GDPR-MEDARBEJDERHÅNDBOG

Hvordan må jeg som medarbejder håndtere personoplysninger?

solar

INDHOLDSFORTEGNELSE

HISTORIK **3**

INDLEDNING **3**

FORMÅL **5**

1 HVAD ER PERSONOPLYSNINGER? **7**

2 HVORNÅR SKER DER BEHANDLING AF PERSONOPLYSNINGER? **10**

3 BEHANDLINGSGRUNDLAG **12**

4 GRUNDLÆGGENDE PRINCIPPER **14**

5 OVERORDNEDE RETNINGSLINJER **16**

6 INDSAMLING, ANVENDELSE OG VIDEREGIVELSE AF PERSONOPLYSNINGER **18**

7 DE REGISTREREDES RETTIGHEDER **21**

8 OVERFØRSEL TIL TREDJELANDE **23**

9 BRUG AF DATABEHANDLERE **25**

10 OPBEVARING OG SLETNING **27**

11 BRUD PÅ PERSONDATASIKKERHEDEN **31**

12 OVERTRÆDELSE, SANKTIONERING OG AFVIGELSER **33**

BILAG A - BEHANDLINGSGRUNDLAG **34**

3.1 BEHANDLINGSGRUNDLAG FOR ALMINDELIGE PERSONOPLYSNINGER 35

3.2 BEHANDLINGSGRUNDLAG FOR FØLSOMME PERSONOPLYSNINGER 36

3.3 BEHANDLINGSGRUNDLAG FOR NATIONAL ID-Nummer 37

3.4 BEHANDLINGSGRUNDLAG FOR STRAFFEDOMME OG LOVOVERTRÆDELSER 37

HISTORIK

Version	Indhold	Godkendt af	DATO
1.0	Dokument oprettet	Mette Brix	01 May 2023

INDLEDNING

Solar A/S (herefter "Virksomheden") indsamler oplysninger om fysiske personer ("personoplysninger") som led i den daglige drift.

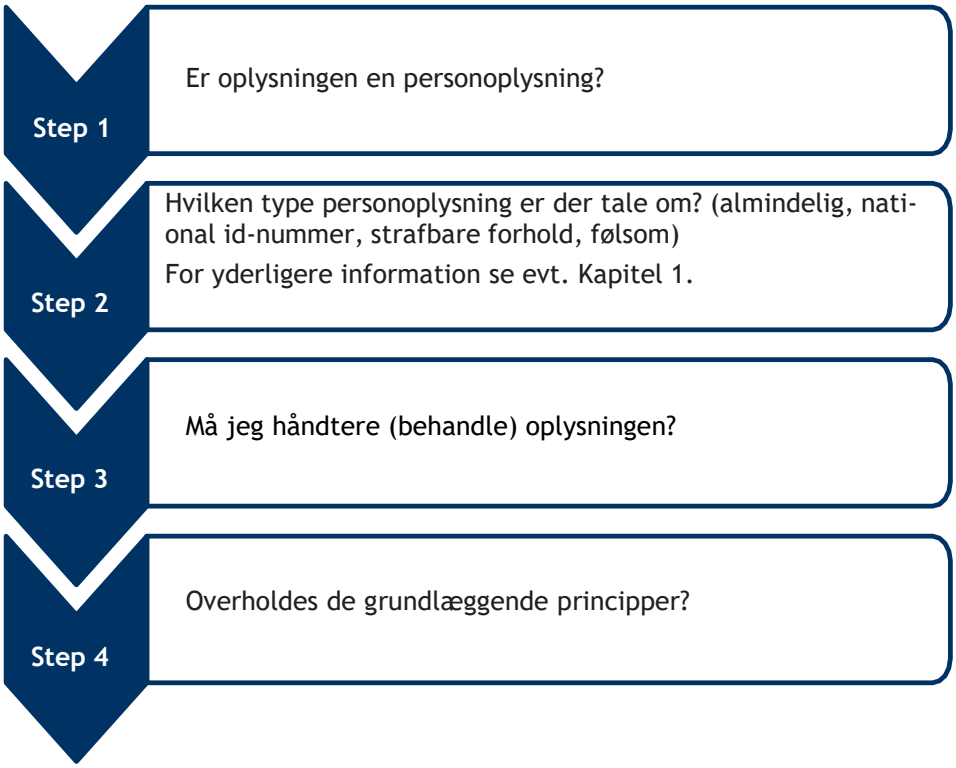
Denne GDPR-Medarbejderhåndbog tager udgangspunkt i de behandlinger, vi foretager i forbindelse med behandling af personoplysninger i den daglige drift. Det kan f.eks. være personoplysninger om vores kunder eller kollegaer, personoplysninger om vores samarbejdspartnere og personoplysninger om vores eventuelle kursister mv.

Denne GDPR-Medarbejderhåndbog er udarbejdet i overensstemmelse med Virksomhedens General GDPR Policy, som er styrende for al den behandling af personoplysninger, der foretages i Virksomheden.

Når du som medarbejder behandler personoplysninger som led i udførelse af dit arbejde, skal du overordnet være bekendt med nærværende retningslinjer, og de principper der gælder for behandling af personoplysninger. Det er derfor vigtigt, at du som medarbejder gennemgår disse retningslinjer, og at du deltager i de aktiviteter (f.eks. træning og undervisning), som fastlægges af Virksomheden på området.

Denne GDPR-Medarbejderhåndbog er udarbejdet for at give dig det nødvendige kendskab til de databeskyttelsesretlige regler. Håndbogen er udarbejdet som et opslagsværk, hvor du hurtigt kan finde svar, råd og vejledning til de spørgsmål, som du måtte støde på som led i dine opgaver i Virksomheden.

