# DATABEHANDLERAFTALE

Databehandleraftalen foreligger mellem

LaserTryk.dk A/S

P. O. Pedersensvej 26
8200 Aarhus N

CVR. nr. 21 68 64 33

(i det følgende betegnet ”Dataansvarlig”)

og

Zitcom A/S

Højvangen 4
8660 Skanderborg

CVR. nr. 29 41 20 06

(i det følgende betegnet ”Databehandler”)

(herefter samlet benævnt "Parterne" og hver for sig "Part")

har indgået følgende databehandleraftale (”Databehandleraftalen”) om Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige.

## 1 BAGGRUND, FORMÅL OG OMFANG

1.1 Som led i Databehandlerens levering af services (herefter benævnt ”Hostingaftalen”), foretager Databehandleren behandling af personoplysninger, som den Dataansvarlige er ansvarlig for.

1.2 Databehandleren overholder lovgivningens til enhver tid stillede krav til databehandlere, herunder fra d. 25. maj 2018; Persondataforordningen

(Europa-Parlamentets og Rådets forordning 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger) med tilhørende retsakter samt heraf afledt national lovgivning.

1.3 Det er et krav i Persondatalovgivningen, at der mellem Parterne indgås skriftlig aftale om den behandling, som skal foretages; en såkaldt 'databehandleraftale'. Denne Databehandleraftale udgør en sådan databehandleraftale.

1.4 Begrebet "Hostingaftalen" dækker over alle gældende hostingaftaler, som er indgået, eller som indgås mellem den Dataansvarlige og Databehandleren, herunder hører de produkter, som den Dataansvarlige har og fremtidigt erhverver hos Databehandleren. Såfremt Databehandlerens leverance ændres, i et sådant omfang, at den Dataansvarliges instruks skal ændres, vil Parterne skulle indgå en ny Databehandleraftale.

## 2 PERSONOPLYSNINGER OMFATTET AF DATABEHANDLERAFTALEN

2.1 Databehandleraftalen og tilhørende instruks omfatter alle typer personoplysninger, som overlades af den Dataansvarlige til Databehandleren i henhold til den mellem Parterne indgåede Hostingaftale. Der kan være tale om følgende oplysningstyper:

| **Almindelige oplysninger** | **Følsomme oplysninger** |
|---|---|
| • Alle øvrige oplysninger som ikke er følsomme oplysninger | • Oplysninger om race eller etnisk oprindelse<br>• Politisk, religiøs eller filosofisk overbevisning<br>• Fagforeningsmæssigt tilhørsforhold<br>• Helbredsoplysninger<br>• Oplysninger om seksuelle forhold og orientering<br>• Oplysninger om strafbare forhold<br>• (På sigt også genetiske og biometriske data) |

2.2 Kategorierne af de registrerede personer, som personoplysningerne vedrører, kan eksempelvis udgøre brugere, ansatte, ansøgere, kandidater, kunder, forbrugere, patienter eller lign.

## 3 GEOGRAFISKE KRAV

3.1 Den behandling af persondata, som Databehandleren foretager efter aftale med den Dataansvarlige, må alene foretages af Databehandleren eller underdatabehandlere,

jf. pkt. 5, indenfor det Europæiske Økonomiske Samarbejde (EØS). Databehandleren er ingenlunde berettiget til at lade databehandling foregå udenfor EØS uden den Dataansvarliges skriftlige samtykke, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

## 4 INSTRUKS

4.1 Den primære databehandling som Databehandleren udfører, er opbevaring af de data, som den Dataansvarlige overlader til Databehandleren i forbindelse med indgåelsen af Hostingaftalen. Såfremt den Dataansvarlige ønsker andre former for databehandling, som ikke er relateret til de standard services Databehandleren leverer, skal den Dataansvarlige give Databehandleren tydelig dokumenteret instruks herom.

4.2 Databehandleren handler alene efter dokumenteret instruks fra den Dataansvarlige. Databehandleren skal sikre, at de overladte personoplysninger ikke benyttes til andre formål eller behandles på anden måde, end hvad der fremgår af den Dataansvarliges instruks. Alle de for afviklingen af Hostingaftalen nødvendige og beskrevne behandlinger betragtes som dokumenterede.

4.3 Såfremt en instruktion efter Databehandlerens opfattelse er i strid med lovgivningen, skal Databehandleren orientere den Dataansvarlige herom.

