Basen
IT-håndbog

Indhold

Informationssikkerhedspolitik for Basen

1. Introduktion

Formålet med denne it-sikkerhedspolitik er at sætte retningslinjerne for hvordan medarbejdere og leverandører skal forholde sig til anvendelsen af it-udstyr, der er ejet af Basen eller er koblet op til Basens it.

Basen ønsker at opretholde og løbende udbygge et it sikkerhedsniveau på højde med de krav, ledelsen sætter, hvilket er at al anvendelse af it skal ske efter 'God it-skik', dvs.;

- Udvikling og opretholdelse af it sker i en samlet proces i tråd med Basens strategiske mål og forretningsstrategi.
- Ansvar for anvendelse og styring er synligt.
- Ledelsen har ansvar for at træffe beslutninger på it-området.
- Alle i Basen skal kende og respektere de regler, der er for anvendelsen af it.
- Alle medarbejdere uddannes til at anvende it korrekt.
- Der etableres sikkerhedsforanstaltninger og beredskabsplaner i overensstemmelse med behov og risici.
- Ændringer planlægges så de sker uden unødige forstyrrelser.

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at Basen fremstår troværdigt samt at elever og forældre kan være trygge ved Basens behandling af deres følsomme oplysninger. Det er altafgørende for Basen at oplysninger om Basens elever opbevares fortroligt, samt at oplysninger til en hver tid er korrekte.

Disse mål er kommunikeret til vores medarbejdere og er indarbejdet i vores aftaler med leverandører.

2. Risikovurdering

Ledelsen skal mindst hvert år sikre sig, at risikovurderingen vedrørende it-anvendelsen i virksomheden er opdateret og afspejler de reelle trusler mod virksomheden, samt vurdering af risici for registrerede ifm. virksomhedens behandling af persondata.

Ledelsen skal periodisk sikre sig, at de implementerede kontroller og processer virker efter hensigten. Til sikring af dette, er der udarbejdet et årshjul, som indeholder en række kontroller til at sikre at kravene i informationssikkerheds- og GDPR-politikken overholdes, samt generel efterlevelse af GDPR, databehandleraftaler og god IT-skik.

3. Implementerede sikkerhedsforanstaltninger

Hos Basen har vi på baggrund af risikovurderingen, besluttet at implementere it-sikkerhedsregler:

3.1 Tekniske sikkerhedsforanstaltninger

- Anti-virus:

    - Der er Sophos Intercept X på servere.
    - Der Windows Defender på alle klienter

- Firewall:
    - Der er installeret FortiGate-60F generation firewall på filservere.
    - De fire lokationer har hver sin VPN og disse er samlet ind til CuraIT.
    - IDS- og IPS-funktionalitet er aktiveret i firewallen.
    - Nogle medarbejdere kan tilgå filserver hjemmefra via VPN.

- Kryptering:
    - Der er installeret 'Send sikkert'/SEPO funktion i O365 som sikre tunnelkryptering.

- Logning:
    - Der logges i SkoleIntra hvem, der har tilgået filerne online.
    - MS-aktivitets-/systemlog på filserver.
    - Der er logning i OneDrive.
    - Der er implementeret Follow-me print ved Papercut Hive

- Patching:
    - Opdateringer rulles på månedligt efter patch tuesday og genstartes herefter. Dette sikrer at der altid er nyeste version.
    - Klienter er sat op til automatisk opdatering.
    - Printserver bliver manuelt opdateret af IT-leverandør.

- Backup og genetablering
    - Der tages dagligt backup af filserveren.
    - Der er dagligt backup på O365 programmer.
    - Der sker backup af printserveren ca. en gang om året (dette gøres primært for at kunne skabe hurtig reetablering, men er ikke forretningskritisk.
        - Det valideres en gang årligt (1. juni) at backuppen kan anvendes til at genskabe systemerne rettidigt

3.2 Adgangsstyring

- Medarbejderes adgang til it-systemer og data er altid baseret på et arbejdsbetinget behov og være godkendt af relevant leder.
- Alle medarbejdere er oprettet med egen konto til systemer og denne må ikke deles med andre.
- Alle brugere er tildelt roller ud fra deres arbejdsbetinget behov.

- Det er kun få lokale medarbejdere (superbrugere), som er lokaladministratorer. Dette betyder at lærere ikke selv kan installere programmer, men skal kontakte den lokale superbruger, som kan installere hvis det er et godkendt program. Ved tvivl kontaktes IT-leverandør.

- Det er påkrævet at den ansatte skifter passwordet som det første når Pc'en overdrages.
- Adgangskoder til pc'er skal være:
    - Mindst 8 karakterer

    - Mindst 3 ud af følgende 4 krav opfyldt:
        - Et lille bogstav
        - Et stort bogstav
        - Et tal
        - Et speciel tegn fx !"#¤%&/()=?

- Mobiltelefoner skal være sikret mod at uvedkommende får adgang via PIN kode, 4 tegn eller adgangskode og evt. fingeraftryk.

- Tildeling af adgange: Ved opstart af nye ansatte kontaktes økonomichef, Henrik Thorning, som kontakter IT for oprettelse af medarbejderen.

- Ved opsigelse af medarbejder: IT informeres, herefter skiftes adgangskode til brugeren og denne beholdes aktiv i 30 dage. Herefter slettes bruger, hvor der så er 30 dage til restore af backup.

3.3 Organisatoriske foranstaltninger

- Alle nye medarbejdere bliver introduceret til informationssikkerhedspolitikken og relevante procedurer for databehandling. Relevant dokumentation sendes til den nye ansættelse ved opstart.
- I forbindelse med ansættelse udføres der efterprøvning af medarbejdere som omfatter:
    - Referencer fra tidligere ansættelser
    - Straffeattest
    - Børneattest
- Alle medarbejdere er underlagt tavshedspligt via deres ansættelseskontrakt. Tavshedspligten gælder også efter endt ansættelsesforhold.
- Ved fratrædelse inddrages aktiver og alle brugerens adgange og rettigheder til systemer fjernes eller bliver gjort inaktive.
- Der gennemføres løbende awareness-træning, hvor medarbejdere bliver undervist i regler for it-sikkerhed samt regler for behandling af persondata.

