ERHVERVSSTYRELSEN

Blip Systems A/S
Hækken 2
Vester Hassing
9310 Vodskov

26. marts 2015
Sag
/JV

ERHVERVSSTYRELSEN
Dahlerups Pakhus
Langelinie Allé 17
2100 København Ø

Tlf. 35 29 10 00
Fax 35 29 10 01
CVR-nr 10 15 08 17
E-post erst@erst.dk
www.erst.dk

ERHVERVS- OG
VÆKSTMINISTERIET

Afgørelse
Erhvervsstyrelsen finder ikke, at systemet Bliptrack's indsamling af MAC-adresser fra brugeres terminaludstyr er omfattet af kravet om afgivelse af information og indhentelse af samtykke fra slutbrugeren i § 3, stk. 1, i bekendtgørelse om krav til information og samtykke ved lagring eller adgang til oplysninger i slutbrugerens terminaludstyr ("cookiebekendtgørelsen").

Sagsfremstilling
Den 26. januar 2015 modtog Erhvervsstyrelsen en henvendelse fra Blip Systems A/S, om, hvorvidt virksomhedens løsning for trafikmåling Bliptrack er omfattet af reglerne i "cookiebekendtgørelsen", samt hvad virksomheden i bekræftende fald ville kunne gøre anderledes for at undgå, at løsningen overtrådte lovgivningen.

Bliptrack
Blip Systems A/S' trafikovervågningssystem (Bliptrack) registrerer, hvor mange bilister der er på en given vej på et givent tidspunkt (og hvor lang deres transporttid mellem to målepunkter er).

Systemet anvendes bl.a. af en del kommuner med kraftig myldretidstrafik til at registrere, hvor tæt trafikken er forskellige steder på forskellige tidspunkter.

Det konkrete systems formål er primært at nedbringe transporttider og benzinforbrug i tættere bebyggede områder, men ikke til at spore de enkelte registrerede personers færden.

Løsningen fungerer ved, at en enhed placeret ved vejen registrerer, hvor mange mobiltelefoner eller andre terminalenheder, der passerer.

Når samme terminalenhed passerer det andet målepunkt, hvor en anden antenneenhed er placeret, opfanges MAC-adressen igen, og systemet kan, ved at se på tidspunkterne, hvor den samme MAC-adresse registreres af de to antenner, udregne trafikantens hastighed (og dermed f.eks. konstatere om, der er kødannelse på vejen).

Registreringen sker ved anvendelse af to teknologier; Wifi og Bluetooth.

Wifi-registreringen foregår ved, at Bliptrack-enheden indeholder et wifi-modul, som lytter efter enheder i nærheden, der forsøger at opnå kontakt til skjulte wifi-net (poller). Dette sker passivt, idet wifi-modulet, uden selv at tilkendegive

sin eksistens, blot opfanger de signaler, som brugernes terminaler udsender for at opnå kontakt med wifi-net i nærheden. I dette signal indgår den enkelte terminals MAC-adresse, som er den identifikator, som systemet benytter til at fastslå, hvor mange forskellige enheder der passerer.

Bluetooth-registreringen foregår ved, at Bliptrack-enhedens bluetooth-modul kontinuerligt udsender et signal på alle tilgængelige kanaler, hvor den annoncerer sin tilstedeværelse overfor andre bluetooth-enheder i nærheder. Denne annoncering er ikke rettet mod nogen specifik enhed.

Bliptrack-sensoren fungerer som master-enhed. Andre Bluetooth-enheder, som befinder sig i nærheden, vil, hvis de er slået til og af brugeren er konfigureret til at være i "Discoverable Mode", opfange master-enhedens signal, og give sig til kende som slave-enhed overfor master-enheden. I forbindelse med denne handling, vil slave-enheden bl.a. sende sin MAC-adresse til master-enheden (Bliptrack) med henblik på at oprette forbindelse. Bliptrack-sensoren opretter ikke forbindelse til de enheder, som giver sig til kende, men registrerer kun slave-enhedens MAC-adresse.

Bliptrack indsamler således MAC-adresser på de forbipasserende enheder, som via deres indstillinger er sat til enten automatisk at søge (polle) efter wifi-net i nærheden eller at give sig til kende og acceptere forbindelse via Bluetooth (ofte blot kendetegnet ved, at Bluetooth er "slået til"). Men hvor Bliptrack i forbindelse med wifi kun passivt lytter efter terminalernes egen udsendelse af MAC-adresser, initierer systemet ved anvendelse af Bluetooth selv den kommunikation, som leder til, at brugerens terminalenhed udleverer sin MAC-adresse.

Bliptrack hasher de indsamlede data efter en tilfældig algoritme i sensoren og data sendes krypteret til en central server. Efter denne hashing er det ikke længere muligt at gå tilbage og udlede den reelle MAC-adresse.

Efter 24 timer ændres algoritmen, som beregner hashværdien, automatisk, hvorefter det ikke længere er muligt at identificere og overvåge slutbrugeren og dennes handlingsmønster på baggrund den hashede værdi.

Lovgrundlag
Området er reguleret af det fælleseuropæiske e-databeskyttelsesdirektiv[1].