4.4 Såfremt behandlingen af personoplysninger hos Databehandleren sker helt eller delvist ved anvendelse af fjernopkobling, herunder hjemmearbejdspladser, skal Databehandleren fastsætte retningslinjer for medarbejdernes behandling af personoplysninger ved anvendelse af fjernopkobling, som i øvrigt skal opfylde de i Databehandleraftalen stillede krav.

4.5 Databehandleren skal så vidt muligt bistå den Dataansvarlige med opfyldelse af den Dataansvarliges forpligtelser til at besvare anmodninger om udøvelse af de registreredes rettigheder, herunder om indsigt, berigtigelse, begrænsning eller sletning, hvis de relevante personoplysninger behandles af Databehandleren. Modtager Databehandleren sådan henvendelse fra den registrerede, orienterer Databehandleren den Dataansvarlige herom.

4.6 Den Dataansvarlige hæfter for alle Databehandlerens omkostninger ved sådan bistand, jf. pkt. 4.5, herunder til underdatabehandlere. Databehandlerens bistand afregnes til Databehandlerens til enhver tid gældende timetakst for sådant arbejde.

## 5 BRUG AF UNDERDATABEHANDLER

5.1 Den Dataansvarlige giver Databehandleren samtykke til anvendelse af underdatabehandlere, forudsat at de i Databehandleraftalen stillede betingelser for dette er opfyldt. Den Dataansvarlige kan altid se Databehandlerens underdatabehandlere på Databehandlerens hjemmeside på www.zitcom.dk/compliance, hvor Databehandleren orienterer om ændringer i valg af underdatabehandlere.

5.2 Underdatabehandleren er under Databehandlerens instruks. Databehandleren har indgået skriftlig databehandleraftale med underdatabehandleren, hvori det er sikret, at underdatabehandleren opfylder krav tilsvarende dem, som stilles til Databehandleren af den Dataansvarlige i medfør af Databehandleraftalen.

5.3 Omkostninger forbundet med etablering af aftaleforholdet til en underdatabehandler, herunder omkostninger til udarbejdelse af databehandleraftale og eventuel etablering af grundlag for overførsel til tredjelande, afholdes af Databehandleren og er således den Dataansvarlige uvedkommende.

5.4 Såfremt den Dataansvarlige måtte ønske at instruere underdatabehandlere direkte, bør dette alene ske efter drøftelse med og via Databehandleren. Hvis den Dataansvarlige afgiver instruks direkte overfor underdatabehandlere, skal den Dataansvarlige senest samtidig underrette Databehandleren om instruksen og baggrunden for denne. Hvor den Dataansvarlige instruerer underdatabehandlere direkte, a) er Databehandleren fritaget for ethvert ansvar, og enhver følge af sådan instruks er alene den Dataansvarliges ansvar, b) hæfter den Dataansvarlige for enhver omkostning, som instruksen måtte medføre for Databehandleren, herunder er Databehandleren berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al arbejdstid, som en sådan direkte instruks måtte medføre for Databehandleren og c) den Dataansvarlige er selv ansvarlig overfor underdatabehandlere for enhver omkostning, vederlag eller anden betaling til underdatabehandleren, som den direkte instruks måtte medføre.

5.5 Den Dataansvarlige accepterer ved indgåelsen af nærværende Databehandleraftale, at Databehandleren er berettiget til at skifte underdatabehandler, forudsat, at a) en eventuel ny underdatabehandler overholder tilsvarende betingelser, som stilles i nærværende pkt. 5 til den nuværende underdatabehandler og, at b) den Dataansvarlige senest ved en eventuel anden underdatabehandlers påbegyndelse af behandlingen af personoplysninger, som den Dataansvarlige er dataansvarlig for, fremgår af Databehandlerens hjemmeside.

5.6 Såfremt den Dataansvarlige ikke ønsker, at Databehandleren anvender en ny underdatabehandler som varslet, jf. pkt. 5.6, skal den Dataansvarlige gøre skriftlig indsigelse til Databehandleren mod anvendelsen af sådan ny underdatabehandler senest 14 dage efter modtagelse af orientering eller at den Dataansvarlige er blevet opmærksom på underdatabehandleren på Databehandlerens hjemmeside. I tilfælde

af, at Databehandleren ikke ser sig i stand til at imødekomme en eventuel indsigelse fra den Dataansvarlige mod en ny underdatabehandler, meddeles dette til den Dataansvarlige snarest mulig, og den Dataansvarlige kan i så fald herefter opsige Hostingaftalen med en måneds varsel fra d. 1. i en måned. For at indsigelsen skal resultere i dette opsigelsesvarsel, skal indsigelsen være sagligt begrundet.

