

Lexplore, datahantering och GDPR



Lexplore



Lexplore, datahantering och GDPR

Redan när forskningen från Karolinska Institutet skulle möta den svenska marknaden var en säker datahantering högsta prioritet för Optolexia som sedan skulle komma att bli Lexplore. Vana vid forskningens krav på säkra metoder och verifierbara resultat var det ett arbetssätt som man var van vid. Flera utredningar gjordes med hjälp av interna och externa specialister med spetskompetens inom juridik och datasäkerhet. Samtliga kom fram till samma resultat: Lexplore mötte, eller överträffade, de krav som fanns på säker databehandling enligt GDPR, The General Data Protection Regulation, eller dataskyddsförordningen som den heter på svenska.

Nya tider – nya krav

Under de fyra år som Lexplore har funnits har mycket hänt och kraven på en säker databehandling i samhället har ökat, inte minst sedan införandet av dataskyddsförordningen. För Lexplores del har införandet av dataskyddsförordningen inte inneburit en förändring, våra system var redan byggda utifrån de hårda krav som finns i förordningen.

För att säkerställa att Lexplore fortfarande möter de hårda krav som finns har en uppföljande utredning av juridisk expertis gjorts. Vi ville helt enkelt ha svar på tre frågor:

Frågorna vi ställde

1. Är röst- och ögonrörelseinspelningarna att betrakta som biometriska uppgifter enligt dataskyddsförordningen?
2. Kan analysen av elevernas läsförmåga betraktas som hälsodata?
3. Gör vi rätt i att betrakta personuppgifterna som extra skyddsvärda och möter vi i så fall de krav som finns på extra skyddsvärd behandling?

Utredningens slutsats

1. Artikel 9 i dataskyddsförordningen om biometriskt data är inte tillämplig i Lexplores fall då ögonrörelse- och röstinspelningarna inte används i identifieringssyfte.
2. AI-analysen testar nivå av läsförmåga. En elevs läsförmåga är inte hälsodata utan pedagogiska data som redan används i skolan.
3. De personuppgifter som hanteras är extra skyddsvärda. Lexplore möter de krav som finns på extra skyddsvärd behandling.

GDPR

GDPR, dataskyddsförordningen, gäller i hela EU och syftar bland annat till att skapa "en enhetlig och likvärdig nivå för skyddet av personuppgifter" (Datainspektionen). Innan den lagen trädde i kraft fanns PUL, personuppgiftslagen, och till stora delar liknar PUL och GDPR varandra. De flesta organisationer hade därför redan innan dataskyddsförordningen trädde i kraft en vana vid att arbeta med att skydda personuppgifter.

Din rätt till skydd av personuppgifter

Rätten till privatliv uttrycks i flera lagar inom EU och Sverige bland annat i 2 kap. 6§ andra stycket i regeringsformen. Dataskyddsförordningen gäller för i princip all automatiserad behandling av personuppgifter men även viss manuell behandling. Dataskyddsförordningen gäller för företag, föreningar, organisationer och privatpersoner med undantag för privatpersoners privata behandling av personuppgifter. Ett annat undantag är när någon behandlar personuppgifter i samband med sin yttrande- eller informationsfrihet.

Personuppgifter

Namn, personnummer och adress är kanske självklara personuppgifter men även bilder eller röstinspelningar kan vara personuppgifter även om inte namnet nämnts. Avgörande är att det kan knytas, ensamt eller tillsammans med andra uppgifter, till en levande person. Det betyder att t.ex. cookies, och ip-nummer räknas till personuppgifter om de kan kopplas till en fysisk person.

Personuppgiftsansvariga och personuppgiftsbiträde

Den som behandlar personuppgifter är antingen personuppgiftsansvarig eller personuppgiftsbiträde. Personuppgiftsansvarig är den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Skolan är i det här fallet personuppgiftsansvarig och Lexpire personuppgiftsbiträde.



