

Persondatapolitik for MKR IT

Hjælp til databehandleraftaler:

Ønsker du som kunde hjælp til en databehandleraftale med MKR IT, så kan du vælge og klikke på nedenstående databehandleraftaler (bemærk: er i **Word-97**-format):

[Databehandleraftale for Campet Server-kunder](#)

[Databehandleraftale for HOSTING hos MKR IT](#)

[Databehandleraftale for Private CLOUDS](#)

[Databehandleraftale for IT Infrastruktur: leveringer og services](#)

En kundeservice !

MKR IT behandler som databehandler typisk ikke persondata hos en kunde, men har adgang til disse gennem sin funktion. I sagens natur er der ingen praksis endnu omkring GDPR, så derfor har MKR IT valgt en "livrem & seler-løsning" med at tilbyde kunder, der måtte ønske det, skabelonerne (til venstre) til en eventuel databehandleraftale - opdelt på de typiske ydelser, som MKR IT tilbyder.

Persondatapolitik for behandling af kunde- og leverandøroplysninger

1. Dataansvarlig

MKR IT A/S (herefter forkortet MKR) er dataansvarlig.

MKR's kontaktoplysninger er:

MKR IT A/S

Skibsværftsvej 4, 2. sal, 4900 Nakskov

Tlf: 54 95 15 65

Fax: 54 95 15 60,

E-mail: mkr@mkr.dk

MKR håndterer alle personlige oplysninger i overensstemmelse med gældende persondatalovgivning og Persondataforordningen (GDPR).

MKR indgår aftale med kunder og leverandører om levering og services samt rådgivning inden for IT infrastruktur. MKR arbejder kun i business to business (BtB) og business to organizations (BtO) segmenterne og har således ikke privatkunder (BtC).

Når en kunde bestiller og køber én eller flere af MKR IT's ydelser, og som led heri afgiver sine personoplysninger til MKR, giver denne kunde samtidig sit samtykke til, at kundens/leverandørens personoplysninger kan behandles af MKR.

Det samme gør sig gældende for så vidt angår de eventuelle personoplysninger, som leverandører til MKR A/S afgiver til MKR i forbindelse med afgivelse af tilbud eller indgåelse af aftaler.

2. MKR indsamling af personoplysninger

Personoplysninger indsamles af MKR på følgende vis:

- Når en kunde – eller en repræsentant for denne – vælger at indhente tilbud på og/eller købe en af MKRs serviceydelser/produkter, eller når en leverandør afgiver tilbud eller sælger produkter eller serviceydelser til MKR.
- Fra B2B marked.
- I forbindelse med MKRs brug af digitale ydelser på nettet mhp. opfyldelse af indholdet i en given kundes tilbud og/eller kontrakt samt køb.
- Når leverandører indgår aftaler med MKR eller afgiver tilbud til MKR.
- I tilfælde af kunde- og leverandørbesøg hos MKR via videoovervågning (uden lydoptagelse)

Indsamling og behandling af personoplysninger, jf. ovenstående vil altid ske i henhold til gældende persondatalovgivning.

Videoovervågning internt hos MKR sker som led i kriminalitetsforebyggelse og fungerer derudover som et tryghedsskabende tiltag for medarbejdere og kunder med udstyr placeret hos MKR.

3. Oplysninger som MKR indsamler

MKR kan indsamle følgende personoplysninger:

- Navn, adresse, telefonnummer, e-mailadresse samt andre almindelige ikke personfølsomme personoplysninger.
- Betalingskortoplysninger.
- Demografiske oplysninger.
- Købs- og dokumentationshistorik såfremt kunden/en måtte ønske dette (specielt samtykke) udover de i lovgivningen fastlagte opbevaringsterminer (fx bogføringsloven, forældelsesloven m.fl.) .
- Browserinformationer indhentet som led i gennemførelse af et tilbud, serviceydelse og/eller produktrådgivning.
- Oplysninger om kundens virksomhed og relevante kontaktpersoner.
- Oplysninger om leverandørers virksomhed samt oplysninger om relevante kontaktpersoner og nøglepersoner herunder key accounts og supporters.

En kunde eller leverandør kan - frivilligt og efter eget valg - give MKR yderligere personoplysninger, som denne mener, kan have betydning for MKRs betjening/servicering af kunden/leverandøren, eller som den pågældende mener bør gives af sikkerhedsmæssige hensyn.

