J.NR. 221771
UDKAST * VER. 2
DATO 7.06.18

INTERN PERSONDATAPOLITIK

For virksomheden:

VVS, ERIK NIELSEN A/S
CVR. nr. 21022705
Høgevej 8
3400 Hillerød

(Herefter omtalt "Virksomheden")

Senest revideret 7. juni 2018

Dataansvarlig:

_____
Mads Myhlendorph Nielsen

1. VIRKSOMHEDENS BEHANDLING AF MEDARBEJDERNES PERSONOPLYSNINGER

Som led i ansættelsesforholdet behandler virksomheden personoplysninger om medarbejderne, herunder de personoplysninger, medarbejderen selv har afgivet i forbindelse med ansættelsen.

Behandling af personoplysninger sker i overensstemmelse med den til enhver tid gældende persondatalovgivning som fastsat af EU og nationale myndigheder.

Ændringer af denne politik annonceres via mail.

1.1. Indhentning af personoplysninger hos andre parter

I løbet af ansættelsesforholdet indhenter virksomheden skattekort til brug for skatteindeholdelse.

Herudover indhenter virksomheden medarbejderens navn, Cpr. nr., bankoplysninger, adresseoplysninger, mobiltelefonnummer og mailadresse til brug for identifikation af medarbejderen og til brug for opfyldelse af ansættelsesforholdet i form af udbetaling af løn til medarbejderen.

Desuden behandler virksomheden oplysninger om helbredsforhold i forbindelse med sygemelding for at kunne søge dagpengerefusion mv. Denne form for personlysning har karakter af følsomme personoplysninger, hvorfor virksomheden behandler denne oplysning med særlig agtpågivenhed.

1.2. Virksomhedens håndtering af følsomme personoplysninger

Som nævnt ovenfor kan virksomheden behandle følsomme helbredsoplysninger i forbindelse med håndtering af sager om sygefravær, hvor lovgivning tilsiger dette. Herudover vil følsomme personoplysninger ikke blive behandlet uden medarbejderens samtykke.

1.3. Videregivelse af personoplysninger til eksterne parter

I visse tilfælde videregives oplysninger til tredjemand, herunder:

- Offentlige myndigheder
- Eksterne samarbejdspartnere, som efter aftale med virksomheden udfører opgaver for virksomheden, herunder i forbindelse med lønudbetaling og HR-udviklingsaktiviteter
- Pensionsselskaber
- Sundhedsforsikringsselskab

I forbindelse med løsning af opgaver for offentlige myndigheder, herunder f.eks. Slots- og Kulturstyrelsen, skal Virksomhedens medarbejdere sikkerhedsgodkendes via PET til klassifikationsniveauet "Til Tjeneste". I forbindelse med sikkerhedsundersøgelsen skal den enkelte medarbejder underskrive en samtykkeerklæring, der videregives til myndigheden. Ved udfyldning af samtykkeerklæringen giver den enkelte medarbejder sin accept til, at oplysningerne videregives.

1.4. Opbevaring af medarbejdernes oplysninger

Virksomheden opbevarer dels selv oplysninger om medarbejderne. Virksomheden overholder gældende krav til IT-sikkerhed.

Herudover opbevarer Virksomheden oplysninger om medarbejderne hos eksterne leverandører indenfor EU/EØS. Samarbejdet med leverandørerne er omfattet af skriftlige databehandleraftaler, som overholder de gældende regler. Virksomheden kontrollerer, at de af virksomhedens anvendte databehandlere har tilstrækkelig IT-sikkerhed.

1.5. Periode for opbevaring af oplysninger om medarbejdere

Virksomheden opbevarer alene medarbejderoplysninger, så længe det er nødvendigt. I forbindelse med medarbejderens fratræden kan visse oplysninger blive gemt i op til 5 år blandt andet for at opfylde lovmæssige forpligtelser, eksempelvis bogføringsloven, og henset til at forældelsesfristen for medarbejder krav er 5 år.