Biometriskt data som syftar till identifikation (regleras i artikel 9 i GDPR)



Fingeravtryck



Ögonigenkänning



Ansiktsigenkänning



DNA

Biometriskt data som har andra syften



Ögonrörelser
för att mäta läsförmåga



Röstinspelning för
att bedöma läsning



Skolfoto



Inspelningar i klassrum i
undervisningssyfte

Biometriska personuppgifter

Dataskyddsförordningen definierar biometriska uppgifter som *”personuppgifter som härrör från specifik teknisk bearbetning avseende fysiska, fysiologiska eller beteendemässiga egenskaper hos en fysisk person, som tillåter eller bekräftar den fysiska persons unika identitet”*.

När du använder fingeravtrycket eller ansiktsavläsning för att låsa upp din mobiltelefon har du använt biometriska data för att göra det. Biometriska data, eller personuppgifter, är alla personuppgifter som kommer från din kropp. För att omfattas av dataskyddsförordningen krävs att uppgifterna syftar till att användas för att identifiera, eller bekräfta din identitet som fingeravtrycket eller ditt ögas unika iris. Biometriska data är särskilt skyddsvärda personuppgifter och har därför ett extra skydd i dataskyddsförordningen.

Ögonrörelseinspelningar skiljer sig från fotograferingar av ögats iris

De ögonrörelseinspelningar som Lexplore gör används för att hitta elevens läsmönster, inte för att identifiera elever. Det är enbart hur ögonen rör sig över texten som spelar roll och det är också det enda som registreras i inspelningen.

Iris-scanning för identifikation

Ditt ögas iris är lika unikt som ditt fingeravtryck; färgen och formen varierar med varje individ och en ögonscanning kan därför användas för att identifiera människor. För Lexplore spelar ögonens utseende inte någon roll, så vi använder inte alls sådan teknik.

Hälsodata

Hälsodata är alla uppgifter som är relaterade till din fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus. Enligt Datainspektionen omfattas följande aspekter av en persons hälsa av definitionen: ”uppgifter om hälsa som kommer från tester eller undersökningar, uppgifter som sjukdom, sjukdomsrisk, sjukdomshistoria, funktionshinder oavsett vilken källa uppgifterna kommer ifrån”.

För skolan innebär det till exempel att uppgifter som rör en elevs hälsa hanteras av elevhälsans personal som skolläkare, skolsköterska eller logoped och inte av lärare eller fritidspedagoger.