3.4. Fysisk sikkerhed

- Servere hos GlobalConnect i Tåstrup, som har høj fysisk sikkerhed. Der udarbejdes årligt erklæring på datacentret. Backup ligger i andet datacenter hos GlobalConnect.
- O365 (Onedrive mv.) hostes af MS, der er valgt EU region til placering af data.
- Der er lås på døren samt aktiveret alarm udenfor åbningstiden på kontorer og lokationer
- Der er skærmlås på klienterne på 10 min.
- Der er opsat makuleringscontainere, som skal benyttes til destruktion af fortrolige og personoplysninger.
- Ved udfasning af bærbare destruerer it-leverandøren harddiske og bekræfter serienumre på destruerede klienter.

4. Drift af it

- Der er indgået en aftale med CURAit vedrørende drift af server.

- Outsourcing af it-drift dokumenteres i forhold til aftale og der fremstilles hvert år en erklæring eller udtalelse, der verificerer, at 'God it Skik' og kontrakten overholdes.
- Overvågning af it-leverandører sker løbende af kontaktpersonen og rapporteres til ledelsen.

IT-kontakt	**Sekundær IT-kontakt**
Philip Dysted Frank Email: phf@basen.dk Tlf: 7192 0636	CuraIT Tlf: 70 22 35 45

5. Overholdelse af lovgivning

- Alle medarbejdere er ansvarlige for at de i deres daglige virke er med til at overholde gældende lovgivning.
- Det er ledelsens ansvar at oplyse medarbejderne om hvordan de skal overholde lovgivningen.
- Hvis en medarbejder ikke overholder de fastlagte retningslinjer, kan det føre til sanktioner mod den ansatte.

GDPR

1. Hvad er persondata?

Persondata er enhver form for information, der kan henføres til en bestemt person – det gælder også film, fotos mv.

Persondata kan endvidere opdeles i følgende kategorier:

Almindelige personoplysninger:
Navn, adresse, telefonnummer, e-mail, fødselsdag, økonomi, skat, gæld, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato, stilling, arbejdsområde, arbejdstelefon mv. Under de almindelige personoplysninger ligger også cpr-nummeret og evt. strafferetslige forhold, som dog samtidig skal behandles fortroligt.

Følsomme personoplysninger:
Fx race, etnisk oprindelse, religiøs, filosofisk overbevisning, fagforening, genetiske data, helbredsoplysninger, seksuelle forhold eller orientering mv.

Basen håndterer både almindelige personoplysninger, herunder CPR-numre, samt følsomme personoplysninger i forbindelse med skole og dagbehandlingstilbud. Oplysningerne er nødvendige for at Basen på bedst mulig vis kan faciliterer læring, som udvikler eleven socialt, personligt, og fagligt med henblik på at mestre eget liv.

3. Basen som dataansvarlig

Når Basen er dataansvarlig, betyder det, at Basen fastlægger formålet med de persondata, vi opbevarer og behandler. I Basen har vi som dataansvarlig to typer persondata:

1. Persondata om medarbejdere, herunder ansøgere, ansatte og fratrådte.
2. Persondata, der vedrører kunder, samarbejdspartnere og leverandører, dvs. kontaktpersoner.

3.1 Behandling af persondata om ansatte

Når medarbejdere bliver ansat i Basen, oprettes en personalesag med medarbejderens oplysninger. I personalesagen registreres og opbevares de oplysninger, herunder personoplysninger, som er nødvendige og relevante i forhold til medarbejderens ansættelse hos Basen.

3.2 Oplysninger om kontaktpersoner og leverandører

Basen kommer typisk kun i kontakt med kontaktpersoner og leverandørers personoplysninger, når vi modtager dem selv eller finder dem i offentligt tilgængelige oversigter som fx telefonnumre på hjemmesider mv.

Der vil typisk være tale om almindelige jobmæssige kontaktinformationer, hvor deling ikke vurderes at udgøre en risiko for den pågældende.

Oplysninger om kontaktpersoner og leverandører mv. opbevares på administrations-fildrevet og slettes løbende, når der ikke længere er behov for disse. Oplysningerne beskyttet iht. Basens IT-sikkerhedspolitik.

4. Basen som databehandler

Basen tilbyder skole- og dagbehandlingstilbud for normaltbegavede børn og unge med særlige udfordringer som autismespektrumforstyrrelser, angst, OCD, depression, isolationsproblematikker, skolevægring eller andre psykiatriske vanskeligheder samt ADHD.

Basens kerneopgave er at facilitere læring, der udvikler eleven socialt, personligt og fagligt med henblik på at mestre sit eget liv.

Elever på Basen dækker 4.-10. klasse. Basen har lokationer på Østerbro, i Birkerød under navnet Basen Nord, samt i Odense og Taastrup.

Visitering til Basen går via egen sagsbehandler og/eller den lokale PPR (Pædagogisk Psykologisk Rådgivning) i den kommune eleven bor i, som vurderer behovet for skole/dagbehandling. Dette betyder, at Basen er databehandler for den pågældende Kommune, som er dataansvarlig, dog kun i det omfang det vedrører elevens trivsel og overordnede udvikling, som beskrevet i hovedaftalerne med kommunerne. Basen er selv dataansvarlig for de oplysninger, der genereres via undervisning, for eksempel i læringsportaler.

Hvor Basen er i rollen som databehandler følges nedenstående retningslinjer.

