Utvalda juridiska aspekter rörande personuppgifter vid träning av NLP-modeller med patientjournalstexter

Sebastian Berg, jurist

| techlaw

1

Juridisk information

Denna presentation utgör allmän information. Presentationen är inte avsedd att vara uttömmande eller tillräcklig som grund för att fatta beslut i konkreta frågor utan är endast ämnad att användas i informationssyfte och utgör inte rådgivning. Vid en specifik rättslig fråga bör en kvalificerad jurist konsulteras. Samtliga exempel och scenarier i denna presentation är hypotetiska och utgör förenklingar av verkligheten.

2

Avgränsningar

- Syftet med denna presentation: belysa utvalda juridiska aspekter avseende användning av anonymiserade patientjournaler för träning av NLP-modeller
- Presentationen är begränsad till enskilda juridiska aspekter avseende den allmänna dataskyddsförordningen (GDPR) och patientdatalagen (2008:355, PDL) hos offentliga vårdgivare

3

Framtagning av NLP-modeller inom hälso-och sjukvården

- AI har stor potential för effektivisering inom och förbättring av hälso- och sjukvården
- Tänkbara tillämpningar av NLP-modeller inom sjukvården är verktyg för kvalitetssäkring och beslutsstöd
- Framtagning av NLP-modeller kräver tillgång till träningsdata som exempelvis patientjournalstexter
- Patientjournaltexter innehåller (känsliga) personuppgifter
- Träning av NLP-modeller innebär en behandling av personuppgifter
- Reglerna i GDPR och PDL blir tillämpliga

4

Framtagning av NLP-modeller inom hälso-och sjukvården

- PDL kompletterar GDPR på området hälso-och sjukvård
- Patientjournaler omfattas av särskilt restriktiva krav som till exempel:
  - Krav på lagreglerad tystnadsplikt
  - Strikt reglering av ändamålen för vilka patientjournalerna får användas
- Offentliga vårdgivare kan ha ett intresse av att undvika behandling av personuppgifter vid träning av NLP-modeller

5

Ändamålsbegränsning

- Personuppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (principen om ändamålsbegränsning, art. 5.1 b GDPR)
  - Särskilda ändamål → olika ändamål måste avgränsas från varandra
  - Uttryckligt angivna ändamål → krav på dokumentation och information
  - Berättigade ändamål → förenligt med lag, sedvana m.m. (går utöver kravet på rättslig grund)
- Behandling för andra ändamål kan vara tillåten om detta är förenligt med det ursprungliga ändamålet (krav på kompatibilitetsbedömning, art. 6.5 GDPR)
- Principen om ändamålsbegränsning är av central betydelse
- PDL begränsar för vilka ändamål personuppgifter får behandlas inom hälso- och sjukvården (2:4 PDL)

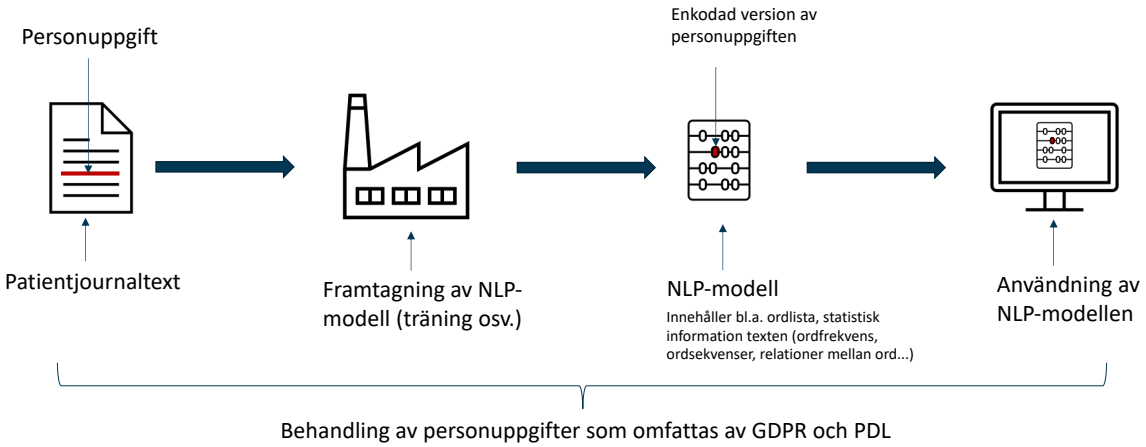
6

Principer för behandling av personuppgifter

- Art. 5 GDPR
- Principer:
  - Laglighet, korrekthet och öppenhet
  - Ändamålsbegränsning
  - Uppgiftsminimering
  - Riktighet
  - Lagringsminimering
  - Integritet och konfidentialitet
  - Ansvarsskyldighet
- Syfte: skydda de registrerades rättigheter och friheter genom att skydda deras personuppgifter

7

Scenario 1: Offentlig vårdgivare tar fram en NLP-modell med icke-anonymiserade patientjournaltexter



8

Exempel på utmaningar med Scenario 1

- För vilka ändamål kommer NLP-modellen att användas?
- Är dessa ändamål förenliga med ändamålsbegränsningarna i PDL?
- Vilken rättslig grund kan användas som stöd för personuppgiftsbehandlingen?
- Hur säkerställs att patienterna informeras på det sätt som krävs?
- Hur säkerställs att patienterna kan utöva sina rättigheter?
- ...