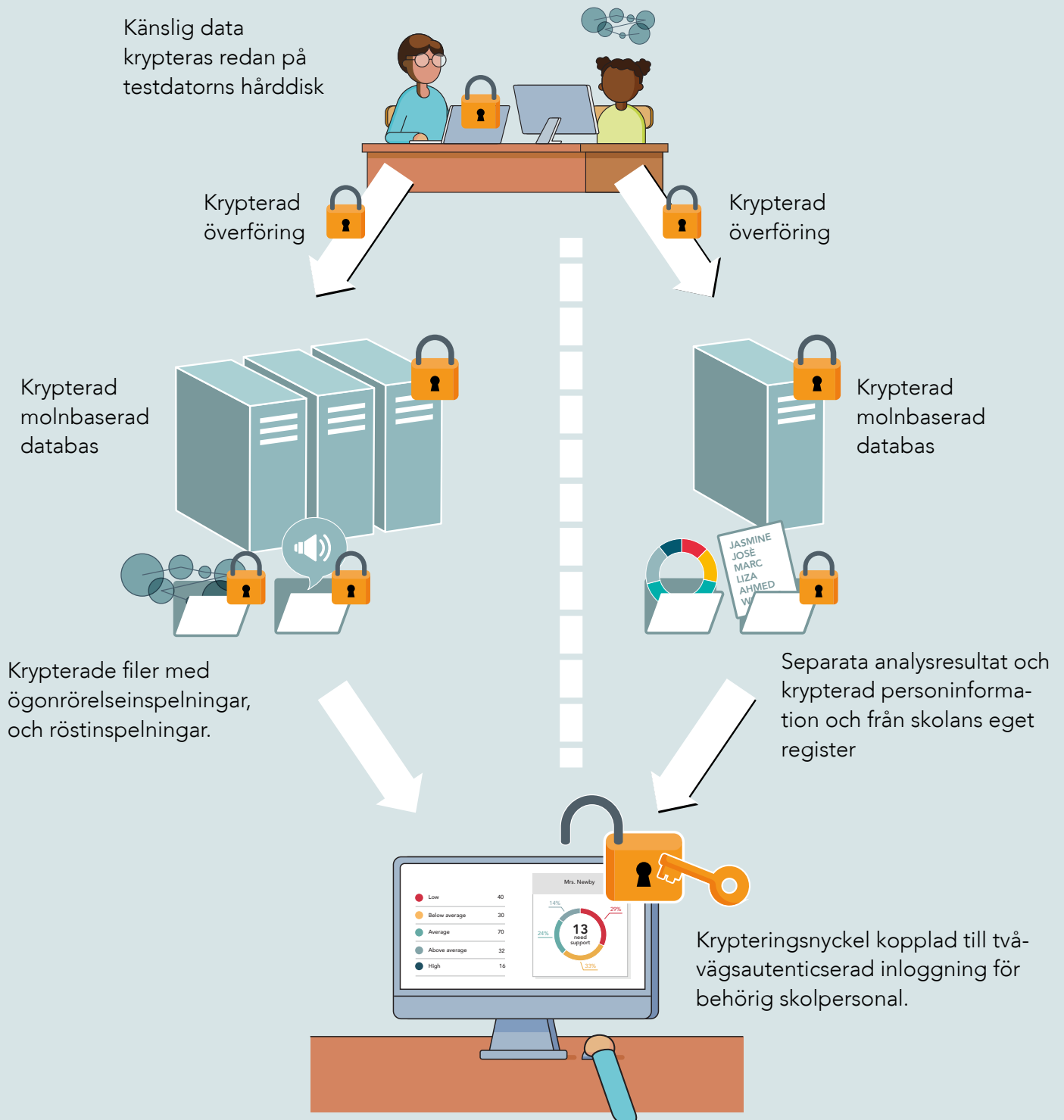
Lexplore hanterar inte hälsodata. Det går inte att diagnostisera en elev för vare sig sjukdomar eller funktionsnedsättningar med den screening som görs.

Inte förbjudet att hantera personuppgifter

Alla organisationer, föreningar och företag i någon form hanterar personuppgifter. Den lilla koloniträdgårdsföreningen som har ett register över medlemmarna i föreningen hanterar personuppgifter, din arbetsgivare hanterar personuppgifter och fotbollsklubben din dotter spelar i hanterar personuppgifter. Det är inte på något sätt förbjudet att hantera personuppgifter, kravet är att du ska ha ett giltigt skäl för att göra det och att du gör det på ett säkert sätt.

Kryptera och separera

En grundprincip för hanteringen av Lexplores data är att separera informationen där det går och kryptera så mycket som möjligt. Det betyder att ögonrörelseinspelningar och röstinspelningar sparas, (utan namn, personnummer och analysresultat), på en plats. Personuppgifterna, dvs namn, personnummer etc., samt analysresultat sparas istället i en egen databas för varje organisation. Först när resultaten ska visas i resultatportalen så sammanförs de båda med hjälp av en krypteringsnyckel. Vad du kan se i resultatportalen bestäms av den behörighetsnivå som din skola har bestämt.



Lexplore och dataskyddsförordningen

Lexplore är ett ungt företag och i relation till dataskyddsförordningen har det varit en fördel. Istället för att behöva ändra på system och rutiner har vi kunnat utgå ifrån dataskyddsförordningen när it-system och rutiner har tagits fram.

Det kallas för privacy by design.