4.1 Indgåelse af databehandleraftaler

Når Basen skal behandle persondata på vegne af en dataansvarlig, skal det som det første sikres, at der er indgået en databehandleraftale mellem den dataansvarlige og Basen.

Når Basen har modtaget en databehandleraftale fra den dataansvarlige, gennemgås denne af økonomichefen og it-konsulenten, som sikre, at Basen kan leve op til den givne instruks, herunder instruksen stemmer overens med Basens informationssikkerhedspolitik, procedurer og sikkerhedsforanstaltninger.

Hvis der er krav om sikkerhedsforanstaltninger el.lign. som ikke svarer til Basens nuværende setup skal det vurderes og drøftes med den dataansvarlige om krav skal undgå eller om Basen kan håndtere kravet på kraven. Som udgangspunkt ændres der dog ikke i Basens setup for at imødekomme enkelte aftaler. Hvis Basen ikke modtager en databehandleraftale, behandles persondata alligevel iht. Basens politikker og procedurer.

Ved indgåelse af kontrakt og databehandleraftale, skal det desuden sikres, at den ønskede databehandling er lovlig. Hvis Basen får instruks om behandling af persondata, som ikke vurderes lovlig, skal den dataansvarlige kontaktes hurtigst muligt.

4.2 Behandling af persondata på vegne af den dataansvarlige

Basen behandler kun persondata efter instruks fra den dataansvarlige. Personoplysninger, som modtages og udarbejdes ift. leverance af skole- og dagsbehandlingstilbud, bliver udelukkende brugt til at facilitere læring, der udvikler eleven socialt, personligt og fagligt.

Oplysninger opbevares udelukkende i de systemer og lokationer, som fremgår af databehandleraftaler eller på anden vis, er godkendt af den dataansvarlige.

Personoplysninger, som behandles i forbindelse med skole- og dagsbehandlingstilbud, bliver i udgangspunktet behandlet og opbevaret på følgende måde:

Indskrivning af nye elev:

Ved potentielle nye elever modtager Basen sagsakter og andet relevant materiale om eleven til at vurdere, om Basen vil være et godt sted for ham/hende at starte. Hvis de er et match, udfyldes stamkort og eleven oprettes i relevante systemer.

Behandling og undervisning:

Ifm. elevers forløb hos Basen udarbejdes og indsamles oplysninger om eleverne med henblik på at yde den bedst mulige behandling og undervisningsforløb for den enkelte. Dette indebærer bl.a. månedsstatusser og statusrapporter, mål og planer for uddannelse og udvikling samt kommunikation til sagsbehandler og forældre.

VISO:

Basen leverer rådgivning og/eller udredning eller bistand til udredning under VISO på vegne af Socialstyrelsen. I forbindelse med et VISO-forløb behandles persondata om borgeren.

4.3 Sikkerhedsforanstaltninger

I forbindelse med behandling af persondata er der implementeret en række sikkerhedsforanstaltninger ud fra en risikovurdering. Disse er beskrevet i Basens IT-sikkerhedspolitik.

For al opbevaring og behandling på vegne af dataansvarlige gælder herunder at:

1. Adgang til personoplysninger er begrænset til medarbejdere med et arbejdsbetinget behov.
2. Personoplysninger skal være korrekte og opdateres efter behov.
3. Personoplysninger på elever behandles så længe denne går hos Basen. Når en elev stopper, slettes data om eleven efter en vis periode.
4. Det skal til enhver en tid være muligt for registrerede at få oplyst hvilke personoplysninger, Basen opbevarer og formålet hermed.

Alle medarbejdere som behandler persondata på vegne af dataansvarlige er blevet introduceret til og skal arbejde iht. denne politik, samt Basens IT-sikkerhedspolitik. Medarbejdere har desuden modtaget undervisning i korrekt behandling og håndtering af persondata. Alle medarbejdere er hertil underlagt tavshedspligt iht. deres ansættelseskontrakter.

4.4 Sletning

Basen sletter persondata iht. krav i databehandleraftaler med dataansvarlige. Hvis der i databehandleraftalen ikke er angivet krav til sletning, opbevares oplysningerne om eleven, så længe denne er tilmeldt Basen og op til 24 mdr. efter eleven stopper. Data opbevares efter eleven er stoppet for at kunne dokumentere elevens forløb og beslutninger truffet om eleven, hvis det bliver nødvendigt.

Sletning vil herefter ske medmindre sletningen vil forårsage, at Basen bryder gældende lovgivning i EU eller national lovgivning. I så fald oplyses dataansvarlige om dette.

5. Brug af databehandlere og underdatabehandlere

Basen benytter en række databehandlere og underdatabehandlere til indsamling, opbevaring, behandling og sletning af personoplysninger.

I forbindelse med anvendelse af databehandlere, hvor Basen er dataansvarlig sikres det, at databehandlere overholder denne politik og gældende lovgivning.

Basen benytter også en række underdatabehandlere ifm. skole- og dagtilbud for elever som er visiteret af en dataansvarlig kommune. Her benyttes underdatabehandlere til behandling af persondata på vegne kommunen. Se afsnit 5.1 for procedurer ift. dette.

Der foretages en risikovurdering af alle databehandlere og underdatabehandlere og gennemføres løbende og mindst en gang årligt tilsyn med data- og underdatabehandlere. Tilsynet med sker enten via spørgsmål til leverandøren eller ved indhentning og gennemgang af relevante erklæringer.

5.1 Anvendelse af underdatabehandlere på vegne af dataansvarlige

Basen benytter en række faste underdatabehandlere til behandling af persondata på vegne af de dataansvarlige. Ifm. kontraktindgåelse er der indgået databehandleraftaler med disse underdatabehandlere, hvor det er sikret, at de lever op til det samme beskyttelsesniveau, som det der er aftalt med den dataansvarlige. Underdatabehandlere fremgår i oversigten i årshjulet.

