

PERSONDATAPOLITIK

Solstrålen Privat Børnehave behandler de indsamlede personoplysninger i overensstemmelse med en række principper for behandlingen af personoplysninger, hvilket følger af Databeskyttelsesforordningens artikel 5 samt i overensstemmelse med kravet til fornøden behandlingssikkerhed, der følger af Databeskyttelsesforordningens artikel 32, jf. artikel 5, stk. 1, litra f.

God databehandlingskik

De personoplysninger, som Solstrålen Privat Børnehave behandler, vil blive behandlet lovligt, rimeligt og på en gennemsigtig måde i forhold de registrerede, således at kravet om god databehandlingskik overholdes.

Princippet følger af Databeskyttelsesforordningens artikel 5, stk. 1, litra a.

Solstrålen Privat Børnehave vil behandle oplysningerne lovligt, idet der alene vil behandles personoplysninger, som hviler på et af følgende behandlingsgrundlag, der følger af Databeskyttelsesforordningens artikel 6, stk. 1, litra a-f:

- Den registreredes samtykke til behandlingen af sine personoplysninger til et eller flere specifikke formål (litra a),
- Behandlingen er nødvendig af hensyn til opfyldelsen af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt (litra b),
- Behandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler Solstrålen Privat Børnehave (litra c),
- Behandlingen er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser (litra d),
- Behandlingen er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som Solstrålen Privat Børnehave har fået pålagt (litra e),
- Behandlingen er nødvendig for, at Solstrålen Privat Børnehave eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn (litra f).

Forinden der foretages nogen form for behandling af personoplysninger, herunder særligt indsamling, vil Solstrålen Privat Børnehave foretage en vurdering af om den pågældende behandling beror på et af de ovennævnte behandlingsgrundlag, idet behandlingen dermed vil være lovlig. I modsat fald vil Solstrålen Privat Børnehave ikke foretage behandlingen, da den vil være ulovlig.

Solstrålen Privat Børnehave har udfærdiget en fortegnelse, der viser den komplette behandling af personoplysninger samt hvilket kilder, de behandlede personoplysninger stammer fra. Behandlingen af disse oplysninger er sikret således, at behandlingen foretages, da behandlingen hviler på et af de ovennævnte behandlingsgrundlag, såsom at de nødvendige personoplysninger om barnet behandles på grundlag af kontrakten om pasningen indgået mellem institutionen og barnets forældre. Øvrige personoplysninger om barnet, der ikke er nødvendigt til opfyldelse af kontrakten, f.eks. portrætbil- leder, der ophænges offentligt i institutionen, samt særligt følsomme personoplysninger, såsom hel- bredsoplysninger, behandles på grundlag af forældrenes samtykke.

Solstrålen Privat Børnehave vil endvidere sikre, at behandlingen foregår på en rimelig og gennem- sigtig måde, således at de registrerede opnår kendskab til en behandlingens eksistens samt bliver behørigt orienteret, når der indsamles oplysninger om dem. Dermed fremsendes bl.a. oplysnings- skrivelser efter henholdsvis artikel 13 og 14 til de registrerede, der gives meddelelse til personale m.v. om bl.a. overvågning af internethistorik samt e-mails, der foretages om nødvendigt underret- ning af de berørte registrerede ved et eventuelt sikkerhedsbrud samt foretages underretning til de berørte, såfremt der sker en utilsigtet offentliggørelse af personoplysninger på internettet.

Særligt i forhold til brud på persondatasikkerheden, vil Solstrålen Privat Børnehave anmelde dette til Datatilsynet uden unødigt forsinkelse og om muligt senest 72 timer efter, at være blevet bekendt med bruddet. Såfremt bruddet på persondatasikkerheden vurderes, at vil indebære en høj risiko for de registrerede, vil Solstrålen Privat Børnehave i udgangspunktet underrette disse herom uden unø- dig forsinkelse.

