Datatilsynet

Endelig kontrollrapport		
Saksnummer: 14/00030 Dato for kontroll: 31.01.2014 Rapportdato: 13.05.2014	Kontrollobjekt: Pixima AS Sted: Drammen	Utarbeidet av: Andreas Jensen Hofstad Marius Engh Pellerud

1 Innledning

Datatilsynet gjennomførte kontroll hos Pixima 31. januar 2014. Kontrollen ble utført med hjemmel i personopplysningsloven § 44, jf. § 42, 3. ledd.

Temaet for kontrollen var virksomhetens behandling av personopplysninger, særlig i forbindelse med de oppgaver Pixima gjør som databehandler for bensinstasjoner. Datatilsynet ønsket særlig å belyse de databehandleravtaler Pixima har med sine oppdragsgivere og hvordan Pixima følger opp disse avtalene, spesielt hva gjelder internkontroll og informasjonssikkerhet, herunder rutiner for retting og sletting av personopplysninger. Kontrollen fant sted ved virksomhetens faste forretningsadresse.

I det følgende vil Datatilsynet beskrive de faktiske forhold som ble avdekket under kontrollen. Kontrollrapporten danner grunnlag for Datatilsynets vurderinger og eventuelle pålegg.

2 Tilstede under kontrollen

2.1 Fra virksomheten:

- Stein Erik Larsen, daglig leder
- Odd Kjelsberg, ansvarlig for utvikling

2.2 Fra Datatilsynet:

- Andreas Jensen Hofstad, rådgiver, juridisk avdeling
- Marius Engh Pellerud, rådgiver, tilsyns- og sikkerhetsavdelingen

3 Generelt

Pixima AS ble etablert i 2005 og leverer videoanalysetjenester til bensinstasjoner for å håndtere pumpeavstikk. Pumpeavstikk innebærer at personer fyller drivstoff på bensinstasjon uten å betale. I de fleste tilfeller kommer pumpeavstikk av forglemmelse, men også tyveri av bensin omtales som pumpeavstikk. Pixima gjør slike tjenester for 100 bensinstasjoner i Norge. Selskapet holder til i Drammen.

4 Kort om bruk av personopplysninger samt formålet med behandlingene

Det er bensinstasjonen selv som melder fra om at et pumpeavstikk har forekommet. Pixima kan få melding om pumpeavstikk umiddelbart, i løpet av noen timer eller dagen etter. I noen tilfeller er meldingen om pumpeavstikk automatisert, mens det i andre tilfeller er en manuell jobb.

Pixima har i mange tilfeller online tilgang til bensinstasjonens videoserver. I mange bensinstasjoner genereres melding om pumpeavstikk fra kassesystemet og legges automatisk på videoserveren. Pixima henter så opp den elektroniske kassebongen fra videoserveren. Dette skjer ofte dagen etter at pumpeavstikket har skjedd. Pixima henter samtidig opp videoovervåkningen fra bensinstasjonens kameraovervåkningssystem for noen minutter før og etter pumpeavstikket fant sted, og lagrer videomaterialet på sin server. Pixima analyserer så videomaterialet. I noen tilfeller gjør betjeningen ved bensinstasjonen en beskrivelse av bilen eller hendelsen. Dette gjøres noen ganger på kassebongen, mens i noen tilfeller sendes slike beskrivelser på e-post til Pixima.

Pixima tar ut opp til fire stillbilder fra videomaterialet og lagrer disse sammen med andre opplysninger om det enkelte pumpeavstikk som grunnlag for kravet som sendes ut. Pixima benytter sitt eget saksbehandlingssystem, basert på Microsoft Access. Alt bilde- og videomateriale ut over stillbildene slettes automatisk fra deres server når det har gått 30 dager fra opptaket ble gjort.

Etter å ha identifisert et bilskilt, eller andre identifiserende kjennetegn ved en bil, og deretter eier av bilen, sender Pixima normalt en beskjed til et innkrevingsselskap, hovedsakelig KredittGjenvinning AS. Beskjeden inneholder detaljer om pumpeavstikket: antall liter, beløp, tidspunkt og navn og adresse på bilens eier. Innkrevingsselskapet sender deretter brev til bilens eier med en redegjørelse for at det har blitt fylt bensin som ikke ble betalt, og med en vennlig oppfordring til å gjøre opp det utestående beløpet. I noen få tilfeller sender Pixima selv brevet til bilens eier, på vegne av den behandlingsansvarlige og i dennes navn.

