Databehandler Audit
December 2022

Dette dokument er en rapport over den Dataansvarliges kontrol med Databehandleren:

Zenegy Danmark ApS
Slotsmarken 16
2970 Hørsholm
Denmark
CVR: 38266041

Rapporten er udarbejdet med udgangspunkt i revisionsstandarden ISAE 3000 og sker ved den Dataansvarliges informationsindsamling fra Databehandleren for at kontrollere og få bekræftet Databehandlerens efterlevelse af kontrolmål og aktiviteter.

Rapporten er udarbejdet for at kontrollere og dokumentere Databehandlerens overholdelse og efterlevelse af Europa-Parlamentets og Rådets forordning (EU) 2016/ 679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger (herefter benævnt "GDPR") og databeskyttelsesloven.

Beskrivelse af system og behandling

Databehandleren stiller, på abonnementsbasis, de af den dataansvarlige valgte cloudbaserede tjenester ("Tjenester") til rådighed for den dataansvarlige og dennes medarbejdere.

Tjenesterne kan dels tilgås via databehandlerens hjemmeside, Zenegy , og dels via databehandlerens app. Den dataansvarliges brug af databehandlerens cloud-baserede Tjenester sker ved den dataansvarliges selvbetjening via databehandlerens hjemmeside, og/eller via databehandlerens app.

Den dataansvarliges medarbejdere kan ligeledes tilgå deres egne oplysninger, så som lønsedler, fraværsoversigter, ferieover-sigter, og de dokumenter, som medarbejderen eller kunden har indlæst, eksempelvis ansættelseskontrakt.

Både den dataansvarliges og dennes medarbejderes brug af tjenesten kræver et unikt bruger ID og en adgangskode.

Behandlingens karakter

Ydelserne og behandlingsaktiviteterne omfatter hovedsageligt følgende:

Ved den dataansvarliges brug af den cloud-baserede **Zenegy Payroll** – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget lønadministrator - behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere i forbindelse med den dataansvarliges lønadministration for egne medarbejdere, herunder lønkørsel, ferie- og fravær, kørsel og tidsregistrering, indberetning til SKAT og andre myndigheder.

Ved den dataansvarliges brug af den cloud-baserede **Zenegy HR** – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget administrator - behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere i forbindelse med den dataansvarliges HR-administration for egne medarbejdere, herunder administration af enheder og adgange tildelt den enkelte medarbejder, kursus-administration, håndtering af medarbejderen udlæg for den dataansvarlige, og lagring af dokumenter, eksempelvis ansættelseskontrakt.

Ved den dataansvarliges brug af den cloud-baserede **Zenegy ERP** – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget administrator - behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere, kunder og samarbejdspartnere i forbindelse med den dataansvarliges bogførings- og regnskabsmæssige aktiviteter.

Ved den dataansvarliges brug af den cloud-baserede **Zenegy Expense** – hvad enten sådan brug foretages af den dataansvarlige eller en af denne udpeget administrator - behandler databehandleren persondata vedrørende den dataansvarliges medarbejdere, kunder og samarbejdspartnere i forbindelse med den dataansvarliges expense-management aktiviteter.

Zenegy Payroll
Zenegy leverer cloud-baseret lønservice til virksomheder af alle størrelser. Servicen hjælper og automatiserer mange komplicerede lønadministrationsprocesser ved at holde styr på fraværs-, time-, kørsels- samt tillægs- og fradragsregistreringer, herunder godkendelses-flow for de førnævnte registreringer samt på selve lønkørslen. Zenegy bibringer overblik over medarbejdere, afdelinger, pårørende, pensionsaftaler, betalinger og rapportering til Skat. Gennem et rolle-system sikrer Zenegy rolleadskillelse for de forskellige brugertyper. Zenegy logger alle brugeres handlinger i systemet således, at der kan gennemføres digital audit. Gennem et rapporteringsmodul giver Zenegy brugerne mulighed for at trække relevante rapporter på de forskellige funktioner.