Solstrålen Privat Børnehave vil dermed gøre det gennemsigtigt for de pågældende fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles, og i hvilket omfang personoplysningerne behandles eller vil blive behandlet. Information og kommu- nikation til de registrerede herom vil være lettilgængelig og blive præsenteret letforståeligt, da Sol- strålen Privat Børnehave vil benytte et klart og enkelt sprog.

Princippet om formålsbestemthed samt finalité

Solstrålen Privat Børnehave vil alene indsamle personoplysninger til udtrykkeligt angivne og sag- lige/legitime formål, dvs. specificerede, udtrykkelige og saglige/legitime formål (princippet om for- målsbestemthed), hvor der ikke vil blive foretaget en senere behandling, som måtte være uforenelig med de formål, som personlysninger oprindeligt var indsamlet til (finalitéprincippet). Dette uanset om personoplysninger er indsamlet direkte hos den registrerede eller hos tredjemand.

Princippet følger af Databeskyttelsesforordningens artikel 5, stk. 1, litra b.

Dermed vil Solstrålen Privat Børnehave altid fastlægge til hvilket formål indsamlingen finder sted. Fastlæggelsen af formålet vil blive tilstrækkeligt veldefineret og velafgrænset, således at formålet vil være så åbenbart og udtrykkeligt, at de involverede har den samme utvetydige forståelse af formå- let.

Fastlæggelsen af formålet vil indledningsvist defineres i fortegnelsen, men vil ligeledes også blive defineret og afgrænset i bl.a. samtykkeerklæringen samt oplysningsskrivelsen til de registrerede.

Behandlingen vil altid varetage et sagligt/legitimt formål, dvs. at Solstrålen Privat Børnehave forinden behandlingen vil foretage en konkret vurdering i forhold til om behandlingen falder inden for Solstrålen Privat Børnehave kompetenceområde eller lovlige forretningsområde, som er drift af daginstitution, dvs. pasning af børn.

Solstrålen Privat Børnehave vurdering af om en senere behandling vil være i strid med finalitéprincippet, vil bero på alle relevante omstændigheder, herunder:

- Forholdet mellem det oprindelige formål og genbehandlingsformålet, dvs. i hvilken grad formålet med den nye brug af personoplysningerne adskiller sig fra det formål, der blev specificeret ved oplysningernes indsamling,
- Sammenhængen hvori personoplysningerne er blevet indsamlet, herunder om behandlingen af personoplysningerne foretages på samme behandlingsgrundlag,
- Hvorvidt den registrerede med rimelighed måtte forvente en genbehandling,
- Typen af personoplysningerne, herunder særligt om der er tale særlige kategorier af personoplysninger i henhold til Databeskyttelsesforordningens artikel 9 eller artikel 10,
- Hvilken indflydelse, som en genbehandling vil få for den registrerede,
- Hvorvidt det vil være forbundet med stor ulempe, at indhente et nyt samtykke til genbehandlingen,
- Hvilken indflydelse, som en genbehandling vil få for sikkerhedsgarantierne, som Solstrålen Privat Børnehave har vedtaget for at sikre en rimelig behandling og for at hindre unødigt indvirkning på den registrerede, herunder særligt om datakvaliteten forringes,
- Hvorvidt genbehandlingen sker til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål.

En senere behandling af de pågældende personoplysninger til arkivformål i samfundets interesse, til videnskabelige formål eller historiske formål eller til statistiske formål, vil Solstrålen Privat Børnehave ikke anse for, at være uforenelige med det formål, som oplysningerne oprindeligt blev indsamlet til.

Endvidere vil en senere behandling af personoplysningerne på baggrund af den registreredes samtykke hertil eller i medfør af henholdsvis EU-ret eller national ret, ikke blive anset for uforenelig.

