www.pwc.dk

Happenings Group A/S

Uafhængig revisors ISAE 3000-erklæring med begrænset sikkerhed om informationssikkerhed og foranstaltninger pr. 1. september 2022 i henhold til databehandleraftale med dataansvarlige

September 2022

Indholdsfortegnelse

1. Ledelsens udtalelse

Happenings Group A/S (Happenings) behandler personoplysninger på vegne af dataansvarlige i henhold til databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Happenings Group's app til events, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som den dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne") er overholdt.

Happenings anvender Scaleway SAS som underdatabehandler for hosting, Reepay A/S til betalingsløsning og Mailjet SAS til udsendelse af mails. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som underdatabehandlere varetager for Happenings.

Happenings bekræfter, at:

- Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af Happenings Group's app til events, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesreglerne pr. 1. september 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

  (i) Redegør for, hvordan Happenings Group's app til events var udformet og implementeret, herunder redegør for:

  - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
  - De processer i både it-systemer og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
  - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
  - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
  - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
  - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning af de registrerede
  - De processer, der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen 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
  - Kontroller, som vi med henvisning til Happenings Group's app til events afgrænsning har forudsat ville være implementeret af den dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne Happenings Group's app til events til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved Happenings Group's app til events, som den enkelte dataansvarlige måtte anse vigtigt efter sine særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 1. september 2022. Kriterierne anvendt for at give denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret, og

(ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

c) Der er etableret passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesreglerne.

Rasmus Jensing
Aarhus, 23. september 2022

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med begrænset sikkerhed om informationssikkerhed og foranstaltninger pr. 1. september 2022 i henhold til databehandleraftale med dataansvarlig

Til: Happenings Group A/S og dataansvarlige

Omfang

Vi har fået som opgave at afgive erklæring om Happenings' beskrivelse i afsnit 3 af deres Happenings Group's app til events i henhold til databehandleraftale med dataansvarlig pr. 1. september 2022 (beskrivelsen) og om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Nærværende erklæring omfatter, om Happenings har udformet hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår af afsnit 4. Erklæringen omfatter ikke en vurdering af Happenings' generelle efterlevelse af kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesreglerne").

Happenings anvender Scaleway SAS som underdatabehandler for hosting, Reepay A/S til betalingsløsning og Mailjet SAS til udsendelse af mails. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som underdatabehandlere varetager for Happenings.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

Vores konklusion udtrykkes med begrænset grad af sikkerhed.

Happenings' ansvar

Happenings er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Happenings' beskrivelse samt om udformningen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 (ajourført), "Andre erklæringer med sikkerhed end revision eller review af historiske finansielle oplysninger", og de yderligere krav, der er gældende i Danmark, med henblik på at opnå begrænset grad af sikkerhed for, at beskrivelsen i alle væsentlige

henseender er tilfredsstillende præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af deres Happenings Group's app til events samt for kontrollernes udformning. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i ledelsens udtalelse.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

Omfanget af de handlinger vi har udført, er mindre end ved en erklæringsopgave med høj grad af sikkerhed. Som følge heraf er den grad af sikkerhed, der er for vores konklusion, betydeligt mindre end den sikkerhed, der ville være opnået, hvis der var udført en erklæringsopgave med høj grad af sikkerhed.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en databehandler

Happenings' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved Happenings Group's app til events som hver enkelt dataansvarlig måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Under vores arbejde er vi ikke blevet bekendt med forhold, der giver os anledning til at konkludere,

a) at beskrivelsen af Happenings Group's app til events, således som det var udformet og implementeret pr. 1. september 2022, ikke i alle væsentlige henseender er tilfredsstillende præsenteret, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, ikke i alle væsentlige henseender var hensigtsmæssigt udformet pr. 1. september 2022.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Happenings Group's app til events, og som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af om kravene i databeskyttelsesreglerne er overholdt.

Aarhus, den 23. september 2022
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

3. Beskrivelse af behandling

3.1 Introduktion

Denne fremstilling beskriver hvordan Happenings overholder databeskyttelsesforordningen ("GDPR"), samt supplerende national lovgivning i behandlingen af personoplysninger i forbindelse med leveringen af Happenings.

