POWERNET

Databehandleraftale

Standardkontraktsbestemmelser i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger.

Changelog

VERSION	ÆNDRINGER	UDGIVELSE
1.0	Ny databehandleraftale baseret på datatilsynets standardkontraktbestemmelser v1.2 marts 2024	Juli 2024

Standardkontraktsbestemmelser

mellem

Kunden

herefter "den dataansvarlige"

og

PowerNet ApS

Herstedvang 8, 2620 Albertslund

CVR: 35240136

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

1. Indholdsfortegnelse

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af It-ydelser behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

1 Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

a. Pseudonymisering og kryptering af personoplysninger

b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

   Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

   a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
   b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
   c. behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

   Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
   c. indsigtsretten
   d. retten til berigtigelse
   e. retten til sletning (”retten til at blive glemt”)
   f. retten til begrænsning af behandling
   g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
   h. retten til dataportabilitet
   i. retten til indsigelse
   j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

   b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

2. Parterne skal i bilag C angive de passende tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

   a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
   b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
   c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for

den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

2. Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

    a. Den til enhver tid gældende Bekendtgørelse om generel og udifferentieret registrering af trafikdata (tidligere Logningsbekendtgørelsen) forpligter vores underdatabehandler som teleudbyder, til at opbevare visse personoplysninger i en periode på op til 12 måneder. Disse oplysninger kan omfatte oplysninger om kommunikationens start- og sluttidspunkt, telefonnumre, IP-adresser og lokationer. Formålet med bekendtgørelsen er at give politiet og andre myndigheder mulighed for at efterforske alvorlig kriminalitet ved at kunne efterspore kommunikationen mellem mistænkte. Teleudbyderen er forpligtet til at sikre, at oplysningerne opbevares sikkert og kun gøres tilgængelige for myndighederne i henhold til gældende lovgivning. Databehandleren forpligter sig til alene at behandle personoplysningerne til dette formål, i den periode og under de betingelser, som bekendtgørelsen foreskriver.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

5. Underskrift

   Bestemmelserne træder i kraft, når parterne underskriver eller skriftligt bekræfter aftalen om levering af tjenesterne eller når bestemmelserne underskrives separat.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner

   Databehandler kan kontakte dataansvarlig på den aftale mail og telefonnummer, som dataansvarlig oplyser på mail ved bekræftelse af aftalen.
   Dataansvarlig er forpligtet til at oplyse databehandler ved ændringer af disse kontaktoplysninger.

   Dataansvarlig kan kontakte PowerNets DPO på gdpr@powernet.dk eller tlf. 70 22 32 35.

Bilag A - Oplysninger om behandlingen

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Parterne har aftalt at databehandleren skal levere følgende ydelser

A.1.1 Levering, hosting og drift

Formålet med behandlingen er levering og hosting af dataansvarliges it-systemer, telefoni-systemer, TV-løsninger herunder overvågning, vedligehold og support som nærmere specificeret i aftalen vedrørende levering af tjenesterne indgået mellem parterne. Herunder også specifikke opgaver bestilt af den dataansvarlige.

A.1.2 Konsulentydelser

Formålet med behandlingen er at udføre specifikt aftalte konsulentopgaver. Formålet vil derfor variere, men altid have en sammenhæng til en aftalt konsulentopgave.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Databehandleren yder levering og hosting samt eventuelt drift og support af den dataansvarliges it-systemer. Derfor er det primære formål med behandlingen at drifte systemerne. Dette omfatter opbevaring, overvågning, backup og vedligehold af den dataansvarliges oplysninger som de anvender i systemerne.

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Kategorierne af personoplysninger som *ikke* knytter sig til levering af telefoni (PowerNet Connect), vil i udgangspunktet kunne indeholde alle kategorier af personoplysninger, da det er dataansvarlig som egenrådigt bestemmer hvilke kategorier som registreres i systemerne, som ofte er cloudplatforme, og dermed bliver behandlet af databehandleren.

Kategorierne som behandles i produktet PowerNet Connect (telefoni og Communicator Desktop App) er følgende:

Brugerdata - tilføjet af brugeren selv

- Titel, afdeling, fødselsdato, adresse, status og statusbesked, profilbillede, telefonbogs-kontaktpersoner

CDR aggregeret statistik

- CDR, tlf. nummer, navne, gns. ventetid, gns. opkaldstid, gns. accepterede opkald, gns. viderestillede opkald, gns. ubesvarede opkald

Voicemail (telefonsvarer)

- Indholdet af voicemails og velkomstbesker

SMS-beskeder

- Indholdet af sms-beskeder

Optagelse af telefonsamtaler

- Indholdet af optagede samtaler

CPR-nummer

- CPR på patienter eller borgere (som ringer til dataansvarlig og afgiver CPR-nummer gennem tastetryk)

Communicator X mobile app:

Brugerdata - tilføjet af brugeren selv

- Profilbillede, statusbesked, lokations beskrivelse, kø-indmeldelse, lokations zone

FAX-to-Mail:

Indholdet af kommunikation

- FAX indhold

A.4. Behandlingen omfatter følgende kategorier af registrerede

Dataansvarligs medarbejdere.