Dette kan f.eks. være oplysninger om:

- Bruger- og adgangsoplysninger til systemer
- Sikkerhedsklassifikationer af medarbejdere hos en kunde/leverandør

Hvis en kunde/leverandør *frivilligt og efter eget valg* vælger at afgive sådanne oplysninger, opfatter MKR dette som et samtykke til at kunne registrere og gemme disse følsomme oplysninger om den

pågældende, så længe engagementet er aktivt, hvorefter disse oplysninger slettes senest et år efter engagementets ophør (medmindre lovgivningen angiver anden tidstermin).

Udover de oplysninger som MKR modtager direkte fra kunder/leverandører, vil MKR i nogle tilfælde indhente eller behandle yderligere personoplysninger, som MKR har modtaget af tredjeparter fx CSIS i tilfælde af en kunde er ramt af ransomware (hvor kunden anmoder MKR om hjælp) e.lign.

Hvor dette er tilfældet er den pågældende tredjepart pligtig til at informere de pågældende kunder/leverandører om MKRs vilkår og betingelser samt MKRs persondatapolitik. Det er også den pågældende tredjeparts ansvar at sikre, at der er det fornødne juridiske grundlag til indsamling og behandling af de pågældende oplysninger, herunder indhente evt. fornødent samtykke til behandling af eventuelle følsomme oplysninger.

4. Betaling

MKR anvender over for kunder kun almindelig fakturering via bankoverførsler eller FI-koder på faktura og modtager således ikke betaling via kreditkort, mobilpay e.lign.

5. Hvad er formålet med indsamlingen og behandlingen?

MKR indsamler alene personoplysninger, som er nødvendige for at opfylde de aftaler, der indgås med kunder/leverandører om levering, installation og servicering samt rådgivning i fm. produkter og serviceydelser.

Det er den enkelte aftales indhold/serviceydelsens karakter, som er bestemmende for, hvilke personoplysninger MKR indsamler og behandler, og som er bestemmende for formålet med indsamlingen.

6. Hjemmel – det juridiske grundlag – for behandlingen

MKR vil oftest behandle personoplysninger, fordi det er nødvendigt for at opfylde en aftale med MKR, som en kunde og/eller en leverandør er part i. Det kan for eksempel være i forbindelse med:

- Tilbudsgivning
- Rådgivning i fm. IT Infrastruktur og konkrete produkter samt systemer
- Løsning af IT-problemer som fx nedbrud, IT-sikkerhedsbrister, performance, systemfejl o.lign.
- Installation af hardware og software
- I rollen som systemadministrator, herunder også overordnet systemadministration for Cloud-løsninger såsom Office365 m.fl.
- Rådgivning i fm. IT-strategier, herunder også anvendelsen af IT som forretningsunderstøttelse hos en given kunde
- Interne kurser hos kunder

I nogle tilfælde vil MKRs behandling af personoplysninger finde sted som led i, at MKR forfølger en legitim/saglig interesse, som går forud for den kundens/leverandørens (den registreredes) interesser jf. bestemmelserne i GDPR.

En sådan legitim interesse, kan eksempelvis være udarbejdelse af statistik, kundeundersøgelser, markedsføring og analyse af IT-sikkerhed samt konsekvenser ved IT-sikkerhedsbrister, som har til hensigt generelt at forbedre oplevelsen hos MKR og kvaliteten af MKRs serviceydelser og produkter.

7. Den registreredes rettigheder

Efter reglerne i persondataforordningen (GDPR), har de registrerede forskellige rettigheder.

- En registreret har til enhver tid ret til at få indsigt i, hvilke personoplysninger MKR behandler om den registrerede.
- En registreret har til enhver tid ret til at få berigtiget og opdateret de personoplysninger, som MKR har om den registrerede.
- En registreret har til enhver tid ret til at få slettet de personoplysninger, som MKR har om den registrerede. Hvis en registreret anmoder om sletning, slettes alle de oplysninger, som MKR ikke efter lovgivning er forpligtet til at skulle gemme. En sletning af den registreredes oplysninger kan i nogle tilfælde betyde, at MKR ikke kan opfylde evt. indgåede aftaler eller levere visse serviceydelser til den registrerede.

Hvis nogle af de oplysninger, som MKR har om den registrerede er givet på baggrund af den registreredes samtykke, har denne til enhver tid ret til at trække samtykket tilbage, hvilket betyder, at oplysningerne slettes eller ikke længere anvendes af MKR. Dette gælder ikke for oplysninger, jf. ovenfor som MKR er lovmæssigt forpligtede til at gemme.