Zenegy HR
Zenegy leverer visse cloud-baserede HR-løsninger til virksomheder af alle størrelser. Løsningen er en samling af flere forskellige produkter, der støtter op om virksomhedens processer, herunder et enheds- og adgangsmodul, som hjælper virksomheden med at styre ud- og tilbagelevering af materiale og værktøjer, og oprettelse af adgange og sletning af disse. Desuden indeholder løsningen et modul til styring og tilmelding til både fysiske og virtuelle kurser og events. Løsningen indeholder også et skabelon- og dokumentmodul. Skabelonmodulet hjælper virksomheden til at vedligeholde og skabe dokumenter i form af kontrakter eller aftaler. Dokumentmodulet giver mulighed for at uploade dokumenter på den enkelte medarbejder, så som ansættelseskontrakter eller MUS samtaler. Brugere med de tilladte adgangs-rettigheder kan også dele

dokumenter med alle medarbejdere i en virksomhed, for eksempel i form af medarbejderhåndbøger eller arbejdspladsvurderinger.

Zenegy ERP
Zenegy leverer cloud-baserede bogføringsløsninger til virksomheder af alle størrelser. Løsningen er et bogføringssystem til fakturering af kunder, kontering af udgifter og indtægter. Løsningen indeholder flere moduler i form af produkt-, kunde- og leverandørkartotek, kontoplaner, dagbøger, moms håndtering, dimensioner, enhedssystem, betalingsoversigter, valuta håndtering og valutakurser samt indkomst år. Zenegy Expense Zenegy leverer cloud-baserede udgiftsløsninger til virksomheder af alle størrelser. Løsningen muliggør håndtering af medarbejder-betalingskort samt håndtering af leverandør-udgifter. Desuden indeholder løsningen opsættelse af godkendelses flow samt bogføringsløsning til kontering og kategorisering af udgifter.

Zenegy Storage
Zenegy tilbyder en cloud-baseret mulighed for medarbejdere hos den dataansvarlige til at opbevare deres data i Applikationen efter abonnementsaftalens ophør eller efter at en medarbejders tilknytning til den dataansvarlige er ophørt.

Databehandlerens databehandling medfører, at Databehandleren behandler følgende almindelige typer personoplysninger:

- Navn
- Adresse
- Telefonnummer
- e-mail
- Brugernavn
- Adgangskode
- CPR-nummer (eller tilsvarende udenlandsk identitetsnummer)
- Alder
- Medarbejder ID og Foto
- Bankoplysninger (kontooplysninger)
- Titel
- Løn og lønoplysninger
- Skatteoplysninger
- Rejseoplysninger
- Fraværsoplysninger
- Fakturerings- og bogføringsbilag
- Cookies

På trods af ovenstående beskrivelser kan Databehandleren ikke med sikkerhed vide, hvilke personoplysninger der behandles af Databehandleren som databehandler, fordi Databehandleren hoster personoplysninger, som Databehandleren ikke har fuld kontrol over eller indblik i.

Generelt om Databehandlerens kontroller

Zenegy benytter Wired Relations til at føre kontrol med sine aktiviteter i et årshjul.

Herunder udarbejder Zenegy årligt en ISAE 3402.
I denne dokumenteres:

Processer
- Dokumentation på udarbejdelse af processer.
- Løbende, og mindst en gang årligt, vurderinger af, om Databehandlerens procedurer, politikker og fortegnelser skal opdateres.

Leverandører
- Dokumentation på leverandør processer.
- Udarbejdelse af Databehandler aftale med alle leverandører
- Udarbejdelse af TIA for leverandører uden for EU.
- Årlig gennemgang af TIA for leverandører uden for EU.
- Udarbejdelse af Risikovurdering på alle leverandører der behandler data for vores kunder.
- Årlig gennemgang af Risk Risikovurdering på leverandører.
- Årlig gennemgang af databehandler aftaler for alle leverandører.

Fysisk adgang
- Dokumentation på proces for tildeling og tilbagelevering af fysiske adgange til faciliteter.
- Løbende, og mindst en gang årligt, gennemgang af fysiske adgange.

Virtuelle adgange
- Dokumentation på proces for tildeling og tilbagelevering af virtuelle adgange til systemer.
- Løbende, og mindst en gang årligt, gennemgang af virtuelle adgange.

Systemer
- Genoprettelseskontrol af systemet minimum en gang årligt.
- Årlig penetration test.

Medarbejdere
- Baggrundscheck af medarbejdere inden ansættelse, herunder gennemgang af straffeattester.

Uddannelse
- Løbende uddannelse af medarbejdere inden for IT og Sikkerhed.
- Årlig test af medarbejdernes kendskab inden for IT og Sikkerhed.
- Løbende uddannelse af medarbejdere inden for GDPR.
- Årlig test af medarbejdernes kendskab inden for GDPR.

Kontrolmål A - Instruks

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

Kontrol aktivitet 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 en gang årligt, vurdering af, om procedurerne skal opdateres.