Dataansvarligs egne kunder og deres medarbejdere.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Så længe servicen leveres til dataansvarlig.

Bilag B - Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Telecom X ApS	35645845	Herstedvang 8, 2620 Albertslund	Telefoni og TV-løsninger
Microsoft Ireland Operations, Ltd.		One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Cloud platform. Microsoft O365
Teamviewer Germany GmbH		Bahnhofsplatz 2 D-73033 Göppingen Germany	Software til fjernsupport
WebPros International GmbH		Vordergasse 59, 8200 Schaffhausen / Switzerland	Plesk web hosting
Visma e-conomic A/S	29403473	Gærtorvet 3, 1799 København V	Regnskabsprogram til fakturering
Kaseya, Datto		701 Brickell Ave #400, Miami, FL 33131	Backup af MS365 tenants
One.com Group AB	559205-2400	Carlsgatan 3 Malmö, 211 20 Malmö, Sverige	Hosting, webhotel

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

Ved ændringer i godkendte underdatabehandlere skal databehandler varsle dataansvarlig mindst 30 dage før den nye behandling starter.

Bilag C - Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Opbevaring, overvågning, backup og vedligehold af den dataansvarliges personoplysninger som de anvender i systemerne.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

- At der i de fleste tilfælde behandles almindelige personoplysninger.
- At der på de universelle cloud-platforme (Office365 f.eks.) antages at dataansvarlig registrerer følsomme personoplysninger og der omkring behandlingen af disse personoplysninger skal etableres et højt sikkerhedsniveau.
- At der ved anvendelse af CPR-funktioner i telefonisystemet behandles fortrolige personoplysninger og der omkring behandlingen af disse personoplysninger skal etableres et højt sikkerhedsniveau.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Kyptering og pseudonymisering

- Der anvendes kryptering i henhold til best practice og videst muligt omfang for at beskytte fortroligheden og integriteten af data, både under overførsel og i lagret tilstand.
- Processer for nøglehåndtering er implementeret for at sikre, at fortroligheden, integriteten og tilgængeligheden af krypteringsnøgler beskyttes.
- Hashing og tokenisering anvendes ved autentificerings mekanismer som sker over det offentlige internet.

Driftsikkerhed

- Der vedligeholdes en redundant, komplet og fysisk adskilt infrastruktur for opbevaring af de data som er hostet af databehandler selv.
- Der foretages backup og disaster recovery sikkerhedskopieringer.
- Logs fra systemerne aggregeres og overvåges aktivt, for at bidrage til at opdage og vurdere unormale aktiviteter i kritiske systemer.

Kommunikationssikkerhed

- Netværk er logisk eller fysisk segmenteret for at adskille tjenester, brugere og systemer på en passende måde.
- Der anvendes best practice i design og konfiguration af netværksstyringsteknologier.
- Der arbejdes med strength in-depth tilgang til foranstaltninger i netværkslagene.
- Der er implementeret opdagende og korrigerende foranstaltninger ift. udefrakommende angreb mod tilgængeligheden af systemer og netværk.

Fysisk sikring.

- Datacentre som anvendes til behandling af personoplysninger, opretholder ISAE 3402 type 2 erklæringer.
- Kontorer er sikret mod ekstern indtrængen i overensstemmelse med anerkendte standarder og er vedvarende videoovervåget.
- Fysisk adgang gives kun til medarbejdere eller til eksterne partnere og lignende, som har et legitimt behov for at tilgå data eller it-infrastruktur.
- Alarmsystemer benyttes for at afholde uvedkommende fra at tilgå data eller it-infrastruktur.
- På kontorerne er der en clear desk politik, og alle personoplysninger uden opsyn er aflåst.