Når du skal afgøre, om du lovligt kan behandle en personoplysning, skal du følge denne proces:



I GDPR-Medarbejderhåndbogen finder du den information, som du skal bruge for at besvare disse spørgsmål.

FORMÅL

De databeskyttelsesretlige regler gælder uanset om personoplysningerne behandles elektronisk eller på papir.

Alle personoplysninger, som Virksomheden behandler, skal indsamles og anvendes på en lovlig, rimelig og gennemsigtig måde, og de skal opbevares sikkert.

Virksomheden og du som medarbejder skal sammen sørge for, at personoplysninger ikke kommer til uvedkommendes kundskab.

Du må kun behandle personoplysninger, hvis der er et arbejdsbetinget behov for det. Det betyder f.eks. at medarbejderoplysninger alene må behandles af nærmeste leder, HR og lønkontoret. På samme måde må kunde-, kursist og leverandøroplysninger alene behandles af de afdelinger, som har et arbejdsbetinget behov herfor.

Hvis du er i tvivl om, hvorvidt der kan foretages en indsamling eller behandling af personoplysninger, skal du forinden indsamlingen eller behandlingen foretages kontakte den GDPR-ansvarlige, der kan vejlede og hjælpe.

Kontaktoplysninger kan findes her på din lokale GDPR-ansvarlige:
https://solargroup.sharepoint.com/sites/sggdpr

KAPITEL 1

HVAD ER PERSONOPLYSNINGER?

1 HVAD ER PERSONOPLYSNINGER?

Personoplysninger er enhver form for information, der kan henføres til bestemte personer.

Dette omfatter også oplysninger som f.eks. medarbejdernummer, billede m.v. når det er muligt at henføre oplysningerne til en bestemt fysisk person.

De databeskyttelsesretlige regler gælder uanset om personoplysningerne behandles elektronisk eller på papir.

Personoplysninger, er alle oplysninger, der direkte eller indirekte kan henføres til en fysisk person. Personoplysninger inddeles i fire kategorier:

- Almindelige personoplysninger
- Oplysninger om national id-nummer
- Oplysninger om straffedomme og lovovertrædelser
- Følsomme personoplysninger

Herunder findes eksempler på personoplysninger inddelt i de fire overordnede kategorier (listen er ikke udtømmende).

ALMINDELIGE PERSONOPLYSNINGER	▪ Identifikationsoplysninger
	  ▪ Eksempelvis navn, adresse, telefonnummer, fødselsdato, e-mailadresse og billeder
	▪ Civilstand
	▪ Interne familieforhold
	▪ Økonomiske forhold
	▪ Arbejds- uddannelses- og ansættelsesmæssige forhold
	  ▪ Eksempelvis uddannelse/kurser, stilling, arbejdsområde og -opgaver, arbejdstid, løn, skatteoplysninger, sygefravær m.v.

OPLYSNINGER OM NATIONAL ID-NUMMER	▪ En medarbejders nationale ID-nummer ▪ Fødselsdato er en almindelig oplysning
OPLYSNINGER OM STRAFFEDOMME OG LOVOVERTRÆDELSER	▪ Oplysning om at en medarbejder har begået (eller er politianmeldt for) et strafbart forhold ▪ Oplysning om overtrædelse af lovgivningen, uden at det har udløst (eller kan udløse) et egentligt strafansvar, men evt. andre sanktioner, f.eks. rettighedsfrakendelse ▪ Oplysninger på straffeattest eller børneattest ▪ Oplysning om en ren straffeattest er en almindelig oplysning ▪ Oplysning om at en person har adresse i et fængsel ▪ Oplysninger om lovovertrædelser og straffedomme er fortrolige oplysninger
FØLSOMME OPLYSNINGER	▪ Race eller etnisk oprindelse ▪ Politisk, religiøs eller filosofisk overbevisning ▪ Helbredsoplysninger ▪ Fagforeningsmæssigt tilhørsforhold ▪ Seksuelle forhold eller seksuelle orientering ▪ Genetiske og biometriske data

KAPITEL 2

HVORNÅR SKER DER BEHANDLING AF PERSON-OPLYSNINGER?

2 HVORNÅR SKER DER BEHANDLING AF PERSONOPLYSNINGER?

Behandling af personoplysninger omfatter enhver form for håndtering af personoplysninger.

Behandling kan f.eks. være:

- Indsamling
- Registrering
- Systematisering
- Opbevaring
- Brug
- Deling
- Videregivelse
- Arkivering
- Sletning

Behandling af personoplysninger omfatter hele livscyklussen. Det vil sige alle behandlinger af personoplysningerne fra de indsamles til de er slettet hos Virksomheden.

Reglerne gælder uanset, om personoplysningerne behandles elektronisk eller på papir.

Behandling af personoplysninger må kun ske, hvis der er et behandlingsgrundlag. Du kan læse mere om de forskellige behandlingsgrundlag nedenfor i kapitel 3.

KAPITEL 3

BEHANDLINGSGRUNDLAG

3 BEHANDLINGSGRUNDLAG

Behandling af personoplysninger må kun ske, hvis der er et behandlingsgrundlag. Et behandlingsgrundlag er grundlaget for, at selve behandlingen af personoplysningen er tilladt og lovlig.

Eksempelvis hvis en arbejdsgiver ønsker at bruge billeder af medarbejdere på arbejdsgiverens hjemmeside, skal arbejdsgiver have et behandlingsgrundlag til at må bruge billederne af medarbejderne. Her skal arbejdsgiveren indhente medarbejdernes samtykke. Arbejdsgivers behandlingsgrundlag for behandlingen af medarbejderens billede er derfor medarbejderens samtykke.

Den type af personoplysning, som en personoplysning tilhører, bestemmer hvilke behandlingsgrundlag du kan bruge, når du skal afgøre, om det er tilladt at behandle personoplysningen.

Som bilag til denne håndbog findes en tabel i **Bilag A** (Behandlingsgrundlag) med overblik over, hvornår det er lovligt at behandle personoplysninger inddelt i de forskellige kategorier.

For yderligere information om behandlingsgrundlag se Bilag A:

3.1 BEHANDLINGSGRUNDLAG FOR ALMINDELIGE OPLYSNINGER
3.2 BEHANDLINGSGRUNDLAG FOR FØLSOMME OPLYSNINGER
3.3 BEHANDLINGSGRUNDLAG FOR NATIONAL ID-NUMMER
3.4 BEHANDLINGSGRUNDLAG FOR STRAFFEDOMME OG LOVOVERTRÆDELSER

KAPITEL 4

GRUNDLÆGGENDE PRINCIPPER

4 GRUNDLÆGGENDE PRINCIPPER

De databeskyttelsesretlige regler opsætter otte grundlæggende behandlingsprincipper, som Virksomheden *altid* skal efterkomme:

A	LOVLIGHED, RIMELIGHED OG GENNEMSIGTIGHED	Alle personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde.
B	FORMÅLSBEGRÆNSNING	Når personoplysninger indsamles, skal det ske til udtrykkeligt angivne og legitime formål. Personoplysningerne må ikke viderebehandles på en måde, der er uforenelig med det oprindelige formål.
C	DATAMINIMERING	Personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, som personoplysningerne behandles til.
D	RIGTIGHED	Personoplysningerne skal være korrekte og om nødvendigt ajourførte. Personoplysninger skal som udgangspunkt berigtiges eller eventuelt slettes hvis urigtige.
E	OPBEVARINGSBEGRÆNSNING	Personoplysningerne må ikke opbevares længere, end det er nødvendigt i forhold til de formål, som de er indsamlet til. Når det ikke længere er nødvendigt at opbevare personoplysninger af hensyn til opfyldelse af formålet, skal de slettes eller anonymiseres.
F	INTEGRITET OG FORTROLIGHED	Personoplysningerne behandles på en måde, som sikrer personoplysninger mod uautoriseret eller ulovlig behandling, herunder også at flere end dem, der har et arbejdsbetinget behov for at tilgå personoplysninger tilgår dem.
ANSVARLIGHED		De databeskyttelsesretlige regler bygger herudover på et princip om "ansvarlighed". Dette princip fastsætter, at vi som virksomhed skal kunne påvise, at vi overholder behandlingsprincipperne og de databeskyttelsesretlige regler i øvrigt. Det gør vi blandt andet ved at dokumentere, at alle medarbejdere følger og gennemfører undervisning i persondatabeskyttelse, at vi opdaterer vores fortegnelser mv.
INGEN TREDJELANDSOVERFØRSLER		Personoplysningerne må ikke overføres til lande uden for EU, medmindre der er instruks hertil, et overførselsgrundlag samt eventuelle supplerende foranstaltninger, så det sikres, at det land der overføres personoplysninger til, også sikrer et passende niveau af persondatasikkerhed.

KAPITEL 5

OVERORDNEDE RETNINGSLINJER

5 OVERORDNEDE RETNINGSLINJER

Virksomheden har fastsat følgende overordnede retningslinjer for alle medarbejdere:

- Oplysninger, herunder personoplysninger, må kun tilgås, hvis det er nødvendigt for at udføre anviste og pålagte arbejdsopgaver.
- Personoplysninger må ikke deles uformelt og med personer, som ikke har et arbejdsbetinget behov for at behandle oplysningerne.
- Undervisning i persondatabeskyttelse skal følges og prioriteres.
- Der skal i alle situationer udvises påpasselighed for at sikre fortroligheden omkring personoplysninger – både i forhold til kollegaer og i forhold til eksterne parter, som ikke er autoriseret til at modtage oplysningerne.
- Den lokale GDPR-ansvarlige skal forespørges ved enhver tvivl i forhold til behandling af personoplysninger.

Find kontaktoplysninger på din lokale GDPR-ansvarlige her: https://solargroup.sharepoint.com/sites/sggdpr

Hvis du i forbindelse med dit arbejde har behov for andre IT-system/software end det, der er tilgængeligt, skal du altid indhente godkendelse hos **Contract Management** og **Information Security**. Således sikrer vi datasikkerheden i Virksomheden. Som virksomhed er vi forpligtet til at føre fortegnelse over vores systemer og de dertilhørende behandlinger, hvori der indgår personoplysninger.

KAPITEL 6

INDSAMLING, ANVENDELSE OG VIDEREGIVELSE AF PERSONOPLYSNINGER

6 INDSAMLING, ANVENDELSE OG VIDEREGIVELSE AF PERSONOPLYSNINGER

INDSAMLING AF PERSONOPLYSNINGER

Du må kun indsamle personoplysninger, når der er defineret et formål med indsamlingen og den påtænkte brug. Formålet kan være bredt formuleret i relation til udførelse af en arbejdsopgave, men det skal fortsat være så konkret, at det ikke er altomfattende.