Resultat A.1

Databehandleren har udarbejdet skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.

Kontrol aktivitet A.2

Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig

Resultat A.2

Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruksen fra den Dataansvarlige.

Kontrol aktivitet 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.

Resultat A.3

Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter Databehandlerens mening er i strid med GDPR eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Kontrolmål B – Tekniske sikkerhedsforanstaltninger

Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende, og mindst en gang årligt, vurdering af, om procedurerne skal opdateres.

Kontrol aktivitet B.1

Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende, og mindst en gang årligt, vurdering af, om procedurerne skal opdateres.

Resultat B.1

Databehandleren har udarbejdet skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den Dataansvarlige.

Kontrol aktivitet 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 med dataansvarlige aftalte sikringsforanstaltninger.

Resultat B.2
Databehandleren har foretaget en risikovurderingen af den aktuelle behandling af personoplysninger og på baggrund heraf implementeret de tekniske sikkerhedsforanstaltninger, der vurderes relevante for at opnå passende sikkerhed.

Databehandleren har implementeret de, med den Dataansvarlige, aftalte tekniske sikkerhedsforanstaltninger.

Kontrol aktivitet B.3
Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.

Resultat B.3
Databehandleren har installeret et antivirusprogram, som løbende opdateres, for de systemer og databaser, der anvendes til behandling af personoplysninger. End-points er registeret og knyttet til et system som også har real time overvågning i forhold til virus, malware samt phishing. Med systemet kan Databehandleren fjernslette alt indhold på End-point. End-points leveres præ-konfigureret til brugerne. Der foretages løbende vurdering af trusselsbilledet mod End-points.

Kontrol aktivitet B.4
Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.

Resultat B.4
Databehandleren har sikret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.

Kontrol aktivitet B.5
Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.

Resultat B.5
Denne kontrol er ikke relevant for Databehandleren da Zenegy har ikke et netværk der giver adgang til systemer eller databaser. Alle Zenegys systemer er cloud baseret.

Kontrol aktivitet B.6
Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.

Resultat B.6
Databehandleren har sikret, at adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor. Dette sker gennem arbejdsrelateret og rolle baseret adgang, hvor der foretages løbende, og mindst en gang årligt, gennemgang.

Kontrol aktivitet B.7
Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.

Resultat B.7
Databehandlerens systemer og databaser, der anvendes til behandling af personoplysninger, er etableret med systemovervågning med alarmering. Dataansvarlig har desuden mulighed for at slå notifikationer til på deres aftale og vil i så fald modtage notifikationer hvis der foretages væsentlige ændringer.

Kontrol aktivitet B.8
Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.

Resultat B.8
Databehandleren anvender effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail. Man kan ikke tilgå applikationen eller data uden brug af https og data er AES 256 krypteret både i transit og ”at rest”.

Kontrol aktivitet B.9.1
Der er etableret logning i systemer, databaser og netværk af følgende forhold:
(1) Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder,
(2) Sikkerhedshændelser omfattende
- (i) ændringer i logopsætninger, herunder deaktivering af logning og
- (ii) ændringer i systemrettigheder til brugere
Fejlede forsøg på login til systemer, databaser og netværk logges.

Resultat B.9.1
Databehandleren logger ændringer, der udføres af systemadministratorer, ændringer i logopsætninger, herunder deaktivering af logning og ændringer i systemrettigheder til brugere.

Kontrol aktivitet B.9.2
Fejlede forsøg på login til systemer, databaser og netværk logges.

Resultat B.9.2
Databehandleren logger fejlede forsøg på login i Databehandlerens systemer, databaser og netværk.

Kontrol aktivitet B.9.3
Logoplysninger er beskyttet mod manipulation og tekniske fejl.

Resultat B.9.3
Databehandleren har sikret, at logoplysninger er beskyttet mod manipulation og tekniske fejl.

Kontrol aktivitet B.9.4
Logoplysninger gennemgås løbende.

Resultat B.9.4
Databehandleren har sikret, at logoplysningerne løbende gennemgås.

Kontrol aktivitet B.10
Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form.

Resultat B.10
Databehandleren bruger personoplysninger, der anvendes til udvikling, test eller lignende. Disse er altid i pseudonymiseret eller anonymiseret form hvor der ikke bruges demo data fra offentlige kilder. Eksempelvis vedligeholder Skat og CPR deres egne demo data. Har dataansvarlig adgang til et test miljø er dataansvarlig selv ansvarlig for den data det indtastes.

