Rättsutredning av ”Öppna Skolplattformen”

Denna rättsutredning är framtagen av utbildningsförvaltningen i samverkan med stadsledningskontorets juridiska avdelning och stadsledningskontoret avdelningen för IT och digitalisering.

Bakgrund

Den 12 februari 2021 släpptes det en betalapplikation [appen] som heter ”Öppna skolplattformen”. Appen vänder sig till vårdnadshavare med barn i Stockholms stads grund-, gymnasie- och förskolor. Det är inte staden som har utvecklat appen, utan appen har utvecklats av ett privat bolag.

En av apputvecklarna till Öppna Skolplattformen kontaktade utbildningsförvaltningens IKT-enhet för att begära ut allmänna handlingar i form av API:er (applikationsprogrammerings-gränssnitt) samt SDK (Software Development Kit) för skolplattformen, vilket är en samling system upphandlade av staden. Frågeställaren informerades den 3 december 2020 om att det är stadsledningskontoret som äger beskrivningarna av API:er och SDK för hela staden och att utbildningsförvaltningen inte använder öppna API:er. Frågeställaren informerades vidare om att det inte finns möjlighet att utveckla egna applikationer mot Skolplattformen. Denne informerades om att utbildningsförvaltningens instanser av API:er är anpassade till våra leverantörer och innehåller uppgifter om enskilda samt information om hur anrop kan göras. Staden har således tagit ett aktivt beslut om att inte ha öppna API:er i såväl ID-portalen som skolplattformen. Apptillverkaren fick även veta att detta innebär att informationen omfattas av sekretess och fick den 4 mars 2021 ett avslagsbeslut.

Trots detta har denne tillsammans med andra, genom demontering/baklängeskonstruktion (så kallad reverse engineering), med uppsåt skapat en app som speglar innehållet i skolplattformen på ett sätt som inte är av staden godkänt.

Denna rättsutredning har tittat på det juridiska rörande det ovan beskrivna.

Säkerhetsgranskning

Utbildningsförvaltningen anlitade ett oberoende informations- och IT-säkerhetsföretag som har gjort en analys av applikationen samt källkoden för att säkerställa att appen inte behandlar känslig information om registrerade, exempelvis genom lagring eller genom annan behandling. Staden ansvarar för att utreda detta eftersom stadens ansvar för personuppgifterna gäller för all behandling, vilket enligt dataskyddsförordningen innebär exempelvis insamling, bearbetning, strukturering, ändring, läsning, användning, spridning eller tillhandahållande av personuppgifter.

Resultatet visade att utvecklarna genom baklängeskonstruktion skapat en app som visar information från skolplattformen. Appens nuvarande version lagrar inte någon känslig information, men det är möjligt att den källkod som används för att visa informationen skulle falla inom lagens definition av en ”automatiserad behandling” av personuppgifter som används för exempelvis att läsa, sprida eller tillhandahålla personuppgifter. Applikationen hämtar data från skolplattformens endpoints och visar detta på ett alternativt sätt. Då staden inte kontrollerar källkoden som visar (behandlar) informationen, så har staden heller, inte den enligt lagen nödvändiga, kontrollen över hur den automatiserade behandlingen förändras över tid i nuvarande eller framtida versioner.

Appen är byggd med öppen källkod och publicerad på Github, vilket är en plattform för publicering av öppen data/källkod för alla att ta del av.

Dataintrång

Agerandet att tillskansa sig automatiserad tillgång till information genom stadens API innebär enligt stadens mening dataintrång (4 kap. 9 c § brottsbalken), detta då apputvecklarna olovligen och med uppsåt berett sig tillgång till en uppgift som därefter används för en automatiserad behandling. Det är i lagens mening en personsuppgiftsbehandling som utvecklarna ägnar sig åt. Detta har skett trots dialog med apputvecklarna och fortsätter ske i samband med att utbildningsförvaltningen stänger ned delarna som möjliggör tredjepartåtkomst. Apputvecklarna försöker fortlöpande hitta alternativa sätt att nyttja stadens API:er för att fortsättningsvis spegla innehållet i skolplattformen.