## 6 BEHANDLING OG VIDEREGIVELSE AF PERSONOPLYSNINGER

6.1 Den Dataansvarlige indestår for at have fornøden hjemmel til behandling af personoplysningerne omfattet af nærværende Databehandleraftale.

6.2 Databehandleren må ikke uden skriftligt samtykke fra den Dataansvarlige videregive oplysninger til tredjemand, medmindre sådan videregivelse følger af lovgivningen eller af en bindende anmodning fra en retsinstans eller en databeskyttelsesmyndighed, eller det fremgår af denne Databehandleraftale.

## 7 SIKKERHED

7.1 Databehandleren skal træffe passende tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.2 ovenfor.

7.2 Databehandleren skal implementere og opretholde de i bilag 1 beskrevne sikkerhedsforanstaltninger og i øvrigt opfylde de i Hostingaftalen stillede krav.

7.3 Databehandleren er altid berettiget til at implementere alternative sikkerhedsforanstaltninger under forudsætning af, at sådanne sikkerhedsforanstaltninger som minimum opfylder eller giver større sikkerhed end de bilag 1, beskrevne sikkerhedsforanstaltninger og i øvrigt opfylder de i Hostingaftalen stillede krav til sikkerhed. Databehandleren kan ikke uden den Dataansvarliges skriftlige forudgående godkendelse foretage forringelse af sikkerhedsforholdene.

7.4 Hvis Databehandleren er etableret i en anden EU-medlemsstat, skal de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den EU-medlemsstat, hvor Databehandleren er etableret, derudover gælde for Databehandleren. Hvis Databehandleren er etableret i en anden EU-medlemsstat, skal Databehandleren således overholde såvel sikkerhedskrav omfattet af gældende lovgivning i Danmark som sikkerhedskrav i Databehandlerens hjemland. Det samme gælder for underdatabehandlere.

7.5 Databehandleren skal efter nærmere aftale med den Dataansvarlige, så vidt muligt, bistå den Dataansvarlige med at sikre overholdelse af forpligtelserne i forordningens artikel 32 (gennemførelse af passende tekniske og organisatoriske foranstaltninger), 35 (foretagelse af konsekvensanalyse vedrørende databeskyttelse) og 36 (forudgående høring). Såfremt den Dataansvarlige kræver yderligere bistående, end Databehandlerens standard procedurer for overholdelse af ovenstående artikler, er Databehandleren berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al Databehandlerens arbejdstid, som en sådan aftale måtte medføre for Databehandleren, ligesom den Dataansvarlige hæfter for eventuel betaling til underdatabehandleren.

7.6 Såfremt det i pkt. 7.5 anførte fører til skærpede sikkerhedsforanstaltninger i forhold til det allerede aftalte mellem Parterne i medfør af denne Databehandleraftale, implementerer Databehandleren, så vidt det er muligt, sådanne foranstaltninger, forudsat at Databehandleren modtager betaling herfor, jf. pkt. 7.7 nedenfor.

7.7 Omkostninger forbundet med sådan implementering af foranstaltninger, jf. pkt. 7.6, afholdes af den Dataansvarlige og er således Databehandleren uvedkommende. Databehandleren er endvidere berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al Databehandlerens arbejdstid, som sådanne implementeringer måtte medføre for Databehandleren, ligesom den Dataansvarlige hæfter for eventuel betaling til underdatabehandleren.

## 8 TILSYNSRET

8.1 Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige tilstrækkelige informationer til, at denne kan påse, at Databehandleren overholder persondataforordningens artikel 28 og Databehandleraftalen.

8.2 I det omfang den Dataansvarlige tillige ønsker, at dette skal omfatte den behandling, som sker hos underdatabehandlere, oplyses Databehandleren om dette. Databehandleren indhenter herefter tilstrækkelige oplysninger fra underdatabehandleren.

8.3 Såfremt den Dataansvarlige ønsker at foretage tilsyn, som anført i dette pkt. 8, skal den Dataansvarlige altid give Databehandleren et varsel på mindst 30 dage i sådan forbindelse.

8.4 Databehandleren skal én gang årligt på anmodning fra den Dataansvarlige foranledige, at en alment anerkendt og uafhængig tredjepart afgiver en sikkerhedsrevisionsrapport, som er udarbejdet i overensstemmelse med en anerkendt revisionsstandard.

