DATATILSYNET

Dansk Retursystem A/S
Erik Husfeldts Vej 1
2630 Taastrup
Danmark

Sendt med Digital Post

6. juli 2022

J.nr. 2022-431-0188
Dok.nr. 492203
Sagsbehandler
Poul Erik Weidick

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Anmeldelse af brud på persondatasikkerheden

Datatilsynet er blevet gjort opmærksom på, at Dansk Retursystem A/S (herefter Dansk Retursystem) har udviklet applikationen ”Pant” til brug på smartphones.

Det fremgår af de oplysninger Datatilsynet har modtaget, at applikationen indeholder en række indstillinger og funktioner til bl.a. at spore enhedens lokalitet, registrere brugerens anvendelse af applikationen, læse oplysninger på enheden, f.eks. telefonnumre og at kontrollere enhedens kamera, ligesom applikationen forudsætter interaktion med en bank på enheden, for at indlæse et kontonummer mv.

1. Anmodning om oplysninger

På baggrund af de modtagne oplysninger, skal Datatilsynet anmode om en udtalelse.

Spørgsmålene bedes besvaret **separat for hver platform** (f.eks. Android, Apple mv.) i de tilfælde, hvor der er forskel på applikationens udvikling og drift – herunder også Dansk Retursystems brug af databehandlere mv. – til og på forskellige platforme.

1.1. Vedrørende udviklingen og konstruktionen af applikationen

Dansk Retursystem bedes oplyse:

- Hvordan it-arkitekturen i applikationen ”Pant” er konstrueret og udviklet, herunder
  - hvilken udveksling af oplysninger, der finder sted, når brugere anvender applikationen ”Pant”.
- Hvordan applikationens frontend og backend er blevet udviklet, herunder
  - hvordan servicekommunikationen foregår mellem frontend og backend, og
  - hvilke servicebiblioteker og koderepositorier, der er anvendt.

Dansk Retursystem bedes i den forbindelse fremsende et diagram over, hvordan servicekommunikationen mellem frontend og backend i applikationen finder sted, herunder hele teknologistakken den afvikles på.

Datatilsynet skal anmode om, at besvarelsen dækker hele livscyklus for brugerens download, installation og indrullering over ordinær brug til sletning af applikationen.

1.2. Vedrørende risikovurderinger, jf. databeskyttelsesforordningens artikel 32

Dansk Retursystem bedes oplyse:

- Om Dansk Retursystem har udarbejdet risikovurdering for udviklingen, igangsættelsen og driften af applikationen ”Pant”
- Om Dansk Retursystem i andre tilfælde har udarbejdet risikovurdering for applikationen.

Hvis ovenstående besvares bekræftende, bedes Dansk Retursystem fremsende **anonymiseret** eksempel på den risikovurdering, som Dansk Retursystem har udarbejdet i forbindelse med løsningen.

Såfremt Dansk Retursystem ikke har foretaget risikovurdering i overensstemmelse med databeskyttelsesforordningens artikel 32, bedes Dansk Retursystem redegøre for de overvejelser, der ligger til grund herfor.

1.3. Vedrørende konsekvensanalyser, jf. databeskyttelsesforordningens artikel 35
Dansk Retursystem bedes oplyse:

- Om Dansk Retursystem har udarbejdet konsekvensanalyse for udviklingen, igangsættelsen og driften af applikationen ”Pant”
- Om Dansk Retursystem i andre tilfælde har udarbejdet konsekvensanalyse for applikationen.

Hvis ovenstående besvares bekræftende, bedes Dansk Retursystem fremsende **anonymiseret** eksempel på den konsekvensanalyse, som Dansk Retursystem har udarbejdet i forbindelse med applikationen ”Pant”.

Såfremt Dansk Retursystem ikke har foretaget konsekvensanalyse i overensstemmelse med databeskyttelsesforordningens artikel 35, bedes Dansk Retursystem redegøre for de overvejelser, der ligger til grund herfor.

1.4. Vedrørende brug af leverandører, databehandlere og underdatabehandlere
Dansk Retursystem bedes oplyse:

- Om der i forbindelse med driften og/eller borgeres brug af applikationen ”Pant” sker overførsel af borgernes oplysninger til tredjelande, og i bekræftende fald – på hvilket overførselsgrundlag denne overførsel finder sted.

Dansk Retursystem bedes i den forbindelse – uanset om leverandøren, databehandleren eller underdatabehandler befinder sig i et tredjeland – fremsende en liste til Datatilsynet over samtlige leverandører, databehandlere og underdatabehandlere, som Dansk Retursystem har anvendt i forbindelse med udviklingen, igangsættelsen og driften af applikationen ”Pant”.

1.5. Oplysningsminimering
Dansk Retursystem bedes dokumentere de overvejelser, der er gjort for overholdelse af databeskyttelsesforordningens artikel 5, stk. 1, særligt litra a-c, især i forhold til interaktionen og oplysningsindsamlingen med 3.-parts API op imod bank.