En av apputvecklarna har tidigare, innan appen lanserades för allmänheten, tillverkat en liknande app för eget bruk. Den privata användningen innebar dock att denne tidigt beredde sig egen tillgång till stadens API:er och hade informationen på en egen server, enligt uppgifter som apputvecklaren själv lämnat.

Enligt 4 kap. 9 c § brottsbalken döms den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling för dataintrång till böter eller fängelse i högst två år. Uppgifter som är avsedda för automatiserad behandling avser fakta, information eller begrepp som uttrycks i en för en dator anpassad och läsbar form, även program omfattas.

Vidare anges att uttrycket ”bereda sig tillgång till” ska förstås så att man kan få del av uppgifterna. Det krävs däremot inte att någon verkligen tar del av uppgifterna (prop. 2006/07:66 s. 23 f. och 49). För att en handling ska leda till ansvar för dataintrång krävs att handlingen har skett olovligen med uppsåt. Ett förfarande är olovligt om det sker utan tillstånd av den som har rätt att förfoga över uppgiften och saknas stöd i gällande rätt. En motsvarighet till bestämmelsen fanns tidigare i datalagen (1973:289). I förarbetena till datalagen angavs att avsikten med bestämmelsen var att helt allmänt skydda datalagrat material mot obehöriga åtgärder, oavsett om åtgärderna medför otillbörligt integritetsintrång eller inte (prop. 1973:33 s. 105).

Apputvecklarna har också publicerat stadens API:er på den digitala plattformen Github. Utvecklarna har därmed offentliggjort stadens API:er till allmänheten, vilket innebär att vem som helst som tar del av dessa kan anropa databaserna och ha möjlighet att ta del av informationen.

Dataskyddsförordningen

Utbildningsnämnden, stadsdelsnämnderna och arbetsmarknadsnämnden är personuppgiftsansvariga för de personuppgifter som finns i skolplattformen. Därtill är utbildningsnämnden personuppgiftbiträde till stadsdelsnämnderna samt arbetsmarknadsnämnden, då utbildningsnämnden är avtalsansvarig samt förvaltare av skolplattformen. Som personuppgiftsansvariga har nämnderna en skyldighet att se till att i sina behandlingar av personuppgifterna säkerställa att dataskyddsförordningen efterlevs.

Personuppgiftsansvariges skyldigheter och säkerhet

Av art. 24 dataskyddsförordningen framgår att nämnderna som personuppgiftsansvarig, utifrån behandlingarnas art, omfattning med mera, ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå. Av art. 32 dataskyddsförordningen förtydligas hur den riskbaserade bedömningen ska ske för att uppnå den lämpliga säkerhetsnivån. Det framgår också i art. 24 dataskyddsförordningen, som har sin grund i art. 5.2 dataskyddsförordningen, att den personuppgiftsansvarige också ska kunna visa att behandlingarna utförs i enlighet med förordningen.

Det bör också noteras att det i skäl 38 till dataskyddsförordningen framgår att barn är särskilt skyddsvärda och kräver därför ett starkare skydd.

Vidare framgår det av art. 25 dataskyddsförordningen att den personuppgiftsansvarige ska vid behandling av personuppgifter säkerställa att det finns, utifrån behandlingens art, ett adekvat inbyggt dataskydd och dataskydd som standard.

Personuppgiftsbiträde

Som personuppgiftsbiträde för stadsdelsnämnderna samt arbetsmarknadsnämnden har utbildningsnämnden en skyldighet att enbart behandla personuppgifterna på ett sådant sätt som de personuppgiftsansvariga nämnderna har gett instruktioner om. Se art. 29 dataskyddsförordningen.

Överföring av personuppgifter

För att få föra över personuppgifter till en annan organisation (som inte är nämndernas personuppgiftsbiträde) krävs att det finns en laglig grund för transferering.[1] Detta inkluderat att den nye personuppgiftsansvarig behandlar uppgifterna för ett ändamål som är förenligt med det syfte och ändamål som nämnderna har samlat in personuppgifterna för, såvida det inte föreligger en annan laglig grund.