Ved indgåelse af nye databehandleraftaler sikres det, at alle anvendte underdatabehandlere, fremgår af databehandleraftalen med den dataansvarlige eller er på anden specifikt eller generelt godkendt af den dataansvarlige.

Der følges løbende og mindst en gang årligt op på, at underdatabehandlere fortsat efterlever krav i databehandleraftalerne.

Hvis Basen ønsker at ændre en underdatabehandler, som benyttes til behandling af persondata på vegne af den dataansvarlige skal de(n) dataansvarlige kontaktes.

6. Overførsel til tredjelande

Basen overfører ikke personoplysninger til tredjelande.

7. Håndtering af registreredes rettigheder

I proceduren for behandling af persondata i Basen er det overordnet beskrevet, hvordan medarbejdere skal håndtere henvendelser fra registrerede (elever) og deres forældre. Der er dertil udarbejdet en mere detaljeret procedure, for håndtering af registreredes rettigheder.

8. Håndtering af sikkerhedsbrud

I proceduren for behandling af persondata i Basen er det overordnet beskrevet, hvordan medarbejdere skal agere ifm. et sikkerhedsbrud. Der er dertil udarbejdet en mere detaljeret procedure, for håndtering af sikkerhedsbrud, som benyttes af ledelsen/de ansvarlige for håndtering af bruddet.

Procedure for håndtering af sikkerhedsbrud

1. Indledning

Denne procedurer beskriver, hvordan et sikkerhedsbrud skal håndteres, herunder hvornår og hvordan der skal kommunikeres til dataansvarlige, Datatilsynet og de registrerede.

I tilfælde af et sikkerhedsbrud, skal Basen gøre følgende:

i. Standse og/eller begrænse sikkerhedsbrud
ii. Dokumenterer sikkerhedsbruddet og omstændigheder omkring det.
iii. I nogle tilfælde: Underretter den Dataansvarlige og/eller Datatilsynet (og evt. andre tilsynsmyndigheder) samt de registrerede, som er berørte af bruddet.

Hvis en medarbejder opdager et sikkerhedsbrud, potentielt sikkerhedsbrud eller er i tvivl om der er tale om et brud skal økonomichef, Henrik, samt Philip fra IT straks kontaktes:

Kontakt i tilfælde af sikkerhedsbrud:

Økonomichef:	IT-administrator:
Navn: Henrik Thorning E-mail: hth@basen.dk Tlf. nr: 7192 6277	Navn: Philip Dysted Frank E-mail: phf@basen.dk Tlf. nr: 7192 0636

2. Hvad er et sikkerhedsbrud?

Der findes tre typer af persondatasikkerheden:

a) Brud på fortrolighed – dvs. ethvert uautoriseret adgang til, offentliggørelse af eller videregivelse af personoplysninger,
b) Brud på tilgængelighed – dvs. ethvert uautoriseret tab, samt fuldstændig eller delvis destruktion af data, eller
c) Brud på integritet – dvs. enhver uautoriseret ændring af personoplysninger.

Et sikkerhedsbrud kan antage mange former. Det er vigtigt at der i hvert enkelt tilfælde vurderes, om bruddet, også hvis det kun er delvist eller midlertidigt, indebærer en risiko for de registrerede.

Et sikkerhedsbrud kan f.eks. ske ved:

- et brud i det IT-sikkerhedsprogram, hvor personoplysninger er gemt, fx forårsaget af et hackerangreb,
- en e-mail med persondata, der ved en fejl er blevet sendt til den forkerte modtager,
- en e-mail med persondata, hvor der fejlagtigt er anført en e-mailadresse ”cc” i stedet for ”bcc”, eller
- tab af en firmatelefon eller computer, hvorpå der er gemt personoplysninger.

3. Håndtering af sikkerhedsbrud

3.1 Standsning og/eller begrænsning af sikkerhedsbruddet

Når et sikkerhedsbrud er blevet indrapporteret, skal det som det første sørges for at bruddet stoppes og/eller der foretages foranstaltninger for at begrænse konsekvenserne af bruddet.

Hvordan et sikkerhedsbrud standes bedst og/eller hvordan konsekvenserne bedst muligt begrænses, afhænger af det enkelte sikkerhedsbrud.

Standsning og/eller begrænsning af et sikkerhedsbrud kan eksempelvis ske ved:

1. Lukning af sikkerhedshuller, som giver uvedkommende uautoriseret adgang til data
2. Genoprettelse af tabt data fra backups, eller
3. Anmode en utilsigtet modtager af en e-mail om sletning af denne (også fra slettet post) og bekræfte, at dette er sket.

3.2 Vurdering af sikkerhedsbrud

Efter sikkerhedsbruddet er stoppet eller begrænset, skal der foretages en indledende vurdering af bruddet og dets mulige konsekvenser. Økonomichef, Henrik, og IT-administrator, Philip, er ansvarlige for at foretage den indledende vurdering af sikkerhedsbruddet.

Det skal vurderes, hvorvidt sikkerhedsbruddet vil have nogle konsekvenser for de involverede registrerede, herunder for personoplysningernes fortrolighed, tilgængelig og integritet.

I nogle tilfælde kan man med rimelig sikkerhed hurtigt konkludere, at sikkerhedsbruddet er af en sådan karakter, at de ikke har nogle konsekvenser for de registrerede. I disse tilfælde skal bruddet og vurderingen registreres i sikkerhedsloggen uden yderligere handlinger.

Eksempler på sikkerhedsbrud, hvor der umiddelbart ikke vurderes nogen konsekvens for de registrerede:

1. En e-mail med allerede offentligt tilgængelige personoplysninger (fx navn og telefonnummer) sendes til en forkert modtager, som der i øvrigt er tillid til,
2. En medarbejder sletter utilsigtet et dokument fra sin computer, som nemt kan genskabes fra backup, eller
3. Dokumenter til makulering placeres utilsigtet til papirgenbrug, og dette opdages umiddelbart herefter.