Kravene gjøres opp enten direkte til den behandlingsansvarlige eller til innkrevingsselskapet. Pixima har altså ikke ansvar for inndrivelse av kravene.

Alle pumpeavstikkene som har skjedd hos Piximas kunder siden Pixima startet med sin virksomhet i 2006 ligger lagret i deres database. For alle hendelsene som er eldre enn tre år er navn og adresse på bileieren fjernet, men registreringsnummeret og andre omstendigheter rundt pumpeavstikket lagres.

5 Funn og avvik fra lovbestemte krav til behandling av personopplysninger

5.1 Behandlingsansvaret

5.1.1 Pixima som databehandler

En databehandler er den som behandler personopplysninger på vegne av en behandlingsansvarlig, jf. personopplysningsloven § 2 nummer 5. Under den stedlige kontrollen framkom det at Pixima ser på seg selv som en databehandler mens kunden er behandlingsansvarlig. Datatilsynet slutter seg til at Pixima primært vil ha rollen som databehandler for personopplysninger som er relevante for denne kontrollen.

En databehandler skal normalt ikke forholde seg direkte til personopplysningslovens krav, men til de behandlingsregler som oppstilles i databehandleravtalen. Bestemmelsene i

personopplysningsloven § 13 om informasjonssikkerhet og § 15 om databehandleravtaler får allikevel direkte anvendelse for databehandlere.

Virksomheten redegjorde for at ca. halvparten av deres kunder har et selvstendig behandlingsansvar, fordi det dreier seg om franchise-takere, mens den andre halvparten eies og drives fra sentralt hold i de forskjellige bensinstasjonkjedene. I den sistnevnte andelen er mange stasjoner organisert under én behandlingsansvarlig virksomhet. Piximas oversikt over kundeforholdene deres viser at de har 39 ulike behandlingsansvarlige kunder. Se vedlagte kundeoversikt.

Datatilsynet har ikke i denne kontrollen vurdert kravene i personopplysningsloven opp mot de behandlingsansvarlige, når det gjelder kameraovervåkning og bruken av videomateriale til ulike formål. Vi antar likevel at å forebygge og avsløre tyverier er et legitimt og lovlig formål for kameraovervåkning på en bensinstasjon, og at å kreve inn penger fra kunder som av ulike årsaker ikke betaler for bensin er forenlig med dette formålet, jf. personopplysningsloven § 11 jf. §§ 8 og 9. Vi går ikke nærmere inn på disse vurderingene i denne saken.

Spørsmålet blir da om Pixima har gyldig grunnlag for å behandle opplysninger om pumpeavstikk i avtalene med sine oppdragsgivere, og om disse avtalene oppfyller kravene til en databehandleravtale jf. personopplysningsloven § 15. Se nedenfor i punkt 5.2.

5.1.2 Behandling for eget formål

5.1.2.1 Lovens krav

I den grad Pixima behandler personopplysninger for sitt eget formål vil de kunne ha et selvstendig behandlingsansvar. Dette medfører at det må finnes et gyldig behandlingsgrunnlag etter personopplysningsloven § 8, og dersom opplysningene som behandles regnes som sensitive, jf. personopplysningsloven § 2 nummer 8, må også et av vilkårene i § 9 være oppfylt. Definisjonen § 2 nummer 8 bokstav b nevner at «opplysninger om at en person er mistenkt (…) for en straffbar handling» regnes som sensitive.

Videre vil det normalt foreligge konsesjonsplikt for behandling av sensitive personopplysninger, jf. personopplysningsloven § 33.

5.1.2.2 Funn

Under kontrollen ble det sagt at hovedvekten av Piximas saker består i at en person glemmer å betale for bensin, men at en ikke ubetydelig andel (ca 20 % av bensinen som ikke blir betalt) regnes som tyverier. Det ble også sagt at Pixima gir anbefalninger til kundene sine om hvorvidt de bør anmelde forholdet eller ikke, basert på sin egen oppfatning om hvorvidt et enkelttilfelle er et tyveri eller en forglemmelse. Denne vurderingen gjøres blant annet på bakgrunn av hvorvidt bilen er en gjenganger og av omstendighetene ved de tidligere sakene hvor denne bilen har vært involvert. Vi viser her også til tjenesteavtalene mellom Pixima og deres kunder, som spesifiserer at beslutningen om hvorvidt det skal foretas en politianmeldelse gjøres i samråd mellom bensinstasjonen og Pixima.