Der kan være særlige situationer, hvor virksomheden opbevarer oplysninger i en længere periode, fx hvis en medarbejder har været ude for en arbejdsskade eller til brug for kvalitetssikring.

1.6. Håndtering af medarbejderes e-mail ved fratræden

Ved fratræden vil der blive opsat autosignatur på medarbejderens e-mailadresse, hvor der orienteres om, at medarbejderen er fratrådt pr. en given dato, og der vil blive oplyst kontaktoplysninger på den medarbejder, afsenderen skal kontakte i stedet.

E-mailkontoen vil blive holdt åben i en periode – normalt op til 3 måneder, men i visse tilfælde længere, og vil i denne periode blive gennemgået af én eller få konkrete betroede medarbejdere. Private mails – herunder mails markeret PRIVAT i emnefeltet - vil ikke blive læst, men vil blive videresendt til den fratrådte medarbejders private mailadresse, hvis en sådan er oplyst. Besvarelse af evt. forretningsmæssige mails vil ske fra den respektive medarbejders egen mailadresse.

1.7. Medarbejderens rettigheder

I forbindelse med virksomhedens behandling af personoplysninger, har medarbejderen følgende rettigheder:

- Ret til indsigt i, hvilke personoplysninger virksomheden behandler om medarbejderen, herunder formålet. Virksomheden skal normalt svare inden for 1 måned.
- Ret til at få berigtiget fejlagtige oplysninger.
- Ret til at få slettet oplysninger, som ikke længere er relevante for ansættelsen eller hvor grundlaget for behandlingen ikke længere er til stede, herunder hvis samtykke er tilbagekaldt.
- Ret til at tilbagekalde samtykke,

- Ret til at gøre indsigelse mod uberettiget behandling
- Ret til at klage til Datatilsynet (www.datatilsynet.dk).

1.8. Kontaktperson hos virksomheden

Hvis medarbejderen har spørgsmål til virksomhedens håndtering af personoplysninger, eller ønsker at udøve rettigheder nævnt ovenfor, kan medarbejderen kontakte den ansvarlige for håndtering af personoplysninger:

Mads Myhlendorph Nielsen
Mail: mn@en-vvs.dk
Tlf. nr.: 4822 2650

1.9. Brug af mobile enheder

Disse retningslinjer indeholder vigtige informationer, som skal læses af alle medarbejdere, som bruger it – herunder smartphones og mobile enheder – i forbindelse med arbejdet for virksomheden. Overtrædelse af retningslinjerne kan medføre ansættelsesretlige konsekvenser – i yderste tilfælde afskedigelse eller bortvisning.

1.9.1. Mobile enheder

Brugen af mobile enheder skal ske med omtanke. Brug alene sikre netværk med adgangskode.

Benyt firecifret kodeord for at tilgå mobile enheder for at undgå, at der ved tyveri er let tilgang til mails etc. Smartphones og bærbare PC'ere skal være sat op til at kræve kode efter 15 minutters inaktivitet. Koden vedr. tilgang til VPN må ikke gemmes på den mobile adgang.

Apps må installeres på mobile enheder i det omfang, de er arbejdsrelaterede og sikre. Såfremt de(n) mobile enhed er omfattet af beskatning af "fri telefon", må apps installeres efter behov, her skal der skeles til velkendte apps grundet sikkerhed.

Musik må installeres i det omfang, at det ikke påvirker den firmarelaterede brug af den mobile enhed.

Det er ikke tilladt at foretage donationer via sms eller opkald, når abonnementet betales af virksomheden.

1.9.2. *E-mails*

Mails med virksomhedens signatur må alene benyttes til erhvervsmæssige formål. Sendes private mails, skal signatur slettes forinden – og der skal anføres "PRIVAT", "PERSONLIGT" eller tilsvarende i emnefeltet.