Foreligger der nogen form for tvivl om, hvorvidt sikkerhedsbruddet har en sådan karakter, skal den fulde procedure følges. Dette gælder også, hvis arten eller konsekvenserne af sikkerhedsbruddet er vanskelige at fastslå.

4. Håndtering af konstateret sikkerhedsbrud

Såfremt at der efter ovenstående vurdering er konstateret at der er tale om et sikkerhedsbrud (eller potentielt sikkerhedsbrud) skal nedenstående vurderes, beskrives og udføres.

De ansvarlige for håndtering af bruddet indkalder relevante deltagere til gennemgang af nedenstående:

1. Årsag til sikkerhedsbruddet samt omfang
2. Foranstaltninger, der er og evt. skal træffes for at minimere omfanget af sikkerhedsbruddet
3. Anmeldelse til de(n) dataansvarlige, hvis der er tale om oplysninger som Basen er databehandler for.
4. En drøftelse af, om bruddet skal anmeldes til Datatilsynet eller eventuelt andre myndigheder, hvis det er oplysninger som Basen er dataansvarlige for.
5. Om det vil være nødvendigt at underrette de involverede personer (de registrerede), hvis personoplysninger er involveret, og eventuelt den relevante kunde, oplysningerne stammer fra.
6. Hvilke nye foranstaltninger der skal træffes, for at sikre at et lignende brud ikke sker igen
7. Om der skal rettes henvendelse til en ekstern rådgiver for vejledning vedrørende sikkerhedsbruddet

Efter mødet skal der udarbejdes et internt dokument/referat, der dokumenterer og beskriver al relevant information vedrørende sikkerhedsbruddet (brug skabelonen i Bilag 1) og sikkerhedsbruddet registreres i loggen over sikkerhedsbrud.

5. Anmeldelse af bruddet

Basen er ansvarlig for, at sikkerhedsbrud anmeldes til:

- Den/de dataansvarlige uden unødig forsinkelse (hvor Basen er databehandler).
- Datatilsynet inden for 72 timer (hvor Basen er dataansvarlig].
- De registrerede (hvor Basen er dataansvarlig)
- Flere informationer kan findes på Datatilsynets hjemmeside. https://www.datatilsynet.dk/sikkerhedsbrud

Bilag 1 - Registrering af sikkerhedsbrud

Forhold	Forklaring	Beskrivelse
Tidspunkt for opdagelse af databrud	Dato, kl.	
Tidspunkt for indtruffet databrud	Dato, kl.	
Basenr rolle	Dataansvarlige, databehandler eller fælles dataansvarlig)	
Beskrivelse af bruddet	Fx om det drejer sig om et hackerangreb, en forkert fremsendt e-mail, tab af mobil eller computer o.l.	
Kategorier af registrerede	Kategorier af personer, sikkerhedsbruddet omfatter og om der tale om særlige kategorier af registrerede, fx børn.	
Kategorier af personoplysninger	Fx navn, email, adresse.	
Antal berørte personer		
Hvorfra personoplysningerne stammer?	Fx fra et projekt, en kunde eller lignende	
Årsag til databruddet		
Sandsynlige konsekvenser af databruddet	Vurdering af konsekvenser for de registrerede som resultat af databruddet	
Foranstaltninger truffet for at stoppe og afhjælpe negative virkninger af databruddet		
Foranstaltninger truffet for at undgå lignende brud i fremtiden		
Hvis personoplysninger hører under databehandleraftale: Er der sket underretning til dataansvarlige? Hvis ikke, beskriv hvorfor		
Hvis Basen er dataansvarlig: Er der sket anmeldelse til Datatilsynet? Hvis ikke, beskriv hvorfor		
Er der sket underretning af de berørte registrerede? Hvis ikke, beskriv hvorfor		
Tidspunkt for rapportens afslutning		
Underskrift		

Bilag 2 – Kontaktoplysninger

Navn	Rolle	Telefon	Email

Databeskyttelse

1. Indledning

Databeskyttelsesforordningen (GDPR) trådte i kraft den. 25. maj 2018 og indeholder en række skærpede krav til behandling af persondata. Langt de fleste krav til persondatasikkerhed var også gældende før ikrafttrædelsen af GDPR. Af nye krav er det særligt den enkeltes ret til viden om, indsigt i og sletning af egne data, der er skærpet. Dertil kommer, at kravene til dokumentation, løbende kontrol med persondata og opfølgning samt at potentielle bødestørrelser er blevet forhøjet.

I forbindelse med Basens leverance af skole- og dagbehandlingstilbud behandler vi oplysninger om de elever der går hos os. Da der både er tale om børn og følsomme oplysninger er det vigtigt at du som medarbejder følger nedenstående procedurer, så deres oplysninger er beskyttet og vi kan fokusere på at læring og behandling i høj kvalitet.

2. Hvad er persondata?

Persondata er enhver form for information, der kan henføres til en bestemt person – det gælder også film, fotos mv. Persondata kan opdeles i følgende kategorier:

1. Almindelige personoplysninger:

Navn, adresse, telefonnummer, e-mail, fødselsdag, økonomi, skat, gæld, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato, stilling, arbejdsområde, arbejdstelefon mv.

Under de almindelige personoplysninger ligger også cpr-nummeret og evt. strafferetslige forhold, som dog samtidig skal behandles fortroligt.

2. Følsomme personoplysninger:

Fx race, etnisk oprindelse, religiøs, filosofisk overbevisning, fagforening, genetiske data, helbredsoplysninger, seksuelle forhold eller orientering mv.