Att en utomstående part med vilken nämnderna inte har någon avtalsrelation med eller där det saknas en laglig grund för att automatiserade med användning av stadens stängda API:er transferera personuppgifter till bereder sig tillgång till eller försöker bereda sig tillgång till, skulle innebära en transferering som inte är förenlig med förordningen. Nämnderna har en skyldighet att skydda

[1] Men överföring av personuppgifter avses i detta sammanhang den automatiserade överföringen som sker med hjälp av stadens API:er

personuppgifterna och vidta åtgärder för att säkerställa sina skyldigheter enligt förordningen.

Staden ställde den 16 februari 2021 en fråga till Integritetsskyddsmyndigheten (IMY) rörande ansvar för personuppgifter i tredjeparts applikationer som staden inte har ett avtalsrättsligt förhållande med. Den 31 mars 2021 svarade IMY, enligt nedan.
” Det är den personuppgiftsansvariga som har ansvaret att se till att personuppgiftsbehandlingen når upp till säkerhetskraven i dataskyddsförordningen. Således är det även den personuppgiftsansvariga som är skyldig att hantera eventuella personuppgiftsincidenter i den egna verksamheten”.

Utifrån svaret från IMY betyder det att staden har ansvar för personuppgifterna som behandlas i betalappen ”Öppna skolplattformen”.

PSI-lagen

Syftet med lagen (2010:566) om vidareutnyttjande av handlingar från den offentliga förvaltningen (PSI-lagen) är att främja en informationsmarknad genom att reglera vilka inskränkningar som myndigheter får göra avseende *hur myndigheternas handlingar används av enskilda*. Lagen reglerar inte själva tillgången till informationen.

Enligt förarbetena (prop. 2014/15:79 s. 14-15) konstateras att det är en huvudprincip enligt svensk rätt att allmänna handlingar som huvudregel får användas fritt (prop. 2009/10:175 s. 138). Sekretess- och integritetsskäl i offentlighets- och sekretesslagen (2009:400) förkortat OSL, dataskyddsförordningen, registerförfattningar eller av immaterialrättsliga skäl kan dock inskränka vidareutnyttjandet. En sekretessbelagd uppgift kan exempelvis lämnas ut med förbehåll för hur uppgiften får utnyttjas (se 10 kap. 14 § OSL). På grund av sekretess kan det därför finnas hinder för en enskild att vidarebefordra handlingen eller uppgifter ur handlingen till andra. Även dataskyddsförordningen och registerförfattningar kan begränsa tillgången till handlingarna. Den fria användningen av allmänna handlingar kan också begränsas av upphovsrättsliga skäl. Vidare framgår det i prop. 2009/10:175 s. 153 att myndigheter som är utbildningsinstitut är undantagen från PSI-lagen, men att det inte påverkar enskildas rätt att få tillgång till handlingar för vidareutnyttjande. Att en myndighet är undantagen från lagen

innebär inte heller att rätten att vidareutnyttja dess handlingar i något avseende inskränks eller utvidgas.

I 3 § PSI-lagen framgår att lagen inte är tillämplig för handlingar som finns hos utbildningsinstitutioner, vilket utbildningsförvaltningen bedöms vara i enlighet med gällande rätt.

OSL

En av apputvecklarna till Öppna Skolplattformen kontaktade utbildningsförvaltningens IKT-enhet för att begära ut allmänna handlingar i form av API:er samt SDK för skolplattformen. Frågeställaren informerades den 3 december 2020 om att utbildningsförvaltningen avslog dennes begäran och att denne kunde återkomma för ett skriftligt avslagsbeslut. Den 3 mars 2021 inkom frågeställaren med en begäran om att få ett skriftligt avslagsbeslut. Detta skickades till frågeställaren den 4 mars 2021.

Allmänna handlingar och rätten att ta del av digital information

Tryckfrihetsförordningen anger ingen skyldighet att tillgängliggöra handlingar digitalt utan endast att på begäran lämna ut kopia av handling eller göra den tillgänglig på plats hos myndigheten. Sådana skyldigheter måste följa av någon annan lagstiftning. Myndigheter ska dock möjliggöra insyn i digitala handlingar om man har system för detta tillgängliga så som presentationsterminaler. Detta gäller inte för handlingar som inte är allmänna eller om det finns sekretesshinder.