Pixima understreket at det er opp til bensinstasjonene å avgjøre om et tilfelle skal anmeldes, også i de tilfeller hvor det sannsynligvis har skjedd et tyveri. Derfor er den vanlige rutinen at

alle pumpeavstikk behandles som om de var forglemmelser eller unnskyldelige feil og at alle tilfeller derfor håndteres på samme måte – med fakturautsendelse. Dette poenget har Pixima også fremhevet i sitt tilsvar til foreløpig kontrollrapport.

Datatilsynet er inneforstått med at virksomheten ikke lagrer anmeldelsene og at deres vurdering av om den enkelte sak er et tyveri ikke nedtegnes skriftlig. Likevel er det slik at en andel av sakene faktisk blir vurdert som tyverier og resulterer i politianmeldelse. Det er også slik at Pixima lagrer de faktaopplysningene som skaper mistanken om straffbare forhold. Datatilsynets standpunkt er derfor at databasen inneholder sensitive personopplysninger i noen av sakene.

Selv om en skulle komme til at dataene faller utenfor definisjonen i § 2 nummer 8 bokstav b, så vil summen av opplysninger som behandles i databasen være beskyttelsesverdige på linje med sensitive opplysninger. Dermed må for eksempel både informasjonssystemet og databehandleravtalene uansett innrettes etter at det vil bli behandlet personopplysninger med stort behov for konfidensialitetsbeskyttelse.

På Piximas nettside reklamerer de med at de «kan holde en svært god oversikt over notoriske gjengangere», og at de har «oppnådd svært gode resultater i forhold til å få pådømt gjengangere». Videre står det at «[v]år verdi av databasen øker proporsjonalt med antall stasjoner og antall pumpeavstikk».

Datatilsynet ba derfor under kontrollen om at Pixima redegjorde for hvordan de håndterer opplysninger om gjengangere. Vi har valgt å kalle dette «gjengangertjenesten».

Pixima vurderer det slik at de kun behandler gjengangeropplysningene på vegne av hver enkelt kunde. Likevel var systemene deres lagt opp slik at når en ny sak kom inn så viste databasen deres hvor mange ganger samme bil hadde vært involvert i en sak tidligere – uavhengig av hvilken bensinstasjon det tidligere pumpeavstikket hadde funnet sted. Med andre ord knyttes hvert enkelt pumpeavstikk til en bensinstasjon, men alle pumpeavstikkene vises i samme grensesnitt i Piximas saksbehandlingssystem. Pixima forklarte at antallet tidligere saker, samt hva som var hendelsesforløpet i disse sakene, brukes som grunnlag for å vurdere om saken bør anmeldes eller ikke. Det er Pixima som gir råd til sine kunder om hvorvidt sakene bør anmeldes eller ikke.

Et eksempel ble også nevnt, hvor en bestemt bil hadde blitt observert i forbindelse med pumpeavstikk fra flere ulike bensinstasjoner, men hvor eieren systematisk fjernet skiltene fra bilen før han kjørte inn på bensinstasjonen. Opplysninger om pumpeavstikkene ble registrert, men Pixima greide ikke å finne ut hvem som var bilens eier. Ved en tilfeldighet ble en bensinstasjon varslet av en kunde om hvilket registreringsnummer det var på den aktuelle bilen, fordi kunden hadde observert dette i forbindelse med av- eller påmontering av skiltene. Dermed kunne Pixima identifisere bilens eier i alle tilfellene av tyveri hvor denne bilen hadde vært involvert.