Det primære beskyttelseshensyn bag direktivets regler fremgår blandt andet af betragtning 24 i præamblen til det oprindelige e-databeskyttelsesdirektiv:

"Terminaludstyr for brugere af elektroniske kommunikationsnet og alle oplysninger der er lagret på et sådant udstyr, er en del af brugernes privatsfære, der kræver beskyttelse i henhold til den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder. Såkaldt spionsoft-

[1] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation)

ware, såkaldte web bugs, skjulte identifikatorer og andre tilsvarende anordninger kan komme ind i brugerens terminal uden dennes viden for at skaffe adgang til oplysninger, for at lagre skjulte oplysninger eller for at spore brugerens aktiviteter og kan alvorligt krænke brugerens privatliv. Brugen af sådanne anordninger til andet end lovlige formål bør kun være tilladt med de pågældende brugeres viden.
På baggrund af dette fremgår det af det reviderede direktivs art. 5, stk. 3, at:

"Medlemsstaterne sikrer, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har afgivet sit samtykke hertil efter i overensstemmelse med direktiv 95/46/EF at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen."

Bestemmelsen er implementeret i dansk lovgivning i "cookiebekendtgørelsens § 3, stk. 1, som lyder:

"Fysiske eller juridiske personer må ikke lagre oplysninger eller opnå adgang til oplysninger, der allerede er lagret, i en slutbrugers terminaludstyr eller lade tredjepart lagre oplysninger eller opnå adgang til oplysninger, hvis slutbrugeren ikke giver samtykke hertil efter at have modtaget fyldestgørende information om lagringen af eller adgangen til oplysningerne."

Vurdering
Som beskrevet under sagsfremstillingen indsamler Bliptrack både aktivt og passivt MAC-adresser[2].

Som nævnt er formålet med e-databeskyttelsesdirektivet blandt andet at forebygge uberettiget krænkelse af brugernes privatsfære ved anvendelse af elektronisk kommunikation.

I forhold til cookiereglerne, er det Erhvervsstyrelsens vurdering, at reglerne har til formål at undgå, at brugernes færden – fysisk såvel som elektronisk – kan overvåges uden samtykke fra de overvågede, når de bevæger sig i den digitale verden. Det er imidlertid ikke kun brugerens egen fysiske færden, der skal beskyttes. Det følger af e-databeskyttelsesdirektivets betragtninger, at brugerens terminaludstyr er forbundet til brugeren på en sådan måde, at også udstyret bliver en del af privatsfæren. Dette skyldes, at den enkelte bruger i høj grad kan identificeres gennem sit terminaludstyr, idet adresser, historik, indstillinger og anden information effektivt forbinder terminalen til en specifik bruger, som herigennem identificeres.

[2] Nummeret er lagret i udstyret, og hvis man, med et andet formål end at kommunikere direkte, henter dette nummer på brugerens udstyr, er der tale om, at man opnår adgang til allerede lagrede oplysninger. Derved bliver MAC-adresser omfattet af "cookie-reglerne", der er teknologineutrale. Dette er fastslået på europæisk niveau.

Hvis terminaludstyret ikke kan identificeres, kan det ikke kædes sammen med en bruger, som derved ikke vil opleve et indgreb i sin privatsfære, idet brugeren ikke kan identificeres.

I tilfælde hvor systemer ikke kan anvendes til at identificere og overvåge den enkelte slutbrugers færden, vil der ikke være grundlag for at anvende direktivets bestemmelse om information og indhentelse af samtykke på dette forhold, idet der ikke længere er et beskyttelseshensyn i forhold til lagring eller indsamling af information på terminalenheden.

Dette medfører, at privatlivsbeskyttelsen, som direktivets regler skal varetage, allerede fra starten er indbygget i selve løsningen, og den konkrete løsning falder derfor udenfor direktivets anvendelsesområde

En direkte parallel til dette princip findes i persondatabeskyttelsesdirektivet[3], hvorefter anonymiserede personoplysninger falder udenfor direktivets anvendelsesområde, idet der ved anonymiseringen ikke længere eksisterer et beskyttelsesformål.

Efter en konkret vurdering af Bliptracks enkelte elementer er det Erhvervsstyrelsens opfattelse, at systemet ikke giver mulighed for at identificere terminaludstyret eller slutbrugeren og at systemet derfor ikke er omfattet af kravet om afgivelse af information og indhentelse af samtykke i "cookiebekendtgørelsens" § 3, stk. 1, idet data ikke vil kunne anvendes til at overvåge eller følge en bruger på en måde, som udgør et indgreb i dennes privatsfære.

Erhvervsstyrelsen har ved vurderingen lagt vægt på, at Bliptrack ikke har mulighed for at kommunikere direkte med brugerne, hvilket i praksis gør det umuligt at informere brugerne og indhente deres samtykke.

Erhvervsstyrelsen har herudover særligt lagt vægt på, at Bliptrack øjeblikkeligt hasher og krypterer (anonymiserer) de MAC-adresser som systemet indsamler, og at det herefter, selv med hjælp af alle rimelige hjælpemidler, ikke vil være muligt at finde tilbage til den oprindelige MAC-adresse.

Algoritmen, hvormed systemet hasher MAC-adresserne, udskiftes desuden tilfældigt efter 24 timer, hvorefter det ikke længere vil være muligt at overvåge den anonymiserede MAC-adresse, idet hashværdien af MAC-adressen ikke længere er den samme.

Erhvervsstyrelsen vurderer, at denne metode til anonymisering af data umiddelbart er effektiv og reelt umuliggør en efterfølgende identifikation af udstyret.

Erhvervsstyrelsen finder derfor ikke, at systemet Bliptracks indsamling af MAC-adresser fra brugeres terminaludstyr er omfattet af kravet om afgivelse af

[3] Direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger

information og indhentelse af samtykke fra slutbrugeren i § 3, stk. 1 i "cookie-bekendtgørelsen".

Erhvervsstyrelsen bemærker i øvrigt, at systemets eventuelle behandling af persondata, skal ske i overensstemmelse med reglerne i persondataloven.[4]

[4] Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger