



HEDESELKABET

# PERSONDATAPOLITIK (GDPR) FOR BEHANDLING AF PERSONOPLYSNINGER FOR

Hedeselskabet A/S, Dalgasgroup A/S, HedeDanmark a/s, Orbicon A/S  
samt koncernforbundne datterselskaber

(danske, udenlandske, helejede og majoritetsjede)

Klostermarken 12

8800 Viborg

CVR-nr. 42 34 46 13 – CVR-nr. 26 77 02 54 – CVR-nr. 27 62 35 49 – CVR-nr. 21 26 55 43



Behandling af persondata omfatter hele livscyklussen



# HEDESELSKABET

1	INTRODUKTION TIL PERSONDATAPOLITIKKEN.....	3
2	HVAD ER PERSONDATA / PERSONFØLSOMME DATA? .....	3
3	HVORFOR HAR VI DENNE POLITIK? .....	3
4	POLITIKKENS OMFANG .....	4
5	PERSONDATAREGLERNE .....	4
6	DATABESKYTTELSESRISICI .....	6
7	DE REGISTREREDES RETTIGHEDER .....	6
8	VIDEREGIVELSE OG DELING AF PERSONDATA .....	7
9	OVERFØRSLER TIL TREDJELANDE .....	7
10	ANSVAR OG ORGANISATION.....	8
11	KONTAKTPERSON.....	9
12	SAMARBEJDE MED DATATILSYNET .....	9
13	SUPPLERENDE OG RELATEREDE POLITIKKER OG PROCEDURER.....	9
14	VI OPLYSER DE REGISTREREDE OM VORES BEHANDLING .....	10
15	HVILKE DATA HÅNDTERER SELSKABET OM DIG.....	10
16	GENERELLE RETNINGSLINJER FOR ALLE ANSATTE .....	12
17	CLEAN DESK POLICY - OPBEVARING OG ARKIVERING AF PERSONRELATEREDE OPLYSNINGER .....	13
18	BRUD PÅ PERSONDATASIKKERHEDEN.....	14
19	AFVIGELSER OG UNDTAGELSER.....	15
20	OVERTRÆDELSE AF PERSONDATAPOLITIKKEN .....	15
21	BRUG AF DATABEHANDLERE .....	15
22	HEDESELSKABET SOM DATABEHANDLER .....	16





# HEDESELSKABET

## 1 INTRODUKTION TIL PERSONDATAPOLITIKKEN

- 1.1 Hedeselskabet og koncernforbundne datterselskaber (danske, udenlandske, helejede og majoritetsejede samt selskaber med afgørende indflydelse i) (herefter fælles benævnt "Hedeselskabet" i dokumentet) er som erhvervsvirksomhed nødsaget til at indsamle og behandle oplysninger om fysiske personer (persondata-/oplysninger om medarbejdere, kunder, kontaktpersoner m.v.).
- 1.2 Persondatapolitikken beskriver hvordan persondata skal og kan indsamles, opbevares, anvendes, deles, arkiveres og slettes eller på anden måde behandles, for at vi lever op til og overholder persondatareglerne. Reglerne skal efterleves af alle medarbejdere i Hedeselskabet.

## 2 HVAD ER PERSONDATA / PERSONFØLSOMME DATA?

### 2.1 Persondata (ikke udtømmende)

- Navn, adresse, e-mail, tlf.nr.
- Fødselsdato
- Uddannelse
- Beskæftigelse
- Løn
- Skat
- Sygefravær
- CPR-nummer

### 2.2 Personfølsomme data (udtømmende)

- Race og etnisk oprindelse
- Politisk overbevisning
- Religiøs eller filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Genetiske data
- Biometriske data med henblik på entydig identifikation
- Helbredsoplysninger
- Seksuelle forhold eller seksuel orientering.

## 3 HVORFOR HAR VI DENNE POLITIK?

### 3.1 Persondatapolitikken tilsikrer, at vi i Hedeselskabet:

- Overholder de gældende persondataregler og følger god databehandlingskik.
- Overholder vores egne interne standarder og målsætninger for behandling af persondata.





# HEDESELSKABET

- Beskytter individers rettigheder i forhold til brug af personoplysninger om dem – herunder bl.a. ansatte, kunder/kontakter og øvrige, som vi som virksomhed er i besiddelse af oplysninger om.
- Er åbne omkring hvordan vi behandler persondata og skaber en gennemsigtighed for de registrerede personer.
- Sikrer os mod at der indtræder brud på persondatasikkerheden.

## 4 POLITIKKENS OMFANG

### 4.1 Persondatapolitikken for Hedeselskabet omfatter

- Bestyrelsen
- Direktionen
- Alle ansatte
- Alle leverandører og øvrige samarbejdspartnere, som arbejder på Hedeselskabets vegne

### 4.2 Persondatapolitikken gælder for alle oplysninger om fysiske personer – både direkte oplysninger og indirekte oplysninger, uanset om oplysningerne i øvrigt falder udenfor anvendelsesområdet for persondatareglerne (se evt. afsnit 2).

## 5 PERSONDATAREGLERNE

### 5.1 Hedeselskabet er underlagt at overholde Databeskyttelsesforordningen, inklusive de supplerende regler i Databeskyttelsesloven.

### 5.2 Databeskyttelsesforordningen og Databeskyttelsesloven udgør de overordnede og generelle regler for behandling af persondata, og disse regler fastsætter også, hvordan vi i Hedeselskabet kan og skal behandle persondata.

### 5.3 Persondatareglerne gælder uanset om persondata behandles elektronisk eller på papir.

### 5.4 Databeskyttelsesreglerne opsætter otte fundamentale behandlingsprincipper, som vi i Hedeselskabets behandling af persondata altid skal efterkomme. Disse principper siger, at persondata skal;

- 1) behandles lovligt, rimeligt og på en gennemsigtig måde.
- 2) indsamles til udtrykkeligt angivne og legitime formål.
- 3) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til det angivne formål.
- 4) være korrekte og om nødvendigt ajourførte.
- 5) slettes igen, når formålet er udtømt.
- 6) behandles på en måde, som sikrer persondata mod uautoriseret eller ulovlig behandling, herunder også at flere end dem, der har et arbejdsbetinget behov for at tilgå persondataene tilgår dem.
- 7) behandles i overensstemmelse med de registreredes rettigheder.





## HEDESELSKABET

- 8) ikke overføres til lande udenfor EU, med mindre der er et overførselsgrundlag, så det sikres, at det land der overføres persondata til også sikrer et passende niveau af persondatasikkerhed. Hertil kan Hedeselskabet have egne regler, politikker og retningslinjer vedrørende persondata og personfølsomme data, som tilsvarende skal følges.

5.5 Persondatareglerne bygger herudover på et princip om ”ansvarlighed”. Dette princip fastsætter, at vi som virksomhed skal kunne påvise, at vi overholder behandlingsprincipperne og persondatareglerne i øvrigt.

5.6 For at persondata lovligt kan behandles, er det et krav, at der er et behandlingsgrundlag. Dvs. at der er hjemmel i databeskyttelsesreglerne. Når vi i Hedeselskabet behandler persondata, uanset om det er til egne interne formål, eller det er i forbindelse med udøvelse af vores virksomhed, skal vi altid sikre os, og være i stand til at påvise, at vi har et behandlingsgrundlag (hjemmel) for at foretage behandlingen.

Behandlingsgrundlag er i hovedtræk ”klassificeret” i 3 kategorier:

- 1) Lovmæssige forhold  
(*Skat, bogføringslov etc.*)
- 2) Aftalegrundlag forhold  
(*kunde/leverandør aftaler/kontrakter etc.*)
- 3) Samtykke forhold  
(*samtykkeerklæringer medarbejdere etc.*)

5.7 Persondatareglerne fastsætter, at vi skal gennemføre passende sikkerhedsforanstaltninger for at sikre, at vores behandling af persondata sker i overensstemmelse med persondatareglerne. Hedeselskabet har etableret en række sikkerhedsprocedurer, som til sammen skal sikre, at vi har en passende informationsikkerhed – f.eks. men ikke dækkende IT-sikkerhedspolitik og Politik for anvendelse af firma-pc, tablet, mobil og andet IT-udstyr.

### 5.8 Indsamling af persondata / personfølsomme data

5.8.1 Persondata må kun indsamles, når der er defineret et formål med indsamlingen og den påtænkte brug herunder hvilket behandlingsgrundlag der er tilstede. Formålet kan være bredt formuleret i relation til udførelse af en arbejdsopgave, men det skal fortsat være så konkret, at det ikke er altomfattende. Hvor der er behov for et samtykke, skal dette indhentes skriftligt/elektronisk.

5.8.2 Det skal også vurderes, om det er relevant og nødvendigt at indsamle den enkelte oplysning, forinden den indsamles.

5.8.3 Indsamling af persondata / personfølsomme data pr. mail skal som udgangspunkt altid ske ved brug af sikker mail (krypteret mail) via Hedeselskabets IT-infrastruktur/løsning.

### 5.9 Deling af persondata / personfølsomme data

5.9.1 Deling og videregivelse af persondata betragtes som en særskilt behandling. Forinden der sker en videregivelse, skal det derfor sikres, at det falder indenfor de formål oplysningerne er indsamlet under samt at der er behandlingsgrundlag for delingen eller videregivelsen af persondataene.

5.9.2 Deling af persondata / personfølsomme data pr. mail skal som udgangspunkt altid ske ved brug af sikker mail (krypteret mail) via Hedeselskabets IT-infrastruktur/løsning.





## HEDESELSKABET

### 5.10 Sletning af persondata / personfølsomme data

5.10.1 Persondata skal slettes (eksempelvis er det ikke nok at smide i "slettet post" på pc'eren uden efterfølgende at tømme mappen), når de angivne behandlingsformål er udtjent. Du skal dog være opmærksom på, om der i procedurer for arkivering er en forpligtelse til at persondata opbevares i en vis periode, inden de slettes.

5.10.2 Ved print af personoplysninger skal (hvis muligt) systemet/printer sættes op med kode/print-til-boks og automatisk sletning af dokument efter print.

## 6 DATABESKYTTELSESRISICI

6.1 Persondatapolitikken hjælper med at beskytte Hedeselskabet, og medarbejdere som arbejder med persondata og personfølsomme data, mod sikkerhedsrisici, som eks.:

- Brud på fortroligheden – eksempelvis at persondata gøres tilgængelig for tredjemand eller for medarbejdere, som ikke har nogen grund til at tilgå oplysningerne. Dette kan være som følge af en uheldig omgang med persondata eller på grund af tekniske forhold (hacking).
- Brud på integriteten – eksempelvis at de oplysninger vi opbevarer, ikke er korrekte.
- Brud på tilgængeligheden – eksempelvis at vi ikke kan tilgå vores IT-systemer som følge af teknisk nedbrud eller hacking.
- Ulovlig anvendelse af persondata – eksempelvis at vi bruger persondata til andet end de lovlige formål, eller at persondata i øvrigt behandles i strid med persondatareglerne.
- Skade på Hedeselskabets omdømme – eksempelvis som følge af negativ omtale i medierne, med svækket kundetillid som følge.
- Strafansvar med tilhørende bøder og eller sanktioner.

## 7 DE REGISTREREDES RETTIGHEDER

7.1 Persondatareglerne giver registrerede personer en række rettigheder. Det gælder dig som medarbejder og eksterne personer, hvis data vi har registreret. Hedeselskabet er forpligtet til og ønsker naturligvis at efterleve disse regler.

7.2 Som registreret har du generelt ret til:

- Du har ret til at få indsigt i, hvilke kategorier af personoplysninger vi behandler om dig, og til at få udleveret en kopi af oplysningerne. Du har ret til at få oplyst, hvor oplysningerne stammer fra, og med hvilket formål vi behandler oplysningerne. Du har også ret til at få oplyst, om vi videregiver oplysningerne, og hvor længe vi opbevarer dem.
- Hvis du mener, at de personoplysninger vi behandler om dig, er forkerte eller misvisende, har du ret til at få dem rettet eller suppleret.
- Du har ret til at få slettet personoplysningerne, hvis de ikke længere er nødvendige i forhold til det formål, som de er indsamlet til.





## HEDESELSKABET

- Du har til enhver tid ret til at tilbagekalde et samtykke, som du har givet under ansættelsen. Hvis personoplysningerne er indhentet på baggrund af dit samtykke, kan du få oplysningerne slettet, hvis du trækker dit samtykke tilbage. Dog kan vi fortsat behandle oplysningerne, hvis vi har et andet grundlag for det, fx hvis det er nødvendigt at opbevare dem som led i en retstvist.
- Du kan også anmode om at få slettet dine oplysninger, hvis du mener, at de behandles i strid med gældende lovgivning eller andre retlige forpligtelser.
- Vi vurderer din anmodning hurtigst muligt, og i denne periode har du ret til at få behandlingen af dine personoplysninger begrænset, således at vi kun opbevarer dem, mens vi undersøger, om de er korrekte eller skal slettes.
- I nogle tilfælde behandler vi personoplysninger på grundlag af en interesseafvejning, fx når vi offentliggør arbejdsrelaterede oplysninger om dig på vores hjemmeside. Du har ret til at gøre indsigelse mod en sådan behandling, hvis du mener, at din særlige situation betyder, at din interesse i, at behandlingen ophører, vejer tungere end vores interesse i at behandle oplysningerne.
- Du har ret til at få udleveret de oplysninger, som du har givet os i pdf-format (dataportabilitet), når oplysningerne behandles elektronisk som led i opfyldelse af ansættelseskontrakten eller på baggrund af dit samtykke. Hvis du ønsker at gøre brug af dine rettigheder, kan du kontakte os, og vi vil behandle din anmodning hurtigst muligt.

7.3 Hedeselskabet har fastsat procedurer for at håndtere udøvelse af registreredes rettigheder på korrekt vis.

7.4 Hvis du modtager en anmodning fra en registreret person om udøvelse af dennes rettigheder, skal du straks kontakte den dataansvarlige, som har til opgave at bistå med opfyldelse af vores forpligtelser.

## 8 VIDEREGIVELSE OG DELING AF PERSONDATA

8.1 I visse situationer kræver lovgivningen, at Hedeselskabet videregiver persondata til myndigheder. I sådanne tilfælde videregives persondata efter direktionens godkendelse, som foreligger generelt. Hedeselskabet skal i sådanne tilfælde sikre sig, at anmodningen eller kravet om videregivelse af persondata er reelt, og at forpligtelsen for Hedeselskabet er legitimeret.

8.2 Om nødvendigt skal der i tvivlstilfælde altid indhentes konkret assistance fra ledelsen eller den databeskyttelsesansvarlige, forinden oplysninger udleveres.

## 9 OVERFØRSLER TIL TREDJELANDE

9.1 Der gælder særlige regler i persondatalovgivningen for, at persondata kan overføres til et land udenfor EU.

9.2 Overførsel til et land udenfor EU omfatter både den situation, hvor data fysisk flyttes, men også den situation, at der blot skabes adgang til dem fra en lokation udenfor EU (fjernadgang). Overførsel omfatter også de situationer, hvor du som medarbejder rejser til et land udenfor EU og tilgår Hedeselskabets IT-systemer.





## HEDESELSKABET

- 9.3 Forinden du igangsætter en overførsel til et land udenfor EU, skal du kontakte Hedeselskabets databeskyttelsesansvarlige, så det kan fastlægges, om der er et lovligt overførselsgrundlag.
- 9.4 Kun i de tilfælde hvor der er et lovligt overførselsgrundlag, må du derefter overføre persondata til et land udenfor EU.

### 10 ANSVAR OG ORGANISATION

- 10.1 Alle der arbejder for Hedeselskabet har et ansvar for at sikre, at persondata bliver indsamlet, opbevaret og anvendt, delt, arkiveret, slettet og i det hele behandlet på passende vis.
- 10.2 Alle medarbejdere er herunder ansvarlige for, at persondata og databeskyttelsesregler behandles og omgås i overensstemmelse med de retningslinjer, der er nedlagt i denne persondatapolitik, inklusive supplerende politikker og instrukser.
- 10.3 Hedeselskabet har opdelt det overordnede ansvar i forskellige kategorier:

**Bestyrelsen** og **direktionen** er overordnet ansvarlig for, at Hedeselskabet lever op til sine forpligtelser efter databeskyttelseslovgivningen.

Hedeselskabet / koncernforbundne datterselskabers **databeskyttelsesansvarlige** er overordnet ansvarlig for at:

- Holde direktion og bestyrelse opdateret på persondatasikkerheden i Hedeselskabet.
- Review og holde alle politikker og procedurer vedrørende informationssikkerhed opdateret ud fra et fastlagt årshjul.
- Håndtere henvendelser fra bestyrelse, direktion og ansatte omkring Hedeselskabets generelle behandling af persondata samt håndterer henvendelser med konkrete spørgsmål.
- Håndtere henvendelser omkring persondatabehandling fra eksterne aktører, herunder bl.a. kunder, leverandører og øvrige samarbejdspartnere samt tilsynsmyndigheder.
- Besvare henvendelser fra registrerede ved udøvelse af deres rettigheder efter databeskyttelsesreglerne.
- Godkendelse af aftaler med eksterne parter om videregivelse af persondata eller overladelse af behandlingsaktiviteter (databehandleraftaler).

De eller det enkelte selskabs databeskyttelsesansvarlige har til opgave at rådgive ledelse og alle medarbejdere om de forpligtelser der er efter databeskyttelseslovgivningen samt at påse, at vi overholder reglerne og de rammer som denne persondatapolitik opsætter.

Hedeselskabets **IT-ansvarlige** er overordnet ansvarlig for at:

- Sikre at alle IT-systemer, IT-services og alt IT-udstyr, som anvendes af Hedeselskabet og vores medarbejdere ved udførelse af deres arbejde, er i overensstemmelse med acceptable sikkerhedsstandarder.
- Gennemføre periodiske afprøvning af, at sikkerhedskomponenter og -software virker som tilsigtet.







## HEDESELSKABET

- Løbende vurdere kvaliteten og sikkerheden i den software, hardware og IT-services Hedeselskabet anvender og i/ved anskaffelse af nye IT-systemer.
- Hedeselskabets IT-plattform har evnen til vedvarende at sikre fortrolighed, tilgængelighed og robusthed for alle systemer og services.

Vi sikrer og beskytter både vores medarbejderes, kunders og øvrige samarbejdspartneres personoplysninger bedst muligt. Vi henviser til vores IT-sikkerhedspolitik for nærmere oplysninger om IT-sikkerhed. Herudover har vi implementeret en række fysiske og organisatoriske sikkerhedsforskrifter. Hver enkelt medarbejder skal være opmærksom på og følge disse forskrifter, ligesom du straks skal kontakte din nærmeste leder, hvis du oplever forhold/overtrædelser, som er uhensigtsmæssige, i strid med gældende lovgivning eller bør forbedres.

### 11 KONTAKTPERSON

11.1 Spørgsmål omkring behandling af persondata rettes til de respektive databeskyttelsesansvarlige:

- Hedeselskabet, Carsten R. Andersen / caan@hedeselskabet.dk
- HedeDanmark, Jesper Kilsmark / jesk@hededanmark.dk
- Orbicon, Torben B. Christensen / tbch@orbicon.dk
- Xergi, Bill Tobin / bill@xergi.com

11.2 Hvis der opstår mistanke om at vi som virksomhed, eller at en eller flere medarbejdere ikke overholder denne persondatapolitik, skal kontaktpersonen straks kontaktes herom.

### 12 SAMARBEJDE MED DATATILSYNET

12.1 Datatilsynet har kompetencer til at udøve tilsynsvirksomhed overfor Hedeselskabet for at påse, om vi overholder persondatareglerne. Datatilsynet kan gennemføre fysiske inspektioner eller fremsende elektroniske forespørgsler til os.

12.2 Det er vores politik, at Hedeselskabet samarbejder med Datatilsynet under tilsynsforretninger. Dette gælder også for den enkelte medarbejder, som skal samarbejde i overensstemmelse med de instrukser Hedeselskabet giver.

12.3 Du har mulighed for at klage over behandling af personoplysninger til Datatilsynet, Borgergade 28, 5 sal, 1300 København K, tlf.: 33193200, eller via e-mail: [dt@datatilsynet.dk](mailto:dt@datatilsynet.dk).

### 13 SUPPLERENDE OG RELATEREDE POLITIKKER OG PROCEDURER

13.1 Hedeselskabets persondatapolitik indgår i en række af informations- og sikkerhedspolitikker som bl.a. er tilgængelig via intranettet og som foruden persondatapolitikken består af:

- IT-sikkerhedspolitik
- Politik for anvendelse af firma-pc, tablet, mobiltelefon og andet IT-udstyr.
- Procedurer indenfor HR
- Informationsmateriale (GDPR intranet, videoer m.v.) om behandling af personoplysninger.





## HEDESELSKABET

- Beredskabsplan
- Der henvises i øvrigt til de respektive datterselskabers politikker, procedurer m.v.

### 14 VI OPLYSER DE REGISTREREDE OM VORES BEHANDLING

14.1 Hedeselskabet bestræber sig på at sikre, at de personer vi behandler oplysninger om, er og bliver oplyst om, at vi behandler oplysninger om dem, samt at de er bekendt med og forstår.

- Hvordan oplysninger om dem bliver brugt og behandlet
- Hvordan de som registreret kan udøve deres rettigheder

### 15 HVILKE DATA HÅNDTERER SELSKABET OM DIG

15.1 For at kunne opfylde den ansættelseskontrakt, som vi har indgået med dig, og for at sikre, at gældende lovgivning vedrørende alle relevante medarbejderforhold overholdes, behandler og overfører vi data vedrørende dig, herunder bl.a. CPR-nummer, løn, pensionsoplysninger, skatteoplysninger, kontonummer mv., i det omfang det er nødvendigt for at udbetale løn til dig. I forbindelse med udbetaling af løn videresendes oplysninger til bl.a. SKAT, pensionselskab, forsikringsselskab, Feriekonto ligesom at vi sender en elektronisk kopi af din lønseddel til din e-Boks. Vi anvender desuden eksterne IT-leverandører, som hoster vores data og hjælper os med IT-sikkerhed, software mv. IT-leverandørerne (eksempelvis hostingpartnere, cloudleverandører) registrerer brug af internet og e-mails og har ligeledes mulighed for at tilgå data. Endvidere forefindes der forskellige fagsystemer. Der er indgået databehandler aftaler med respektive leverandører.

15.2 Som ansat hos os, opretter vi en personalesag om dig i vore systemer, hvor vi registrerer en række stamdata, såsom dit navn, adresse, CPR-nummer, fødselsdato, stillingsbetegnelse, privat telefonnummer og e-mailadresse, løn, anciennitet, bankoplysninger, pensionselskab, skatteoplysninger mv.

Mange af disse oplysninger fremgår også af din ansættelseskontrakt, som også opbevares i kopi på din personalesag. Hvis du ønsker det, så registrerer vi også navn og kontaktoplysninger på pårørende, så vi kan give besked, hvis du bliver syg eller kommer ud for et uheld.

I personalesagen registreres desuden de oplysninger, som du sendte os sammen med din ansøgning, såsom CV, uddannelsesbeviser og udtalelser fra tidligere arbejdsgivere. Vi opbevarer derudover en kopi af eventuelle indhentede referencer og resultatet af personlighedstests mv. I nogle tilfælde kan vi have indhentet en straffeattest i forbindelse med ansættelsen. Straffeattesten opbevares ikke, men det vil fremgå af et notat i personalesagen, at en straffeattest har været indhentet.

Under dit ansættelsesforhold registrerer vi løbende yderligere oplysninger om dig. Det kan fx være oplysninger om efteruddannelse, orlov, fravær på grund af ferie, sygdom, børns sygdom mv. Disse oplysninger anvendes desuden til at føre statistik over sygefravær, efteruddannelse mv. Desuden registreres eventuelle påtaler, advarsler, MUS-referater mv.

Nogle af oplysningerne registreres flere steder, fx i tidsregistreringssystemet og i bogholderiet.





## HEDESELSKABET

Vi registrerer dog også følsomme personoplysninger (helbredsoplysninger, fagforeningsforhold m.v.), hvis dette er nødvendigt for at opfylde forpligtelser i de overenskomster, som vi er omfattet af, eller hvis det er påkrævet i henhold til gældende lovgivning, eks. sygedagpengeloven eller m.v.

- 15.3 Tids- og fraværsregistrering: Du skal registrere din arbejdstid og dit tidsforbrug på de enkelte opgaver i vores tidsregistreringssystem. Du skal desuden registrere dit fravær (ferie, feriefridage, afspadsering, sygdom, barns sygedag, barsel mv.).

Tidsregistreringen anvendes bl.a. i forbindelse med lønadministrationen, fraværstatistik, til at søge refusion af syge- og barsels dagpenge og til brug for fakturering af kunder. Tidsregistreringen kan derudover anvendes af ledelsen til kontrol af din arbejdstid.

Du har ikke pligt til at oplyse os om årsagen til sygefravær. Hvis du er blevet bedt om at aflevere en lægeerklæring, har du derfor ret til at fjerne oplysninger om diagnosen, inden du giver den til os.

- 15.4 Adgangslog/videoovervågning: Som ansat på større lokationer som eksempelvis Høje Taastrup, Viby og Viborg modtager du en adgangsbrik, som du skal bruge for at få adgang til disse kontorer via vores adgangskontrol/alarmsystem. Adgangsbrikken skal kun anvendes uden for kontorets åbningstid. Loggere registrerer hvornår og hvem der benytter adgangsbrikkerne. Denne registrering gemmes i 1 måned. På hertil opstillede Pc'er, hvorefter data slettes. På de samme lokationer, er der opsat, og skiltet med, videoovervågning i og omkring bygningerne. Overvågningen er opsat for medarbejdernes tryghed samt for at kunne dokumentere/forebygge ifm. indbrud. Videodokumentation lagres i en periode på 1 måned. Herefter bliver det slettet. Det er kun koncernens ejendoms-koordinatorer som har adgang til dette materiale. På øvrige lokationer kan der findes andre loggere/løsninger, hvilket i givet fald så informeres om.

- 15.5 APV, trivselsundersøgelser mv.: Som led i vores arbejdsmiljøarbejde kan der blive registreret personoplysninger om dig, fx i forbindelse med trivselsundersøgelser, APV mv.

- 15.6 Intranet, hjemmeside og internet: På vores intranet/interne medier/interne databaser m.v. registrerer vi som en naturlig og nødvendig del af Hedeselskabets drift (bl.a. vedrørende identifikation og kommunikation) dit navn, stillingsbetegnelse, ansvarsområde, placering i organisationen, fysisk afdeling, arbejdstelefon og e-mail samt et billede af dig. Billedet skal gøre det muligt for dine kolleger at identificere dig.

Vi kan afhængigt af din funktion offentliggøre dit navn, stillingsbeskrivelse, ansvarsområde, arbejdstelefon og arbejds-emailadresse på Hedeselskabets hjemmeside. For at kunder og andre forretningsforbindelser kan sætte et ansigt på dig, når de taler med dig i telefonen, vil vi gerne offentliggøre et billede af dig på hjemmesiden. Du vil derfor blive bedt om at give samtykke hertil. Samtykket er frivilligt og kan til enhver tid tilbagekaldes.

Når du bruger internettet, registreres det centralt hos vores IT-leverandør, hvilke hjemmesider mv. du besøger. Vi gør opmærksom på, at denne registrering kan anvendes til kontrol af dit brug af internettet. Der henvises til vores IT-sikkerhedspolitik, som er tilgængelig på intranettet.





## HEDESELSKABET

- 15.7 CV og kontaktperson-billeder mv.: Som en naturlig og nødvendig del af Hedeselskabets drift ifm. kundevedtede opgaver, og afhængigt af din eventuelle kundevedtede funktion, kan vi fremsende eksempelvis person-CV's til kunder ifm. projektopgaver, tilbudsgivning med videre.
- 15.8 E-mail og kalender: Det logges centralt, når der sendes eller modtages e-mails fra din e-mail-adresse i virksomheden. Det er tilladt i mindre omfang at anvende e-mailadressen til privat kommunikation. Hvis du vælger at bruge din firmamail til private formål, skal du være opmærksom på at "private mails" bliver behandlet på samme måde som firmamail med hensyn til opbevaring og sletning.
- Du skal registrere alle aftaler, møder, fravær mv. i kalenderen i Outlook. Andre medarbejdere skal have adgang til at se din kalender. Hvis du indsætter private aftaler i kalenderen, bør du derfor markere disse aftaler som private, således at andre kun kan se, at du er optaget. Registreringer i kalenderen gemmes under hele ansættelsen og slettes normalt samtidig med e-mailkontoen ved fratrædelse. Du opfordres til løbende at slette eventuelle private aftaler.
- 15.9 Telefon: Vi har ingen central registrering af dine opkald. Vi har kun fastnettelefoner ifm. vores 3 hovedlokationer / receptioner / omstillingsborde. Du får udleveret en mobiltelefon, som også kan benyttes privat, hvis du har fri telefon. Vi registrerer ikke opkald til eller fra din mobiltelefon. Vi henviser i øvrigt til vores IT-sikkerhedspolitik.
- 15.10 Ved fratrædelse: Når du fratræder din stilling i Hedeselskabet, sletter vi dig jfr. gældende politikker/procedurer, ligesom din personalemappe bliver slettet. Din arbejdsmail blive påført en autosignatur, som oplyser, at du ikke længere er ansat. Signaturen vil være aktiv i op til 12 måneder efter fratrædelsen, herefter lukkes e-mailkontoen ned. E-mailkontoen vil udelukkende blive anvendt til at modtage e-mails, ikke til at sende e-mails. Vi vil ikke videresende eventuelle private e-mails til dig. Der kan gå op til 12 måneder efter din fratræden, før din mailkonto bliver slettet, afhængig af, hvor længe vi har brug for de oplysninger, der ligger i din mailkonto. Personoplysninger slettes også, når formålet med at opbevare oplysningerne ikke længere er tilstede.

Oplysningerne i din personalemappe vil normalt blive opbevaret i 5 år efter din fratrædelse. Dette sker for at sikre dokumentation, hvis der efter fratrædelsen måtte blive rejst krav mv. og under hensyntagen til den gældende forældelsesfrist for krav, der udspringer af ansættelsesforhold. Der kan være særlige forhold, fx en igangværende sag, som gør, at oplysningerne vil blive opbevaret i en længere periode.

## 16 GENERELLE RETNINGSLINJER FOR ALLE ANSATTE

- 16.1 Som del af Hedeselskabets persondatapolitik er fastsat for alle medarbejdere at:
- Oplysninger, herunder persondata, kun må tilgås, hvis det er nødvendigt for at udføre anviste og pålagte konkrete arbejdsopgaver.





## HEDESELSKABET

- For alle medarbejdere gælder, at forinden persondata indsamles og behandles, skal det være klarlagt hvad formålet og behandlingsgrundlaget er. Behandlingsgrundlaget kan være fastlagt i forbindelse med de supplerende politikker og procedurer, som er fastsat.
- Persondata ikke deles uformelt.
- Der skal i alle situationer udvises påpasselighed for at sikre fortroligheden omkring persondata – både i forhold til kollegaer og i forhold til eksterne parter, som ikke er autoriseret til at modtage oplysningerne.
- Hvis du er i tvivl om, hvorvidt du kan foretage en indsamling eller behandling af oplysninger, så skal du forinden indsamlingen eller behandlingen foretages kontakte Hedeselskabets/koncernforbundne datterselskabers databeskyttelsesansvarlige.
- Hvis man modtager persondata eller personfølsomme data og det viser sig, at man ikke er rette modtager, sørge for at meddele afsender om "fejlen" og derefter slette data.
- Udbudt undervisning og informationsmateriale i persondatabeskyttelse skal følges og prioriteres.

### 17 CLEAN DESK POLICY - OPBEVARING OG ARKIVERING AF PERSONRELATEREDE OPLYSNINGER

17.1.1 Persondata skal opbevares på sikker vis. Det betyder, at i overensstemmelse med Hedeselskabets IT-sikkerhedspolitik og særskilte procedurer for arkivering af persondata, så må dokumenter og andet materiale, hvor der indgår persondata kun opbevares i centrale behandlingssystemer og eksempelvis ikke lagres på USB-penne (med mindre den er krypteret) og andre bærbare medier (gælder ikke lokal pc hvor der er adgang/password kontrol).

Når du arbejder med personrelaterede oplysninger, skal du følge nedenstående retningslinjer:

#### 17.1.2 På og uden for arbejdspladsen

Når du forlader dit skrivebord, også selvom det kun er få minutter, skal du;

- Låse din pc, så der ikke står oplysninger på skærmen eller andre kan tilgå den.
- Flytte papirer med personoplysninger, der ligger fremme på fx skrivebordet til skuffe eller skab.

Når arbejdsdagen er slut, skal skuffe eller skab med personoplysninger aflåses.

#### Opbevaring og arkivering inden for arbejdspladsen

- Som udgangspunkt skal persondata opbevares og aktiveres i systemer som er centralt understøttet af backup, adgangs styring, logning mv. Personalesager opbevares på et drev, der er sikret med adgangskode, og kun medarbejdere, der har tilladelse hertil, kan tilgå oplysningerne.





## HEDESELSKABET

- Personoplysninger må kun opbevares i personalefiles og andre systemer, hvor der er overblik over oplysningerne, så de kan fjernes, når formålet med at opbevare oplysningerne ikke længere er tilstede.
- Papirer med personoplysninger skal opbevares aflåst, når de ikke er i brug. Dvs. på en sådan måde, at personer der ikke er autoriseret til at se oplysningerne ikke umiddelbart kan få adgang til dem.

### Opbevaring og arkivering uden for arbejdspladsen

- Som hovedregel tages personoplysninger (persondata) ikke med uden for arbejdspladsen (til eks. hjemmearbejdsplads), men tilgår alene disse via selskabets systemer gennem VPN sikret forbindelse med passwords etc.
- Hvis det er objektivt nødvendigt at arbejde med personoplysninger uden for arbejdspladsen på papirer eller eksternt medie f.eks. USB-stik (kun hvis krypteret), skal du opbevare papirerne / USB-stikket forsvarligt. og sørge for at arkivere, tilintetgøre eller slette oplysningerne umiddelbart efter, at opgaven er afsluttet.

### Bortskaffelse

- Personoplysninger skal slettes, når formålet med at opbevare oplysningerne ikke længere er tilstede.
- Papirer med personoplysninger skal bortskaffes i umiddelbar forlængelse af, at de er blevet brugt til deres formål. Bortskaffelse af papirer med personoplysninger sker ved aktiv makulering (eks. makuleringsmaskine) eller tilsvarende med henblik på at forhindre, at andre får adgang til oplysningerne.
- Ved print af personoplysninger skal (hvis muligt) systemet/printer sættes op med kode/print-til-boks og automatisk sletning af dokument efter print.