Mobilt udstyr og hjemmearbejdspladser

- Computere med adgang til personoplysninger er beskyttet med passwords.
- Fjernadgang til systemer med persondata er beskyttet med multifaktor autentifikation.
- Alt lokalt data på computere er krypteret.
- Brugerkonti er beskyttet mod gentagende mislykkedes adgangsforsøg.
- Fjernadgange til netværk etableres gennem VPN eller SDN-tunneller.
- Computere kan saneres gennem remote wipe, ved tyveri eller tab.
- Computere benytter antivirus software som automatisk og vedvarende opdaterer sine definitioner.

Adgangsstyring

- På understøttede systemer er adgange baseret på et IAM (Identity & Access Management) setup som sikrer:
    - Tildeling af adgang baseret på jobkrav.
    - Princippet om minimumsprivilegier.
    - Funktionsadskillelse.
    - Gruppering af brugere i logiske adgangsgrupper.
    - Administration af tekniske konti og servicekonti.
- Adgangskontrolsystemer er konfigureret til at håndhæve rollebaseret adgangskontrol for brugere og ressourcer med udgangspunkt i medarbejdernes arbejdsfunktion i organisationen.
- Passwordsikkerhed styres gennem politikker som sikrer høj kompleksitet og at alle passwords er unikke.
- MFA (multifaktor autentifikation) kræves på brugere med administrator rettigheder til bl.a. telefonsystemet.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt, inden for det nedenstående omfang og udstrækning, bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Ved brud på behandlingssikkerheden eller andre hændelser som berører dataansvarliges registrerede skal databehandler have procedurer og skabeloner til registrering.

Skabelonerne skal indeholde de informationer som der er krav på fra Datatilsynets side ved en anmeldelse til dem.

Databehandler udfylder ved en hændelse denne skabelon og fremsender til dataansvarlige uden unødig tøven. Dette gør det muligt for ataansvarlige at reagere hurtigt og have alle muligheder for at anmelde bruddet til Datatilsynet rettidigt.

Databehandler har privilegier til at iværksætte relevante korrigerende foranstaltninger så snart at hændelsen opdages, inklusive afbrydelse eller begrænsning af leverancen af servicen til dataansvarlige, hvis dette kan begrænse hændelsens skadevirkninger.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares så længe de aftale services leveres til kunden, hvorefter de slettes hos databehandleren.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren slette personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarliges oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

Databehandlers egne kontorer på adresser i Danmark.

Databehandlers egen infrastruktur (colocation) i datacentre på følgende lokationer i Danmark:

Herstedvang 8
2620 Albertslund

Hørskætten 3
2630 Taastrup

I lande for alle godkendte underdatabehandlere som er angivet i Bilag C.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Alle overførsler af personoplysninger til lande uden for EU/EØS-området skal baseres på de standardkontraktmæssige klausuler (SCC'ere), der er godkendt af EU-Kommissionen som kontraktuelt grundlag for overførsler af personoplysninger.

Databehandler skal kun anvende SCC'er, der er relevante og passende for den specifikke overførsel af personoplysninger, og som opfylder GDPR's krav til beskyttelse af personoplysninger. Databehandler sikrer, at alle modtagere af personoplysninger i lande uden for EU/EØS-området overholder de forpligtelser, der er fastsat i SCC'en og i GDPR's bestemmelser for beskyttelse af personoplysninger.

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Databehandler udfører årlig intern revision af sin GDPR-overholdelse samt overholdelse af instrukserne i databehandleraftaler. Undersøgelsen ledes og koordineres af databehandlers databeskyttelsesrådgiver (DPO). Processen kører sideløbende med databehandlers årlige interne audit af sin ISO 27001 modenhed. Resultatet er en erklæring som vil tjene som den dataansvarliges tilsyn med databehandleren. Erklæringen kan fremsendes på dataansvarliges anmodning.

Revisionen omfatter en analyse af databehandlers behandlingsaktiviteter for at sikre, at de er i overensstemmelse med databehandlingsaftalerne. Der evalueres på de tekniske og organisatoriske sikkerhedsforanstaltninger, som er på plads for at beskytte personoplysninger. Risikovurderingerne som danner grundlag for denne evaluering genbesøges samtidigt, og det aktuelle trusselsbillede samt eventuelle hændelser tages med ind i vurderingen.

Efter revisionen udarbejder databehandler en erklæring, der præsenterer resultaterne og identificerer eventuelle mangler eller områder, der kræver forbedring. Databehandlerens ledelse gennemgår rapporten og rådgives i at træffe beslutninger om nødvendige tiltag for at sikre fortsat overholdelse af GDPR og databehandleraftalerne.

Baseret på resultaterne af den interne revision er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere.