I Basen håndterer vi både almindelige personoplysninger, herunder CPR-numre, samt følsomme personoplysninger i forbindelse med skole og dagbehandlingstilbud. Oplysningerne er nødvendige for at Basen på bedst mulig vis kan faciliterer læring, som udvikler eleven socialt, personligt, og fagligt med henblik på at mestre eget liv.

3. Vores behandling af oplysninger

Det er vigtigt at vi behandler oplysninger om elever sikkert både for at beskytte eleverne, samt for at sikre at vi ikke overtræder reglerne i GDPR. Særligt ved håndtering af følsomme oplysninger og oplysninger om børn har GDPR skærpede regler for hvordan de må behandles og det er derfor ekstra vigtigt, at du er opmærksom på, hvordan oplysninger behandles samt hvor de opbevares.

Personoplysninger, som behandles i forbindelse med skole- og dagsbehandlingstilbud, bliver i udgangspunktet behandlet og opbevaret på følgende måde:

Indskrivning af nye elev:

1. Indstilling af potentiel ny elev: Basen modtager sagsakter på potentiel elev via VIRK.
2. Vurdering: Afdelingsleder vurderer elev. Forældre/sagsbehandler/potentiel elev mødes med afdelingsleder og vurderer behov/match ift. opstart på Basen.

3. Visitering: Hvis Basen vurderes som godt sted for den potentielle elev visiteres eleven til Basen. Afdelingslederen udfylder stamkort på eleven med sagsbehandler, eleven og forældrene.
4. Oprettelse af elev: Sekretæren opretter eleven i de relevante systemer (der er tjekliste for oprettelse af ny elev):
    a. Evt. yderligere oplysninger indsamles.
    b. Elev oprettes i TEA, herefter importeres data til SkoleIntra og yderligere oplysninger tilføjes.
    c. Der udarbejder indskrivningskontrakt, som sendes og underskrives af økonomichef og sagsbehandleren.
    d. Dokumentation slettes fra mails mv. hos sekretær.

Behandling og undervisning:

Ifm. elevers forløb hos Basen udarbejdes og indsamles oplysninger om eleverne med henblik på at yde den bedst mulige behandling og undervisningsforløb for den enkelte. Dette indebærer bl.a.:

1. Skriftlig beskrivelse og elevgennemgang ifm. opstart af ny elev.
2. Klasselog, månedsstatusser og statusrapporter, herunder elevplan.
3. Behandlingsmål, uddannelsesplaner og udviklingsmål.
4. Kompetencepapir ifm. afslutning af elev.
5. Kommunikation ml. sagsbehandler, forældre og Basen via (elektronisk) kontaktbog, beskedsystem i SkoleIntra, mail og sms.
6. Andet: Skolekort/rejsekort, samtykke for elever over 18, UNI-login brugernavne for elever.

VISO-forløb

Basen leverer rådgivning og/eller udredning eller bistand til udredning under VISO på vegne af Socialstyrelsen. I forbindelse med et VISO-forløb behandles persondata om borgeren. Dette indebærer følgende:

- Indledende kommunikation om en ny sag via telefon eller mail.
- Gennemgang af sagsakter mv. i Socialstyrelsens system VIAS.
- Journalisering af udredningsrapporter, møddereferater, dagsordner i VIAS.

4. Hvor må oplysninger opbevares?

4.1 Basens systemer

For at beskytte de personoplysninger vi har på eleverne samt sikre, at databehandleraftaler med kommunerne overholdes, er det vigtigt, at vi kun opbevare personoplysninger de steder som er godkendte til det.

Nedenstående beskriver, hvor og hvordan personoplysninger skal opbevares i det daglige arbejde.

Fælles Fildrev

Basen har en række fælles fildrev, som benyttes ifm. administration af elever, samt for nogle afdelinger til dokumentation af fx procedurer for behandling af oplysninger om eleven.

Administrationsdrev:
Indeholder elevmapper med oplysninger om elever, herunder mails, stamkort, indskrivningskontrakt mv. Oplysninger opbevares for dokumentere elevens historik og forløb. Administrationsdrevet benyttes også til opbevaring af andet fortroligt materiale, fx straffeattester på medarbejdere.

Administrationsdrevet er adgangsbegrænset, så det kun er relevante brugere, som har adgang fx ledelse samt administrationen.

Andre fildrev:
I nogle afdelinger benyttes fildrev også til opbevaring af driftsdokumentation, fx undervisningsmateriale, vejledninger og procedurer.

Lokale fildrev

I forbindelse med udarbejdelse af fx månedsstatusser og statusrapporter kan disse dokumenter opbevares lokalt på medarbejderens pc. Dokumenterne må kun opbevares lokalt, så længe de er under udarbejdelse og skal slettes så snart de er uploaded på SkoleIntra.

OneDrive

OneDrive må benyttes til opbevaring af 'driftsdokumentation', herunder undervisningsmateriale, skabeloner, vejledninger og procedurer.

Der må ikke opbevares personhenførbare oplysninger på OneDrive!
(fx månedsstatusser, elevplaner, uddannelsesmål mv.)

Teams

Teams må benyttes til opbevaring af 'driftsdokumentation', herunder undervisningsmateriale, skabeloner, vejledninger og procedurer.

Teams kan desuden benyttes til onlinemøder med forældre og sagsbehandlere.

Der må ikke opbevares personhenførbare oplysninger på Teams!
(fx månedsstatusser, elevplaner, uddannelsesmål mv.)

Basen Basic

Basen-basic er vores fælles site, hvor der opbevares politikker, procedurer, skabeloner mv. Sitet vedligeholdes af den kommunikationsansvarlige.

TEA

TEA er en central database med daglig opdatering fra CPR-registret, som bruges til indskrivning og udmelding af elever, fraværsregistrering, prøveafvikling, karaktergivning mv.

