Personverntrender 2020

Finans Norges fagsamling for personvern 28 og 29. januar 2020

03.02.2020 | Kaare M. Risung

SCHJØDT

BASIS FOR PV-TRENDER

- Dommer
- Saker som har vært oppe for tilsyn
- EDPB (og tilsyns) opinions/guidelines/drafts
- Rådets arbeidsliste og utvikling av GDPR - https://www.consilium.europa.eu/register/en/content/out?&typ=ENTRY&i=ADV&DOC_ID=ST-14994-2019-REV-1
- Nasjonale tilsyns innspill til utvikling av GDPR
- Teori
- Næringslivets egne erfaringer

AGENDA

- Datasikkerhet blir viktigere
- Mer fokus på kravene til innebygget personvern
- Økt bruk av felles behandlingsansvar
- Personvern på vei inn i M&A
- Krav til samtykke tar liv av flere tjenester
- Berettiget interesse viser seg nyttig
- Fler retningslinjer
- Mindre formalisme?
- Økt robotisering
- «NAV-lærdom»?

ØKT OPPMERKSOMHET RUNDT DATASIKKERHET

- BA-saken
- Hydro-saken - ikke den siste i Norge
- Nasjonalstaters bruk av cyberkrigføring
- Sjekk IBMs «Cost of a Data Breach Report 2019» https://www.ibm.com/security/data-breach
- MÅ INSTALLERE SIKKERHETSOPPDATERINGER REGELMESSIG!

MER FOKUS PÅ KRAVENE TIL INNEBYGGET PERSONVERN

- Saker
  - https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-20192/endelig-vedtak-om-gebyr-til-bergen-kommune/ [18.3.19. MNOK 1,6. Brukernavn og passord for administratortilgang i åpen mappe, gjenbruk av passord, enfaktorautentisering]
  - https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-20192/gebyr-til-oslo-kommune/ [11.10.19. MNOK 0,5. Sykehjems arbeidsliste i Word i usikret sone. Ikke pekt på GDPR art 5]
  - https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2019/gebyr-til-oslo-kommune-utdanningsetaten/ [11.10.19. MNOK 1,2. Skolemelding. Manglende sikring av API, feil i logikk i autentisering, manglende kobling innlogget og hvem man kunne hente informasjon om]
  - https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-20192/arendal-kommune-ma-avslutte-behandlingen-av-personopplysninger-i-spekter/ [Spekter – informasjon om mobbing. Mangelfull informasjon, men også felter med mulig sensitive PO]

INNEBYGGET PV….

- Tyske DPA
  - *In the view of the German DPAs, the data protection by design requirement in Article 25(1) GDPR does not cover the target group of **producers** and has thus hardly caught on in practice. It covers data controllers that often do not develop hardware and software themselves but rely on contractors' services. Suggested solution: **The GDPR should be amended to oblige producers to implement data protection by design and the liability section in Article 82 GDPR should be extended to producers**.*
- Nye retningslinjer:
  - https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-20192/retningslinjer-for-innebygd-personvern-og-personvern-som-standardinnstilling-pa-horing/

ØKT BRUK AV FELLES BEHANDLINGSANSVAR

- Mange tvister om rolleforståelse
- Mange nye argumenter for felles behandlingsansvar, som kan løse binære tvister om roller som behandlingsansvarlig-databehandler
- C-210/16 (Facebook fan page)
- C-40/17 (Facebook like button)

PERSONVERN PÅ VEI INN I M&A

- Marriott-saken
- «Smitting»
- Betydning av grundig DD
- Datasikkerhets-DD vil bli mer vanlig
- Dreier seg om å sikre verdier, ikke bare å kontrollere risiko

KRAV TIL SAMTYKKE TAR LIV AV FLERE TJENESTER

- Nettkapsler til markedsføring på vei ut
  - Googles pågående kampanje, Apple, Facebook
  - C-673/17 (Planet49), pkt 2: … *not to be interpreted differently according to whether or not the information stored or accessed on a website user's terminal equipment is personal data…*
  - Belgiske DPA: Although an improved version of the website did seek consent, the consent obtained was not sufficiently granular. According to the SA, users should be able to consent to different categories of cookies used for different non-essential purposes. While consent on a per-cookie level is not required, the SA said it would welcome such a development;…
- Innspill Tyske tilsyn: *only possible legal bases for profiling should be consent or contractual necessity*
- Ugyldig samtykke til ansiktsgjenkjenning: https://www.datainspektionen.se/nyheter/sanktionsavgift-for-ansiktsigenkanning-i-skola/
- PSD2
  - Hvordan skal nye aktører håndtere krav til samtykke? Aktiv bruk av GDPR

BERETTIGET INTERESSE FUNGERER

- Oslo tingretts dom 17. desember 2019 i sak 19-098312 – Legeforeningen – Personvernnemda (legeliste-saken)

FLER RETNINGSLINJER KOMMER

- EU Rådet
  - Pkt 12: .. *the Council deems that controllers and processors need more clarification and guidance…. The Commission's upcoming evaluation report should also highlight the broad need for practical guidelines and other suitable means to meet this need.*
  - Pkt 19: … *The Commission is encouraged to review and revise* [**SCC**] *in the near future to take into account the needs of controllers and processors*.
  - Pkt 13: Measures to encourage the drafting of such codes of conduct should be increased and further developed.
- På tide å se flere Codes of conduct - nyttig virkemiddel og tiden har gått….
- Danske datatilsynets DBA kan faktisk brukes

  https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/ny-standard-databehandleravtale-som-kan-brukes-i-norge/

MINDRE FORMALISME?