8.5 Såfremt Databehandleren får udarbejdet en sikkerhedsrevisionsrapport, som

beskriver sikkerhedsforholdene hos Databehandleren i overensstemmelse med pkt. 8.4, er den Dataansvarlige berettiget til at få udleveret en kopi heraf. Kopi af sådan sikkerhedsrevisionsrapport kan den Dataansvarlige altid hente på Databehandlerens hjemmeside.

8.6 Såfremt den Dataansvarlige ønsker at få udarbejdet anden eller yderligere sikkerhedsrevisionsrapport udover de rapporter som Databehandleren allerede får udarbejdet på eget initiativ, eller at der i øvrigt ønskes foretaget tilsyn af Databehandlerens eller underdatabehandlerens persondatabehandling, herunder såfremt den Dataansvarlige ønsker sikkerhedsrevisionsrapport udarbejdet på et nærmere bestemt tidspunkt, aftales dette nærmere med Databehandleren. Databehandleren eller underdatabehandleren kan til enhver tid kræve, at en sådan sikkerhedsrevisionsrapport udarbejdes i overensstemmelse med en anerkendt revisionsstandard (fx ISAE 3402 med referenceramme til ISO 27002:2014 eller lignende) af en alment anerkendt og uafhængig tredjepart, som beskæftiger sig med sådanne forhold.

8.7 Den Dataansvarlige afholder alle omkostninger i forbindelse med tilsyn af sikkerhedsforhold hos Databehandleren samt i forhold til underdatabehandleren, herunder er Databehandleren berettiget til at fakturere den Dataansvarlige med sin sædvanlige timetakst for al Databehandlerens arbejdstid, som sådant tilsyn måtte medføre for Databehandleren, ligesom den Dataansvarlige hæfter for eventuel betaling til underdatabehandleren.

## 9 PERSONDATASIKKERHEDSBRUD

9.1 Såfremt Databehandleren måtte blive bekendt med et persondatasikkerhedsbrud, hvorved forstås et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, er Databehandleren forpligtet til uden unødig forsinkelse at søge at lokalisere et sådan brud og søge at begrænse opstået skade i videst muligt omfang, samt i det omfang det er muligt reetablere eventuelt mistede data.

9.2 Databehandleren er endvidere forpligtet til uden unødig forsinkelse at underrette den Dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden. Databehandleren skal herefter uden unødig forsinkelse, i det omfang det er muligt, give skriftlig meddelelse til den Dataansvarlige, som så vidt muligt skal indeholde:

a) En beskrivelse af karakteren af bruddet, herunder kategorierne og det omtrentlige antal berørte registrerede og registreringer af personoplysninger.
b) Navn på og kontaktoplysninger for databeskyttelsesrådgiveren.
c) En beskrivelse af de sandsynlige konsekvenser af bruddet.

d) En beskrivelse af de foranstaltninger, som Databehandleren eller underdatabehandleren har truffet eller foreslår truffet for at håndtere bruddet, herunder foranstaltninger for at begrænse dets mulige skadevirkninger.

9.3 For så vidt det ikke er muligt at give de i pkt. 9.2 anførte oplysninger samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse.

9.4 Tilsvarende er underdatabehandlere pålagt uden unødig forsinkelse at underrette Databehandleren i overensstemmelse med pkt. 9.2 og 9.3.

## 10 TAVSHEDSPLIGT

10.1 Databehandleren skal holde personoplysningerne, som behandles i henhold til Databehandleraftalen, fortrolige, og er således alene berettiget til at anvende personoplysningerne som led i opfyldelsen af sine forpligtelser og rettigheder i henhold til Databehandleraftalen. Databehandleren skal pålægge medarbejdere og eventuelle andre, herunder underdatabehandlere, der er autoriserede til at behandle de i Databehandleraftalen omfattede personoplysninger, fortrolighed om disse. Sådan fortrolighed finder tillige anvendelse efter Databehandleraftalens ophør.

## 11 FORRANG

11.1 Medmindre andet fremgår af Databehandleraftalen, har bestemmelser i Databehandleraftalen forrang i forhold til tilsvarende bestemmelser i andre aftaler mellem Parterne, herunder Hostingaftalen.