Virksomheden foretager sikkerhedskopiering af e-mail korrespondance på virksomhedens mailadresser. Dette sker med henblik på at kunne genskabe forretningsmæssig relevant korrespondance i forbindelse med it-nedbrud, hackerangreb etc.

Virksomheden foretager ikke generelt overvågning af medarbejdernes brug af virksomhedens e-mail adresser, men forbeholder sig ret til at lade en betroet medarbejder gennemgå en medarbejders korrespondance i tilfælde, hvor medarbejderen er fraværende i længere tid, f.eks. pga. sygdom. Endvidere kan der foretages gennemgang af en medarbejders e-mailkorrespondance, hvor der er en konkret begrundet mistanke om overtrædelse af disse retningslinjer eller videregivelse af fortrolige oplysninger til uvedkommende.

E-mails, der er af privat karakter, vil ikke blive gennemgået.

1.9.3. *Visning af personoplysninger på skærm*

Når medarbejdere behandler personoplysninger på deres computerskærm skal de sikre, at andre ikke kan se skærmen.

Når medarbejdere forlader sit skrivebord skal skærmen være slukket.

1.9.4. *Personoplysninger på papir*

Når medarbejdere udskriver personoplysninger på en printer, skal vedkommende tilsikre, at andre ikke får adgang til de udprintede personoplysninger.

Personoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug.

Når dokumenter skal smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til personoplysningerne.

Dette gælder også jobansøgninger o.l. anvendt i forbindelse med rekruttering. Al sådan materiale på papir skal opbevares aflåst under rekrutteringsprocessen samt makuleres eller returneres til Mads Myhlendorph Nielsen efter rekrutteringsprocessen er afsluttet.

1.9.5. *It-sikkerhed*

Den enkelte medarbejder har ansvaret for at overholde de til en hver tid gældende It-sikkerhedspolitikker i virksomheden, der er gældende for medarbejderens arbejdsopgaver og

indrapportere eventuelle sikkerhedsbrud eller mistanke herom til ledelsen. Heri ligger ligeledes, at medarbejderens brug af netværk, internet etc., skal være af sobert indhold.

Virksomheden har tillid til, at medarbejderne anvender virksomhedens internetforbindelse og mails mv. med omtanke. Der foretages ingen systematisk logning eller overvågning af medarbejderes besøg på hjemmesider, men It-afdelingen kan i konkrete tilfælde ud fra it-sikkerhedsmæssige overvejelser foretage gennemgang af en konkret trafik.

Kodeord er egne og skal holdes hemmelige, ligesom låsning af computer, mobile enheder etc. skal ske, når man forlader enheden. Kodeord skal skiftes mindst hver 3. måned.

1.9.6. Hjemmearbejdspladser

Enkelte medarbejdere får stillet hjemmearbejdspladser til rådighed. Disse er baseret på, at medarbejderen via en VPN-løsning kan få adgang til virksomhedens systemer og servere, hvortil der skal anvendes kode.

Koden til VPN må aldrig være den samme kode, som den, der anvendes som adgangskode til pc.

Der må ikke gemmes virksomhedsoplysninger, herunder personoplysninger om virksomhedens kunder, samarbejdspartnere og medarbejdere, lokalt på den maskine, der anvendes på hjemmearbejdspladsen. Dette er dels for at sikre, at der tages backup af oplysningerne, dels for at sikre, at personoplysninger og forretningskritiske oplysninger ikke falder i forkerte hænder ved tyveri af udstyret.

Der må som udgangspunkt ikke foretages fysisk udskrivning på hjemmearbejdspladsen. Hvor det undtagelsesvist sker, skal alle udskrifter ved først givne lejlighed medbringes på virksomheden med henblik på behørig arkivering eller makulering.

Udstyret på hjemmearbejdspladsen kan efter konkret tilladelse anvendes til private formål, men det må aldrig ske, når udstyret er koblet på virksomhedens systemer.