Fremstillingen beskriver alle relevante forhold vedrørende behandlingssikkerhedens tekniske og organisatoriske foranstaltninger samt ansvaret mellem vores kunder som dataansvarlige og Happenings Group A/S som databehandler.

3.2 Happenings platformen

Happenings Group A/S' behandlinger består i at udvikle, drifte og distribuere Happenings platformen, som udbydes som en 'pay-per-use' service under brandet Happenings.

3.2.1 Applikations- og platformbeskrivelse

Happenings produkter til kunder/uddannelsesinstitutioner består primært af billetformidling til alle skolens fester og fredagscaféer. Derudover består produktporteføljen hovedsageligt af en lang række af ydelser til opkrævninger, f.eks. ratebetalinger til studieture og salg af produkter i appen på vegne af den dataansvarlige, såsom drinkskuponer. Yderligere indeholder appen et digitalt studiekort, som erstatter det fysiske plastic studiekort, hvor Happenings verificerer eleverne via Unilogin eller WAYF.

3.2.2 Grundlaget for behandlingen

Ved leveringen af Happenings plaformen behandler Happenings Group A/S personoplysninger som databehandles på vegne af kunden, som i denne sammenhæng dermed er dataansvarlig. Behandlingen sker efter gældende regler og i overensstemmelse med den databehandleraftale, der indgås med kunden. Kunden er typisk en selvejende/privat institution, kommune eller virksomhed.

I databehandleraftalens bilag med tilhørende ydelsesbilag er ydelserne, typerne af behandlinger af personoplysninger samt den dataansvarliges instruks beskrevet. Den konkrete adgang til de digitale læremidler gives enten via Styrelsen for IT og Lærings ("STIL") login løsning, Unilogin, Danmarks Tekniske Universitets ("DTU") login løsning, WAYF, eller Happenings egen loginløsning.

3.3 Karakteren af behandlingen

Happenings behandlinger på vegne af den dataansvarlige drejer sig primært om:

- Opbevaring af de data, som den dataansvarliges brugere (elever, ansatte og øvrige brugere) indtaster på de platforme, som brugerne har adgang til via. den dataansvarliges Partner-konto i Happenings.
- Administration af begivenheder/'happenings' og andre opkrævningsarter med administration af brugere og tilknyttede adgange til Happenings Partners.
- Behandling af anonymiserede anvendelsesdata til brug for rapportering til den dataansvarlige om anvendelsen/udnyttelsen af den dataansvarliges konto.
- Support af brugere ifm. tjenester Happenings udbyder. I denne forbindelse behandles der oplysninger i fornødent omfang, såsom navn, kontaktoplysninger og bruger-ID.

Indsamling af oplysninger om de registreredes brug af Happenings platformen – herunder køb af billetter – sker kun i det omfang, det er nødvendigt for at levere Happenings platformen. Alle øvrige behandlinger – herunder effektuering af den registreredes rettigheder – udføres alene efter den dataansvarliges instruks.

3.4 Personoplysninger

Oplysninger om kunden

• Navn på institutionen

• Type uddannelsesinstitution

• Institutionsnummer

Almindelige personoplysninger (jf. Databeskyttelsesforordningen, artikel 6)

• Navn og efternavn(e)

• E-mailadresse

• Telefonnummer

• Bopælsadresse

• Køn

• Betalingsoplysninger

• Foretrukne sprog

• Billede(r)

• Betalingsoplysninger

• Købshistorik

• Fremmøde til 'happenings'

• Gruppeid (Dette er alt lige fra klasser, fag, studiegrupper osv)

• Gruppenavn

• Gruppetype, f.eks. hold, valgfag

• Årgang (1.g, 2.g, 3.g, HF, osv)

• Klasse beskrivelse, f.eks. A,B,C osv

• Start og slut på elevens skoletid

• Type (forbeholdt studerende på videregående uddannelser, kan være "elev" eller "stud")

• Elevnummer

• Unilogin-brugernavn (forbeholdt grundskoler, 10. klasser/efterskoler og gymnasier)

• European Student Identifier (forbeholdt videregående uddannelser)

• Studieretning

Oplysninger om CPR-numre (jf. Databeskyttelsesloven § 11)

• Fødselsdato ud fra CPR (ikke de sidste 4-cifre)

3.5 Praktiske tiltag

Happenings Group A/S har flere ansatte, der beskæftiget sig fuld tid med IT- og cybersikkerhed.