Såfremt Solstrålen Privat Børnehave finder, at der kan foretages en senere behandling af personoplysningerne, vil Solstrålen Privat Børnehave forud for viderebehandlingen, give den registrerede oplysninger om det nye formål og andre relevante yderligere oplysninger efter Databeskyttelsesforordningens artikel 13, stk. 3, jf. stk. 2 samt artikel 14, stk. 4, jf. stk. 2.

Princippet om dataminimering

Solstrålen Privat Børnehave vil alene behandle personoplysninger, der findes at være tilstrækkeligt, relevante og begrænset til det formål, som oplysningerne er indsamlet til.

Princippet følger af Databeskyttelsesforordningens artikel 5, stk. 1, litra c.

Dermed vil Solstrålen Privat Børnehave foretage en konkret vurdering, hvorvidt behandlingen af de pågældende personoplysninger er i overensstemmelse med princippet om dataminimering, hvilket vil bero på en proportionalitetsafvejning.

Princippet om rigtighed

Solstrålen Privat Børnehave vil tilrettelægge behandlingen af personoplysningerne således, at der foretages en fornøden ajourføring af oplysninger, dermed forstået, at Solstrålen Privat Børnehave vil tage ethvert rimeligt skridt for, at sikre en kontrol af, at der ikke behandles urigtige eller vildledende/ufuldstændige oplysninger i forhold til det formål, hvortil de behandles. Dermed stiller Solstrålen Privat Børnehave krav til datakvaliteten i forbindelse med behandlingen af personoplysningerne.

Princippet følger af Databeskyttelsesforordningens artikel 5, stk. 1, litra d.

Solstrålen Privat Børnehave vil regelmæssigt foretage fornøden kontrol for at sikre, at der ikke registreres urigtige eller vildledende/ufuldstændige oplysninger, og at der snarest muligt foretages sletning eller berigtigelse, såfremt det viser sig, at Solstrålen Privat Børnehave har behandlet urigtige eller vildledende/ufuldstændige oplysninger, medmindre der er et behov for fortsat opbevaring, hvilket fx kan være offentlighedslovens § 15.

Karakteren af de personoplysninger, deres anvendelse samt indsamlingens pålidelighed, vil afgøre omfanget af og hvor ofte at den interne kontrol er nødvendig, dog således, at ajourføring foretages umiddelbart efter, at et behov herfor er konstateret, uanset tidspunkt for den førstkommande normale ajourføring.

Den normale ajourføring vil foretages hver tredje måned, da bl.a. karakteren af personoplysningerne ikke nødvendiggør en oftere intern kontrol samt at indsamlingen har en høj pålidelighed, da personoplysningerne indsamles direkte hos de registrerede, hvor det formodes, at disse foretager en henvendelse til Solstrålen Privat Børnehave, hvis der sker ændringer i deres personoplysninger, fx skift af bopælsadresse.

Den interne ajourføring vil ske i form af udfyldning af en compliance analyse.

Såfremt Solstrålen Privat Børnehave konstaterer urigtige eller vildledende/ufuldstændige personoplysninger, vil disse blive slettet straks, medmindre at Solstrålen Privat Børnehave er pålagt, at opbevare disse oplysninger, som følge af f.eks. offentlig lovgivning.

Solstrålen Privat Børnehave vil foretage sletningen i overensstemmelse med Datatilsynets IT-sikkerhedstekst ST3, dvs. personoplysningerne uigenkaldeligt fjernes fra alle lagringsmedier, hvorpå de har været lagret således, at personoplysningerne på ingen måde kan genskabes.

Princippet om opbevaringsbegrænsning

Solstrålen Privat Børnehave vil ikke opbevare personoplysninger i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles, dog således, at en fortsat opbevaring kan forekomme, såfremt behandlingen sker til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger.

Princippet følger af Databeskyttelsesforordningens artikel 5, stk. 1, litra e.

Solstrålen Privat Børnehave vil foretage en konkret vurdering af hvilket tidsrum, der er nødvendigt at opbevare personoplysninger sammenholdt med det formål, hvortil oplysningerne er indsamlet.

Dog vil personoplysningerne blive slettet efter en absolut frist på 10 år efter indsamlingen, medmindre oplysningerne skal benyttes af dokumentationsmæssige årsager, fx Arkiv- eller bogføringsloven, eller som følge af andre forhold. Dette som følge af, at den normale absolutte forældelsesfrist udgør 10 år ifølge forældelseslovens § 3, stk. 2.

Solstrålen Privat Børnehave vil løbende gennemgå sine arkiver for, at kontrollere, at der ikke opbevares personoplysninger, som vil være i strid med princippet om opbevaringsbegrænsningen.

Den sædvanlige gennemgang vil foretages af Solstrålen Privat Børnehave hver tredje måned, dvs. kvartalsvis, henset til at karakteren af personoplysningerne samt de implementerede tekniske og organisatoriske foranstaltninger ikke nødvendiggør en oftere gennemgang.

Den interne ajourføring vil ske i form af udfyldning af en compliance analyse.

Såfremt Solstrålen Privat Børnehave modtager en anmodning fra de registrerede om bl.a. sletning, vil gennemgangen foretages uden unødigt forsinkelse, dog i udgangspunktet senest en måned efter modtagelsen af anmodningen i overensstemmelse med Databeskyttelsesforordningens artikel 12, stk. 3.

Såfremt der findes personoplysninger, der opbevares i strid med princippet, vil Solstrålen Privat Børnehave foretages sletning af oplysningerne i overensstemmelse med Datatilsynets IT-sikkerhedstekst ST3, dvs. personoplysningerne uigenkaldeligt fjernes fra alle lagringsmedier, hvorpå de har været lagret således, at personoplysningerne på ingen måde kan genskabes.

Princippet om behandlingssikkerhed

Solstrålen Privat Børnehave vil behandle personoplysningerne på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger.

Princippet om behandlingssikkerhed er præciseret i Databeskyttelsesforordningens artikel 32, jf. 5, stk. 1, litra f.

Solstrålen Privat Børnehave har vurderet, at en passende behandlingssikkerhed opnås ud fra en kombination af henholdsvis tekniske og organisatoriske foranstaltninger.

Tekniske foranstaltninger

a. Adgangskode

I forhold til de *tekniske foranstaltninger* implementeres en procedure for udformningskrav og periodiskift for den adgangskode, som det autoriserede personale benytter, som adgangsnøgle til de behandlede personoplysninger. Dette med henblik på, at opnå den bedst mulige behandlingssikkerhed og dermed fx undgå et Brute-Force-angreb.

Det autoriserede personale skal selv vælge deres adgangskode til det elektroniske system, men denne skal udformes således, at den ikke vil være forudsigelig, hvorfor adgangskoden skal opfylde følgende krav i overensstemmelse med Datatilsynets IT-sikkerhedstekst ST10:

- Koden skal have en minimumslængde på 10 tegn,
- Koden skal minimum indeholde et stort bogstav, et lille bogstav, et tal samt et specialtegn, fx #%&=+?§,
- Koden skal bestå af forskellige tegn, altså må det samme tegn ikke indgå i koden,
- Koden må ikke være identisk med den ansattes bruger-id, navn, adresse, fødselsdato, børn eller lignende forudsigelige indikatorer,
- Koden må ikke være identisk med en tidligere anvendt kode,
- Koden skal skiftes mindst hver 3 måned,
- Koden må ikke være nedskrevet fysisk eller elektronisk i nærheden af computeren,
- Koden må ikke auto-huskes i form af visse login-funktioner, fx "Husk mit login" eller "Keep me logged in".

Mnemoteknik kan hjælpe med dannelsen af tilpas komplekse adgangskoderkoder. Eksempelvis kan man anvende:

- Det første bokstav i ordene fra en sætning.
- Anvende store bokstaver ved navneord.
- Anvende tal til at erstatte dele af ord (entreprenør = en tre pr en ør = 13pr1ør)

b. Brugerprofiler

For at sikre imod brud på persondatasikkerheden, har ansatte en individuel brugerprofil med tilknyttet adgangskode til hhv. computere, servere og visse programmer.

Solstrålen Privat Børnehave skal føre logning af brugernes aktiviteter, så bl.a. brud på persondatasikkerheden lettere kan identificeres. Anvendelse af fællesbrugere forbydes dermed, da eventuelle sikkerhedsbrud ikke vil kunne forebygges præventivt.

Førnævnte logning omfatter brugeres aktiviteter, anormaliteter og hændelser, der relaterer sig til sikkerhed. Logningen gemmer hændelser over en løbende periode, som ikke oversiger seks måneder, medmindre dette er krævet efter lovgivningsmæssige forpligtelser. Som minimum skal logningen omfatte det enkelte brugernavn samt dato og klokkeslæt for adgangens begyndelse og

afslutning. I visse tilfælde vil de aktiviteter, som brugeren foretager sig og typen af data, der er blevet tilgået og/eller ændret være nødvendige at opbevare.

Brugere skal informeres om foretagelsen af logning. Logningsudstyret og –informationerne er sikret ved at være utilgængelig for de personer, hvis brugere logges. Det er således alene autoriserede personer, der har adgang til logfilerne. Der foretages en gennemgang af de loggede informationer med henblik på at finde anormaliteter, såfremt der er en begrundet mistanke om anormaliteter.

Solstrålen Privat Børnehave sikrer, at de ansattes adgang til elektronisk opbevarede personoplysninger vil blive begrænset ud fra en nødvendighedsafvejning, således at en ansat med sin brugerprofil kun får adgang til de personoplysninger, som den givne ansatte har brug for i forhold til dennes arbejde. En bruger gives ikke flere rettigheder, end denne behøver for at varetage sine pligter. Ved ophør af behovet for at kunne tilgå et barns fulde oplysninger, vil adgangsretten blive fjernet helt eller begrænset således, at den ansatte fortsat kun har adgang til de nødvendige personoplysninger.

Med henblik på at sikre arbejdsstationer anvendes der en automatisk log-ud funktion, når en computer ikke har været anvendt i [indsæt minutter] minutter.

c. IT-sikkerhedsprogrammer m.v.

Solstrålen Privat Børnehave beskytter tillige personoplysninger ved kontinuerligt, at opdatere henholdsvis firewall og antivirus, hvormed sikres, at udefrakommende fjendtlige angreb forhindres, da IT sikkerheden dermed er bedst muligt rustet mod nye IT trusler. Hvor det er muligt, konfigureres programmer således, at der sker automatisk opdatering af sikkerhedssoftware.

Ved anvendelse af fjernkontrolsprogrammer, såsom TeamViewer, skal brugeren samtykke til fjernkontrollen forinden denne etableres. Brugeren skal være i stand til at identificere fjernkontrollens ophørstidspunkt. Det er forbudt at anvende downloadet software, som ikke kommer fra en sikker kilde.

d. Mobilt udstyr

For at mindske muligheden for brud på persondatasikkerheden må mobilt udstyr, som eksterne harddiske og USB-pinde, kun anvendes i begrænset omfang. Autorun for flytbare medier skal være slået fra. Mobilt udstyr krypteres, når dette er muligt.

Ved transmission mellem samarbejdspartnere krypteres mobilt udstyr altid, inden der sker en overdragelse af personoplysninger via disse. Personoplysninger, der sendes elektronisk, beskyttes alt efter deres karakter ved f.eks. kodeord og/eller kryptering. Et kodeord sendes når muligt via en anden kanal end den krypterede eller kodelåste data.