Skat: https://skat.dk/data.aspx?oid=2245110

CPR: https://cprservicedesk.atlassian.net/wiki/spaces/CPR/pages/11436127/Testdata

Digitaliseringsstyrelsen: https://digst.dk/it-loesninger/faellesoffentligt-testdatasaet/om-faellesoffentligt-testdatasaet/

Kontrol aktivitet B.11
De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.

Resultat B.11
Databehandleren har sikret, at etablerede tekniske sikkerhedsforanstaltninger løbende testes ved sårbarhedsscanninger og penetrationstest. Zenegy har årlig penetration test. Zenegy benytter SNYK og White Source Bolt til at overvåge svagheder i koden.

Kontrol aktivitet B.12
Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.

Resultat B.12
Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches. Zenegy følger udviklings standarder hvor at al kode peer-reviews. Når kode er udviklet, gennemgås den af en Teamlead som, ved godkendelse, ligger den på et QA miljø. På QA miljøet gennemgås den forretningsmæssige logik inden koden sendes til et Beta miljø. På beta miljøet gennemgås den forretningsmæssige logik af en Product Owner eller en Business Analyst.

Kontrol aktivitet B.13.1
Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger.

Resultat B.13.1
Databehandleren har formaliseret forretningsgange for tildeling og tilbagekaldelse af brugeradgange til personoplysninger.

Kontrol aktivitet B.13.2
Brugeres adgang revurderes regelmæssigt, herunder at brugerrettigheder fortsat kan begrundes i et arbejdsbetinget behov.

Resultat B.13.2
Brugeres adgang revurderes regelmæssigt, og minimum en gang årligt, herunder om brugerrettigheder fortsat kan begrundes i et arbejdsbetinget behov. Dette gælder både fysiske og virtuelle adgange.

Kontrol aktivitet 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 to-faktor autentifikation.

Resultat B.14
Databehandleren anvender som minimum to-faktor autentifikation for adgang til Databehandlerens systemer og databaser, hvori der sker behandling af personoplysninger, der medfører høj risiko for de registrerede personer.

Kontrol aktivitet 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.

Resultat B.15
Databehandleren har etableret fysiske sikkerhedsforanstaltninger, således at kun personer, som er autoriseret, kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Zenegy har implementeret kort adgang til kontor faciliteter. Adgange tildeles og kontrolleres via et system. Der foretages løbende, og mindst en gang årligt, gennemgang ad fysiske adgange.

Kontrolmål C – Organisatoriske sikkerhedsforanstaltninger

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

Kontrol aktivitet C.1.1
Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere.

Resultat C.1.1
Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder relevante medarbejdere.

Kontrol aktivitet C.1.2
Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende, og mindst en gang årligt, vurdering af, om informationssikkerhedspolitikken skal opdateres.

Resultat C.1.2
Databehandlerens informationssikkerhedspolitik tager udgangspunkt i den gennemførte risikovurdering. IT og sikkerhedspolitikken opdateres og godkendes minimum årligt ved ledelsesmøde og distribueres herefter til alle medarbejdere.

Kontrol aktivitet C.2
Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.

Resultat C.2
Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.

Kontrol aktivitet C.3
Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.

Resultat C.3
Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.
Efterprøvningen omfatter i relevant omfang:
(1) Referencer fra tidligere ansættelser
(2) straffeattest
(3) eksamensbeviser
(4) baggrundskontrol via internetsøgninger

Kontrol aktivitet C.4.1
Ved ansættelse underskriver medarbejdere en fortrolighedsaftale.

Resultat C.4.1
Databehandlerens medarbejdere underskriver en fortrolighedsaftale ved ansættelse. Dette er en integreret og ufravigelig del af ansættelsesaftalen.

Kontrol aktivitet C.4.2
Medarbejderen bliver introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.

Resultat C.4.2
Databehandlerens medarbejdere bliver introduceret til it-sikkerhedspolitikker og procedurer vedrørende databehandling samt anden relevant information i forbindelse med deres behandling af personoplysninger. Dette sker både ved ansættelses og mindst en gang årligt.

Kontrol aktivitet C.5
Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.

Resultat C.5
Databehandleren har implementeret en proces og et system, som sikrer, at brugerens rettigheder ved fratrædelse bliver inaktive eller ophører, herunder at aktiver inddrages. Herudover gennemgås alle adgange, fysiske og virtuelle, minimum en gang årligt.