Et evt. trådløst netværk på hjemmearbejdspladsen skal være krypteret og beskyttet med kode.

1.9.7. Håndtering af udstyr ved fratræden

Ved ophør af ansættelsesforhold returneres al hardware i ordentlig stand, renset for alle private kontakter, sms'er, billeder, apps etc. til den IT-ansvarlige. Opkaldslister på mobiltelefoner skal slettes forinden indleveringen.

Hvis medarbejderen selv har stillet udstyr til rådighed (herunder smartphones), eller medarbejderen efter aftale overtager virksomhedens udstyr ved fratræden, skal disse indleveres til den IT-ansvarlige med henblik på sletning/overførsel af virksomhedsrelevante oplysninger samt nulstilling af adgange til virksomhedens systemer.

1.10. GPS overvågning

Der foretages GPS-overvågning af biler og maskiner. Formålet er dels for registrering af kørsel, og derved for dokumentation af forbrugt tid overfor Virksomhedens kunder, og dels af kriminalitetsbekæmpende formål ved at forhindre svig. Retsgrundlaget for behandlingen er EU persondataforordningens artikel 6, stk. 1, litra f. Registreringerne gemmes i maksimum 30 dage, hvorefter de slettes, medmindre de skal anvendes til dokumentation overfor kunden.

1.11. Adgangskontrol

Hver medarbejder har fået udleveret en nøglebrik til brug for adgang til Virksomhedens bygning, hvor den enkelte medarbejder kan identificeres. Formålet med adgangskontrollen er dels for tidsregistrering og dels sikkerhedsmæssige hensyn. Der sker kortvarigt logning af medarbejderens bevægelser, der alene gemmes i op til 30 dage, medmindre de skal anvendes til opklaring af en lovovertrædelse.

2. VIRKSOMHEDENS BEHANDLING AF ØVRIGES PERSONOPLYSNINGER

Disse retningslinjer indeholder vigtige informationer, som skal læses af alle medarbejdere, som behandler personoplysninger i forbindelse med arbejdet for virksomheden.

Retningslinjerne er udarbejdet som led i virksomhedens bestræbelser på at overholde gældende lovgivning, herunder persondataloven samt EU-forordningen om persondata, som er vedtaget af EU-parlamentet og som finder anvendelse fra 25. maj 2018.

Da overtrædelse af persondatareglerne kan være forbundet med meget betydelige bødesanktioner mod virksomheden samt påføre virksomheden betydelig imagemæssig skade, er det vigtigt, at alle medarbejdere, som behandler persondata, læser denne instruks og erklærer at ville følge den samt evt. yderligere instrukser, der måtte blive udstedt af virksomheden eller en af denne udpeget persondataansvarlig person. Såfremt du i forbindelse med behandlingen af persondata overtræder instruksen, kan det få ansættelsesretlige konsekvenser – i yderste konsekvens i form af afskedigelse eller bortvisning.

2.1. Personoplysninger

Personoplysninger er informationer, der kan henføres til en specifik person, herunder kunder, ansatte mfl.

Oplysningerne kan være navne, billeder, cpr.nr. mv.

Personoplysninger kan inddeles i følgende to overordnet kategorier:

- Almindelige personoplysninger:
  - Navn, adresse, e-mail, telefonnummer mv.
  - CPR-nummer.
- Følsomme personoplysninger:

- Racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold.
- Oplysninger om andre rent private forhold, herunder strafbare forhold, væsentlige sociale problemer mv.

Personoplysninger må kun indhentes, behandles, gemmes, videregives mv. ved udtrykkelig hjemmel.

2.2. Behandling

Med behandling menes, at personoplysninger indsamles, anvendes, kommunikeres, videregives, gemmes eller lignende ved anvendelse af it-system eller papir og blyant.