Hvis underdatabehandlere er forpligtet gennem aftaler, til at udarbejde revisionserklæringer, indhenter databehandler disse årligt. Revisionserklæringerne tjener som en ekstern, uafhængig vurdering af databehandlerens overholdelse af GDPR samt deres evne til at beskytte og sikre personoplysninger.

Databehandleren driver derudover procedurer for tilsyn med underdatabehandlere ved udsendelsen af et standardiseret spørgeskema. Spørgeskemaet skal udfyldes og returneres til databehandler og er designet til at evaluere underdatabehandlernes GDPR-compliance. Dette tjener til at vurdere, om underdatabehandleren har implementeret passende tekniske og organisatoriske foranstaltninger for at beskytte personoplysninger.

Bilag D - Parternes regulering af andre forhold

D.1 Tilføjelse af instrukser fra dataansvarlig

Hvis dataansvarlig har andre instrukser end denne aftale indeholder, forbeholder PowerNet sig retten til at betragte dette som en ordreafgivelse der afføder aktiviteter hos os, som kunden selv afholder udgifterne for. Vi vil afsætte ressourcerne til at imødekomme disse ordrer efter bedste evne og vi vil først være forpligtet til at udføre dem når vi har modtaget bekræftelse fra dig.

D.2 Parternes samarbejde i opfyldelse af deres forpligtigelser omkring oplysning og underretning om databrud overfor de registrerede.

Følgende har udelukkende relevans for kunder der har PowerNet Connect (telefoniløsninger).

Fordi dataansvarlig har den direkte kontakt til brugerne, har databehandleren brug for at kunden samarbejder på to områder. Nogle af de personoplysninger som indsamles om brugerne af systemet er PowerNet og udbyderen af telefonsystemet dataansvarlige for.

Uden kundens samarbejde er det ikke muligt for databehandleren og underdatabehandleren at leve op til kravene i databeskyttelsesforordningens Artikel 14 som omhandler pligt til oplysning når personoplysningerne ikke er indsamlet af den dataansvarlige.

De to område hvor PowerNet har brug for kundens omgående og fulde samarbejde er:

a. Henvise kundens medarbejdere til PowerNets privatlivspolitik, hvis de vil gøre brug af deres rettigheder.
b. Ved brud på datasikkerheden at underrette den registrerede.

D. 2.1 Forhandleren og Udbyderens oplysningspligt

Følgende har udelukkende relevans for kunder der har PowerNet Connect (telefoniløsninger).

Både udbyderen (PowerNets underdatabehandler) og PowerNet behandler oplysninger fra registrerede som de ikke har et (kontraktuelt) forhold med. Dette er i de fleste tilfælde den dataansvarliges medarbejdere.

Fordi databehandler og underdatabehandler ikke modtager oplysningerne direkte fra slutbrugerne selv, men de bruger oplysningerne til egne formål, har de pligt til at levere den information som er beskrevet i databeskyttelsesforordningen Artikel 14 stk. 1 og stk. 2. til slutbrugeren. Da dette ikke er praktisk muligt for PowerNet påhviler det kunden at formidle denne information til de registrerede.

Ønsker de registrerede (kundens brugere af telefonisystemet) at gøre brug af deres rettigheder i forhold til de personoplysninger databehandler og underdatabehandler er dataansvarlig for, skal kunden derfor henvise sine medarbejdere til PowerNets privatlivspolitik: https://www.powernet.dk/privatlivspolitik/ (se afsnittet PowerNet Connect – telefoniløsninger).

D. 2.2 Underretning om databrud.

Følgende har udelukkende relevans for kunder der har PowerNet Connect (telefoniløsninger).

Databehandler og underdatabehandler har procedurer for at opdage, håndtere og rapportere brud på informationssikkerheden som berører de registrerede. Dette både for de data PowerNet er dataansvarlig for, og de data der behandles på vegne af kunden.

I scenarier hvor data, som kunden er dataansvarlig for, bliver kompromitteret vil bestemmelserne i Afsnit 10 være gældende. Det er derefter kundens ansvar som dataansvarlig at informere sine registrerede om databruddet. Du kan se hvordan PowerNet bistår dig i bl.a. denne informering i Afsnit 9 og Bilag C punkt 3.

Drejer bruddet sig om data, som databehandler eller underdatabehandler er dataansvarlige for, har databehandler brug for kundens samarbejde til at informere de registrerede. Databehandler sender hurtigst muligt - efter at underretning til Datatilsynet - en e-mail til kunden med en tekst som kunden forpligter sig til at sende til de registrerede om muligt eller på anden vis formidle. Dette skal fra kundens side foregå uden unødige ophold og uden at ændre i den fremsendte tekst.