Det skal altid vurderes, om det er **relevant og nødvendigt** at indsamle den enkelte personoplysning, forinden den indsamles. Eksempelvis ved indsamling af kundeoplysninger, hvis en ny kunde kontakter dig mv., må du kun indsamle de nødvendige personoplysninger for etablering af kundeforholdet. Det betyder eksempelvis, at som sælger må du indhente de personoplysninger på en kunde, som er nødvendige og relevante for at aftalen kan indgås. Det kan være navn, adresse, telefonnummer, bankoplysninger mv. på kunden. Det betyder samtidig, at du ikke må indhente personoplysninger på kunden, som ikke er relevant for aftaleindgåelse. Det kan være følsomme oplysninger eller oplysninger om strafbare forhold.

Inden personoplysninger indsamles, skal det også afgøres, hvilket **behandlingsgrundlag** der er til stede. Hvor der er behov for et samtykke, skal dette indhentes skriftligt og med anvendelse af Virksomhedens blanketter herfor.

Der skal eksempelvis indhentes et samtykke, forinden der tages billeder af medarbejdere eller kunder. Hos Solar har vi både interne og eksterne samtykkeerklæringer, som skal bruges i disse situationer. Find vores samtykkeerklæringer her: https://solargroup.sharepoint.com/sites/sgGDPR/SitePages/Documents.aspx

Ved indsamling af personoplysninger skal de registrerede personer have meddelelse om, hvordan Virksomheden behandler deres personoplysninger. Se nærmere herom i kapitel 7.

Kontakt din lokale GDPR-ansvarlige, hvis du er i tvivl. Find kontaktoplysninger på din lokale GDPR-ansvarlige her: **https://solargroup.sharepoint.com/sites/sggdpr**

ANVENDELSE AF PERSONOPLYSNINGER

De personoplysninger der indsamles og opbevares, må kun bruges til opfyldelse af de formål, de er indsamlet til i forbindelse med udførelse af dit arbejde.

Det betyder, at du f.eks. ikke må videregive navn og e-mail på en kunde til en anden virksomhed, medmindre du har kundens samtykke.

Med andre ord må personoplysningerne ikke bruges til **andre formål**, end de formål som personoplysningerne i første omgang er indsamlet til.

DELING OG VIDEREGIVELSE AF PERSONOPLYSNINGER

Deling og videregivelse af personoplysninger betragtes som en **særskilt behandling**. Det betyder, at hvis du ønsker at dele eller videregive personoplysninger til andre, skal der foretages en separat og konkret vurdering af delingen/videregivelsen af personoplysninger. Forinden der sker en deling/videregivelse, skal det derfor sikres, at det falder indenfor de formål personoplysningerne er indsamlet under, samt at der er behandlingsgrundlag for delingen eller videregivelsen af personoplysninger.

I visse situationer kræver lovgivningen, at Virksomheden videregiver personoplysninger til myndigheder. Eksempelvis ved udbetaling af løn er Virksomheden underlagt lovgivning om indberetning til skattemyndigheder. Når der er tale om typiske videregivelser af personoplysninger til myndigheder, som en del af en fast og godkendt rutine af den nærmeste leder, kan du som medarbejder videregive disse personoplysninger til myndigheden uden yderligere godkendelse.

Hvis der er tale om udlevering af personoplysninger til myndigheder i særlige eller ekstraordinære situationer, som du ikke har modtaget anmodning på før eller er i tvivl om, skal dette godkendes af din lokale GDPR-ansvarlige før videregivelse til myndigheden. Virksomheden skal i sådanne tilfælde sikre sig, at anmodningen eller kravet om videregivelse af personoplysninger er reel, og at forpligtelsen for Virksomheden er legitimeret.

I tvivlstilfælde skal der altid rettes henvendelse til **din lokale GDPR-ansvarlige** eller **GDPR Group Team** via gdpr@solar.dk (mailen sendes på engelsk), forinden personoplysninger videregives.

KAPITEL 7

DE REGISTREREDES RETTIGHEDER

7 DE REGISTREREDES RETTIGHEDER

Databeskyttelsesforordningen giver registrerede personer en række rettigheder. Registrerede personer er de personer, som de behandlede personoplysninger omhandler.

Som registreret har man generelt ret til blandt andet:

- At modtage oplysninger om, at vi behandler personoplysninger om den registrerede
- At få indsigt i, om vi behandler personoplysninger om dem, og i så fald hvilke oplysninger vi behandler
- At få berigtiget urigtige personoplysninger, herunder også at få suppleret oplysningerne, så de fremstår fuldstændiggjort
- At få slettet de personoplysninger, vi behandler, i visse situationer
- At kræve, at vi begrænser vores behandlingsaktiviteter
- At trække et samtykke tilbage

Hvis du som medarbejder modtager en anmodning fra en registreret person om udøvelse af dennes rettigheder, skal du følge Virksomhedens lokale workflows. Find de lokale workflows her: https://solargroup.sharepoint.com/sites/sgGDPR/SitePages/Documents.aspx

Hvis du er i tvivl om håndteringen af den registreredes rettighedsanmodning skal du altid kontakte den lokale GDPR-ansvarlige. Find din lokale GDPR ansvarlige her: https://solargroup.sharepoint.com/sites/sggdpr

Virksomheden har i sin privatlivspolitik på hjemmesiderne oplyst den registrerede om, hvordan Virksomheden behandler den registreredes personoplysninger ved besøg på vores hjemmesider.