Der arbejdes målrettet med at sikre fortrolighed, integritet og tilgængelighed i vores løsninger, og vi arbejder kontinuerligt for at sikre et passende sikkerhedsniveau, således at kvaliteten i vores produkter lever op til både Happenings', kunders og de registreredes krav og behov. Nedenstående tiltag er implementeret med henblik på at sikre et passende sikkerhedsniveau.

Listen indgår de i denne rapports vurderede tiltag, men er ikke begrænset hertil:

- Informationssikkerhedspolitik

- Slettepolitik

- Sikkerhedsbeskrivelse

- Retningslinjer for brug af IT og behandling af personoplysninger

- Informationssikkerhedsudvalg – træffer principielle beslutning på overordnet niveau

- Change management

- Incident management

- Awarenesstræning

Når der foretages ændringer i programmer og databaser følges Happenings' procedure på området, som har til formål at eliminere risikoen for fejl i processen fra udvikling til test og til produktion. Happenings har en informationssikkerhedspolitik, der dækker medarbejdere relateret til at udvikle ydelsen. I denne beskrives de overordnede initiativer og retningslinjer for sikker behandling af personoplysninger, samt generel sikker behandling af IT. Som led i den løbende indsats for at styrke hensigtsmæssig brug af IT er der udarbejdet politikker, vejledninger og retningslinjer for håndtering af bl.a. IT, persondata og medier.

Disse dokumenter fremsendes til relevante medarbejdere ved væsentlige ændringer og opdateringer. Dokumenter er altid tilgængelige på vores intranet, således at alle medarbejdere kan fremfinde dem efter behov.

Happenings Group A/S' juridiske afdeling sikrer, at Happenings' informationssikkerhedspolitik og persondatapolitik vedligeholdes og opdateres løbende.

Herudover sikres at retningslinjer for sikker behandling af IT opdateres løbende, og at kontrolrapporter følger et årshjul. Happenings afholder løbende træning af medarbejdere. Dette sker via. et elektronisk træningsmodul, hvor den enkelte medarbejder uddannes i sikker håndtering af persondata og cybersikkerhed. Der føres kontrol med, at alle medarbejdere gennemfører modulet.

Ligeledes er der etableret funktionsadskillelse og begrænsede adgange til data efter rollebaseret behov, hvilket medfører adgangsminimering til de dataansvarliges data.

Der udføres mindst en gang om året periodisk gennemgang af de udvidede rettigheder til sikring af, at tildelte adgangsrettigheder fortsat udgør et arbejdsbetinget behov. Ved ansættelse af nye medarbejdere vurderer Happenings Group A/S behovet for efterprøvning fra ansættelse til ansættelse og kan omfatte:

- Referencer fra tidligere ansættelser

- Straffeattest

- Eksamensbeviser

Der indhentes, som udgangspunkt altid referencer fra tidligere ansættelser, mens straffeattest og eksamensbeviser kun bliver indhentet, såfremt der er et særligt behov. Happenings gemmer ikke dokumentation for hvilken type af efterprøvning af ansættelse, der er blevet foretaget. Happenings pålægger, ved ansættelse af nye medarbejdere, sine medarbejdere tavshedspligt, som medarbejdere ligeledes skriftligt gøres opmærksomme på fortsat er gældende ved fratrædelse.

3.6 Risikovurdering

Happenings har vurderet konsekvenserne for de registrerede i forhold til fortrolighed, integritet og tilgængelighed ved behandlingerne af personoplysninger i forbindelse med leveringen af Happenings platformen. Herudover er den fulde systemportefølje risikovurderet i forhold til administrativt- og teknisk mitigerende tiltag med henblik på at implementere en passende grad af sikkerhed.