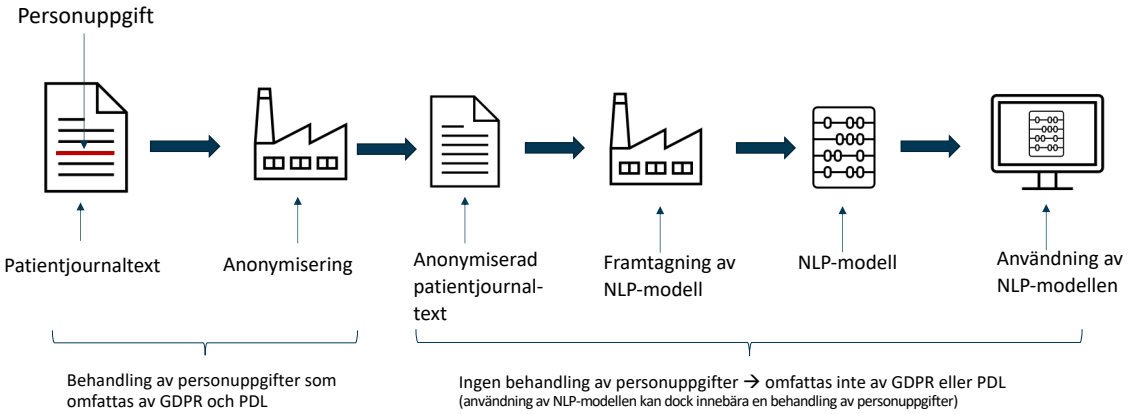
9

Anonymiserade personuppgifter

- Personuppgift är en uppgift som avser en identifierad eller identifierbar fysisk person (art. 4.4 GDPR)
- En fysisk person är identifierbar om den kan identifieras direkt eller indirekt (art. 4.4 GDPR)
- Information som inte hänför sig till en identifierad eller identifierbar fysisk person utgör inte en personuppgift (skäl 26 GDPR)
- Personuppgifter som anonymiserats på ett sådant sätt att fysiska personer inte längre är identifierbara (anonymiserade personuppgifter) utgör inte personuppgifter (skäl 26 GDPR)
- Behandling av anonymiserade personuppgifter faller utanför GDPR:s och PDL:s tillämpningsområde (jmf. art. 2 GDPR och 1:1 PDL)

10

Scenario 2: Offentlig vårdgivare tar fram en NLP-modell med anonymiserade patientjournaltexter



11

Exempel på utmaningar med Scenario 2

- Jämfört med Scenario 1 reduceras den juridiska komplexiteten
- Anonymiseringsprocessen är en behandling av personuppgifter som omfattas av reglerna i GDPR och PDL → efterlevnad av reglerna måste säkerställas
- Anonymisering av personuppgifter är en komplicerad process

12

Anonymisering av personuppgifter är komplicerat (men inte omöjligt)

- Anonymisering kräver att personuppgifter bearbetas så att en enskild individ inte längre kan identifieras med alla hjälpmedel som rimligen kan komma att användas
- Det finns inte några absoluta kriterier för att fastställa när en uppsättning av personuppgifter ska anses vara anonymiserade eller inte
- GDPR:s kriterier är allmänt hållna (teknikneutral och framtidssäker lagstiftning)
- Dataskyddsmyndigheter har utvecklat ett riskbaserat angreppsätt för anonymisering

13

Riskbaserat angreppsätt för anonymisering

- AG-29, Yttrande 05/2014 om avidentifieringsmetoder, WP 216
- Risken för en potentiell återidentifering ska sänkas till en acceptabel nivå
- Detta innebär att riskerna för särskiljbarhet, länkbarhet och inferens ska sänkas till en acceptabel nivå
- Vilken risknivå som är acceptabel avgörs i det enskilda fallet och mot bakgrund av den senaste tekniska utvecklingen
- Sannolikheten för att anonymiserade personuppgifter kan komma att återidentifieras ökar över tid på grund av den tekniska utvecklingen
- En regelbunden utvärdering av den kvarstående risken för återidentifiering krävs
- Det kan vara svårt att fastställa den exakta gränsen för när personuppgifter övergår till anonymiserade personuppgifter
- Det finns inte särskilt mycket rättspraxis på området

14

Anonymisering av patientjournaltexter

- Exempel på metoder för att anonymisera patientjournaltexter:
  - Avidentifiering (de-identification)
  - Borttagning av delar av texten (obfuscation)
  - Differentiell integritet (differential privacy)
- Huruvida dessa metoder möjliggör en effektiv anonymisering av texterna är omdiskuterat (särskilt när träningsdata omfattar stora mängder text)
- En viss typ av inferensattack (membership inference attack) diskuteras regelbundet som risk för återidentifiering av enskilda vid användning av NLP-modeller
- Att det förs en sådan diskussion innebär dock inte att anonymisering av texterna per automatik är omöjlig
- Det krävs nyanserade juridiska analyser

15

Sammanfattning

- Juridiken avseende användning av anonymiserade patientjournaler för träning av NLP-modeller hos en offentlig vårdgivare är komplicerad
- Det finns inga enkla svar
- Det krävs nyanserade juridiska analyser och bedömningar i varje enskilt fall
- Mer arbete för att analysera gränsdragningen mellan personuppgifter och icke-personuppgifter i sammanhanget patientjournalstexter behöver göras
- Juridisk kompetens bör involveras löpande i NLP-projekt
- Anonymisering av personuppgifter är endast en av många aspekter som behöver beaktas vid träning av NLP-modeller

16

Tack!

17

| techlaw

Sebastian Berg, jurist
sebastian@techlaw.se

TechLaw Sweden AB | Västmannagatan 13, 111 24 Stockholm | +46 8 559 25 200 | techlaw.se

18