Der udleveres eksempelvis også oplysninger om Virksomhedens behandling af personoplysninger i nedenstående tilfælde:

- I rekrutteringsforløb når vi har modtaget en ansøgning gennem vores rekrutteringssystem
- I ansættelsesforhold når den registrerede er ansat sker udlevering af privatlivspolitik sammen med ansættelseskontrakten
- I forbindelse med den registreredes tilmelding som kursist
- Ved den registreredes besøg på vores hjemmeside
- Tilmelding af nyhedsbreve og deltagelse af konkurrencer
- I forbindelse med ordreafgivelse fra kunder via vores hjemmeside
- I forbindelse med opstart af samarbejde med samarbejdspartnere

KAPITEL 8

OVERFØRSEL TIL TREDJELAND

8 OVERFØRSEL TIL TREDJELANDE

Der gælder særlige regler i de databeskyttelsesretlige regler ved overførsel af personoplysninger til et land uden for Den Europæiske Union (EU)/Det Europæiske Økonomiske Samarbejdsområde (EØS) (et "tredjeland").

Overførsel til et land uden for EU/EØS omfatter både den situation, hvor personoplysninger fysisk flyttes, men også den situation, at der blot skabes adgang til dem fra en lokation uden for EU (fjernadgang).

Hvis der sker overførsel af en registerets personoplysninger til et tredjeland ved anvendelsen af en databehandler, skal der tilsvarende rettes henvendelse til **Contract Management** og **Information Security** for at sikre, at tredjelandsoverførslen kan foretages lovligt.

Forinden du igangsætter en overførsel til et land uden for EU/EØS, skal du **altid** kontakte **Contract Management** og **Information Security**, så det kan fastlægges, om der er et lovligt overførselsgrundlag, og hvorvidt der skal iværksættes supplerende foranstaltninger.

KAPITEL 9

BRUG AF DATABEHANDLERE

9 BRUG AF DATABEHANDLERE

I nogle situationer overlader Virksomheden til leverandører at foretage behandling af personoplysninger på Virksomhedens vegne. Leverandøren bliver i disse situationer Virksomhedens databehandler. Dette er primært aktuelt for vores IT-anvendelse, samt for enkelte samarbejdspartnere; herunder til brug for HR/lønbehandling, marketing, CRM-system, salg mv.

De databeskyttelsesretlige regler fastsætter, at vi udelukkende må anvende databehandlere, som kan stille de fornødne garantier for, at de vil gennemføre passende, tekniske og organisatoriske foranstaltninger på en sådan måde, at de databeskyttelsesretlige regler overholdes.

Databeskyttelsesforordningen fastsætter også, at Virksomheden altid skal have en skriftlig aftale med databehandleren. Virksomheden har en skabelon for databehandleraftaler, som skal bruges, når Virksomheden indgår databehandleraftaler. Denne skabelon indeholder en række punkter, som Virksomheden skal tage stilling til hver gang der indgås databehandleraftaler.

Virksomheden fører løbende kontrol med databehandlerne, hvor Virksomheden sikrer, at databehandlerne bliver ved med at leve op til de krav, som Virksomheden stiller til dem.

Alle databehandlere med tilhørende databehandleraftaler og kontroller skal registreres i vores kontaktsystem.

- Den enkelte medarbejder må ikke indgå aftaler med nogen om, at de skal udføre opgaver vedrørende behandling af personoplysninger for Virksomheden, eller indgå databehandleraftaler.

- Alle beslutninger om at anvende databehandlere og indgå databehandleraftaler skal godkendes af Virksomhedens **Contract Management & Information Security** og i samarbejde med **din lokale GDPR-ansvarlige**.

- Du må heller ikke anvende IT-løsninger, som ikke er autoriseret af **Contract Management & Information Security**. Tilsidesættelse heraf er en alvorlig overtrædelse af *General GDPR Policy*.

KAPITEL 10

OPBEVARING OG SLETNING

10 OPBEVARING OG SLETNING

Virksomheden må som udgangspunkt kun opbevare personoplysninger så længe det er nødvendigt for at opfylde det formål, hvortil de er indhentet. Det betyder, at personoplysninger skal slettes igen, når de ikke længere er nødvendige at opbevare i forhold til dit arbejdsbetingede formål med at indsamle personoplysningerne.

Vær opmærksom på at det **kun er lovligt** at indsamle og gemme personoplysninger, som er nødvendige, for at du kan løse din arbejdsopgave.

Såfremt personoplysninger viser sig urigtige eller unødvendige i forhold til formålet, skal du slette eller berigtige personoplysningerne.

Personoplysninger skal opbevares på sikker vis. Det betyder, at dokumenter og andet materiale, hvor der indgår personoplysninger, kun må opbevares i de af Virksomhedens anviste behandlingssystemer, f.eks. CRM-system, ERP-system og HRM-System, men ikke på USB-stik mv.

MEDARBEJDEROPLYSNINGER

Personoplysninger om dig som medarbejder indsamles til personaleadministrative formål og opbevares under hele din ansættelsesperiode. Efter din fratræden, opbevares medarbejderoplysninger efter ansættelsesforholdets ophør i henhold til de lokalt gældende regler.

KUNDEOPLYSNINGER

Kundeoplysninger indsamles til brug for behandling af ordrer mv. fra kunder og oplysningerne opbevares så længe, der er et aktivt kundeforhold. Oplysninger omkring fakturering opbevares i henhold til de lokalt gældende regler.

KURSISTOPLYSNINGER

Virksomheden indsamler og opbevarer personoplysninger om kursister. Personoplysningerne opbevares indtil efter uddannelsens afslutning. Derefter slettes personoplysninger i overensstemmelse med lokalt gældende regler om bogføring.

