sikkerhedsforanstaltninger adgangskontrol og godkendelsesmekanismer, der kan gennemføres, også selv om der anvendes pseudonymer.

4. Børn og mindreårige

Sociale netværk bruges for en stor dels vedkommende af børn/mindreårige. Arbejdsgruppens udtalelse nr. WP147[26] fokuserede på anvendelsen af principperne for databeskyttelse i skole- og uddannelsesmiljøet. Udtalelsen understregede behovet for at tage hensyn til barnets tarv, som også fastlagt i FN's Konvention om Barnets Rettigheder. Arbejdsgruppen ønsker at understrege vigtigheden af dette princip også i relation til sociale netværkstjenester. Der er taget nogle interessante initiativer[27] af datatilsynsmyndigheder i hele verden, der primært fokuserer på at skabe bevidsthed omkring sociale netværkstjenester og mulige risici. Arbejdsgruppen tilskynder til yderligere undersøgelser af mulige løsninger på problemerne med tilstrækkelig aldersverifikation og bevis for informeret samtykke.

Arbejdsgruppen finder med udgangspunkt i de hidtidige overvejelser, at beskyttelse af børns personoplysninger i forbindelse med sociale netværkstjenester bedst sikres med en flerstrenget strategi. Denne strategi kunne tage udgangspunkt i:

- oplysningsinitiativer, der er afgørende for at sikre, at børn inddrages aktivt (i skolerne, ved at lade edb på grundniveau indgå i læseplanerne, ved at udforme ad hoc-uddannelsesværktøjer, gennem samarbejde mellem kompetente nationale organer)

- fair og lovlig behandling af personoplysninger i forhold til mindreårige, f.eks. ved ikke at bede om følsomme oplysninger i tilmeldingsformularerne, ingen direkte markedsføring specifikt rettet mod mindreårige, indhentning af forældrenes samtykke inden tilmeldingen, og en passende grad af logisk adskillelse mellem netværk for børn og netværk for voksne

- gennemførelse af privatlivsfremmende teknologier (PET) – f.eks. privatlivsvenlige standardindstillinger, pop-up-advarselsbokse på passende trin, software for aldersverifikation)

---

[26] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf.

[27] F.eks. det portugisiske "Dadus"-initiativ http://dadus.cnpd.pt/, den danske chatmærkeordning, http://www.fdim.dk/.

- selvregulering fra udbydernes side med henblik på at tilskynde til vedtagelsen af retningslinjer for god praksis (codes of practice) med effektive håndhævelsesforanstaltninger, der også indebærer disciplinære sanktioner

- om nødvendigt lovgivningsmæssige ad hoc-foranstaltninger, der skal modvirke unfair og/eller vildledende praksis inden for rammerne af sociale netværkstjenester.

5. Oversigt over forpligtelser/rettigheder

Anvendelse af EU's direktiver

1. Direktivet om beskyttelse af personoplysninger finder generelt anvendelse på sociale netværkstjenesters behandling af personoplysninger, også på tjenester med hovedsæde uden for EØS.

2. Udbydere af sociale netværkstjenester er dataregisteransvarlige i medfør af direktivet om beskyttelse af personoplysninger.

3. Applikationsudbydere kan betragtes som dataregisteransvarlige i medfør af direktivet om beskyttelse af personoplysninger.

4. Brugerne betragtes som registrerede i forhold til sociale netværkstjenesters behandling af deres personoplysninger.

5. Brugernes behandling af personoplysninger falder i de fleste tilfælde ind under undtagelsen ved udøvelse af familiemæssige aktiviteter. Der er tilfælde, hvor en brugers aktiviteter ikke falder ind under denne undtagelse.

6. Sociale netværkstjenester falder uden for definitionen af elektronisk kommunikationstjeneste, og direktivet om lagring af data finder således ikke anvendelse på sociale netværkstjenester.

Sociale netværkstjenesters forpligtelser

7. Sociale netværkstjenester bør informere deres brugere om deres identitet og levere omfattende og klare oplysninger om formålene og om de forskellige måder, hvorpå de har til hensigt at behandle personoplysninger.

8. Sociale netværkstjenester bør tilbyde privatlivsvenlige standardindstillinger.

9. Sociale netværkstjenester bør levere information og passende advarsler til brugerne om risici for privatlivets fred, når de uploader oplysninger til netværket.

11. Brugerne bør af den sociale netværkstjeneste adviseres om, at billeder eller oplysninger om andre personer kun bør uploades med den pågældende persons samtykke.

12. Det sociale websted bør som minimum indeholde et link til en klagebehandlingsmyndighed med oplysninger om forhold vedrørende beskyttelse af personoplysninger til brug for både medlemmer og ikke-medlemmer.

13. Markedsføringsaktiviteter skal overholde reglerne i direktivet om beskyttelse af personoplysninger og e-datadirektivet.

14. Sociale netværkstjenester skal fastsætte maksimumtidsfrister for lagring af oplysninger om inaktive brugere. Inaktive konti skal slettes.

15. For så vidt angår mindreårige, bør sociale netværkstjenester træffe passende foranstaltninger til begrænsning af risiciene.

<u>Brugerrettigheder</u>

16. Både medlemmer og ikke-medlemmer af sociale netværkstjenester har i det konkrete tilfælde rettigheder som registrerede i medfør af bestemmelserne i artikel 10 – 14 i direktivet om beskyttelse af personoplysninger.

17. Både medlemmer og ikke-medlemmer bør have adgang til en klagebehandlingsprocedure, der er let at bruge, og som netværkstjenesten etablerer.

18. Brugerne bør generelt have mulighed for at anvende et pseudonym.

Udfærdiget i Bruxelles, den 12. juni 2009

På gruppens vegne

Alex TÜRK
Formand