SPV

PRAKTISKE PROBLEMSTILLINGAR FOR GDPR-PROSJEKT

Finans Norges juskonferanse 2017

Håvard Hanto-Haugse

SparebankenVest

PRAKTISK TOLKING

SparebankenVest

OVERORDNA MÅLSTJINGAR

EU sine mål:

- Godt personvern
- Like reglar i EU

Våre mål:

- Etterleva krava
- God drift

VÅRT PROBLEMET

- Vanskeleg å forstå kva EU meiner skal til for eit godt personvern:
  - Rot med omgrep
  - Tvetydige omgrep
  - Uklare intensjonar
  - Manglande gjennomføring av klare intensjonar
  - Mangel på rettskjelder
- Kostbart å oppfylla

EU SIN MOTIVASJON FOR Å LAGA REGELVERK

- Krav til tryggleik og dokumenterte prosedyrar kjem fordi nokon har tabba seg ut. Operasjonell risiko skal koma under kontroll.
- Rettar til dei registrerte kjem fordi nokon har misbrukt tillit. Dei registrerte sine forventningar skal møtast.

EQUIFAX

Avfallsservice AS

SAMANFALLANDE INTERESSER

- God kontroll med operasjonell risiko gjev grunnlag for stabile resultat.
- Å møta kunden sine forventningar er grunnlaget for god kundetilfredsheit, som igjen er grunnlaget for vekst.
- Drivarne for EU sitt regelverkarbeid er dei same som momenta som burde vera drivarane for vår drift!

OVERSIKT OVER HANDSAMINGS-AKTIVTETAR

- Artikkel 30

SparebankenVest

PLIKT

- Handsamingsansvarleg pliktar å føra “protokoll over behandlingsaktiviteter”, jf. GDPR artikkel 30.1.
- Artikkel 30 gjeld i utgangspunktet berre dei med meir enn 250 tilsette eller
  - dersom handsaminga medfører risiko for dei registrerte sine rettar og fridomar,
  - handsaminga ikkje skjer ved høve («leilighetsvis»), eller
  - handsaminga omfattar sensitive personopplysningar eller opplysningar om straffbare handlingar.
- Alle finansføretak handsamar personopplysningar systematisk (ikkje ved høve) og dei flest har sensitive personopplysningar.

FORNUFT

- Kontroll med operasjonell risiko krev at ein har oversikt over «butikken».
- Praktisk som sjekklista når ein går i gang med dokumentasjon etter art. 5.
- Elementa i oversikten er i stor grad eit produkt av plikter ein uansett er pålagt å utføra.
- Elementa i oversikten kan lett utvidast for å dekka annan risiko verksemda er opptatt av.

KVA ER EIN «BEHANDLINGSAKTIVITET»?

- Ein “behandling” består av eit sett med “operasjoner”, til dømes innsamling, lagring, utlevering eller sletting av opplysningar.
- Uklart kor store sett med operasjonar som kan inngå i ei handsaming. Grensa går ein stad mellom operasjonar som er naudsynte for å “skanne giro ved mottak” og alt som naturleg fell inn under “betalingstenester”.
- Ingen omtale i fortalen, ingen rettspraksis eller forvaltningspraksis.
- Dessutan uklart om «behandling», jf. art 4 2) og «behandlingsaktivitet», jf. art 30.1 og 30.2 er det same.

KVA GJEV GOD KONTROLL?

- Rimeleg god oversikt over verksemda.
- På eit nivå som er eigna til styring.
- Synleggjera moment som medfører særlege plikter eller risiko, til dømes ulike heimlar, automatiserte avgjerder, bruk av sensitive personopplysningar.
- Mogeleg å halda oppdatert:
  - Klarer ikkje å halda oppdatert dersom alle små endringar utløyser trong for revisjon.
  - Må vera lett å identifisera når det skjer endring om utløyser trong for revisjon og å laga oppdatert dokumentasjon.

SPV SIN HYPOTESE

- BIAN 5.0 er eit godt utgangspunkt:
  - Gjennomarbeidd for «alt» bankar driv med.
  - «Medium» detaljert (ca. 300 «services» totalt, ikkje alle brukar personopplysningar og ikkje alt vi driv med).
  - Same systematikk som banken sin virksomhetsarkitektur er bygd på.
  - Same systematikk som banken sin største systemleverandør bygger på.
  - Mogeleg å koma i mål raskt nok til at vi kan implementera innan mai -18 der vi finn utfordringar.
  - Dersom det er for lite detaljert, har BIAN delt kvar «service» opp i ulike «business scenarios» som ein kan jobba vidare med.
- Men ikkje utforma med tanke på GDPR:
  - Tek ikkje omsyn til at ulike «set of operations» innanfor same «service» kan ha ulike heimlar etter artikkel 6 og 9.
  - Tek ikkje omsyn til særleg risiko for dei registrerte sine rettar.