5.1.2.3 Datatilsynets vurdering og konklusjon

Det å sammenholde informasjon fra ulike pumpeavstikk på forskjellige bensinstasjoner, å bruke disse til å identifisere gjengangere, og deretter gi råd til bensinstasjonen om de bør anmelde saken eller ikke, er en bruk av opplysningene som hver enkelt bensinstasjon ikke har myndighet til å beslutte. Tjenesten er kun teknisk mulig å tilby så lenge Pixima samler flere kunders pumpeavstikk i samme database. I realiteten innebærer det at de benytter sine kunders data til sitt eget rådgivningsformål. Datatilsynet vurderer det derfor slik at Pixima har behandlingsansvar for denne bruken av opplysningene.

Når det gjelder gjengangertjenesten så foreligger det i de en del tilfeller mistanke om tyveri. Dermed er det snakk om sensitive personopplysninger om personer som ikke har noe kundeforhold til Pixima. Dette krever konsesjon etter personopplysningsloven § 33. Datatilsynets foreløpige konklusjon er at det ikke foreligger et gyldig behandlingsgrunnlag for denne behandlingen, jf. personopplysningsloven §§ 8 og 9. Vi viser i denne sammenheng også til både skriftlig saksbehandling (vår referanse 05/01656) og veiledning under et møte i 2006, som nevnt nedenfor.

5.1.2.4 Merknader til tidligere dialog mellom Pixima og Datatilsynet

Vi vil for ordens skyld kommentere hendelsesforløpet fra 2006 nærmere. Pixima søkte Datatilsynet om en tillatelse til opprettelsen av en felles database for pumpeavstikk-gjengangere. Registeret hadde det formål å sammenstille data om pumpeavstikk fra ulike bensinstasjoner for bedre å kunne identifisere og forfølge personer som gjentatte ganger stjeler bensin. Pixima skisserte at det var nødvendig med lagring i 12 måneder for dette formålet. Datatilsynet avslo søknaden.

I et etterfølgende møte, som Pixima har referert, ble gjengangertjenesten diskutert nærmere. Datatilsynet understreket, i følge Piximas referat, at det ikke under noen omstendighet vil være tillatt å samkjøre data eller la data om pumpeavstikk fra én behandlingsansvarlig bensinstasjon tilflyte en annen. Videre er det referert at de ulike behandlingsansvarlige ikke måtte få direkte innsyn i databasen. Pixima erklærer også i referatet at de ikke vil «utføre noe etterbehandling eller sammenstilling eller utføre andre aktiviteter av noe slag som tillegger politiet». Datatilsynet uttrykte videre, i følge referatet, at opplysninger fra et pumpeavstikk kunne beholdes inntil saken var oppgjort.

5.2 Databehandleravtaler

5.2.1 Lovens krav

En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige, jf. personopplysningsloven § 15. En behandlingsansvarlig kan heller ikke, uten slik avtale, overlate personopplysninger til en databehandler.

En databehandleravtale skal etablere instruksjonsmyndighet mellom to rettssubjekter som i utgangspunktet er innbyrdes uavhengige. Formålet er å gjøre den behandlingsansvarliges rutiner gjeldende i databehandlerens virksomhet, for å sikre at personopplysningslovens bestemmelser etterleves ved behandlingen. Databehandleravtalen er å anse som en nødvendig

del av den behandlingsansvarliges internkontrollsystem, jf personopplysningsforskriftens § 3-1 siste ledd. For databehandleren representerer avtalen det rettslige grunnlaget for behandlingen; den skal angi rammene for behandlingen og oppstille nærmere behandlingsregler. Manglende eller mangelfull databehandleravtale medfører en uakseptabel risiko for at personopplysningslovens øvrige bestemmelser ikke blir etterlevd ved behandlingen.

Hvilke konkrete krav som stilles til databehandleravtalens form og nærmere innhold, avhenger av den aktuelle behandlingens formål og omfang, og av opplysningenes art.

5.2.2 Funn

Det som finnes av avtaler mellom Pixima og de behandlingsansvarlige er tjenesteavtalene. Disse beskriver Piximas oppdrag og hvilken betaling Pixima skal ha for sine tjenester. Det finnes to typer tjenesteavtale: "Pixima Premium" og "Pixima Light".

Pixima Premium

Oppdraget som Pixima skal utføre er relativt godt beskrevet i tjenesteavtalen, slik som beskrevet ovenfor i punkt 4.