OPLYSNINGER OM SAMARBEJDSPARTNERE OG LEVERANDØRER

Oplysninger om samarbejdspartnere og leverandører kan inddeles i to underkategorier:

1) Virksomhedsoplysninger såsom navn på virksomheden, økonomi, adresse mv.
2) Personoplysninger på de medarbejdere, der arbejder i virksomheden såsom navn, e-mail, telefonnummer mv.

Virksomhedsoplysninger kan som udgangspunkt indsamles og opbevares så længe det ønskes og er nødvendigt for Virksomheden. Virksomhedsoplysninger er ikke omfattet af de databeskyttelsesretlige regler. Den gælder kun for fysiske personer.

Oplysninger om fysiske personer fra virksomheden/samarbejdspartneren, eksempelvis kontaktperson hos en virksomhed, er derimod personoplysninger, og omfattet af de databeskyttelsesretlige regler. Det betyder, at personoplysninger (om den pågældende kontaktperson) skal slettes når de ikke længere er nødvendige at opbevare for at opfylde det formål, de er indsamlet til.

Eksempelvis hvis personen ikke længere er ansat hos samarbejdspartneren/leverandøren, eller når det ikke længere er nødvendigt for Virksomheden at opbevare personoplysningerne på grund af endt samarbejde.

FYSISKE DOKUMENTER

Hos Virksomheden opfordres alle medarbejdere til at undgå modtagelse af fysiske dokumenter og derimod modtage dokumenterne digitalt.

Hvis du modtager dokumenterne fysisk, eksempelvis CV'er, ansøgninger mv., bør dokumenterne indscannes og gemmes i det relevante system, medmindre der ikke er et behov for at gemme dokumenterne. De fysiske dokumenter skal derefter makuleres. Såfremt der ikke er et behov for at gemme dokumenterne, skal dokumenterne ligeledes makuleres og ikke indscannes.

Såfremt du undtagelsesvist har fysiske dokumenter, som ikke bliver scannet ind, skal disse opbevares i et fysisk arkiv med angivelse af indhold og år. Herudover skal personoplysningerne opbevares på et sikkert sted, dvs. på en sådan måde, at personer – interne som eksterne – der ikke er autoriseret til at se personoplysningerne ikke umiddelbart kan få adgang til dem, f.eks. i et aflåst skab eller en aflåst skuffe. Når dokumenterne ikke længere skal opbevares, skal de makuleres.

BEHANDLING AF MAILS I OUTLOOK

Virksomheden anvender Outlook til behandling af mails.

Outlook har til formål at understøtte korrespondance, og indbakken i Outlook skal som udgangspunkt ikke anvendes til opbevaring.

Alle medarbejdere skal oprette undermapper i Outlook til journalisering af mails, der indeholder personoplysninger, vedrørende kunder, kursister, leverandører og private forhold. Disse undermapper skal navngives, så det sikres, at kun nødvendige personoplysninger gemmes.

Alle e-mails som ikke er journaliseret i en undermappe (inkl. indbakke, papirkurv, vedhæftede filer, sendt post og arkiverede filer), der indeholder personoplysninger, skal slettes hver 6. måned efter modtagelse/afsendelse.

Personoplysninger, der defineres som følsomme eller fortrolige, må ikke opbevares i indbakken Outlook, og skal derfor straks slettes eller journaliseres efter modtagelse.

Private mails skal overføres til en undermappe navngivet "Privat mappe", når det vedrører forhold af privat karakter, som ikke er relevant for Virksomheden. Der må ikke opbevares personoplysninger af fortrolig eller følsom karakter i "Privat mappen".

Det er Virksomheden uvedkommende, hvad der indeholdes i Privat mappen, og medarbejderen har ansvaret for at opbevaringen af personoplysningerne kan ske lovligt.

Bemærk: Medarbejderen må ikke bruge Privat mappen til fortroligt eller følsomt indhold af privat karakter, da Virksomheden forholder sig ret til at føre kontrol med, at Privat mappen ikke anvendes til andre formål end de angivne.

Bemærk: Medarbejderen kan blive udtaget til intern kontrol, hvor Virksomheden vil få adgang til mappens indhold.

Bemærk: Indhold fra Privat mappen vil kunne komme til Virksomhedens kendskab, når Virksomheden foretager tværgående søgninger på tværs af alle Outlook-konti.

KAPITEL 11

BRUD PÅ PERSONDATASIKKERHEDEN

11 BRUD PÅ PERSONDATASIKKERHEDEN

Der foreligger et brud på persondatasikkerheden, når et sikkerhedsbrud fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

Du skal **straks** rette henvendelse til **Group Service Desk "GSD"** hvis du bliver opmærksom på, eller har mistanke om et brud på persondatasikkerheden.

Et brud på persondatasikkerheden kan f.eks. rent teknisk ske, når Virksomhedens it-systemer med personoplysninger ikke er tilstrækkelig sikret, så udefrakommende får adgang til personoplysningerne (f.eks. hacking). Det kan også være Virksomhedens egen håndtering af personoplysningerne, der kan forårsage et brud, f.eks. hvis en medarbejder videregiver eller ændrer personoplysninger uden ret til det eller sender en e-mail til en forkert person.

Hvis der sker et brud på persondatasikkerheden, som kræver anmeldelse til den kompetente tilsynsmyndighed, skal denne anmeldelse ske senest 72 timer, efter at bruddet er kendt. Der skal ikke ske anmeldelse, hvis det er usandsynligt, at sikkerhedsbruddet har indebåret en risiko for en fysisk persons rettigheder. Denne vurdering foretager **den lokale GDPR-ansvarlige** og **GDPR Group TEAM**, hvorfor der skal sendes en mail til GDPR@solar.dk på engelsk.