Sekretess

18 kap. 8 § 3 p. OSL tycks ha en vid tillämpning kring vad som kan sekretessbeläggas, till exempel en sådan sak som uppgift om vilket operativsystem som används. Den borde därför kunna användas för information som ger insyn i detaljer kring ett digitalt systems funktionssätt. Beskrivningar av hur ett program fungerar i stora drag och vilka typer av uppgifter som bearbetas i ett program bör alltid kunna lämnas utan att uppgifter som omfattas av bestämmelsen behöver röjas.

21 kap. 7 § OSL är relevant i sammanhanget men föremålet för sekretessen är själva personuppgifterna. Bestämmelsen kan alltså inte användas för att sekretessbelägga information som potentiellt kan ge tillgång till personuppgifter, såvida man inte kan få in det under definitionen ”personuppgift”. Där är det GDPR-definitionen som styr, vilken förvisso är vid.

Upphovsrätten

År 1996 infördes ett rättsligt skydd för databaser i EU genom databasdirektivet (Direktiv 96/9/EG om rättsligt skydd för databaser), vilken innehåller bestämmelser om en så kallad sui generis-rätt (”en rätt av sitt eget slag”).

Detta skydd återfinns i 49 § upphovsrättslagen (URL) gällande ”framställning av kataloger med mera”. Staden bedömer att den information som finns i skolplattformen är en fråga om att vara en eller flera databaser då det är en samling information som är organiserad, där det går att söka fram information i helhet eller bitvis. För att 49 § ska vara tillämplig krävs också att databasen är resultatet av en kvantitets- eller kvalitetsmässig väsentlig investering (ekonomisk, materiell eller mänskligt) i antingen anskaffning, granskning eller presentation av innehållet. Staden menar att det är en fråga om en databas. Staden menar vidare att de inskränkningar i sui generis-skyddet, som kan utläsas i art. 8 och 9 i direktivet, inte är tillämpliga då det här inte är fråga om vare sig utdrag eller rätt för behörig användare att återanvända icke-väsentliga delar av databasen.

Det är vidare inte tillåtet att för privat bruk (12 § 1, 2 och 4 st URL) kopiera offentliggjorda sammanställningar i digital form när sammanställningen i fråga redan är i samma form. Rätten enligt 49 § 1 st URL, gäller tills dess att femton år har förflutit från att databasen gjordes tillgänglig för allmänheten. Skolplattformens databaser har tillgängliggjorts för allmänheten genom startsidan för vårdnadshavare samt via stadens app. Databasen ifråga uppfyller villkoren för automatiskt skydd.

Källkod till ett datorprogram skyddas av upphovsrätten om rekvisiten för upphovsrätt är uppfyllda och även API skulle kunna falla in under upphovsrätten.

Införskaffande av produkter/applikationer i staden

I princip alla inköp av varor och tjänster i offentlig verksamhet omfattas av lagen om offentlig upphandling (LOU). Beroende på vad som ska köpas och till vilket pris, så blir olika bestämmelser aktuella. Som upphandlande myndighet får staden alltså inte ingå avtal med en leverantör på sådant sätt som en privat aktör får.

Ett avtalsförhållande mellan staden och en leverantör föregås i de flesta fall av ett upphandlingsförfarande. Vad gäller skolplattformen har staden valt att göra ett flertal upphandlingar med flera

leverantörer som ska samverka. Det är här viktigt att framhålla att när ett avtal väl finns på plats har staden och leverantören skyldighet att följa avtalet, precis som i vilken avtalssituation som helst. Avtalsparterna har inte rätt att göra sådana ändringar i leverans att det påverkar avtalets innehåll. Det finns dock givetvis utrymme för utveckling och förbättring inom ramen för avtalet, men om ändringar görs som frångår föremålet för upphandlingen bryter staden mot lagen om offentlig upphandling (LOU).