## 18 BRUD PÅ PERSONDATASIKKERHEDEN

18.1 I tilfælde af brud på persondatasikkerheden skal den databeskyttelsesansvarlige hos Hedeselskabet og respektive datterselskaber straks underrettes.

18.2 Som eksempler på brud på persondatasikkerheden kan nævnes:

- Andre personer end den eller de personer hos Hedeselskabet, der er autoriseret til det, får (uautoriseret) adgang til personoplysninger. Det kan både være personer uden for eller inden for Hedeselskabets organisation.
- Hedeselskabets medarbejdere ændrer eller sletter personoplysninger ved et uheld.
- Brud på Hedeselskabets server, hvor uvedkommende har fået indsigt i personoplysninger – f.eks. kundedatabasens CPR-oplysninger, kreditkortoplysninger el.lign.





## HEDESELSKABET

- Hedeselskabets medarbejdere videregiver ubevidst eller bevidst personoplysninger om en borger/kunde eller medarbejder til en anden person – eller måske ligefrem flere andre uvedkommende personer.
- Når manglede kryptering af Hedeselskabets hjemmeside indeholdende f.eks. et kundelogin resulterer i, at en eller flere uvedkommende får direkte adgang til kundens personoplysninger.

18.3 Hedeselskabet har fastsat særskilt procedure for håndtering af brud på persondatasikkerheden. Efter persondatareglerne, er vi som udgangspunkt forpligtet til at rapportere til Datatilsynet, og nogle gange vil vi også være forpligtet til at kontakte de berørte personer.

### 19 AFVIGELSER OG UNDTAGELSER

19.1 Hvis der opstår situationer, hvor kravene i persondatapolitikken ikke kan efterleves, skal Hedeselskabets databeskyttelsesansvarlige kontaktes.

### 20 OVERTRÆDELSE AF PERSONDATAPOLITIKKEN

20.1 Alle medarbejdere i Hedeselskabet er forpligtet til at efterleve persondatapolitikken i den til enhver tid gældende form, med tilhørende retningslinjer og procedurebeskrivelser. En overtrædelse af persondatapolitikken kan efter omstændighederne medføre ansættelsesmæssige konsekvenser.

### 21 BRUG AF DATABEHANDLERE

21.1 I nogle situationer overlader vi til vores leverandører at foretage behandling af persondata på vores vegne. Leverandøren bliver i disse situationer vores databehandler. Dette er primært aktuelt for vores IT-anvendelse, hvor Hedeselskabet eksempelvis har outsourcet IT-driften/benytter cloud-tjenester mv.

21.2 Databeskyttelsesreglerne fastsætter, at vi udelukkende må anvende databehandlere, som kan stille den fornødne dokumentation for, at de vil gennemføre passende og tekniske og organisatoriske foranstaltninger på en sådan måde, at persondatareglerne overholdes.

21.3 Persondatareglerne fastsætter også, at vi altid skal have en skriftlig aftale med databehandleren.

21.4 Hedeselskabet har derfor etableret en procedure for at vurdere (potentielle) databehandlere samt for indgåelse af databehandleraftalerne.

21.5 Den enkelte medarbejder må derfor ikke indgå aftaler med nogen om, at andre skal udføre databehandlingsopgaver for os, eller indgå databehandleraftaler. Alle henvendelser og spørgsmål herom skal rettes til respektive selskabers databeskyttelsesansvarlige og forretnings IT-ansvarlige.

21.6 Der indgås endvidere fortrolighedsaftaler med hver leverandør, der måtte have adgang til systemsupport/arbejde.





## HEDESELSKABET

### 22 HEDESELSKABET SOM DATABEHANDLER

- 22.1 I nogle situationer optræder vi i Hedeselskabet også selv som databehandler. Dette er eksempelvis tilfældet i forhold til alle de oplysninger kunder indlæser i f.eks. medlemsregistrering eller andet – også koncern-interne behandlingsaktiviteter. Her behandler vi persondata på kundernes vegne og til opfyldelse af kundernes fastsatte formål.
- 22.2 Eksempelvis skal der være databehandleraftaler de koncern-interne-selskaber imellem, hvor der er henholdsvis dataansvarlige- og databehandlerforhold gældende.
- 22.3 Når vi i Hedeselskabet er databehandlere, er det et krav, at vi kun handler efter kundernes instruks, sådan som de er fastsat i vores kunde-/medlemsaftaler m.v. og standardvilkår.
- 22.4 Inden vi i Hedeselskabet får overladt persondata fra en kunde skal du sikre, at der er indgået en databehandleraftale.
- 22.5 Inden du tilgår en kundes data, skal du derfor sikre dig, at du har lov hertil, og det skal være klarlagt hvorfor du tilgår oplysningerne. Hvis din tilgang ikke er i overensstemmelse med aftalen med kunden, må persondataene ikke tilgås.
- 22.6 Hvis du er i tvivl, så kontakt Hedeselskabets databeskyttelsesansvarlige / koncern IT-ansvarlige.

\*\*\*