Kontrol aktivitet 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, databehandleren udfører for de dataansvarlige.

Resultat C.6
Ved fratrædelse orienteres Databehandlerens medarbejdere om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.

Kontrol aktivitet C.7
Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.

Resultat C.7
Zenegy gennemfører løbende, og minimum årligt, awareness-træning af sine medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.

Kontrolmål D – Procedurer for sletning og tilbagelevering af personoplysninger

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

Kontrol aktivitet 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 en gang årligt, vurdering af, om procedurerne skal opdateres.

Resultat D.1
Databehandleren har implementeret skriftlige interne procedurer, som forpligter og oplyser Databehandleren og dennes medarbejdere om, hvordan der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den Dataansvarlige.

Systemet der stilles rådighed har indbygget funktionalitet til at eksportere data fra systemet. Systemet har indbygget funktionalitet til automatisk sletning af data, hvor det kan indstilles hvor lang tid data skal beholdes mens Dataansvarlig bruger systemet aktivt.

Ved abonnementsaftalens ophør får den dataansvarlige valget imellem, om data skal slettes efter 7 dage, eller om den dataansvarlige ønsker opbevaring af og adgang til data i 6 måneder. Data samles og dataansvarlige gøres opmærksom på at denne kan hente sin samlede data.

Hvis den dataansvarlige inden udløbet af en valgt 7 dages eller 6 måneders periode fortsat ønsker opbevaring af data hos databehandleren, skal den dataansvarlige genaktivere abonnementet.

Kontrol aktivitet D.2
Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.

Resultat D.2
Databehandleren har aftalt - eller er blevet instrueret i - specifikke krav til opbevaringsperioder og sletterutiner af den Dataansvarlige.

Kontrol aktivitet D.3
Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige enten (1) tilbageleveret til den dataansvarlige og/eller (2) slettet, hvor det ikke er i modstrid med anden lovgivning

Resultat D.3
Det bekræftes, at data i henhold til aftalen med den Dataansvarlige tilbageleveres og slettes, hvor det ikke er i modstrid med anden lovgivning, når behandlingen af personoplysninger ophører.

Kontrolmål E – Opbevaring af personoplysninger

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

Kontrol aktivitet 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 en gang årligt, vurdering af, om procedurerne skal opdateres.

Resultat E.1

Databehandleren har skriftlige procedurer, som forpligter og oplyser Databehandleren og dennes medarbejdere om, at der alene må foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den Dataansvarlige.

Kontrol aktivitet E.2

Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.

Resultat E.2

Databehandleren foretager kun behandling af personoplysninger inklusive opbevaring for den Dataansvarlige på de af den Dataansvarlige godkendte lokaliteter, lande eller landområder.

Kontrolmål F – Underdatabehandlere

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

Kontrol aktivitet 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 en gang årligt, vurdering af, om procedurerne skal opdateres.

Resultat F.1

Databehandleren har skriftlige procedurer, som indeholder krav til Databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.

Kontrol aktivitet F.2

Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.

Resultat F.2

Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den Dataansvarlige.

Kontrol aktivitet F.3
Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.

Resultat F.3
Databehandleren underretter den Dataansvarlige rettidigt ved ændringer i anvendelsen af generelt godkendte underdatabehandlere, mens ændringer i specifikt godkendte underdatabehandlere kun sker efter specifik godkendelse fra den Dataansvarlige.

Kontrol aktivitet F.4
Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.

Resultat F.4
Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen eller lignende med den Dataansvarlige.

Kontrol aktivitet F.5
Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af (1) Navn, (2) CVR-nr., (3) adresse og (4) beskrivelse af behandlingen.

Resultat F.5
Databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere med angivelse af navn, CVR-nr eller lignende international identifikation., adresse, og beskrivelse af den behandling, som underdatabehandlerne foretager.

Kontrol aktivitet F.6
Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende.

Resultat F.6
Databehandleren foretager opfølgning på den enkelte under-databehandler og dennes aktivitet ved møder, inspektioner, gennemgang af revisionserklæring eller lignende på baggrund af ajourført risikovurdering.

Kontrol aktivitet F.7
Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.

Resultat F.7
Databehandleren orienterer ikke den Dataansvarlige om foretagne opfølgninger med underdatabehandlere.

Kontrolmål G – Overførsel af personoplysninger

Der efterleves procedurer og kontroller, som sikrer, at Databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med de(n) dataansvarlige på baggrund af et gyldigt overførelsesgrundlag.