Arbejdstelefoner er sikret med sim-kode, automatisk skærmlås og yderligere kode for at låse denne op. Såfremt der er en sandsynlighed for modtagelse af følsomme personoplysninger, sikres der yderligere kodebeskyttelse for adgang til f.eks. e-mail og "downloadede filer"-mappen.

e. Hjemmearbejdspladser

For at sikre hjemmearbejdspladser må der alene anvendes arbejdscomputere til behandling af personoplysninger. Filer gemmes for så vidt muligt på Solstrålen Privat Børnehaves server, som er tilgængelig via fjernadgang. Kun undtagelsesvist gemmes filer direkte på arbejdscomputere. Gemmes filer lokalt på arbejdscomputere, skal disse krypteres.

For at beskytte det interne netværk er alle trådløse netværk sikret med kryptering (WPA2 eller WPA2-PSK med en komplekst adgangskode). Netværk der er åbne til gæsteb brug er separeret fra det interne netværk.

c. Backup

Der vil løbende blive foretaget backup af de behandlede personoplysninger, hvormed at adgangen til personoplysningerne kan genoprettes inden for et kortere tidsrum i tilfælde af hændelser, så som brand, hacking, ransomware eller overgravede datakommunikationskabler.

Ovenstående samt øvrige tekniske foranstaltninger vil implementeres af tredjepart, såsom LDD, og vil beskrives af disse, hvorfor deres beskrivelse udgør et tillæg til nærværende persondatapolitik. LOU advokatfirma har ikke medvirket til udfærdigelsen eller implementeringen af ovennævnte foranstaltninger, hvorfor der henvises til tredjepart herom.

Organisatoriske foranstaltninger

a. Begrænset autoriseret personale

I forhold til de *organisatoriske foranstaltninger* implementeres forskellige adgangsniveauer for personalet, hvormed sikres, at ansatte alene har adgang til de personoplysninger, som er nødvendigt for, at udføre deres arbejde. Dermed er det alene bestemte medarbejdere, som har fuld adgang til de behandlede personoplysninger, altså begrænset autoriseret personale. Dette vil f.eks. være i forhold til behandlingen af forældrenes CPR-nr., der ikke behøves at være kendt af samtlige ansatte, hvorfor disse oplysninger alene må kendes og tilgås af lederen samt en stedfortræder. Ligeledes med de ansattes oplysninger, såsom ansættelseskontrakt, MUS-samtaler, sygdomshistorik, lønsedler m.v.

b. Aflåsning af fysisk materiale

I den henseende vil personoplysninger, der behandles, aflåses fysisk, medmindre at det er nødvendigt for institutionens drift, at have oplysningerne offentlig i institutionen eller som følge af indhentet samtykke fra de registrerede. Aflåsningen vil foretages i skabe, hvor der vil være henholdsvis et ledelsesskab samt et skab til de øvrige medarbejdere således, at det førnævnte princip om begrænset autoriseret personale overholdes. Personoplysninger, der vil være nødvendig at have offentlig i institutionen er f.eks. fremmøde lister, hvilket er af hensynet til brandmyndighederne, der skal bruge de pågældende lister i tilfælde af brand.

De personoplysninger, der opbevares og behandles i institutionen, som henset til deres formål ikke kræver offentliggørelse eller videregivelse til besøgende, behandles og opbevares udelukkende i rum som hverken børn, forældre eller andre besøgende ikke har adgang til eksempelvis et personalerum eller kontor.

Med henblik på bl.a. at sikre imod brud på persondatasikkerheden holdes der en liste over alle personer, som besidder nøgler til præmiserne. Alle døre, der giver adgang til præmiserne, låser automatisk når døren lukker, bortset fra døren i hovedindgangen i åbningstiden.

c. Medarbejdere underlagt tavshedspligt

Derudover vil samtlige medarbejdere blive underlagt tavshedspligt i forhold til de personoplysninger, som de ansatte opnår kendskab til, som led i deres arbejde.