Når en elev skal starte på Basen, kontaktes administrationen som opretter eleven i TEA med navn og CPR-numre. Herefter trækkes alle yderligere oplysninger om eleven fra offentlige registre, hvilket om natten synkroniseres til SkoleIntra.

SkoleIntra

SkoleIntra er vores primære arkiveringssystem til opbevaring af oplysninger om elever, herunder stamoplysninger, sagsdokumentation, månedsstatusser, lægerklæringer, klasselog mv.

Der er to forskellige logins til SkoleIntra, som er tilknyttet hver deres CVR-nummer, den ene for Fyn + Basen Nord og den anden for Stranden og CNA. Der benyttes to CVR-numre.

Ved oprettelse af ny elev, tilføjes oplysninger om sagsbehandler for den enkelte elev manuelt i SkoleIntra efter at stamoplysninger på eleven er importeret fra TEA.

VIAS

VIAS er et journaliserings- og sagsbehandlingssystem for sager under VISO, som håndteres på vegne af Socialstyrelsen. Alt dokumentation i relation til et VISO-forløb lægges under den konkrete sag. Det er kun godkendte VISO-specialister hos Basen, som har adgang til systemet.

VISO-koordinatoren håndterer indkomne sager og formidler kontakt til Socialstyrelsen ift. oprettelse af brugere.

E-protokol

E-protocol er et system til registrering af møde og fravær på elever. Systemet benyttes ikke på alle Basens lokaliteter.

Terapi 360

Dette er vores journalisering portal, hvor psykologerne journalisere deres forløb med børnene. Terapi 360 overholder lovgivning på området, og er er beskyttet af End-to-End SSL-kryptering, firewalls og bruger autentifikation, adgangskontrol og autorisation.

E-mail (O365)

Vi benytter e-mail til kommunikation med sagsbehandlere, PPR'er og forældre. Se pkt. 5.1. om 'Send-sikkert' funktionen.

Mobiler (SMS + Opkald)

Vi har ofte kontakt med forældre og sagsbehandlere over telefonen. Hvis vi bliver ringet op af en person, som ønsker at få oplysninger om en elev er det vigtigt, at vi sikrer os at det er den rigtige person vi taler med, samt at denne person må få udleveret oplysningerne. Der kan fx være nogle forældre, som ikke må få oplysninger om eleven eller at eleven ikke ønsker, at andre skal vide at eleven går på Basen.

Hvis du ikke selv er primæransvarlig for eleven, skal du desuden altid henvise til den relevante afdelingsleder, som kan hjælpe med at vurdere, hvilke oplysninger der kan gives om eleven.

Du må fortsat gerne bruge SMS som kontaktform. Dette er forudsat at SMS'er slettes fra telefonen når de er læst, og evt. noteret i elevens klasselog. Dette gælder både ift. kontakt med elever og forældre. Tænk desuden over, om det er passende at benytte sms til den slags kommunikation du skal foretage eller om det fx vil være bedre at foretage et opkald eller sende en krypteret mail.

WhatsApp

WhatsApp kan også bruges til kontakt med elever. Her gælder samme regler som ved SMS, dvs. at

SMS'en skal

Fysiske papirer

Ifm. forskellige administrationsopgaver benyttes der fysiske papirer fx til gennemgang af tjeklister mm. Der er også situationer, hvor vi modtager breve med posten eller mails, som er printet ud ifm. diverse administrationsopgaver.

Derudover, kan vi også benytte printede stamkort, som udfyldes i hånden sammen med eleven og forældre ifm. opstart af nye elever.

Når fysiske papirer ikke benyttes, må disse ikke ligge fremme og skal opbevares forsvarligt, når du forlader kontoret fx i et aflåst skab.

Det er også vigtigt, at dokumenter med personoplysninger bliver makuleret så snart de ikke skal bruges længere.

4.2 Tildeling af adgange

Ved tildeling af nye adgange følges følgende procedure:

- Fildrev og O365: Kontakt økonomichef (Henrik Thorning) som kontakter IT. Adgang tildeles ud fra lokation, rolle og ansvarsområder.
- SkoleIntra og TEA: Kontakt administrationen. Denne opretter den nye medarbejder i TEA og SkoleIntra med adgangsbegrænsning til den/de relevante afdelinger og klasser.
- VIAS: Kontakt VISO koordinator, Josephine Björgheim. Denne kontakter VISO, som skal godkende bruger på baggrund af CV og herefter står for oprettelse af brugeren.

Hvis en medarbejder skifter afdeling eller rolle skal ovenstående kontaktes, så adgange kan blive lukket ned og/eller ændre så medarbejdere altid kun har de adgange de har behov for.

5. Send og modtag dokumenter

I forbindelse med indskrivning af nye elever, samt i løbet af undervisnings- og behandlingsforløb skal der løbende kommunikeres med forskellige aktører, herunder særligt sagsbehandlere og forældre.

Når der skal udveksles informationer, er det vigtigt, at vi bruger de rette kanaler, så vi er sikre på at oplysninger sendes krypteret og dermed ikke kan komme uvedkommende til kendskab.

5.1 Send sikkert via e-mail

Hvis du skal sende følsomme personoplysninger, fx månedsrapporter, skal disse sendes via 'Send sikkert', SEPO, funktionen i din e-mail. Hvis du ikke har funktionen installeret eller ikke kan få den til at fungere kan du kontakte Nikolaj fra IT. Det er ikke tilladt at sende følsomme personoplysninger uden at disse er krypteret.

Hvis du ikke kan få SEPO på din computer (fx ved MAC), skal du få hjælp fra en kollega, typisk sekretær, til at sende.

Hvis du skal sende til en modtager, som ikke kan modtage krypterede e-mails, skal du kontakte Nicolaj fra IT for at finde alternativ løsning.