Privacy by design

Privacy by design innebär att dataskyddsförordningen har fungerat som en ledstjärna i arbetet med att ta fram it-systemen. I varje steg i processen har överväganden gjorts för att till exempel se till att inga personuppgifter lagras om de inte behövs, data som behöver skickas ska vara krypterat och att en tvåvägsautentisering för inloggningen har varit standard. Inget har därför behövt ändras eller anpassas till dataskyddsförordningen, kraven har varit mötta redan från start.

Vilka uppgifter hanteras?

Lexplore hanterar personuppgifter som namn och personnummer men också röst-

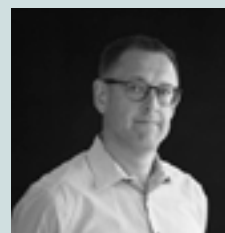
inspelningar och ögonrörelseinspelningar. Inspe­lingarna ses som särskilt skyddsvärda, precis som personnumret, och hanteras därför med en utökad säkerhet som grund.

Ögonrörelse- och röstinspelningarna är biometrisk data eftersom de härrör från kroppen, men de används inte för att identifiera en elev. Syftet med inspelningarna är att bedöma hur långt eleven kommit i sin läsutveckling – inte identifikation. Elevens identitet är redan känd vid screeningtillfället.

Även om inspelningarna i sig är biometrisk så räknas de därför inte som biometrisk personuppgifter enligt dataskyddsförordningen då enbart personuppgifter som används för identifikation faller under artikel 9.

Inbyggd datasäkerhet – privacy by design

Peter Norman CTO
(Chief Technical officer
/ Teknikchef) på
Lexplore



Vad har privacy by design, eller inbyggd datasäkerhet på svenska, haft för betydelse för Lexplore?

Rent konkret betyder det att vi utgick ifrån den dokumentation, checklistor och rekommendationer som fanns hos Datainspektionen och Sveriges kommuner och landsting när vi designade våra it-system. Vi behövde aldrig anpassa eller ändra i gamla system utan kunde göra rätt från start.

Kan du ge exempel på vad som menas med inbyggd datasäkerhet?

Det kan till exempel vara att vi använder kryptering på den data som finns och att vi separerar den i olika databaser. Det kan också vara multifaktorsautentisering, att man tänker på behörighetsnivåer och att ingen data behandlas om den inte är nödvändig. Vi har också loggar som visar om en behörighet för en användare ändras, möjlighet att anonymisera elever och krypterar både vid hårddiskar och databaser.

Tack vare att vi är ett så ungt bolag har vi kunnat bygga ett säkert system från start.

Skolan och bedömning av läsförmågan

Alla skolor måste bedöma läsförmågan hos eleverna

Alla skolor i Sverige har en skyldighet att mäta elevernas läsförmåga för att bedöma hur väl eleven har nått kunskapskraven för årskursen. Det innebär att skolan, för att klara sitt uppdrag, kommer att behöva göra mätningar av läsförmågan på olika sätt. Det kan vara traditionella prov med papper och penna som H4, DLS och ordkedjor, digitala prov på dator eller Ipad men det kan också betyda att läraren behöver sitta bredvid och lyssna på när en elev läser högt.

Resultaten behöver sparas

Resultaten av bedömningen sparas sedan för att kunna följa elevens utveckling. Hur man sparar resultaten varierar mellan skolor. Det kan vara i fysiska pärmar, mappar på datorn eller i en digital lärplattform. För de skolor som använder Lexplore så sparas informationen i en krypterad databas. Informationen är bara tillgänglig för de medarbetare som skolan specifikt har utsett. En lärare har till exempel enbart tillgång till sina egna elevers resultat och inte några andra elever.

En enklare lösning med Lexplore

När Lexplores screening togs fram utvärderades det bland annat utifrån de prov som redan används i skolan idag. Vi kunde konstatera att Lexplores screening ersätter de, ofta tidskrävande, prov som lärare traditionellt har använt.