Happenings Group A/S arbejder kontinuerligt med IT- og Cybersikkerhed og Happenings holder sig orienteret om potentielle trusler. Happenings' risikometode er baseret på principperne fra ISO 27001. Happenings Group A/S' foretager indledningsvist og løbende risikovurderinger af sine underdatabehandlere, og indhenter såvidt muligt en erklæring fra sine underdatabehandlere, for at opretholde høj grad af sikkerhed for de registrerede.

Det er Happenings Group A/S' vurdering, at Happenings behandlinger af oplysninger i forbindelse med leveringen af Happenings platformen medfører en lav risiko for den registrerede, som følge af behandlingernes natur samt de implementerede sikkerhedstiltag.

3.7 GDPR & Happenings' rolle og ansvar som databehandler

3.7.1 Happenings bistand til den dataansvarlige

Som nævnt er Happenings databehandler ved levering af Happenings platformen til kunden, som dermed er dataansvarlig. Happenings understøtter den dataansvarliges forpligtelser til håndtering af den registreredes rettigheder – herunder f.eks. besvarelser af anmodninger om indsigt. Til det formål har Happenings udarbejdet generelle procedurer for håndtering af den registreredes rettigheder, samt mere specifikke procedurer for Happenings' ITs konkrete håndtering. Såfremt Happenings modtager en direkte henvendelse fra en registreret, anmodes den registrerede om først at rette henvendelse til den dataansvarlige. Herudover har Happenings Group A/S udarbejdet supplerende privatlivspolitikker til brugere af Happenings' produkter, hvori det fremgår, at Happenings agerer som databehandler og behandler oplysningerne på vegne af den dataansvarlige.

3.7.2 Happenings sletteprincipper

Happenings' sletterutiner er defineret i databehandleraftalen og de tilhørende ydelsesbilag. Happenings sletter udelukkende oplysninger på baggrund af den dataansvarliges instruks samt efter principperne beskrevet nedenfor.

Happenings sletter – herunder anonymiserer – data efter følgende principper:

1. På forlangende af dataansvarlige.

2. Når Happenings modtager nye dataset – her forstås opdateret liste over registrerede tilknyttet en dataansvarlig – fra den dataansvarlige.

3. Tidligst 90 dage og senest 24 måneder efter, at en registreret forlader en dataansvarlig. Dog med undtagelse af visse oplysninger for at opfylde kravene til anden dansk lovgivning, herunder f.eks. Bogføringsloven.

3.7.3 Happenings underdatabehandlere

I forbindelse med driften af Happenings benyttes en række underdatabehandlere. Happenings Group A/S har indgået databehandleraftaler med disse, ligesom at der føres tilsyn med, at underdatabehandlerne overholder deres forpligtelser efter persondatalovgivningen og databehandleraftalen. Tilsyn føres ved undersøgelser af erklæringer og fysiske tilsyn, hvor dette er muligt og relevant.

Ved leveringen af Happenings platformen benyttes følgende underdatabehandlere:

- **Scaleway SAS**, VAT FR35433115904 - Hosting af Happenings' services, og opbevaring af de studerendes data, og data for dataansvarliges medarbejdere.

- **Mailjet SAS**,FR67524536992 - Mailjet bliver brugt til at sende emails ud, eksempelvist når de studerende modtager kvittering for deres køb.

- **Reepay A/S**, DK32097901, Reepay er en betalingsløsning, som bliver brugt til at håndtere Visa, Mastercard (Betalingskort) og Google Pay og Apple Pay.

3.8 Kontrolforanstaltninger

3.8.1 Tekniske sikkerhedsforanstaltninger

Happenings vurderer løbende, hvilke praktiske sikkerhedstiltag der skal indgå i vores løsninger. Vi forholder os til aktuelle trusler og mulige mitigerende tiltag for at afværge sådanne trusler, ligesom vi løbende vurderer nye typer af sikkerhedsmålrettet IT for på den måde at sikre, at vi kontinuerligt tilpasser vores arbejde med sikring af data.