Inköp av licens kan göras via en av staden upphandlad licensadministratör. Förnärvarande är staden avtalslösa rörande licensadministratör men det pågår en upphandling för hela staden För att en avtalssituation mellan stadens licensadministratör och leverantören för en viss tjänst ska kunna uppstå behöver tjänsteleverantören dels ingå avtal med licensadministratören, dels ett samverkansavtal med berörd förvaltning inom staden. För att berörd förvaltning inom staden ska kunna ingå ett sådant samverkansavtal med tjänsteleverantören krävs att informationsäkerhetsansvarig på berörd förvaltning gör en informationsklassning av tjänsten samt att ett personuppgiftsbiträdesavtal med instruktion skrivs av personuppgiftsansvarig. Leverantören blir därmed personuppgiftsbiträde och behandlar stadens personuppgifter för stadens (som är personuppgiftsansvarig) räkning.

Eftersom utbildningsförvaltningen inte tillhandahåller några öppna API:er (utbildningsverksamhet är undantagna PSI-direktivet) så krävs det en affärsförbindelse för att en tredje part ska få behandla personuppgifter och annan information. Eftersom det krävs en affärsförbindelse så måste utbildningsförvaltningen följa lagen om offentlig upphandling, LOU.

Tidigare utveckling

Den av apputvecklarna som initialt utvecklade en egen app, hade genom automatiserad överföring via API:er hämtat uppgifterna från skolplattformen, både uppgifter om sina egna barn samt klasslistor med mera på egen server. Eftersom utbildningsnämnden inte fick någon begära om utlämnande av allmän handling så har nämnden inte kunnat genomföra någon sekretessbedömning.

Enligt ovan kan agerandet vid utvecklingen av den egna appen utgöra ett dataintrång i enlighet med bestämmelserna i brottsbalken, behandlingen av personuppgifter sker utan laglig grund i enlighet

med dataskyddsförordningen, vara ett intrång i upphovsrätten samt kan eventuellt ett röjande enligt OSL ha förelegat.

Sammanfattning

När det gäller No Free Beer HB [bolaget], som står bakom appen Öppna skolplattformen, så finns det i dagsläget inget avtalsförhållande med staden för den personuppgiftsbehandling som bolaget genomför. För ett avtalsförhållande krävs en upphandling i enlighet med lagen om offentlig upphandling eller köp av licens via stadens licensadministratör. I dagsläget är staden avtalslösa ifråga om licensköp.

I enlighet med ovan kan bolaget inte anses vara biträde till utbildningsnämnden, stadsdelsnämnderna samt arbetsmarknadsnämnden för att behandla nämndernas personuppgifter i sin app. Oavsett om det föreligger ett biträdesförhållande eller ej mellan bolaget och utbildningsnämnden krävs det att det finns en laglig grund för att få behandla och transferera personuppgifter till en tredje part. Om det skulle finnas en sådan laglig grund måste utbildningsnämnden säkerställa att bolaget kan upprätthålla lämplig säkerhet samt att överföringen sker på ett säkert sätt. Vidare måste utbildningsnämnden säkerställa att bolaget inte behandlar personuppgifterna för ett annat syfte och ändamål än för det som nämnderna har samlat in uppgifterna för.

Det är tydligt att utvecklarna av appen är väl medvetna om att dessa saknar tillstånd till personuppgiftsbehandlingen, samt att förfoga över stadens API:er och SDK. Det finns inget övrigt stöd i gällande rätt för deras agerande och dataintrånget kan därför polisanmälas. Vid beslut om polisanmälan ska göras eller inte, bör likabehandlingsprincipen enligt kommunallagen beaktas. Vidare faller dataintrång under allmänt åtal, detta innebär att exempelvis en vårdnadshavare kan välja att polisanmäla apptillverkarna.

Det är i sammanhanget viktigt att betona att apptillverkarna i enlighet med offentlighet- och sekretesslagen fått ett avslagsbeslut då information om API:er och SDK omfattas av sekretess. Att apptillverkarna genom baklängeskonstruktion (reverse engineering) berett sig tillgång till uppgifterna och därefter publicerat stadens API:er tillsammans med appens kod på en offentlig plattform, Github. Agerandet har därmed inneburit att sekretessbelagd information har blivit röjd.