

CHARITY GUARD ApS
Gråbrødre Plads 4, 2.
5000 Odense C
Danmark

23. oktober 2026

J.nr. 2026-441-12362
Dok.nr. 948544
Sagsbehandler
Anders Chemnitz

Sendt med Digital Post

Datatilsynet indleder undersøgelse af Charity Guard ApS i anledning af et brud på persondatasikkerheden

1. Charity Guard ApS' anmeldelse af et brud på persondatasikkerheden

Datatilsynet har den 5. oktober 2026 modtaget en anmeldelse fra Charity Guard ApS om et brud på persondatasikkerheden. Anmeldelsen har følgende referencenummer:

a108a7f9130b8c3202b0db5a16cd6e8d222cfeec

Det fremgår af anmeldelsen bl.a., at der er konstateret en uautoriseret adgang via en adgang til CPR Direkte, og at en aktør har anvendt adgangen til opslag i CPR, og at antallet af opslag anslås til at være ca. 15 millioner.

Datatilsynet har på den baggrund besluttet at indlede en nærmere undersøgelse.

2. Anmodning om oplysninger

Ud over det anførte i anmeldelsen, har Datatilsynet brug for yderligere oplysninger vedrørende de faktuelle forhold i forbindelse med hændelsen.

Datatilsynet skal derfor anmode om en udtalelse til brug for sagens behandling. Datatilsynet skal anmode om, at spørgsmålene besvares enkeltvis.

1. Datatilsynet anmoder Charity Guard ApS om at beskrive, hvilke af virksomhedens systemer der har haft mulighed for at foretage opslag i CPR-registret. Virksomheden bedes herunder redegøre for, hvilke formål opslagene i CPR-registret har tjent.
2. Datatilsynet har modtaget anmeldelsen om bruddet på persondatasikkerheden fra Charity Guard ApS. Virksomheden bedes oplyse, om de omhandlede opslag i CPR-registret er foretaget via Charity Guard ApS, og om det er Charity Guard ApS, der har indgået aftalen om tilslutning til CPR-systemet.
3. Charity Guard ApS bedes beskrive, hvordan det har været muligt at logge ind på virksomhedens systemer via internettet, og virksomheden bedes udtømmende redegøre for, hvilke sikkerhedsforanstaltninger der har været anvendt ved login, herunder eventuel multifaktorautentifikation eller lign.

Datatilsynet

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

CVR 11883729

4. Charity Guard ApS bedes redegøre for, hvordan uvedkommende har opnået adgang til virksomhedens systemer og derigennem har kunnet foretage opslag i CPR-registret.
5. Charity Guard ApS bedes oplyse, om virksomheden regelmæssigt har kontrolleret opslagene i CPR-registret med henblik på at identificere eventuel uautoriseret brug af adgangen.
6. Charity Guard ApS bedes beskrive virksomhedens procedurer for oprettelse, ændring og nedlæggelse af brugeradgange. Virksomheden bedes herunder fremsende dokumentation for eventuelle udførte kontroller af, om medarbejdernes adgang fortsat har været nødvendig.
7. Charity Guard ApS bedes oplyse, hvor mange opslag i CPR-registret virksomheden normalt har foretaget som led i den daglige drift.
8. Charity Guard ApS bedes oplyse, om virksomheden har foretaget en vurdering af de risici, som virksomhedens aktiviteter kan indebære for de registreredes rettigheder og frihedsrettigheder. Hvis en sådan vurdering er foretaget, bedes virksomheden fremsende risikovurderingen. Hvis virksomheden ikke har foretaget en sådan vurdering, bedes årsagen hertil oplyst.
9. Charity Guard ApS bedes redegøre for, om virksomheden har haft procedurer eller tekniske foranstaltninger, der har sikret, at der kun er blevet foretaget opslag på CPR-numre, som virksomheden i forvejen var i besiddelse af. Hvis dette er tilfældet, bedes det nærmere uddybet, hvilket procedurer eller foranstaltninger, der har været tale om. Hvis der ikke har været sådanne procedurer, bedes grunden hertil så vidt muligt oplyst.
10. Er Charity Guard ApS bekendt med de gældende retningslinjer for opslag i CPR-registret? Hvis dette er tilfældet, bedes virksomheden beskrive, hvordan arbejdet med at overholde disse retningslinjer har været tilrettelagt.

3. Orientering om eventuel selvinkriminering

Datatilsynet kan på nuværende tidspunkt ikke udelukke, at sagens oplysninger vil kunne få betydning for bedømmelsen af en mulig overtrædelse af databeskyttelsesforordningen og databeskyttelsesloven, der kan medføre straf. Datatilsynet skal derfor gøre opmærksom på, at virksomheden ikke er forpligtet til at afgive oplysninger i sagen, idet der i givet fald kan være risiko for, at der afgives oplysninger om et strafbart forhold. Der henvises i den forbindelse til retssikkerhedslovens¹ § 10, der er vedlagt som bilag.

Hvis virksomheden vælger at besvare Datatilsynets spørgsmål, vil tilsynet betragte dette som et samtykke til at afgive oplysninger til brug for nærværende sag. De oplysninger, som virksomheden fremkommer med, vil derfor kunne indgå i Datatilsynets vurdering af sagen og i en eventuel efterfølgende straffesag.

4. Afsluttende bemærkninger

Datatilsynet anmoder om svar **senest 3 uger fra dags dato**.