For Happenings platformen er der etableret funktionsadskillelse og begrænsede adgange til data efter rollebaseret behov, hvilket medfører adgangsminimering til de dataansvarliges data.

Der er implementeret en change- og release log for Happenings platformen for at tracke ændringer foretaget i vores systemer, samt for at kunne lokalisere og forklare evt. sikkerhedsbrister.

Der er ligeledes implementeret et SIEM-system på relevante logfiler, så Happenings bliver advaret ved mistænkelig adfærd – f.eks. ved tildeling af udvidede rettigheder. Derudover har vi sikret Happenings platformen ved kryptering, firewall, antivirussystemer, endpoint protection og systemovervågning.

Ved tilgang fra en ikke-Happenings lokation er det påkrævet at være logget på via Happenings' VPN for at kunne tilgå Happenings' netværk. Happenings Group A/S har desuden i foråret 2022 implementeret multifaktor-autentificering (MFA) for dets medarbejdere ved tilgang via VPN til Happenings' systemer.

Herudover arbejdes der med kunstige data udviklet af STIL i vores test- og udviklingsmiljøer, hvorfor der aldrig indgår personhenførbare data i vores udvikling og test.

Endvidere har Happenings implementeret formaliserede og ledelsesgodkendte backupprocedurer, hvilket bevirker, at vi i tilfælde af en sikkerhedsbrist kan reetablere vores servere.

Derudover har Happenings implementeret kontroller til sikring af indhentelse af erklæringer fra underdatabehandlere om overholdelse af persondatalovgivningen. Kontrollerne sikrer, at alle erklæringer vurderes ud fra et sikkerhedsperspektiv.

Kontrolmål og -aktiviteter fremgår af afsnit 4.

3.9 Komplementerende kontroller de dataansvarlige

Den dataansvarlige er selv ansvarlig for at anvende Happenings på en måde, der er i overensstemmelse med lovgivningens krav.

Dette omfatter blandt andet, at kunden som dataansvarlig er ansvarlig for:

- At den fornødne hjemmel til behandlingen, jf. art. 6, er til stede
- At sikre fornøden oplysning til de registrerede om udøvelsen af deres rettigheder og kontrollere identiteten af de registrerede, der ønsker at udøve deres rettigheder
- At behørigt orientering af den registrerede iht. art. 13
- At kontrollere identiteten på den, der anmoder om berigtigelse
- At kontrollere identiteten på den, der anmoder om sletning
- At sikre at instruksen er lovlig set i forhold til den til enhver tid gældende databeskyttelsesretlige regulering
- At sikre at instruksen er hensigtsmæssig set i forhold til denne databehandleraftale og hovedydelsen
- At sikre at den dataansvarliges brugere er ajourførte
- At sikre at udøvelsen af den registreredes rettigheder sker rettidigt, herunder besvarelse af den registreredes anmodninger og begrundelse af eventuelt afslag
- At eventuelle integrationer til andre systemer overholder lovgivningen

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A:

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til databehandlingens omfang.	Ingen bemærkninger.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige.	Forespurgt om hvordan ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks, og vurderet hensigtsmæssigheden heraf. Inspiceret dokumentation for, at ledelsen har foretaget vurdering af databehandlingen efterleves af databehandleren og underdatabehandlere.	Ingen bemærkninger.

Kontrolmål A:

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede databehandleraftale.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Forespurgt om der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Forespurgt om der forligger formaliserede procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Vurderet om det er sandsynligt, at der vil ske underretning af den dataansvarlige hvis instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Ingen bemærkninger.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til aftalte sikringsforanstaltninger.	Ingen bemærkninger.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Forespurgt om den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Forespurgt databehandler om hvilke tekniske foranstaltninger der er implementeret, og hvordan disse sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret dokumentation for at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med en enkelt udvalgt dataansvarlig.	Ingen bemærkninger.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Forespurgt om der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret dokumentation for at antivirus software er installeret og opdateret på et system og en database.	Ingen bemærkninger.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Forespurgt om ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret dokumentation for at den seneste kontrol af at firewallen konfigureret i henhold til intern politik herfor.	Ingen bemærkninger.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for vurdering af om segmentering er behørig.	Ingen bemærkninger.
B.6	Adgang til personoplysninger er isoleret til brugere med et arbejdsbetinget behov herfor.	Forespurgt om der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Forespurgt om der foreligger formaliserede procedurer for periodisk opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret dokumentation for at periodisk opfølgning er udført efter planen. Inspiceret for en enkelt bruger for hver gruppe af brugere at brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen bemærkninger.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Forespurgt om der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret for en tilfældig udvalgt alarm, at der er sket opfølgning, samt at forholdet er meddelt de dataansvarlige i behørigt omfang.	Ingen bemærkninger.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme. Forespurgt om teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Inspiceret opsætning af enkelte tilfældigt udvalgte transmissions veje at kryptering er effektiv. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i erklæringsperioden, samt om de dataansvarlige er behørigt orienteret herom.	Ingen bemærkninger.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
B.9	Der er etableret logning i systemer, databaser og netværk af følgende forhold: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser Logoplysningerne er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Forespurgt om der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Forespurgt om logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, har været konfigureret og aktiveret i hele erklæringsperioden. Forespurgt om opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning. Inspiceret ud fra en tilfældigt udvalgt dags logning, at logfiler har det forventede indhold i forhold til opsætning, samt inspiceret dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser, aktiviteter udført af systemadministratorer og andre med særlige rettigheder mv.	Ingen bemærkninger.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Forespurgt om der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Inspiceret ved for en tilfældigt udvalgt udviklings- henholdsvis testdatabase, at personoplysninger heri er pseudonymiseret eller anonymiseret.	Ingen bemærkninger.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Forespurgt om der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests. Inspiceret dokumentation for de seneste tests af de etablerede tekniske foranstaltninger. Forespurgt om evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	Ingen bemærkninger.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Forespurgt om der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved udtræk eller opslag af tekniske sikkerhedsparametre og -opsætninger, for en enkelt af hver type systemer, databaser og netværk der anvendes, at disse er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen bemærkninger.

Kontrolmål B:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
B.13	Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugernes adgang revurderes regelmæssigt, herunder om rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Forespurgt om der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret for en enkelt medarbejder for hver gruppe af medarbejdere at adgange til systemer og databaser, er godkendt, og at der er et arbejdsbetinget behov. Inspiceret for en enkelt tilfældig udvalgt fratrådt medarbejder, at dennes adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret dokumentation for at periodisk vurdering og godkendelse af tildelte brugeradgange er udført efter planen.	Ingen bemærkninger.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører høj risiko for de registrerede, sker som minimum ved anvendelse af tofaktorautentifikation.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede. Observeret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen bemærkninger.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Observeret for tilfældigt udvalgte lokaler og datacentre, hvori der opbevares og behandles personoplysninger, at det er sandsynligt at kun autoriserede personer har haft fysisk adgang hertil i erklæringsperioden.	Ingen bemærkninger.

Kontrolmål C:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én gang årligt – vurdering af, om informationssikkerhedspolitikken skal opdateres.	Forespurgt om der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Forespørg om hvordan informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen bemærkninger.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret ved en repræsentativ databehandleraftale, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen bemærkninger.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser	Forespurgt om der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret for en tilfældigt udvalgt nyansat medarbejder i erklæringsperioden, at der er dokumentation for, at efterprøvningen har omfattet: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser	Ingen bemærkninger.

Kontrolmål C:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
C.4	Ved ansættelse underskriver medarbejderne en fortrolighedsaftale. Endvidere bliver medarbejderne introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejdernes behandling af personoplysninger.	Inspiceret for en tilfældigt udvalgt nyansat medarbejder i erklæringsperioden, at den pågældende medarbejder har underskrevet en fortrolighedsaftale og er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information	Ingen bemærkninger.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Forespurgt om der foreligger procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Inspiceret for en tilfældigt udvalgt fratrådt medarbejder i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Ingen bemærkninger.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, som databehandleren udfører for de dataansvarlige.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Inspiceret for en tilfældigt udvalgt fratrådt medarbejder i erklæringsperioden, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen bemærkninger.