Du skal **straks** rette henvendelse til **Group Service Desk "GSD"** hvis du bliver opmærksom på, eller har mistanke om et brud på persondatasikkerheden.

Ring venligst til telefonnummer: +45 79300155

Derefter skal du kontakte din lokale GDPR-ansvarlige og sende en mail til **GDPR Group TEAM** via GDPR@solar.dk på engelsk.

Du kan læse mere om, hvad du som medarbejder skal gøre, hvis der sker et brud på persondatasikkerheden i Virksomhedens *GDPR-Guidelines for personal data breach* og *contingency plan for personal data breach*.

KAPITEL 12

OVERTRÆDELSE, SANKTIONERING OG AFVIGELSE

12 OVERTRÆDELSE, SANKTIONERING OG AFVIGELSER

OVERTRÆDELSE

Du er som medarbejder i Virksomheden forpligtet til at efterleve *General GDPR Policy* i den til enhver tid gældende form, med tilhørende retningslinjer og procedurebeskrivelser herunder denne GDPR-Medarbejderhåndbog.

Find *General GDPR Policy*, med tilhørende retningslinjer og procedurebeskrivelser her: https://solargroup.sharepoint.com/sites/sggdpr

SANKTIONERING

Den lokale GDPR-ansvarlige påser overholdelsen af retningslinjer og procedurer. Såfremt du som medarbejder bryder de gældende retningslinjer og procedurer for behandling af personoplysninger, kan det få ansættelsesretlige konsekvenser.

AFVIGELSER, UNDTAGELSER OG UREGELMÆSSIGHEDER

Den lokale GDPR-ansvarlige skal kontaktes med anmodning om dispensation fra reglerne, hvis der opstår situationer, hvor kravene i retningslinjer og procedurer ikke kan efterleves.

Afvigelse må ikke foretages, førend der foreligger skriftlig dispensation fra den lokale GDPR-ansvarlige.

Alle spørgsmål omkring behandling af personoplysninger skal rettes til **din lokale GDPR-ansvarlige**.

Såfremt der opstår mistanke om, at Virksomheden eller at en eller flere medarbejdere ikke overholder procedurerne og retningslinjerne, skal **GDPR Group Team** straks kontaktes herom.

BILAG A - BEHANDLINGSGRUNDLAG

TABEL 3.1 – BEHANDLINGSGRUNDLAG FOR ALMINDELIGE PERSONOPLYSNINGER

TABEL 3.2 – BEHANDLINGSGRUNDLAG FOR FØLSOMME PERSONOPLYSNINGER

TABEL 3.3 – BEHANDLINGSGRUNDLAG FOR NATIONAL ID-NUMMER

TABEL 3.4 – BEHANDLINGSGRUNDLAG FOR STRAFFEDOMME OG LOVOVERTRÆDELSER

I de følgende tabeller får du et overblik over, hvornår det er lovligt at behandle personoplysninger.

Tabellerne viser lovlige behandlingsgrundlag for de fire overordnede kategorier af personoplysninger.

3.1 BEHANDLINGSGRUNDLAG FOR ALMINDELIGE PERSONOPLYSNINGER	
Behandlingsgrundlag	Anvendelsesområde (ikke udtømmende)
Samtykke. Databeskyttelsesforordningens artikel 6(1)(a)	Personoplysninger bør kun behandles på basis af et samtykke, hvis de øvrige behandlingsgrundlag ikke kan anvendes. Et samtykke skal være en "frivillig, specifik, informeret og utvetydig viljestilkendegivelse" fra den registrerede, hvor den registrerede bekræfter, at personoplysninger, der vedrører den pågældende, behandles.
Opfyldelse af en kontrakt, som den registrerede er part i. Databeskyttelsesforordningens artikel 6(1)(b)	Eksempelvis Virksomhedens behandling af personoplysninger om vores kunder. Kan kun bruges, når den registrerede er part i kontrakten.
Foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt. Databeskyttelsesforordningens artikel 6(1)(b)	Eksempelvis arbejdsgivers behandling af personoplysninger under rekrutteringsprocessen.
Overholdelse af en retlig forpligtelse, som påhviler den dataansvarlige. Databeskyttelsesforordningens artikel 6(1)(c).	Behandling, som er nødvendig for at overholde lovgivningen, f.eks. indberetning af ansattes løn til skattemyndigheder, anmeldelse af arbejdsskader m.v.
Beskytte den registreredes eller anden fysisk persons vitale interesser. Databeskyttelsesforordningens artikel 6(1)(d)	Behandlingen skal vedrøre interesser, som er af fundamental betydning for den registrerede. F.eks. hvis personen er på grund af sygdom er ude af stand til at give samtykke til en behandling af personoplysninger, som vil sikre personen mod at lide et væsentligt økonomisk tab eller lide væsentlig skade.
Udførelse af en opgave i samfundets interesse. Databeskyttelsesforordningens artikel 6(1)(e).	Omfatter opgaver af almen interesse, dvs. opgaver, som er af betydning for en bredere kreds af personer.
Offentlig myndighedsudøvelse som den dataansvarlige har fået pålagt. Databeskyttelsesforordningens artikel 6(1)(e).	Denne regel retter sig primært mod behandling af personoplysninger for offentlige myndigheder, der sker som led i myndighedsudøvelse.
Behandlingen er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser går forud herfor. Databeskyttelsesforordningens artikel 6(1)(f).	Behandling kan ske, når den dataansvarliges interesser – efter en konkret afvejning – går forud for den registreredes interesse i, at behandlingen ikke sker. Afvejning skal foretages på grundlag af de konkrete omstændigheder i det enkelte tilfælde.