Behandling af almindelige personoplysninger må finde sted, hvis en af følgende betingelser er opfyldt:

- Den registrerede har givet sit samtykke,
- Behandlingen er nødvendig af hensyn til opfyldelse af en aftale, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en sådan aftale,
- Behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige,
- Behandlingen er nødvendig for, at den dataansvarlige eller tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse, og hensynet til den registrerede ikke overstiger denne interesse.

Et samtykke kan altid trækkes tilbage.

2.3. Hvor og hvordan må man behandle personoplysninger

Når man vil behandle personoplysninger, er der både nogle generelle principper, man altid skal følge, og skal man have et konkret grundlag – en såkaldt "hjemmel" til at foretage netop den konkrete behandling. Begge dele skal være opfyldt. Man kan f.eks. ikke basere en behandling af personoplysninger på, at man har "hjemmel" i form af et samtykke fra den berørte person, hvis man ikke samtidig kan argumentere for, at der er et sagligt behov for behandlingen.

2.3.1. Grundlæggende principper

Følgende grundlæggende principper skal være overholdt for at personoplysningerne må behandles:

- Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.
- Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål.

- Personoplysningerne skal være tilstrækkelige og relevante for den givne behandling, men der må heller ikke indsamles flere oplysninger end nødvendigt.
- Personoplysninger skal være korrekte og ajourførte, og fejlagtige oplysninger skal slettes eller berigtiges.
- Personoplysninger må ikke opbevares i en længere periode end nødvendigt for at opfylde det formål, hvortil de er indsamlet, med mindre der foreligger grundlag for en videre behandling.
- Personoplysninger skal – gennem anvendelse af passende tekniske og organisatoriske foranstaltninger – opbevares og behandles på en måde, der skaber tilstrækkeligt sikkerhed for, at der ikke sker uautoriseret eller ulovlig behandling, samt at der ikke sker tab, tilintetgørelse eller beskadigelse af oplysninger.

2.4. Ansvaret for behandlingen

Ansvaret for, at de anførte principper overholdes, ligger hos virksomhedens som sådan (den dataansvarlige), men enhver medarbejder, der behandler personoplysninger, har en pligt til at sætte sig ind i disse regler og i tvivlstilfælde at søge tvivlen afklaret hos Mads Myhlendorph Nielsen, der i det daglige har det overordnede ansvar for behandlingen af persondata og sikkerheden i forbindelse med denne.

Selv om virksomheden måtte benytte sig af eksterne samarbejdspartnere til behandling af personoplysninger (f.eks. lønbureauer, rekrutteringsfirmaer eller lignende), påhviler det endelige ansvar fortsat virksomheden som dataansvarlig. Det er et lovkrav, at der laves skriftlige databehandleraftaler i sådanne tilfælde.

2.5. Kun nødvendige oplysninger

Der må ikke behandles flere personoplysninger end højst nødvendigt og ikke i længere tid end nødvendigt.

Virksomheden anvender kun personoplysninger, som er nødvendige for opfyldelse af formålet med behandlingen.

Virksomheden må f.eks. ikke anvende personoplysninger til andet formål end det oplysningerne blev indsamlet til.

2.6. God databehandlingsskik

Indsamlingen af personoplysninger i Virksomheden sker alene til det udtrykkeligt angivne og saglige formål i overensstemmelse med det indhentede samtykke, og senere behandling må ikke være uforenelig hermed.

Virksomheden foretager løbende en ajourføring af oplysningerne. Virksomheden foretager ligeledes årligt en kontrol for at sikre, at der ikke behandles urigtige eller vildledende oplysninger. Vildledende eller urigtige oplysninger slettes eller berigtiges.

Virksomheden opbevarer ligeledes ikke personoplysninger på en sådan måde, at der gives mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

2.7. Den registreredes rettigheder

Det almindelige princip om gennemsigtighed indebærer en række konkrete pligter over for de registrerede, som er beskrevet i EU-forordningens kapitel III. Generelt indebærer bestemmelserne heri, at den dataansvarlige skal assistere den registrerede med at udnytte sine rettigheder.