## 12 VARIGHED OG OPHØR AF DATABEHANDLERAFTALEN

12.1 Databehandleraftalen træder i kraft ved Parternes underskrift.

12.2 Nærværende Databehandleraftale erstatter eventuelt tidligere indgåede databehandleraftaler mellem Parterne.

12.3 I tilfælde af at Hostingaftalen ophører, uanset årsag, ophører Databehandleraftalen også.

12.4 Databehandleren er dog forpligtet af denne Databehandleraftale, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige, idet den Dataansvarlige snarest muligt og senest 14 dage efter ophør af Databehandleraftalen skal oplyse Databehandleren skriftligt, hvorvidt

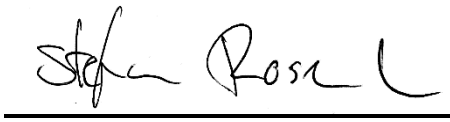
Databehandleren skal tilbagelevere eller slette de behandlede personoplysninger. 30 dage efter ophøret af Databehandleraftalen er Databehandleren berettiget til at slette alle personoplysninger, som er blevet behandlet under den ophørte Hostingaftale på vegne af den Dataansvarlige. Databehandleren må dog altid opbevare de behandlede data, såfremt dette følger af EU-retten eller medlemsstaternes nationale ret.

## 13 BILAG

Bilag 1: Sikringsmiljø (Zitcom)

## 14 UNDERSKRIFT

14.1 Ovenstående tiltrædes hermed med virkning fra Parternes underskrift.

| For den Dataansvarlige | For Databehandleren |
|---|---|
| 8200 Aarhus N, den | Skanderborg, den 11-05-2018 |
| |  |
| Anders Grønborg | Stefan Rosenlund |

# Præsentation af Zitcoms sikringsmiljø

| | |
|---|---|
| **Version:** | **1.1** |
| **Dato:** | 1. marts 2018 |

ISO 27001

ISAE 3402 Type 2
Revisorerklæring

# Indholdsfortegnelse

## Indledning

Som hostingleverandør er vores vigtigste sikkerhedsopgave at passe godt på dine data og sørge for, at du til enhver tid lever op til sikkerhedskravene fra dine kunder. Sikkerhed er derfor et område, som vi tager meget seriøst - på alle niveauer.

Formålet med dette dokument er at give dig et indblik i, hvordan vi sikrer vores platform, så du som kunde ikke behøver at bekymre dig om sikkerhed, men i stedet kan bruge tid og energi på at udvikle din forretning.

## Organisering af sikkerhed

Vi har etableret et brancheledende informationssikkerhedsprogram (ISMS), der giver vores kunder den bedste beskyttelse og højeste grad af tillid.

Programmet følger ISO 27001-sikkerhedsstandarden, som vi har været certificeret efter siden 2015.

## Politikker, procedurer og standarder

Vi har defineret et sæt af politikker, procedurer og standarder for, hvordan vi opererer i virksomheden og bedst passer på dine data. Dokumenterne opdateres løbende, i takt med at trusselsbilledet ændrer sig. På den måde sikrer vi, at vi hele tiden prioriterer vores indsats dér, hvor der er mest brug for den.

Hvordan vi prioriterer indsatsen, afhænger af vores risikovurdering, der opdateres løbende, og som udgør kernen i vores informationssikkerhedsprogram.

## Medarbejdersikkerhed

Alle medarbejdere og konsulenter med adgang til systemer og faciliteter er underlagt vores sikkerhedspolitikker. Alle gennemgår obligatorisk undervisning, hvor de bliver præsenteret for alle relevante og aktuelle privacy- og sikkerhedsemner. Dette sker både ved start og løbende gennem deres ansættelse. Formålet er at ruste medarbejderne til at modstå aktuelle trusler mod virksomhedens og kundernes data.

For at højne det generelle niveau i branchen og for at vedligeholde egne kompeencer deltager vores medarbejdere aktivt i communitites og ERFA-grupper. Vi opfordrer vores medarbejdere til hele tiden at være på forkant med den nyeste udvikling og til at erhverve de højeste certificeringer inden for sikkerhed, netværk, osv.

## Dedikerede sikkerheds- og persondatakompetencer

Vores sikkerchef er ansvarlig for at implementere og vedligeholde vores informationssikkerhedsprogram. Vores interne revisor gennemgår regelmæssigt vores sikkerhedssetup og rapporterer direkte til ledelsen. Endelig har vi interne, juridiske kompetencer inden for persondata, som sikrer, at persondata behandles efter de gældende regler både internt i virksomheden og på vegne af vores kunder.

## Operationel sikkerhed - Beskyttelse af kundedata

Den vigtigste opgave i vores sikkerhedsprogram er at passe godt på dine data. For at gøre det er vores sikringsmiljø inddelt i flere lag:

- **Fysisk sikkerhed**

Vores datacentre er state-of-the-art og placeret i Danmark. Du kan derfor være sikker på, at dine data bliver inden for landets grænser. Vores datacenterleverandør er ansvarlig for de fysiske rammer som fx strøm, køl, brandslukning og adgangskontrol, og vi fører skarp kontrol med, at vores underleverandører til en hver tid efterlever de gældende sikkerhedsregler på området.