¹ LBK nr. 1121 af 12/11/2019 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter

For yderligere information henvises til Datatilsynets vejledning om håndtering af brud på persondatasikkerheden, som findes på tilsynets hjemmeside.

Side 3 af 6

Hvis ovenstående giver anledning til spørgsmål, er Charity Guard ApS velkommen til at kontakte undertegnede telefonisk på [REDACTED].

Med venlig hilsen

Anders Chemnitz

Uddrag af databeskyttelsesreglerne

Det fremgår af databeskyttelsesforordningens artikel 32, stk. 1, at den dataansvarlige og databehandleren, 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 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.

Ifølge artikel 32, stk. 2, tages der ved vurderingen af, hvilket sikkerhedsniveau der er passende, 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.

Af databeskyttelsesforordningens præambelbetragtning 75 og 76 fremgår det, at risiciene for fysiske personers rettigheder og frihedsrettigheder, af varierende sandsynlighed og alvor, kan opstå som følge af behandling af personoplysninger, der kan føre til fysisk, materiel eller immateriel skade, navnlig hvis behandlingen kan give anledning til forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser. [...]

Risikoens sandsynlighed og alvor for så vidt angår den registreredes rettigheder og frihedsrettigheder bør bestemmes med henvisning til behandlingens karakter, omfang, sammenhæng og formål. Risikoen bør evalueres på grundlag af en objektiv vurdering, hvorved det fastslås, om databehandlingsaktiviteter indebærer en risiko eller en høj risiko.

Ved brud på persondatasikkerheden anmelder den dataansvarlige ifølge forordningens artikel 33, stk. 1, uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, bruddet på persondatasikkerheden til den tilsynsmyndighed, som er kompetent i overensstemmelse med artikel 55, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Foretages anmeldelsen til tilsynsmyndigheden ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen.

Ifølge forordningens artikel 33, stk. 5, skal den dataansvarlige dokumentere alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at denne artikel er overholdt.

Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødigt

forsinkelse den registrerede om bruddet på persondatasikkerheden. Det følger af forordningens artikel 34, stk. 1.

Side 5 af 6

Artikel 34, stk. 2 fastslår, at underretningen af den registrerede i henhold til denne artikels stk. 1 skal i et klart og forståeligt sprog beskrive karakteren af bruddet på persondatasikkerheden og mindst indeholde de oplysninger og foranstaltninger, der er omhandlet i artikel 33, stk. 3, litra b), c) og d).

Ifølge bestemmelsens stk. 3, kan underretning efter stk. 1, undlades, hvis en af følgende betingelser er opfyldt:

- a) den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering
- b) den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1 sandsynligvis ikke længere er reel
- c) det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

LBK nr. 1121 af 12/11/2019 om retssikkerhed ved forvaltningens anvendelse af tvangsindgreb og oplysningspligter (uddrag).

§ 9. Hvis en enkeltperson eller juridisk person med rimelig grund mistænkes for at have begået en strafbar lovovertrædelse, kan tvangsindgreb over for den mistænkte med henblik på at tilvejebringe oplysninger om det eller de forhold, som mistanken omfatter, alene gennemføres efter reglerne i retsplejeloven om strafferetsplejen.

Stk. 2. Reglen i stk.1 gælder ikke, hvis tvangsindgrebet gennemføres med henblik på at tilvejebringe oplysninger til brug for behandlingen af andre spørgsmål end fastsættelse af straf.

Stk. 3. Reglerne i stk. 1 og 2 finder tilsvarende anvendelse, hvis der i sagen rettes et tvangsindgreb mod andre end den mistænkte.

Stk. 4. Den mistænkte kan meddele samtykke til fravigelse af stk. 1 og 3. Samtykke skal være skriftligt og skal meddeles på et frivilligt, specifikt og informeret grundlag. Et samtykke kan til enhver tid tilbagekaldes. Meddeler den mistænkte samtykke til fravigelse af stk. 1 og 3, finder reglerne i §§ 2-8 tilsvarende anvendelse ved de i § 1, stk. 1, nævnte tvangsindgreb.

§ 10. Hvis der er konkret mistanke om, at en enkeltperson eller juridisk person har begået en lovovertrædelse, der kan medføre straf, gælder bestemmelser i lovgivningen m.v. om pligt til at meddele oplysninger til myndigheden ikke i forhold til den mistænkte, medmindre det kan udelukkes, at de oplysninger, som søges tilvejebragt, kan have betydning for bedømmelsen af den formodede lovovertrædelse.

Stk. 2. I forhold til andre end den mistænkte gælder bestemmelser i lovgivningen m.v. om pligt til at meddele oplysninger, i det omfang oplysningerne søges tilvejebragt til brug for behandlingen af andre spørgsmål end fastsættelse af straf.

Stk. 3. En myndighed skal vejlede den mistænkte om, at vedkommende ikke har pligt til at meddele oplysninger, som kan have betydning for bedømmelsen af den formodede lovovertrædelse. Hvis den mistænkte meddeler samtykke til at afgive oplysninger, finder reglerne i § 9, stk. 4, 2. og 3. pkt., tilsvarende anvendelse.

Stk. 4. Den mistænkte kan meddele samtykke til anvendelse af en oplysningspligt over for andre med henblik på at tilvejebringe oplysninger til brug for en straffesag mod den mistænkte. Reglerne i § 9, stk. 4, 2. og 3. pkt., finder tilsvarende anvendelse.