Der gælder således en oplysningspligt ved enhver indsamling af personoplysninger, uanset om disse indsamles fra den registrerede selv(*) eller tredjemand(**). Der skal generelt gives oplysning om:

- Den dataansvarliges identitet og kontaktinformation – herunder på en person, der i virksomheden er udpeget som ansvarlig (Mads Myhlendorph Nielsen)
- Formålet med og grundlaget for behandlingen
- Den legitime interesse, hvis grundlaget er interesseafvejningsregel
- Hvem der modtager oplysningerne (herunder eksterne lønbureauer og koncernforbundne virksomheder)
- Om der sker overførsel til tredjelande (udenfor EU/EØS)
- Hvor længe oplysningerne opbevares
- Retten til at kræve indsigt i egne oplysninger
- Muligheden for at trække et evt. samtykke tilbage
- Muligheden for at klage til Datatilsynet

Ved oplysninger indhentet fra den registrerede selv, skal der yderligere afgives oplysning om:

- Hvorvidt den registreredes afgivelse af oplysningerne er nødvendige for at opfylde en kontrakt eller lovmæssige forpligtelser
- Hvorvidt oplysningerne kan forventes anvendt til et andet formål, end de er indhentet

Ved oplysninger indhentet fra tredjemand, skal der yderligere afgives oplysning om:

- Hvilken tredjemand, der har givet oplysningerne
- Hvilke kategorier af oplysninger, der er indhentet (fra tredjemand)

Den nævnte oplysningspligt skal opfyldes i forbindelse med indsamling af oplysningerne hos den registrerede eller senest en måned efter indsamlingen, hvor denne sker hos tredjemand. Oplysningerne skal gives i et let forståeligt sprog og bør gives på skrift – evt. pr. e-mail. Oplysningspligten kan efter omstændighederne godt opfyldes via virksomhedens intranet, men det duer ikke, at medarbejderne selv skal finde oplysningerne – der skal være en konkret henvisning til disse i et dokument, der udleveres til medarbejderen – f.eks. i ansættelsesaftalen.

Den registrerede har desuden en indsigtsret, dvs. vedkommende kan til enhver tid ret til at kræve de oplysninger, også selv om virksomheden har opfyldt sin oplysningspligt.

Anmodninger om indsigt skal besvares skriftligt inden 1 måned efter, de fremsættes. Den registrerede kan kræve oplysningerne udleveret på maskinlæsbart format, f.eks. på en USB-stik (gælder fra maj 2018).

Den registrerede har ret til at få berigtiget urigtige oplysninger uden unødig forsinkelse.

Den registrerede har endvidere ret til at få slettet personoplysninger, som ikke længere er nødvendige for det formål, de er indsamlet til, eller hvor der ikke længere er et lovligt grundlag for at behandle dem, herunder hvor et meddelt samtykke, som behandlingen baseres på, trækkes tilbage. Dette kaldes "retten til at blive glemt". Sletning bør ske inden for en 1 måned, forudsat anmodningen er berettiget og sletning ikke strider mod andre regler.

Den registrerede kan endvidere kræve, at behandlingen af personoplysninger begrænses til de formål, der er lovlige, ligesom det kan kræves, at behandlingen suspenderes, mens rigtigheden af personoplysninger undersøges, en interesseafvejning foretages, eller et retskrav fastlægges. I sidstnævnte tilfælde må oplysningerne ikke slettes, men skal opbevares, mens den anførte afklaring finder sted.

2.8. Videregivelse af personoplysninger til medarbejder

Personoplysninger må kun videregives til andre medarbejdere, som er nødvendige for opfyldelse af formålet.

Såfremt en medarbejder får utilsigtet adgang til personoplysninger, skal dette straks rapporteres til Mads Myhlendorph Nielsen.

Denne persondatapolitik ajourføres årligt. Den er senest revideret den 7. juni 2018.