d. Løbende instruktion/oplæring i GDPR

Der vil løbende afholdes kursuser i Databeskyttelsesforordningen og dens krav for, at højne de ansattes viden herom. Dette ud fra tankegangen, at ingen kan overholde det, som de ikke ved hvad er. Solstrålen Privat Børnehave vil derfor sikre, at samtlige allerede ansatte medarbejdere samt fremtidige vil modtage information og oplæring om Databeskyttelsesforordningen på et overordnet niveau, herunder information om institutionens persondata- og sikkerhedsbrudspolitik.

e. Clean Desk Policy

Solstrålen Privat Børnehave vil ligeledes implementere clean desk policy, dvs. at samtlige personoplysninger vil blive arkiveret i et aflåst arkivskab ved arbejdsdagens ophør, som kun autoriseret personale har adgang til, således at rengøringspersonale eller øvrigt uautoriseret personale ikke vil kunne få fysisk adgang til personoplysningerne.

f. Gæster m.v.

Besøgende som gæster har kun Solstrålen Privat Børnehaves lokaler via hovedindgangen, hvor gæster typisk vil blive mødt af en ansat. Det tillades ikke, at udefrakommende vandrer frit på præmiserne uden opsyn.

Reparatører mv. anmodes om at underskrive en tavshedspligtserklæring, såfremt der forelægger en risiko for, at reparatøren i forbindelse med sin reparation får adgang til personoplysninger.

g. Alarmsystemer

Der er yderligere installeret alarmsystem, som ved uretmæssig forsøg på at opnå adgang til institutionen igangsætter alarmer og tilkalder vagter. Alle ansatte er instrueret i, at slå alarmsystemet til når den sidste ansatte forlader præmiserne samt slå systemet fra ved ankomst. Hver ansat har en individuel kode, som kan deaktivere alarmerne.

For at sikre bl.a. imod tab af persondata er der installeret røgalarmer.

h. Hjemmearbejdspladser

Såfremt der benyttes hjemmearbejdspladser, vil Solstrålen Privat Børnehave sikre, at personoplysningerne ikke beskyttes ringere end det niveau, som institutionen har internt f.eks. i forhold til aflåsning m.v. Dermed skal personoplysninger i fysisk format, der er omfattet af forordningen, bl.a. anonymiseres forinden hjembringelsen. Beskyttelsesniveauet skal være tilsvarende højt for transportvejen fra institutionen og til hjemmearbejdspladsen, men ligeledes også for selve arbejdspladsen.

Når der transporteres personoplysninger i ubeskyttede fysiske medier mellem arbejdspladsen og hjem, forretningssteder, samarbejdspartnere m.v., skal de fysiske medier være i den ansattes besiddelse, men ude af syne for uvedkommende. Dette kan ske ved at opbevare disse i en aflåst taske, som ikke lades ude af syne. Alternativt skal de fysiske medier opbevares aflåst og ude af syne for uvedkommende. Dette kan opnås ved at placere de fysiske medier i en taske i bagagerummet af en aflåst bil. Transport af ubeskyttede fysiske medier skal begrænses.

For at sikre, at Solstrålen Privat Børnehave kontinuerligt er i compliance med Databeskyttelsesforordningens krav, vil Solstrålen Privat Børnehave hver tredje måned foretage såvel en ekstern som intern compliance analyse. Dette i form af en skematisk gennemgang af de områder, hvor Databeskyttelsesforordningen stiller krav til Solstrålen Privat Børnehave databehandling af personoplysninger, der er omfattet af forordningen.

Den interne ajourføring vil ske i form af udfyldning af en compliance analyse.

Sikkerhedsbrudsprocedure

Solstrålen Privat Børnehave har indført en "sikkerhedsbrudsprocedure" til håndteringen af brud på persondatasikkerheden. Denne kan findes som bilag 1. For at sikre, at procedurerne kan gennemføres, er der blevet oprettet et responshold, og samtlige medarbejdere er blevet oplært i at identificere brud på persondatasikkerheden samt at følge sikkerhedsbrudsprocedurens krav om at meddele et potentielt brud til responsholdet.