Den nærmere håndteringen av personopplysninger etter at det primære oppdraget er utført er derimot noe mangelfullt regulert. For eksempel er det angitt i avtalens punkt B, femte kulepunkt, at bildematerialet fra pumpeavstikket skal lagres som dokumentasjon for kravet om betaling. Det er ikke beskrevet når bildematerialet eller de øvrige opplysningene om pumpeavstikket skal slettes.

Pixima Light

I denne tjenesteavtalen er Piximas oppdrag mer begrenset. Kunden skal selv hente ut stillbilder fra kameraovervåkningsanlegget sitt, og registrere sine ubetalte fyllinger sammen med stillbildene på Pixima sin server gjennom en web-tilgang med brukernavn og passord. Pixima sjekker deretter opp identiteten til bileier og sender opplysningene til KredittGjenvinning AS for fakturering. Ut over dette er det ikke beskrevet hvordan opplysningene skal håndteres, når de skal slettes, osv.

5.2.3 Datatilsynets vurdering og konklusjon

Avtalene mellom Pixima og bensinstasjonene har ingen bestemmelser om hva som skal skje med opplysningene om det enkelte pumpeavstikk etter at kravet er sendt ut, for eksempel om opplysningene skal slettes. Det er ikke angitt noen rutine for informasjonsflyt fra de behandlingsansvarlige til Pixima om at krav blir gjort opp. Resultatet er som nevnt innledningsvis at opplysningene lagres på ubestemt tid, likevel slik at navnet på bileieren fjernes etter tre år.

Avtalene angir heller ikke noe om informasjonssikkerhetsaspektet ved Piximas håndtering av opplysninger.

Datatilsynet er derfor kommet til at tjenesteavtalene etter sitt innhold ikke oppfyller kravet til databehandleravtale jf. personopplysningsloven § 15.

5.3 Internkontroll

Etter den stedlige kontrollen sendte Pixima sitt internkontrollsystem til Datatilsynet. Dette dokumentet er ikke datert og det framgår ikke om og hvor beslutningen om etablering av internkontroll er tatt.

Det framstår som om dokumentet hovedsakelig tar for seg behandlinger av personopplysninger som Pixima er behandlingsansvarlig for, dvs. kundeopplysninger og personalopplysninger. Piximas behandler av opplysninger av pumpeavstikk for eget formål (jf. denne rapportens avsnitt 5.1.2) er ikke behandlet i internkontrollsystemet.

Enkelte bestemmelser i dokumentet omhandler likevel opplysninger Pixima er databehandler for. Dette gjelder blant annet rutinene for informasjon og innsyn. Personopplysningslovens krav til informasjon og innsyn retter seg mot de behandlingsansvarlige og er kun relevant for databehandlere når håndtering av informasjon og innsyn er en del av databehandleravtalen.

Enkelte bestemmelser er det uklart om kommer til anvendelse på opplysninger som Pixima er databehandler for. Dette gjelder blant annet slettebestemmelsene. Det framgår ikke hva som menes med «kunder» i dokumentet, er kunder bensinstasjonene som er Piximas kunder eller er kundene de som har fylt bensin. Piximas internkontroll må åpenbart ha sletterutiner for førstnevnte, mens sletterutiner for sistnevnte skal reguleres av databehandleravtaler, jf. denne rapportens avsnitt 5.2.

Datatilsynet har for øvrig ingen kommentarer til Piximas internkontrollsystem.

5.4 Informasjonssikkerhet

5.4.1 Prossesser og systemer

Pixima har tilgang til bensinstasjonenes videoserver via en VPN-tilkobling. Over denne tilkoblingen henter Pixima kassabonger med innmelte pumpeavstikk og film fra kameraovervåkningen fra det mulige pumpeavstikket. Noen bensinstasjoner har koblet kassene sine til videoserveren slik at data om mulige pumpeavstikk sendes direkte til videoserver. Noen bensinstasjoner skanner inn bongen fra kassa og legger denne på videoserveren.

I noen tilfeller har ikke Pixima direkte tilgang til bensinstasjonens kameraovervåkning. Dette gjelder bensinstasjoner som har en såkalt Pixima Light-avtale. I slike tilfeller henter bensinstasjonen ut bilder fra kameraovervåkningen selv og sender materialet til Pixima på e-post. Mer om Piximas bruk av e-post følger i denne rapportens avsnitt 5.4.2. I noen tilfeller sendes opplysninger om pumpeavstikk per faks.