5.2 Beskeder i SkoleIntra

Al kommunikation med forældre skal i udgangspunktet ske via beskedfunktionen i SkoleIntra.

Hvis en forælder endnu ikke er oprettet i SkoleIntra kan kommunikation ske over e-mail. Her er der dog vigtigt, at der ikke sendes følsomme eller fortrolige oplysninger ukrypteret.

Når du er i kontakt med forældre, skal du generelt altid overveje om det er nødvendigt at have følsomme oplysninger med eller om de kan undlades.

Hvis du modtager følsomme oplysninger om en elev, fx om diagnoser, på e-mail fra en forælder skal du oplyse forælderen om, at kommunikation skal ske via SkoleIntra. Husk at slette oplysninger fra din indbakke og mappen slettet post når de er uploadede til SkoleIntra.

6. Sletning af oplysninger

Når en elev stopper på Basen skal oplysninger, som ikke længere er nødvendige at opbevare slettes. Det er afdelingslederen som har ansvaret for at oplysninger bliver slettet.

6.1 SkoleIntra og TEA:

Når en elev stopper, sammenfattes en 'opsummering' af elevens forløb hos Basen, som kan videregives til sagsbehandler og den kommende skole.

Herefter skal eleven udmeldes i TEA, som herefter synkroniseres med SkoleIntra, hvorefter eleven her vil stå under 'Udmeldte Elever'. Eleven vil fremgå under 'Udmeldte Elever' i et år, hvorefter data slettes. Dette er opsat af SkoleIntra.

Sletning sker ved at kontakte administrationen, som udmelder eleven i TEA. Administrationen skal kontaktes minimum to dage før eleven stopper, så det kan sikres at eleven udmeldes på det rigtige tidspunkt. For elever, som skal starte på en ny skole, er det desuden nødvendigt, at Basen har udmeldt eleven inden denne kan tilmeldes det nye sted.

6.2 Elev mappe på administrationsdrev

Når en elev stopper, flyttes elevens mappe til mappen 'Udmeldte elever'. Her gemmes mappen i et skoleår for at kunne dokumentere ophold, samt afklare spørgsmål fx ifm. opstart på ny skole. Ved afslutning af skoleåret slettes mapper på de udmeldte elever.

Procedure for oprydning af udmeldte elever:

Udmeldte elevers data gemmes i indeværende skoleår, hvorefter eleverne slettes permanent ved gennemgang, når skoleåret afsluttes.

6.3 Øvrig dokumentation (mails, filer, fysiske papirer)

Generelt skal dokumentation som udarbejdes omkring elever slettes så snart, der ikke længere er behov for dem og de fx er færdigudarbejdet og uploaded til SkoleIntra.

Det er den enkelte medarbejders ansvar, at sikre, at der fx ikke opbevares personoplysninger om elever i længere tid end det er nødvendigt. Dette betyder, at den enkelte løbende skal sikre sig, at der fx ikke ligger mails med personoplysninger om elever samt andet dokumentation om eleverne på forskellige drev efter at de er arkiveret i SkoleIntra.

Husk også løbende at slette dokumentation i 'Slettet post' mapper i din e-mail, samt i mappen 'Overførsler' på din computer.

For at sikre ovenstående, anbefales det at medarbejdere gennemgår deres mails og dokumenter en gang i kvartalet og for at sikre, at der ikke ligger oplysninger i drev og mapper.

Det er ikke tilladt at have 'privat' backup af informationer om elever fx OneDrive eller USB-sticks.

7. Håndtering af henvendelser fra registrerede

I henhold til databeskyttelsesforordningen har de registrerede (dvs. vores elever) en række rettigheder ift. vores behandling af deres oplysninger.

Disse er grundlæggende:

- Ret til indsigt: Elever (og dennes forældre, hvis eleven er under 18) har ret til at få at vide, hvilke oplysninger vi behandler om eleven.
- Ret til berigtigelse: Dvs. at få rettet forkerte oplysninger.

- Ret til sletning: Ret til at få slettet oplysninger.
- Ret til begrænsning: At der ikke længere foretages anden behandling af personens personoplysninger end opbevaring.
- Ret til dataportabilitet: Retten til at få udtræk af oplysninger.
- Ret til indsigelse: At man kan gøre indsigelse mod at ens oplysninger bliver behandlet.

Hvis du modtager en henvendelse, fx fra en forælder, er det vigtigt altid at **verificere og kontrollere**, at personen er den han/hun udgiver sig for samt at denne må få adgang til oplysningerne. Der kan være situationer, hvor en forælder fx ikke må blive oplyst om eleven.

Den generelle frist for opfyldelse af den registrerede rettigheder er **uden unødig forsinkelse og senest efter en måned.** Det er derfor vigtigt, at vi håndterer henvendelser, så snart de er modtaget, så fristen ikke risikere at blive overtrådt.

Hvis du modtager en anmodning fra en elev eller en forælder om en eller flere af ovenstående rettigheder skal du kontakte den relevante afdelingsleder, som kan kontakte økonomichef, Brian, og Nikolaj fra IT, som bistår med at vurdere hvordan henvendelsen skal håndteres.

OBS!

- For oplysninger som videregives til sagsbehandler, skal der som udgangspunkt henvises til den relevante kommune, da denne er dataansvarlige for oplysningerne og derfor skal håndtere henvendelsen.
- Basen er også selv dataansvarlige for en række oplysninger om eleverne, som også er dækket af ovenstående rettigheder.

Ved henvendelser følges proceduren: 'Håndtering af registreredes rettigheder'.

8. Andet

Hvis en elev er over 18 år, skal der indhentes samtykke fra denne til at forældre må se oplysninger fx på SkoleIntra. Der skal også indhentes samtykke, hvis Basen ønsker at benyttes billeder af elever fx til hjemmesiden.