Genom att använda ett digitalt verktyg som Lexplore kan arbetsbördan lätta något samtidigt som resultaten för eleverna blir säkrare. Det är två av många anledningar som gör att fler och fler skolor väljer att lämna traditionella tester till förmån för en digital screening.

Samtycke i skolan

Det är upp till varje lärare och skola att bestämma hur de ska bedriva undervisningen. Det gäller även hur de ska bedöma elevernas kunskap och vilka verktyg som ska användas – oavsett om verktygen är digitala eller inte.

Även om ett samtycke därför inte behövs i egentlig mening rekommenderar vi alltid att skolan berättar om Lexplore och varför man har valt att införa en digital screening av elevernas läsförmåga på skolan.

Pedagogisk information - inte hälsodata

Som lärare kan du få mycket information om elevens läsförmåga från screeningen. Det vi däremot inte kan säga är vad resultatet beror på. Ett lågt resultat på en screening kan innebära att eleven har dyslexi men det kan lika gärna bero på bristande lästräning, flerspråkighet som försenat läsutvecklingen, kognitiva funktionsnedsättningar, språkstörning eller en neuropsykiatrisk funktionsnedsättning.

Det finns mycket som kan störa läsningen och det du som lärare får veta från Lexplores screening är hur väl din elevs läsförmåga har utvecklats. Visar det sig att elevens läsförmåga i fortsättningen inte utvecklas som förväntat kan en pedagogisk kartläggning och eventuell utredning behöva göras. Det beslutet fattas av skolan. Screeningresultatet kan här ge viktig information i den pedagogiska kartläggningen som läraren ansvarar för.

En eventuell diagnos ställs däremot alltid av behörig vårdpersonal och kan aldrig baseras enbart på Lexplores screening.

Rättslig grund och personuppgifter i skolans värld

För att behandla personuppgifter så krävs det att det finns en rättslig grund för det. Det måste finnas giltiga skäl för att behandla och spara personuppgifterna. Ett samtycke är den svagaste rättsliga grunden. För skolans värld är samtycket sällan en giltig rättslig grund alls då förhållandet mellan elev och skola inte är jämlikt då skolan är en myndighet.

Den rättsliga grund som är tillämplig i skolan rör därför myndighetsutövning och uppgifter av allmänt intresse. "Myndighetsutövning innebär att någon har statens uppdrag att bestämma över enskilda medborgare. Det