Responsholdets funktion er at vurdere, om der foreligger et brud på persondatasikkerheden og i bekræftende fald at håndtere bruddet i overensstemmelse med Databeskyttelsesforordningens krav herom.

For at dette kan lade sig gøre, skal responsholdet kunne varetage følgende kompetencer:

- Leder, der har direkte kontakt til den øverste daglige ledelse, og er ansvarlig for håndtering af brud på datasikkerheden.
- Projektering, til at koordinerer håndteringsprocessen af et brud.
- Ekspertise indenfor persondata, som kan give holdet den fornødne faglige ekspertise til at følge sikkerhedsbrudsproceduren.
- Viden om virksomhedens drift.
- Adgang til alle fornødne informationer til håndtering af et brud.

En person kan varetage flere af eller alle disse kompetencer.

Her er det leder, der varetager sig af disse

Følgende medarbejder[-e] varetager følgende kompetencer: Leder.

Databeskyttelsesforordningen stiller krav om, at anmeldelse af brud til tilsynsmyndigheden sker uden unødigt forsinkelse og om muligt senest 72 timer. Datatilsynet har i sin vejledning "Vejledning om håndtering af brud på persondatasikkerheden" fastslået, at der ikke tages højde for weekender, helligdage, sygedage eller ferie i denne vurdering.

For at sikre at anmeldelsen kan ske uden unødigt forsikring, består responsholdet af personer, som besidder den fornødne faglige ekspertise til at gennemføre sikkerhedsbrudsproceduren ved brud på persondatasikkerheden. I tilfælde af sygdom eller andet uforudsigeligt fravær, er det sikret, at responsholdet kan komme i kontakt med en ansat der kan sikre responsholdet den fornødne adgang til de oplysninger, som er krævet for at håndtere et brud. Denne kontaktordning sikrer, at proceduren også kan gennemføres i overensstemmelse med lovens krav i tilfælde af sygdom mv.

I tilfælde af at et medlem af responsholdet planlægger at være fraværende, sikrer responsholdet, at det fortsat er kompetente til at håndtere brud. Efter behov tager responsholdets leder kontakt til den øverste daglige ledelse med henblik på at finde en eller flere afløsere.

For at sikre hurtig overholdelse af kravet om anmeldelse og begrænsning af bruddet er der også sikret kontakt til og respons fra:

- IT indenfor maksimalt 24 timer
- HR indenfor maksimalt 24 timer
- Juridisk bistand indenfor maksimalt 24 timer
- Bygningssikkerhed indenfor maksimalt 24 timer
- Ledelse indenfor maksimalt 24 timer

I Solstrålen Privat Børnehave databehandleraftaler sikres det, at:

- databehandleren stiller garanti for at dennes ansatte kan identificere et brud på personsikkerheden.
- databehandleren skal bistå den dataansvarlige i forbindelse med et brud på datasikkerheden. Herunder er databehandleren forpligtet til at følge Lou Advokatfirmas sikkerhedsbrudsprocedure.
- databehandleren skal handle proaktivt, ved straks at indgå dialog med den dataansvarlige med henblik på at præsentere løsningsforslag til at stoppe et brud eller af egen drift straks stoppe et brud, såfremt dette uden konsekvenser kan lade sig gøre.
- databehandleren har pligt til uden unødigt forsinkelse at underrette den dataansvarlige om et brud eller en formodning for brud i overensstemmelse med Databeskyttelsesforordningen.
- databehandleren skal føre fortegnelse over sikkerhedsbrud og hjælpe med at sikre dokumentation. Som minimum skal fortegnelserne indeholde de faktiske omstændigheder ved bruddet, herunder dato og tidspunkt, følgevirkninger af bruddet og de truffe foranstaltninger.

Opdager den ansvarlige for gennemgangen af loggede informationer en anormalitet, giver denne "Responsholdet" besked i overensstemmelse med "Sikkerhedsbrudsproceduren".