Status personvern
- og hva skjer (kanskje) i 2022?

Januar 2022 | Eva Jarbekk

SCHJØDT

AGENDA

- Datatilsynets varslede fokusområder
- Databehandlers bruk av opplysninger fra behandlings-ansvarlig
- Andre områder fremover

DATATILSYNETS VARSLEDE FOKUSOMRÅDER

...DATATILSYNET.DK

Når det gælder de planlagte tilsyn, har Datatilsynet i første halvår af 2019 valgt at fokusere på følgende temaer:

- Brud på persondatasikkerheden hos offentlige myndigheder og private virksomheder
- Databeskyttelsesrådgiverfunktionen hos kommunerne
- Kryptering af e-mails hos private virksomheder
- Autorisation af medarbejdere hos kommunerne
- Den registreredes indsigtsret hos offentlige myndigheder og private virksomheder
- Brug (og genbrug) af data i den kommunale forvaltning
- Aggregering og sammenstilling af data til brug for videresalg hos private virksomheder

...DATATILSYNET.NO 20. JANUAR 2022

Områder vi vil se på vil være oppfyllelse av personvernprinsippene, *innebygd personvern*, behandlingsansvar, ivaretakelse av registrertes rettigheter, om det er opprettet *personvernombud* og dennes plass i organisasjonen, samt kontrollere virksomhetenes styringssystem for personvern og *informasjonssikkerhet*. Vi vil også gjennomføre noen tilsyn med *algoritmer* i løsninger og systemer som benytter kunstig intelligens.

Med andre ord: det meste... i tillegg til AI

MEN: ikke tredjelandsoverføringer *spesifikt* – med mindre en konkurrent eller bruker klager... Da må de ta stilling til det.

DATABEHANDLERS BRUK AV BEHANDLINGSANSVARLIGES PERSONOPPLYSNINGER TIL EGNE FORMÅL - 12. JANUAR 2022

..ofte uenighet leverandør/kunde om hvordan dette kan gjøres

CNIL.

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

MA CONFORMITÉ AU RGPD | THÉMATIQUES | TECHNOLOGIES | TEXTES OFFICIELS | LA CNIL

> Sous-traitants : la réutilisation de données confiées par un responsable de traitement

Sous-traitants : la réutilisation de données confiées par un responsable de traitement

12 janvier 2022

Un sous-traitant ne peut réutiliser des données personnelles pour son propre compte que si cette réutilisation est compatible avec le traitement initial et que le responsable du traitement lui en a donné l'autorisation écrite.

Sous-traitants : une autorisation du client est nécessaire

Conformément au RGPD, le sous-traitant ne peut traiter (utiliser) les données personnelles auquel il a accès que sur instruction documentée du responsable du traitement. Le sous-traitant peut donc licitement traiter les données tant qu'il agit pour se conformer de la meilleure façon et la plus sûre possible aux instructions du responsable du traitement. En revanche, **il ne peut pas réutiliser ces données pour son propre compte, de sa propre initiative,** sauf si un texte national ou européen le lui impose.

Le sous-traitant qui réutiliserait les données de sa propre initiative **serait qualifié de responsable de ce traitement** et **passible de sanctions** pour ne pas avoir agi dans le respect des instructions du responsable du traitement initial.

Le **responsable du traitement peut toutefois, dans les conditions décrites ci-dessous, autoriser son sous-traitant à réutiliser pour son propre compte les données personnelles.** Le sous-traitant devient alors responsable de ce nouveau traitement.

Responsables de traitement : les conditions pour donner une autorisation

Procéder à un « test de compatibilité » avant d'accorder son autorisation

Une réutilisation des données par un sous-traitant pour une finalité propre constitue un traitement dit « ultérieur », c'est-à-dire un traitement qui suit l'opération de collecte et qui a une finalité différente de celle justifiant la collecte initiale.

Le responsable du fichier doit **déterminer si ce traitement ultérieur est compatible avec la finalité pour laquelle les données ont été initialement collectées**, lorsque le traitement ne s'appuie pas sur le consentement de la personne concernée ou sur le droit de l'Union ou le droit d'un État membre.

Pour cela, il doit notamment tenir compte :

- de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données personnelles ont été collectées et les finalités du traitement ultérieur envisagé ;
- du contexte dans lequel les données personnelles ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
- de la nature des données personnelles, en particulier si le traitement porte sur des données sensibles ou des données personnelles relatives à des condamnations pénales et à des infractions;
- des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
- de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

Exemple : un sous-traitant souhaite réutiliser des données pour une finalité d'amélioration de ses prestations de *cloud computing*. Cette réutilisation pourrait être considérée compatible avec le traitement initial, sous réserve de garanties appropriées telle que l'anonymisation des données si ces données identifiantes ne sont pas nécessaires. En revanche, leur réutilisation pour une finalité de prospection commerciale satisferait difficilement le « test de compatibilité ».

Si le test n'est pas satisfait, le responsable du traitement doit refuser de donner son autorisation à la réutilisation des données. Si le test est satisfait, le responsable du traitement est libre de donner ou non son accord.

Pas d'autorisation préalable et générale

Ce « test de compatibilité » doit être réalisé pour un traitement déterminé, en tenant compte des finalités et des caractéristiques de chaque traitement pour lequel le sous-traitant souhaite réutiliser les données.