Kontrolmål C:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Forespurgt om databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Ingen bemærkninger.

Kontrolmål D:

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til aftalte opbevaring og sletning af personoplysninger.	Ingen bemærkninger.
D.2	Der er aftalt krav til databehandlerens opbevaringsperioder og sletterutiner i databehandleraftaler såfremt kunder ønsker dette.	Forespurgt om de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret for en tilfældigt udvalgt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder og sletterutiner.	Ingen bemærkninger.
D.3	Ved ophør af behandlingen af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Forespurgt om der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Inspiceret for en tilfældigt udvalgt ophørte databehandling i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen bemærkninger.

Kontrolmål E:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret for en tilfældigt udvalgt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen bemærkninger.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Forespurgt om databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret for en tilfældigt udvalgt databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen bemærkninger.

Kontrolmål F:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren sikrer en betryggende behandlingssikkerhed ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til anvendelse af underdatabehandlere.	Ingen bemærkninger.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Forespurgt om databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret for en tilfældigt udvalgt underdatabehandler fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige (specifikt eller indirekte).	Ingen bemærkninger.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelsen af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Forespurgt om der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen bemærkninger.

Kontrolmål F:

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren sikrer en betryggende behandlingssikkerhed ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Forespurgt om der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret for en tilfældigt udvalgt underdatabehandleraftale, at denne indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen bemærkninger.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen.	Forespurgt om databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret for en enkelt underdatabehandler at oversigten som indeholder de krævede oplysninger.	Ingen bemærkninger.
F.6	På baggrund af en ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, foretager databehandleren en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Forespurgt om der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af en tilfældigt udvalgt underdatabehandler og den aktuelle behandlingsaktivitet hos denne, samt at de er foretaget planlagt opfølgning i overensstemmelse med risikovurderingen.	Ingen bemærkninger.

Kontrolmål G:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til overførsel af personoplysninger.	Ingen bemærkninger.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Forespurgt om databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret for en tilfældigt udvalgt dataoverførsel fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller udført efter modtaget instruks fra den dataansvarlige.	Ingen bemærkninger.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Forespurgt om der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret for en tilfældigt udvalgt dataoverførsel fra databehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige, samt at der kun er sket overførsler, i det omfang dette er aftalt med den dataansvarlige.	Ingen bemærkninger.

Kontrolmål H:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til bistand til den dataansvarlige.	Ingen bemærkninger.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Forespurgt om de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Vurderet om det er sandsynligt, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen bemærkninger.

Kontrolmål I:

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt om der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Forespurgt om hvornår procedurer er opdateret, og hvilke opdateringer der eventuelt er foretaget. Inspiceret oversigt over skriftlige procedurer og vurdereret om denne forekommer opdateret og tilstrækkelig i forhold til håndtering af sikkerhedsbrud.	Ingen bemærkninger.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik • Opfølgning på logning af adgang til personoplysninger	Forespurgt om databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer mv. Forespurgt om hvordan det sikres at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang.	Ingen bemærkninger.

Kontrolmål I:

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Forespurgt om databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden Forespurgt om databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Forespurgt om samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 72 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Ingen bemærkninger.

Kontrolmål I:

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte vurdering (ved analyse og forespørgsel)	Resultat af vurdering
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet. Disse procedurer skal indeholde anvisninger på beskrivelser af: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Forespurgt om de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Vurderet om det er sandsynligt, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen bemærkninger.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Rasmus Rou Bach Jensing
Kunde
På vegne af: Happenings Group A/S
Serienummer: CVR:40979956-RID:19955246
IP: 86.52.xxx.xxx
2022-09-23 13:39:30 UTC
NEM ID

Jesper Parsberg Madsen
Statsautoriseret revisor
Serienummer: PID:9208-2002-2-427963640472
IP: 208.127.xxx.xxx
2022-09-23 14:00:52 UTC
NEM ID

Penneo dokumentnøgle: FWHWN-0FBE8-4N05W-SVIA8-BXPVF-N8S1S