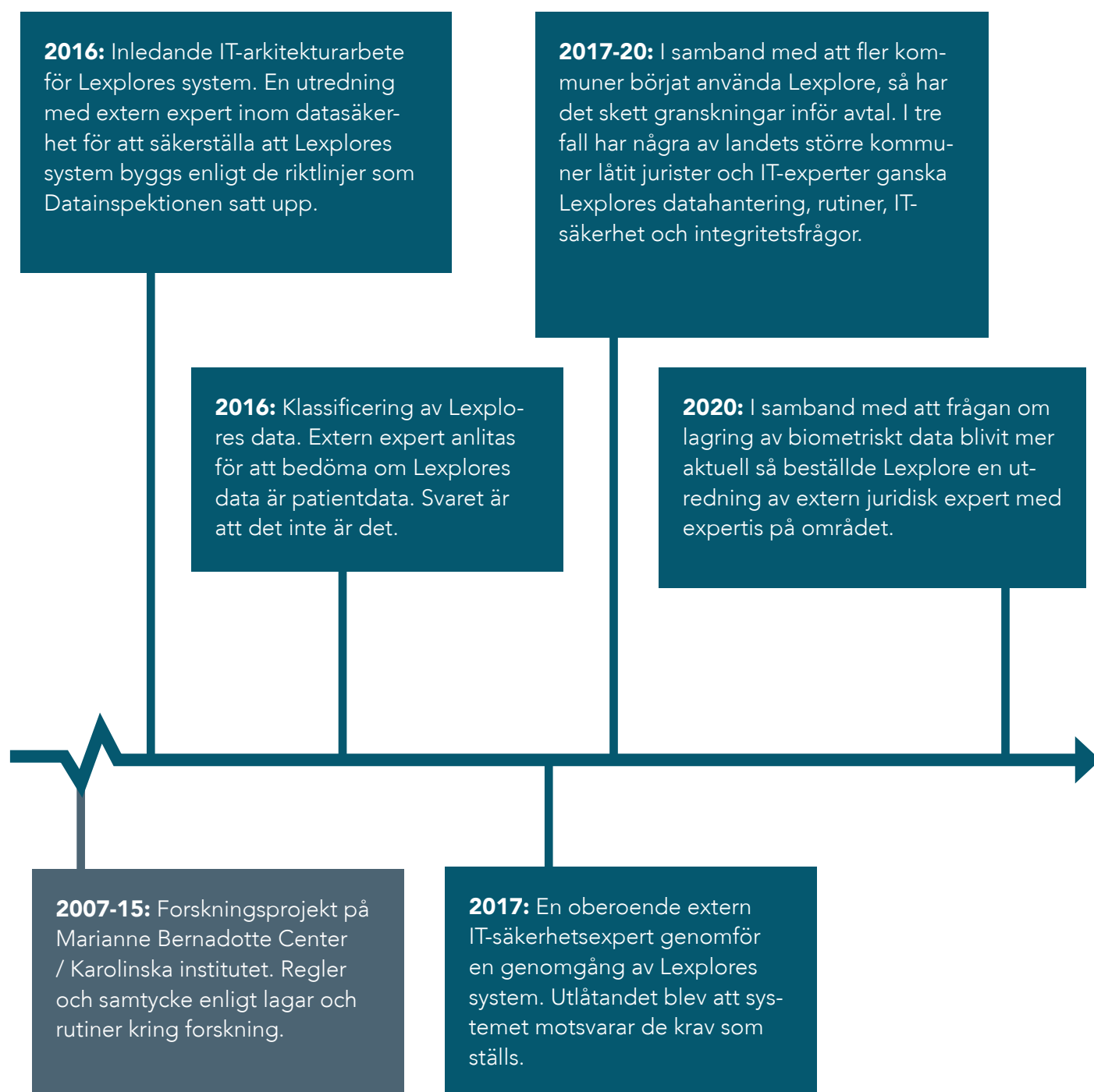
kan innebära att en myndighet beslutar om att en medborgare ska få en viss förmån eller rättighet, eller att hen har en viss skyldighet eller ska få ett straff. Det kan alltså vara beslut som gynnar den enskilde eller beslut som är betungande". (Datainspektionen)

Som myndighet måste skolan bedöma vilken information som ska användas, sparas och vilka bestämmelser i dataskyddsförordningen och skollagen som är tillämpliga.



Hur granskas Lexplore?

Förutom vår egen expertis använder vi oss av externa specialister inom juridik och datasäkerhet för att vara säkra på att vi möter, eller överträffar, de krav som finns. Dessutom gör skolor och kommuner som personuppgiftsansvariga egna granskningar.



Om Lexplore

Vi som jobbar på Lexplore har skilda erfarenheter, bakgrund och roller. Här finns forskare, entreprenörer, pedagoger, utvecklare, litteraturvetare och ingenjörer. Det som förenar oss är vårt engagemang för skolan och drivkraften att alla barn ska upptäcka läsandets och skrivandets magi. Läs- och skrivsvårigheter ska inte hindra någon från att utvecklas och nå kunskapsmålen i skolan.

Det handlar om att få syn på läsningen. Att se elevernas autentiska läsning från avkodning till språkförståelse. Det handlar om att få en objektiv översikt över elevernas läsning för att, i tid, kunna sätta in rätt stöd och stimulans för att främja läsningen. Det handlar om läsutveckling för alla elever.

Därför startade vi Lexplore.



Lexplore