Kontrol aktivitet 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 en gang årligt, vurdering af, om procedurerne skal opdateres.

Resultat G.1

Databehandleren har skriftlige interne procedurer, der forpligter og oplyser Databehandlerens medarbejdere om, at personoplysninger alene må overføres til tredjelande eller internationale organisationer i henhold til aftalen med den Dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Kontrol aktivitet G.2

Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.

Resultat G.2

Det er reguleret i databehandleraftalen, at Databehandleren kun må overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den Dataansvarlige.

Kontrol aktivitet G.3

Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.

Resultat G.3

Databehandleren har interne skriftlige procedurer, der indeholder krav om, at Databehandlerens medarbejdere skal vurdere og herefter dokumentere, at der eksisterer et gyldigt overførselsgrundlag ved overførsel af personoplysninger til tredjelande eller internationale organisationer.

Kontrolmål H – Bistand til den dataansvarlige

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

Kontrol aktivitet 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 en gang årligt – vurdering af, om procedurerne skal opdateres

Resultat H.1

Databehandleren har implementeret interne skriftlige procedurer, der regulerer, hvordan Databehandleren skal yde den bistand, som er reguleret i GDPR, artikel 28, stk. 3, litra e, til den Dataansvarlige ved den Dataansvarliges besvarelse af anmodninger fra registrerede personer.

Kontrol aktivitet 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.

Resultat H.2

Databehandleren har implementeret detaljerede procedurer, der indeholder beskrivelser af Databehandlerens processer ved dennes bistand til den Dataansvarlige vedrørende udlevering, rettelse eller sletning af personoplysninger samt begrænsning af eller oplysning om behandling af personoplysninger til den registrerede. Disse procedurer muliggør en korrekt og rettidig bistand til den Dataansvarlige.
Den Dataansvarlige har adgang til logs, kan trække relevant data og kan opsætte systemet til udlevering, rettelse eller sletning af personoplysninger samt begrænsning af eller oplysning om behandling af personoplysninger til den registrerede.

Kontrolmål I – Sikkerhed

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

Kontrol aktivitet 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 en gang årligt, vurdering af, om procedurerne skal opdateres.

Resultat I.1

Databehandleren har en intern skriftlig procedure for brud på persondatasikkerheden, der regulerer, at Databehandleren skal underrette den Dataansvarlige om et brud på persondatasikkerheden, der har fundet sted hos Databehandleren i overensstemmelse med GDPR, artikel 33, stk. 2.

Kontrol aktivitet I.2
Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden, herunder
(1) awareness hos medarbejdere
(2) overvågning af netværkstrafik
(3) opfølgning på logning af tilgang til personoplysninger.

Resultat I.2
Databehandleren har implementeret tiltag, der skal sikre, at Databehandlerens medarbejdere orienteres og oplæres i identifikation af eventuelle brud på persondatasikkerheden. Sådanne tiltag består eksempelvis af awareness-træning hos Databehandlerens medarbejdere og logning af anormaliteter og gentagne forsøg på adgang til personoplysninger. Databehandleren har ikke et netværk i traditionel forstand da alt data behandles via Cloud løsninger.

Kontrol aktivitet I.3
Databehandleren vil ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse - og inden for den tid som er reguleret i databehandleraftalen - efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.

Resultat I.3
Databehandleren vil, ved eventuelle brud på persondatasikkerheden, underrette den Dataansvarlige uden unødig forsinkelse og inden for den tid, som er reguleret i databehandleraftalen efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos Databehandleren eller hos en underdatabehandler i overensstemmelse med kravet i GDPR, artikel 33, stk. 2.

Kontrol aktivitet I.4
Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet, herunder
(1) karakteren af bruddet på persondatasikkerheden
(2) sandsynlige konsekvenser af bruddet på persondatasikkerheden
(3) foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.

Resultat I.4
Databehandleren har implementeret interne skriftlige procedurer, der regulerer, hvordan Databehandleren skal yde den bistand, som er reguleret i GDPR, artikel 28, stk. 3, litra f, til den Dataansvarlige ved den Dataansvarliges anmeldelse af brud på persondatasikkerheden til Datatilsynet.
Der udarbejdes i en såkaldt Incident rapport som udleveres til den Dataansvarlige i tilfælde af brud på persondatasikkerheden.

Kontakt

Hvis du har spørgsmål eller kommentarer til denne Rapport, kan du rette henvendelse til

Zenegy
Slotsmarken 16
2970 Hørsholm
info@zenegy.com