- SMB-unntak
  - EU Rådet pkt 31: *According to information from some Member States, SMEs are dissatisfied, for example, with the limited derogation from the obligation to maintain a record of processing activities. Article 30(5) of the GDPR exempts enterprises or organisations employing fewer than **250 persons** from the requirement to maintain a record of processing activities, but under a set of **conditions that only seldom apply**. While recognising that the risk-based approach of the GDPR was a choice made by the legislator, the Council considers that it would be important to try and assess how the intended balance between the risk-based-approach, on the one hand, and the need to take into account the **special needs of SME's** (recital 13), on the other hand, works in practice.*
  - EU Rådet pkt 38: *Attention should be paid, in particular, to:. practical tools for SMEs and charitable or voluntary associations, such as a harmonised form for controllers and processors to notify the supervisory authorities of personal **data breach**, or a **simplified record** of processing, as well as other appropriate tools for SMEs to apply the GDPR in view of their specific needs;..*

MINDRE REN FORMALISME?

- Redusere antall avviksmeldinger?
  - Tyske DPA: The German DPAs note that the number of data breach notifications has increased significantly since the GDPR became applicable. Many controllers notify breaches without having done a risk assessment due to the potentially heavy fines, leading to the **notification of trivial and minor breaches**. Suggested solution: The data breach notification obligation should be **limited to cases that are likely to result in more than merely a minimal risk to the rights and freedoms of data subjects**.
- Unngå overflyt av informasjon
  - Tyske DPA: The German DPAs consider it "unrealistic" to provide comprehensive information in accordance with Article 13 GDPR in case of a verbal or telephone contact. They refer to complaints by data subjects about **information overload** in this regard. Suggested solution: It should be sufficient to implement a **layered, risk-based approach**, telling the data subjects where they can find further relevant information.

TYSKE DPA - ØVRIG

- The German DPAs note that the duty to communicate the **contact details of data protection officers** to the supervisory authorities under Article 37(7) GDPR creates additional work for controllers and unnecessary processing of personal data by the supervisory authorities. Suggested solution: Article 37(7) GDPR should be deleted.
- The German DPAs discuss the legal bases and requirements for **further processing** of personal data where the purpose of the processing changes. Suggested solution: Article 6(4) GDPR should be amended to clarify that further processing of personal data shall be limited to that which is carried out by the same controller.
- The German DPAs criticize that their **powers under Article 58(2) GDPR are limited to "processing operations**." However, the GDPR contains obligations that are independent of the processing principles set forth in Article 5 GDPR (e.g., designation of a data protection officer or duty to maintain a record of processing activities). Suggested solution: The reference to "processing operations" in Article 58(2)(a) and (b) GDPR should be deleted.
- The German DPAs note that EU member states have very different traditions regarding direct marketing and, thus, data subject expectations also differ. Suggestion solution: **The EU legislature should create more detailed direct marketing provisions**.
- The German DPAs describe profiling as "one of the key data protection policy challenges of our times". They state that most of the GDPR provisions do not cover "profiling as such" and, thus, assessments usually have to be based on the general elements set forth in Article 6 GDPR. Suggested solution: The GDPR provisions on profiling should be amended, providing greater transparency and more control to data subjects. Further, the **only possible legal bases for profiling should be consent or contractual necessity.**
- Se hele rapporten her: https://www.datenschutzkonferenz-online.de/media/dskb/20191213_evaluation_report_german_dpa_s_clean.pdf

ØKT ROBOTISERING

- FinAuts retningslinjer for robotisert finansiell rådgivning
- Større klargjøring av krav til redegjørelse for «black box»
- Ansvarlig kunstig intelligens – Life 3.0

NAV-LÆRDOM?

- Norsk rett må tolkes i EU-tradisjon, men med særtrekk i Norge som EØS-land, jf. f.eks. Nkom om nettkapsler
- GDPR belagt med overtredelsesgebyr, som er straff etter EMK – krever klar sannsynlighetsovervekt for brudd
- Prop. 93 L (2016-2017), pkt 6.4.4 i tilknytning til mfl:

- *… Legalitetsprinsippet og EMK artikkel 7 krever at bestemmelser som hjemler ileggelse av administrative sanksjoner, må være **tydelige og klare** slik at det for borgerne er **forutberegnelig** når en sanksjon kan ilegges. Dette taler mot adgang til å ilegge overtredelsesgebyr ved overtredelse av regler som er skjønnsmessige*
- *.. både på nasjonalt og europeisk nivå har utviklet seg retningslinjer og praksis på området som i noen grad **klargjør hva som ligger i begrepene***
- *.. avskrekkende overfor enkelte, **særlig useriøse aktører***
- *.. **høy terskel** for bruk av overtredelsesgebyr som sikrer de næringsdrivende tilstrekkelig forutberegnelighet*

++++++

- Ansvarsfordeling identitetstyveri
- Bruk av biometri, herunder ansiktsgjenkjenning
- Ansvarsbegrensning
- Økt markedsføring av personvernvennlige tjenester