Cela signifie qu'une autorisation préalable et générale de réutilisation des données n'est pas légale.

L'autorisation doit être écrite

L'autorisation du responsable du traitement initial doit être établie par écrit, y compris en format électronique.

Le RGPD impose, en effet, un contrat ou tout autre acte juridique écrit pour encadrer le traitement mis en œuvre par un sous-traitant.

Le partage des obligations du RGPD

Le responsable du traitement initial doit informer les personnes concernées

Il revient, en principe, au responsable du traitement initial d'informer les personnes concernées

https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement

BETINGELSER

1. Den behandlingsansvarlige må **godkjenne** behandlingen

2. Formålet med behandlingen må være i tråd med det opprinnelige formålet – se Art. 6 (4) om «**forenlighet**»

3. De registrerte må få **informasjon**

ARTIKKEL 6(4) – DOKUMENTERE FORENLIGHET KONKRET

..for å avgjøre om behandlingen for et annet formål er forenlig med formålet som personopplysningene opprinnelig ble samlet inn for, blant annet ta hensyn til følgende:

a) enhver **forbindelse mellom formålene** som personopplysningene er blitt samlet inn for, og formålene med den tiltenkte viderebehandlingen,

b) i hvilken sammenheng personopplysningene er blitt samlet inn, særlig med hensyn til forholdet mellom de registrerte og den behandlingsansvarlige,

ARTIKKEL 6(4) – DOKUMENTERE FORENLIGHET KONKRET

c) **personopplysningenes art**, især om særlige kategorier av personopplysninger behandles, i henhold til artikkel 9, eller om personopplysninger om straffedommer og lovovertredelser behandles, i henhold til artikkel 10,

d) de mulige **konsekvensene** av den tiltenkte viderebehandlingen for de registrerte,

e) om det foreligger nødvendige garantier, som kan omfatte **kryptering eller pseudonymisering**

ANDRE OMRÅDER FREMOVER

AWS – «NITRO» – CONFIDENTIAL COMPUTING

MS: Hvis NSA pålegger oss å utlevere info (og protest ikke lykkes), åpner vi krypteringen og gir info til NSA

AWS: Vi kan ikke bryte krypteringen i «nitro» og klarer ikke å gi NSA informasjon

Confidential computing:

- Hardware-basert (!), «data in use» er kryptert (eller beskyttet), RAM er lukket,
- Liten/ingen treghet? Fullverdige tjenester?
- Mer info kommer

GOOGLE ANALYTICS

- EU-parlamentet innklaget av NOYB
- 11. januar 2022: EDPS sier bruk av GA må opphøre
- Ingen bot
- Begrunnet i ”Schrems”, US overvåkning
  1. IP-adresser er PO, selv om siste (X) sifre fjernes i innstilllingene i GA – viktig ifht pseudonymiseringskrav
  2. Google gjenkjenner brukere fordi bruker ofte er pålogget google-konto
  3. Ingen hjelp i nye SCC’er

- OBS: 101 andre saker (dalmatinerne) om FB og GA skal avgjøres snart

«EDPS gjorde det klart at bare det å plassere en informasjonskapsel av en amerikansk leverandør på nettstedet er i strid med EUs personvernlovgivning. Ingen skikkelig beskyttelse mot amerikansk overvåking var på plass, til tross for at europeiske politikere er et kjent mål for overvåking», sier Schrems.

https://www.digi.no/artikler/eu-parlamentet-brot-eu-reglene-for-informasjonskapsler/516413

ALTERNATIVER TIL GA (AD-FINANSIERT)

Matomo (største konkurrent, lokal hosting)

Fathom (betalingstjeneste, henter ikke PO, US-basert)

Plausible (EU-made)

Umami

66analythics

Splitbee

Simple analytics

GoatCounter

Ackee

Beampipe

..etc...

FOKUS PÅ INDIA SOM TREDJELAND

EDPB har engasjert **eksterne** rådgivere til å vurdere rettstilstanden i Kina, Russland – og India

Ingen av landene vurderes å ha bra personvern

COOKIE-BØTER

Kun en knapp for å **akseptere** cookies, men ingen enkel knapp for å **avvise** cookies

Google varsles bot på EUR 150 000 000 og Facebook EUR 60 000 000

Tre måneder på seg til å endre praksis, deretter får de 100 000 euro i dagbøter inntil endring skjer

DATATILSYNENES ROLLE – INTERNE UENIGHETER

Kan avtale brukes som hjemmel for markedsføring og profilering? Ja, sier Irland til FB (og «alle» andre tilsyn protesterer), nei sier Luxemburg til AWS

Uenighet om bøteutmåling: WhatsApp

- Irsk datatilsyn foreslo gebyr på EUR 50 mill.
- Andre tilsynsmyndigheter protesterte og ville ha høyere beløp
- EDPB gikk inn, instruerte DPC i å øke gebyret og DPC ga bot på EUR 225 mill.
- WhatsApp saksøker EDPB

Eva Jarbekk

Partner/lawyer
Head of privact & information security
m: +47 900 51 011
d: +47 23 01 18 29
eva.jarbekk@schjodt.com