Informasjonen fra bensinstasjonens kassaapparat og fra videoserver hentes opp på de ansatte i Piximas PCer for analyser. Slike analyser består i å hente ut kundens registreringsskilt om det er synlig og å finne andre måter å identifisere kunden på om registreringsskiltet er skjult. I tillegg vurderer Pixima pumpestikksituasjonen for å vurdere mulighet for gjentakelse og overlegg.

Pixima gjør så oppslag i det sentrale motorvognregisteret. Tilgangen til dette registeret tilbys av Evry. Om registreringsnummer ikke er kjent gjør Pixima andre oppslag, for eksempel i telefonkatalogen eller Brønnøysundregistrene på andre kjennetegn (for eksempel firmanavn som står på bilen).

Resultatene fra Piximas analyser registreres inn i Piximas eget saksbehandlingssystem Pixima DB. Her lagres også opp til fire bilder fra bensinstasjonens overvåkningskamera.

5.4.2 Distribusjon av opplysninger – epost

Pixima sender lister over pumpeavstikk med kundens navn, adresse på bileier, registreringsskilt, dato for pumpeavstikket med mer. Slike filer sendes på ukryptert e-post. Slike filer inneholder ikke dataelementer som i seg selv har behov for konfidensialitetsbeskyttelse, men ettersom datauttrekket består av personer som potensielt har begått lovbrudd må data-filen som helhet vurderes til å ha behov for konfidensialitetsbeskyttelse. Dataene må også vurderes som sensitive, jf. personopplysningsloven § 2 nummer 8 bokstav b. Se for øvrig denne rapportens avsnitt 5.1.2.2.

Pixima sender i enkelte tilfeller meldinger til sine kunder om at spesifikke kunder er gjengangere, altså at aktuelle pumpeavstikkere er tatt i pumpeavstikk tidligere, jf. denne rapportens avsnitt 5.1.2. Dette sendes per e-post. Slike opplysninger må anses som minst like beskyttelsesverdige som filene som sendes bensinstasjonene.

Å behandle beskyttelsesverdige personopplysninger e-postløsning har flere potensielt negative konsekvenser. Løsningen ligger nærme det åpne internett, og kun en liten menneskelig feil fra en saksbehandler kan føre til at personopplysninger kommer på avveie. Sletting av personopplysninger må gjøres manuelt og dette vil føre til stor risiko for at sletting ikke vil gjøres både hos avsender og mottaker.

Konklusjon

Sending av e-post med personopplysninger med behov for konfidensialitetsbeskyttelse internt er et avvik, jf. personopplysningsloven § 13, jf. personopplysningsforskriftens § 2-11, 3. ledd.

5.4.3 Segmentering

En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige, jf. personopplysningsloven § 15. En databehandler skal sikre personopplysningene mot uautorisert innsyn der hvor konfidensialitet er nødvendig, jf. personopplysningsforskriften § 2-11. For å forhindre brudd på konfidensialiteten ved uautorisert bruk skal det etableres tekniske sikkerhetstiltak, jf. personopplysningsforskriften § 2-14. Dette innebærer at det skal etableres tekniske tiltak for å forhindre at opplysninger fra en behandlingsansvarlig samlet inn til ett formål, ikke skal kunne blandes sammen med opplysninger fra en annen behandlingsansvarlig med et annet formål. Tiltak for å segmentere opplysninger fra flere behandlingsansvarlige skal stå i forhold til opplysningens art, antallet behandlingsansvarlige den databehandleren har som kunder, risikoen ved sammenblanding av opplysninger med mer.

I Pixima DB fins alle pumpeavstikksaker samlet på tvers av behandlingsansvarlige. Det er mulig å søke på pumpeavstikkere på tvers av bensinstasjoner. Dette er en nødvendig forutsetning for Piximas gjengangertjeneste, jf. denne rapportens avsnitt 5.1.2. Det er ikke etablert noen form for teknisk segmentering av personopplysningene i Pixima DB.

Konklusjon
Manglende segmentering ved behandling av personopplysninger fra ulike behandlingsansvarlige er et avvik, jf. personopplysningsloven § 13, jf. personopplysningsforskriften §§ 2-11 og 2-14.