3.2 BEHANDLINGSGRUNDLAG FOR FØLSOMME PERSONOPLYSNINGER	
Behandlingsgrundlag	Anvendelsesområde (ikke udtømmende)
Samtykke. Databeskyttelsesforordningens artikel 9(2)(a)	Hvis personen har givet sit samtykke til, at der kan behandles følsomme personoplysninger om personen. Samtykket skal leve op til de samme krav, som et samtykke til behandling af almindelige personoplysninger.
Behandling er nødvendig for at overholde den dataansvarliges eller den registreredes arbejds-, sundheds- og socialretlige forpligtelser. Databeskyttelsesforordningens artikel 9(2)(b)	Eksempelvis kan lovgivningen eller kollektive overenskomster fastsætte specifikke regler om behandling af arbejdstagers personoplysninger i ansættelsesforhold.
Beskytte den registreredes eller anden fysisk persons vitale interesser. Databeskyttelsesforordningens artikel 9(2)(c)	Behandlingen skal vedrøre interesser, som er af fundamental betydning for den registrerede. Kan kun anvendes i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give sit samtykke.
Behandling foretaget af et organ, hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art. Databeskyttelsesforordningens artikel 9(2)(d)	Eksempelvis kan en fagforening som led i sine aktiviteter behandle personoplysninger om fagforeningens medlemmer og tidligere medlemmer og ansatte under overenskomstens område, når behandlingen sker som led i fagforeningens arbejde som faglig organisation.
Personoplysninger som tydeligvis er offentliggjort af den registrerede. Databeskyttelsesforordningens artikel 9(2)(e)	Hvis personoplysningerne er bragt til kendskab hos en bredere kreds af personer, f.eks. på sociale medier som Facebook, Twitter og YouTube. Personoplysningerne skal være offentliggjort på personens egen foranledning. Personoplysninger, som andre af egen drift har offentliggjort om personen, er ikke omfattet.
Behandling er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares. Databeskyttelsesforordningens artikel 9(2)(f)	Bestemmelsen omfatter både behandling i den dataansvarliges, den registreredes og tredjemands interesse. Bestemmelsen omfatter både behandling i forbindelse med en retssag samt administrative og udenretslige procedurer.
Behandling er nødvendig af hensyn til væsentlige samfundsinteresser. Databeskyttelsesforordningens artikel 9(2)(g)	Behandlingen skal ske af hensyn til varetagelse af væsentlige samfundsinteresser og have hjemmel i loven.
Behandling er nødvendig med henblik på forebyggende medicin eller arbejdsmedicin til vurdering af arbejdstagers erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og- tjenester på grundlag af lov eller en kontrakt med en sundhedsperson, der er underlagt tavshedspligt. Databeskyttelsesforordningens artikel 9(2)(h)	Anvendes normalt af offentlige myndigheder, lægefagligt personale m.v. Behandlingen skal have hjemmel i loven, eller der skal indgås en kontrakt med en fagperson, der er underlagt tavshedspligt.
Behandling er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet. Databeskyttelsesforordningens artikel 9(2)(i)	Bestemmelsen omfatter bl.a. beskyttelse mod alvorlige grænseoverskridende sundhedsrisici eller sikring af høje kvalitetsstandarder for sundhedspleje og lægemidler eller medicinsk udstyr. Behandlingen skal have hjemmel i loven.
Behandling er nødvendig af hensyn til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål. Databeskyttelsesforordningens artikel 9(2)(j)	Omfatter alene forskningsmæssige eller statistiske formål. Behandlingen skal have hjemmel i loven.

3.3 BEHANDLINGSGRUNDLAG FOR NATIONAL ID-Nummer	
Behandlingsgrundlag	Anvendelsesområde (ikke udtømmende)
Lovhjemmel. Efter national lovgivning.	Hvis det følger af lovgivningen, at den dataansvarlige har ret til at behandle oplysninger om nationale ID-numre. F.eks. ved indberetninger til skattemyndigheder af forskellige indkomst-relaterede oplysninger.
Samtykke. Efter national lovgivning.	Hvis personen har givet sit samtykke til, at der kan behandles oplysninger om personens nationale id-nummer. Samtykket skal leve op til de samme krav, som et samtykke til behandling af almindelige oplysninger.
Statistiske eller videnskabelige formål. Efter national lovgivning.	Behandling af nationale id-numre med henblik på statistiske eller videnskabelige undersøgelser.
Videregivelse af oplysninger om National ID-nummer. Efter national lovgivning.	Oplysninger om nationale ID-numre kan videregives, når videregivelsen; • er et naturligt led i den normale drift af virksomheder m.v. af den pågældende art, og • når videregivelsen er af afgørende betydning for at sikre en entydig identifikation af den registrerede, eller • videregivelsen kræves af en offentlig myndighed. Hvis navn og fødselsdato er tilstrækkelig identifikation, må national id-nummer ikke videregives.

3.4 BEHANDLINGSGRUNDLAG FOR STRAFFEDOMME OG LOVOVERTRÆDELSER	
Behandlingsgrundlag	Anvendelsesområde (ikke udtømmende)
Lovhjemmel. Databeskyttelsesforordningens artikel 10.	Hvis det følger af lovgivningen, at den dataansvarlige har ret til at behandle personoplysninger om straffedomme og lovovertrædelser. F.eks. i forbindelse med indhentelse af lovpligtige børneattester.