2. Frist for fremsendelse af udtalelse og materiale

Udtalelsen og det ønskede materiale bedes sendt til Datatilsynet **senest onsdag den 10. august 2022** med Digital Post med angivelse af journalnummer 2022-431-0188.

3. Bekræftelse af modtagelse

Dansk Retursystem bedes snarest muligt og **senest onsdag den 13. juni 2022** bekræfte modtagelse af dette brev.

Bekræftelse kan ske til undertegnede på pew@datatilsynet.dk

Hvis ovenstående giver anledning til spørgsmål, er Dansk Retursystem A/S velkommen til at kontakte undertegnede telefonisk på 2949 3252 eller via mail på pew@datatilsynet.dk.

Med venlig hilsen

Poul Erik Weidick

Bilag: Relevante retsregler

Artikel 32. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

a) pseudonymisering og kryptering af personoplysninger
b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Stk. 2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Stk. 3. Overholdelse af en godkendt adfærdskodeks som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1.

Stk. 4. Den dataansvarlige og databehandleren tager skridt til at sikre, at enhver fysisk person, der udfører arbejde for den dataansvarlige eller databehandleren, og som får adgang til personoplysninger, kun behandler disse efter instruks fra den dataansvarlige, medmindre behandling kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

Artikel 35. Hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, foretager den dataansvarlige forud for behandlingen en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger. En enkelt analyse kan omfatte flere lignende behandlingsaktiviteter, der indebærer lignende høje risici.

Stk. 2. Den dataansvarlige rådfører sig med databeskyttelsesrådgiveren, hvis en sådan er udpeget, når der foretages en konsekvensanalyse vedrørende databeskyttelse.

Stk. 3. En konsekvensanalyse vedrørende databeskyttelse som omhandlet i stk. 1 er navnlig påkrævet i følgende tilfælde:

a) en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som er grundlag for afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirker den fysiske person
b) behandling i stort omfang af særlige kategorier af oplysninger, jf. artikel 9, stk. 1, eller af personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10, eller
c) systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

Stk. 4. Tilsynsmyndigheden udarbejder og offentliggør en liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse i henhold til stk. 1. Tilsynsmyndigheden indgiver disse lister til det i artikel 68 omhandlede Databeskyttelsesråd.

Stk. 5. Tilsynsmyndigheden kan også udarbejde og offentliggøre en liste over de typer af behandlingsaktiviteter, for hvilke der ikke kræves nogen konsekvensanalyse vedrørende databeskyttelse. Tilsynsmyndigheden indgiver disse lister til Databeskyttelsesrådet.

Stk. 6. Inden vedtagelsen af listerne i stk. 4 og 5 anvender den kompetente tilsynsmyndighed den sammenhængsmekanisme, der er omhandlet i artikel 63, hvis sådanne lister omfatter behandlingsaktiviteter, der vedrører udbud af varer eller tjenesteydelser til registrerede eller overvågning af sådanne registreredes adfærd i flere medlemsstater, eller som i væsentlig grad kan påvirke den frie udveksling af personoplysninger i Unionen.

Stk. 7. Analysen skal mindst omfatte:

a) en systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige
b) en vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene
c) en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1, og
d) de foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af denne forordning, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

Stk. 8. Overholdelse af godkendte adfærdskodekser, jf. artikel 40, inddrages behørigt ved vurderingen af konsekvenserne af de behandlingsaktiviteter, der udføres af de pågældende dataansvarlige eller databehandlere, navnlig i forbindelse med en konsekvensanalyse vedrørende databeskyttelse.

Stk. 9. Den dataansvarlige indhenter, hvis det er relevant, de registreredes eller deres repræsentanters synspunkter vedrørende den planlagte behandling, uden at det berører beskyttelse af kommercielle eller samfundsmæssige interesser eller behandlingsaktiviteternes sikkerhed.

Stk. 10. Hvis behandling i henhold til artikel 6, stk. 1, litra c) eller e), har et retsgrundlag i EU-retten eller i den medlemsstats nationale ret, som den dataansvarlige er underlagt, og denne ret regulerer den eller de pågældende specifikke behandlingsaktiviteter, og der allerede er foretaget en konsekvensanalyse vedrørende databeskyttelse som led i en generel konsekvensanalyse i forbindelse med vedtagelsen af dette retsgrundlag, finder stk. 1-7 ikke anvendelse, medmindre medlemsstaterne anser det for nødvendigt at foretage en sådan analyse inden behandlingsaktiviteter.

Stk. 11. Den dataansvarlige foretager, hvis det er nødvendigt, en fornyet gennemgang for at vurdere, hvorvidt behandling er foretaget i overensstemmelse med konsekvensanalysen vedrørende databeskyttelse, i hvert fald når der er en ændring af den risiko, som behandlingsaktiviteterne udgør.