SPV SIN BESLUTNING PR 10.10.2017

Bankens protokoll over behandlingsaktiviteter i henhold til artikkel 30 skal føres med utgangspunkt i «tjenester» som beskrevet i BIAN 5.0, med følgende justeringer:

- behandlinger som har flere hjemler etter artikkel 6 og/eller 9, skal deles i en behandlingsaktivitet for hver hjemmel, og
- dersom en behandling omfatter automatiserte avgjørelser, skal hver avgjørelse som omfattes av artikkel 22 skilles ut i en egen behandlingsaktivitet.

INFORMASJONS-KRAV VED SAMTYKKE

- Artikkel 7.2

SparebankenVest

UKLART KRAV OM KLART SPRÅK

- Informasjons skal «fremlegges […]i en forståelig og lett tilgjengelig form og på et klart og enkelt språk».

- Mitt råd:
  - Fokuser på at målet er forventningsavklaring: Kunden skal ikkje oppleva handsaminga som tillitsbrot.
  - Parker den juridiske debatten, ta på LEAN-hatten. Frå eit langsiktig forretningsperspektiv er det ikkje godt nok å ha «ryggen fri». Vi må sikra ei god kundeoppleving.
  - Sjå på samtykka og samtykkeløysinga som verktøy for kundedialog som skal munna ut i tydeleg forventningsavklaring.

FRAMTIDA TIL KONSESJONANE

- Høyringsnotatet kapittel 15.3

SparebankenVest

IKKJE GRUNNLAG FOR Å VIDAREFØRA KONSESJONSPLIKT

- Forordninga opnar berre for plikt til førehandsgodkjenning av handsamingar som vert utført «i allmennhetens interesse», jf. artikkel 36.5. Omgrepet viser tilbake til heimelen i artikkel 6.1 e) første alternativ.
- Artikkel 6.1 e) er eit svært lite praktisk heimelsgrunnlag for finansverksemder, med mogeleg unntak for nokre samarbeidsfunksjonar.

OVERGANGSPERIODE FOR GJELDANDE KONSESJONAR?

- Fortalen avsnitt 171 opnar for vidareføring av «godkjenninger gitt av tilsynsmyndigheter [..] fram til de endres, erstattes eller oppheves».
- Datatilsynet og departementet har tidlegare gitt uttrykk for at konsesjonane skal halda fram å gjelda i ein overgangsperiode. Dei har vore veldig uklare på kva dei legg i det.
- Konsesjonane medfører ein god del begrensningar for finansføretaka. PISP-ar, AISP-ar eller andre som startar butikk her i landet etter mai -18 vil slippa desse. Avhengig av korleis overgangsreglane vert utforma, kan det vri konkurransen.

OVERGANGSREGLAR ER BERRE EIT GODE (FOR OSS)

- Fortalen avsnitt 171 omhandlar fristar for å innretta pågåande handsamingar med forordninga. Det vert berre opna for vidareføring av «godkjenninger».
- Både ordlyd og kontekst tilseier at det berre er opna for at handsamingar som er i strid med forordninga kan halda fram i ein overgangsperiode.
- Det er ikkje opning for å videreføra vilkår i konsesjonane som er strengere enn det som følgjer av forordninga.
- Dersom den handsamingsansvarlege kan dokumentera at handsaminga er i samsvar med forordninga, vil eventuelle ytterlegare skrankar i konsesjon vera ugyldige.

PERSON-OPPLYSNINGAR I TEST

SparebankenVest

PERSONOPPLYSNINGAR I TEST (1 AV 2)

- Forskrift om systemer for betalingstjenester § 3 set krav om «tiltak for å sikre nødvendig konfidensialitet, integritet og tilgjengelighet for tjenestene»
- IKT-forskrifta viser til personopplysningsforskrifta kapittel 2, som set krav om tiltak mot uautorisert innsyn, tiltak for å sikra tilgang og tiltak mot uautorisert endring.
- Forordninga artikkel 32.1 set krav om «egnede tekniske og organisatoriske tiltak for å […] sikre vedvarende fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssytemene og tjenestene».
- Testing av system er eitt slikt tiltak.

PERSONOPPLYSNINGAR I TEST (2 AV 2)

- Testingen må kontrollera funksjonalitet over tid, og integrasjonen mot andre systemkomponentar. Det gjer at datasettet for den enkete testpersonen må vera omfattande.
- Testingen må vera eigna til å avdekka om systemet taklar kjente feil. Det gjer at datasetta må reflektera faktiske hendingar.
- Påstand frå testmiljøet: Erfaring viser at vi får for dårleg kvalitet på datasetta dersom vi prøver å simulera hendinga med syntetiske data. Ved kritiske feil er det heller ikkje tid til å produsera syntetiske datasett.
- Gitt at påstanden kan dokumenterast, må datasett med personopplysningar brukast i nokre testar for å sikra naudsynt konfidensialitet, integritet og tilgang.

VI ER HER.

SparebankenVest