- **Netværk**

Vores netværk er segmentet, så kunder er beskyttet mod hinanden og mod trusler, der bevæger sig på tværs i netværket. Next Generation firewalls begrænser angreb mod kundernes miljøer, og DDoS-beskyttelse begrænser den påvirkning, som evt. angreb måtte have på serverne. Avanceret netværksinspektion opfanger mønstre og angrebsforsøg fra kendte, ondsindede ip-adresser og alarmerer vores driftsafdeling ved behov.

- **Logiske adgange**

Vi tildeler kun rettigheder til de medarbejdere, der har brug for dem, og vurderer dem løbende. Kun særligt privilegerede medarbejdere har adgang til at administrere interne systemer.

- **Overvågning**

Vi overvåger vores infrastruktur og relevante services døgnet rundt. Alle afvigelser registreres i vores incident management-system. Som supplement til overvågningen har vi tilknyttet en 24/7-vagtordning.

- **Logning**

Vi logger alle adgange til management- og kundemiljøer. På den måde sikrer vi integritet og sporbarhed og kan sammenkøre hændelser. Vores centrale logplatform sikrer, at vi hurtigt kan korrelere logs fra mange kilder.

- **Backup**

Vi udfører backup ud fra den indgåede SLA. Backupdata spejles altid mellem to fysisk uafhængige lokationer, så der altid er en tilgængelig kopi i tilfælde af et kritisk nedbrud.

## Beredskab og disaster recovery

Beredskab handler om at være forberedt på hændelser, som kan have kritisk eller katastrofal påvirkning på driften. Vi har derfor beredskabsplaner som fastlægger vores procedurer, rutiner og roller i tilfælde af en katastrofe. Medarbejdere trænes i beredskabet flere gange årligt.

For at sikre vores tekniske infrastruktur og sprede risikoen ved kritiske nedbrud bruger vi flere uafhængige datacenterleverandører. Vi opbevarer altid mindst én kopi af backupdata i et datacenter, hvor vi ikke har produktionsdata.

## Håndtering af underleverandører

For at vi kan operere så effektivt som muligt, bruger vi underleverandører til udvalgte services. Hvis underleverandørerne kan have påvirkning på vores sikringsmiljø, sørger vi for, at de efterlever samme strenge krav som os selv. Det gør vi via kontrakter, databehandleraftaler, revisionserklæringer, egenkontrol og fortrolighedsaftaler. Vi kontrollerer løbende, at vores underleverandører efterlever kravene.

## Revision, compliance og uafhængige tredjepartsvurderinger

Vi har et omfattende compliance-program, som sikrer, at vi efterlever vedtagne standarder, interne politikker og relevant lovgivningen på området, med det formål at understøtte og sikre din forretning:

- ISO 27001

ISO 27001 er en international standard for håndtering af informationssikkerhed. Flere af vores konkurrenter påstår, at de følger standarden, men er ikke certificerede. Vi har været certificeret siden marts 2015. Certificeringen skal fornyes én gang om året og revideres af både en intern og ekstern auditør.

- ISAE 3402 Type 2

ISAE 3402 Type 2 beskriver, hvordan vi sikrer de ydelser, som vi leverer til vores kunder, og indeholder en uafhængig revisors konklusion på, om beskrivelsen af vores kontroller er retvisende, hensigtsmæssigt udformet, og om kontrollerne har fungeret effektivt i hele erklæringsperioden.

- BFIH Hostingcertifikatet

BFIHs Hostingcertikat stiller en række minimumskrav for god hosting, hvad angår kvalitet, stabilitet, gennemsigtighed og kontrol. Hostingcertifikatet læner sig op ad kravene i ISO 27001-standarden, som vi i modsætning til vores nærmeste konkurrenter, har valgt at implementere fuldt ud.

- PCI DSS 3.2

Vores betalingskortmiljø har den højeste PCI DSS level 1-certificering, som årligt fornyes efter de strenge krav i PCI DSS-standarden fra VISA og MasterCard.

- Penetration testing

Vi udfører regelmæssigt penetration tests mod kritiske komponenter i vores infrastruktur for at se, hvordan vores systemer forsvarer sig mod eksterne trusler.

Kunder kan også udføre penetration tests mod egne systemer efter forudgående aftale med os.