Muligheden for at anmode om sletning mv. kan dog være begrænset af hensyn til beskyttelsen af andre personers privatliv, til forretningshemmigheder og immaterielle rettigheder samt f.eks. af hensyn til muligheden for at håndhæve potentielle retskrav samt imødegåelse og undersøgelser af IT-sikkerhedsbrister.

Den registrerede kan til hver en tid skriftligt bede MKR om at få en oversigt over og en kopi af de personoplysninger om den registrerede, som MKR er i besiddelse af. Første gang er dette uden beregning for den registrerede jf. GDPR. Efterfølgende anmodninger vil MKR opkræve betaling for efter tidsanvendelse og til MKRs normale timesatser.

Hvis en henvendelse fra en registreret er via den registreredes relationer til en af MKRs kunder og/eller leverandører (der dermed er dataansvarlig), vil den registrerede få besked om, at henvende sig til den dataansvarlige.

En skriftlig anmodning herom skal underskrives af den registrerede og indeholde dennes navn, adresse, telefonnummer, e-mailadresse.

Den registrerede kan også kontakte MKR, hvis den registrerede mener, at dennes persondata bliver behandlet i strid med lovgivningen eller i strid med andre retlige forpligtelser.

Skriftlig anmodning sendes til MKR, se kontaktoplysninger ovenfor under pkt. 1

MKR vil så vidt muligt indenfor 1 måned efter modtagelsen af den registreredes skriftlige anmodning sende denne til den registrerede. Kan dette ikke opfyldes kontaktes den registrerede inden for 3 uger med angivelse af forventet tidspunkt for levering af informationerne til den registrerede.

Hvis den registrerede beder om rettelse og/eller sletning af sine personoplysninger, vil MKR vurdere, om betingelserne for anmodningen er opfyldt, og MKR vil i så fald gennemføre ændringer eller sletning så hurtigt som muligt.

MKR tager forbehold for at afvise anmodninger, som har karakter af chikanøs gentagelse eller som kræver uforholdsmæssige tekniske foranstaltninger (f.eks. gennemgang af backups) eller som påvirker beskyttelsen af andre registreredes personoplysninger, eller i andre situationer hvor det vil være uforholdsmæssigt ressourcekrævende eller meget kompliceret at imødekomme anmodningen.

8. Sikkerhed og deling af personoplysninger

MKR beskytter den registreredes personoplysninger, og har fastlagt retningslinjer, der beskytter den registreredes personoplysninger mod, at der sker uautoriseret offentliggørelse og mod at uvedkommende får adgang eller kendskab til dem.

Kun de personer/ansatte hos MKR, der har i kraft af deres jobfunktion har behov for de registreredes personoplysninger har adgang hertil.

MKR kontrollerer løbende, at der ikke sker uautoriseret adgang til de registreredes personoplysninger.

MKR tager løbende backup af de registrerede personoplysninger.

I tilfælde af et sikkerhedsbrud, hvor der er en høj risiko for misbrug af de registreredes personoplysninger, herunder f.eks. identitetstyveri, økonomisk tab, tab af omdømme eller anden form for misbrug, vil MKR underrette den pågældende dataansvarlige så hurtigt som muligt, så den ansvarlige kan underrette de registrerede om sikkerhedsbruddet.

Hvis der her er tale om straffelovsovertrædelser (fx børneporno, hvidvaskning o.lign.) vil MKR udover at underrette dette til den dataansvarlige også anmelde dette til politiet.

MKR's sikkerhedsprocedurer bliver løbende revurderet og opdateret i forhold til den teknologiske udvikling.

MKR benytter sig af en række eksterne leverandører af IT-services og IT-systemer etc.

MKR indgår løbende databehandlaftaler med alle MKR's leverandører, hvorved det også i forhold til eksterne databehandlere sikres, at disse fastholder et fornødent og højt beskyttelsesniveau for så vidt angår de registreredes personoplysninger.

MKR er i nogle tilfælde lovmæssigt forpligtede til at videregive personoplysninger eller forpligtede hertil som følge af en afgørelse fra en offentlig myndighed.

MKR sletter personoplysninger, når MKRs lovmæssige forpligtelse ophører, eller når formålet med at indsamle og behandle oplysningerne ikke længere er til stede

9. Klage

Klage over MKRs behandling af personoplysninger kan ske til

DATATILSYNET

BORGERGADE 28, 5, 1300 KØBENHAVN K

TELEFON 3319 3200

[Web: Datatilsynet \(klik her\)](#)

E-MAIL dt@datatilsynet.dk