

# PERSONDATAPOLITIK

## HASLEV PRIVATSKOLE

Senest revideret den:	Underskrift:

## INDSHOLDSFORTEGNELSE

1	Indledning og baggrund .....	3
1.1	Beskrivelse af organisationen.....	4
2	Formål og opbygning .....	4
2.1	Formål .....	4
2.2	Opbygning .....	4
2.3	Fysiske og digitale publikationer af Datapolitikken .....	5
2.4	Årshjul .....	5
3	Roller.....	6
3.1	Rolledefinition .....	6
3.2	Ledelsen .....	6
3.3	Medarbejdere .....	7
3.4	Eksterne samarbejdspartnere .....	7
3.5	Data Protection Officer (DPO).....	8
3.6	Dataansvarlig/databehandler.....	8
4	Datastrømsanalyser .....	8
5	Generel risikovurdering for Haslev Privatskole .....	9
5.1	Formål .....	9
5.2	Gennemførelse af risikovurderingen.....	10
5.3	Håndtering af identificerede risici .....	10
6	Databehandlere .....	11
6.1	Identifikation af databehandlere .....	11
6.2	Fysisk placering af databehandleraftaler .....	11
6.3	Indgåelse af nye databehandleraftaler .....	11
6.4	Tilsyn med databehandlere.....	12
6.5	Håndtering af underdatabehandlere .....	12
7	Fortegnelse over behandlingsaktiviteter .....	13
7.1	Fortegnelsen .....	13
7.2	Fortegnelse over behandlingsaktiviteter – medarbejdere.....	13
7.3	Fortegnelse over behandlingsaktiviteter – børn/elever.....	14
7.4	Ændringer i fortegnelsen.....	14
8	Tekniske og organisatoriske sikkerhedsforanstaltninger .....	14
8.1	Generelt om tekniske og organisatoriske sikkerhedsforanstaltninger .....	14
8.2	Tekniske og organisatoriske sikkerhedsforanstaltninger på Haslev Privatskole .....	15
9	Driftsmæssige retningslinjer og procedurer .....	15
10	Den registreredes rettigheder/orientering til de registrerede .....	16
10.1	Generelt om de registreredes rettigheder .....	16
10.2	Processuelle krav ved håndtering af den registreredes rettigheder .....	17
10.3	Håndtering af oplysningspligten.....	17

11	Databrud.....	18
11.1	Ansvar ved databrud .....	18
11.2	Konstatering af brud på datasikkerheden .....	18
11.3	Dokumentation af brud på persondatasikkerheden .....	19
11.4	Anmeldelse til Datatilsynet om brud på datasikkerheden .....	20
11.5	Underretning af den registrerede om brud på persondatasikkerheden .....	21
12	Opfølgning og opdatering.....	22
12.1	Årlig gennemgang af Datapolitikken .....	22
12.2	Nye arbejds- og driftsområder i organisationen.....	22

## 1 INDLEDNING OG BAGGRUND

## 1.1 Beskrivelse af organisationen

Haslev Privatskole (herefter benævnt Haslev Privatskole) er en privatskole, organiseret som en selvejende institution, beliggende i Haslev, Faxe Kommune.

Denne datapolitik (herefter benævnt Datapolitikken) gælder for følgende enheder under Haslev Privatskole:

- Skolen
- SFO'en

## 2 **FORMÅL OG OPBYGNING**

### 2.1 Formål

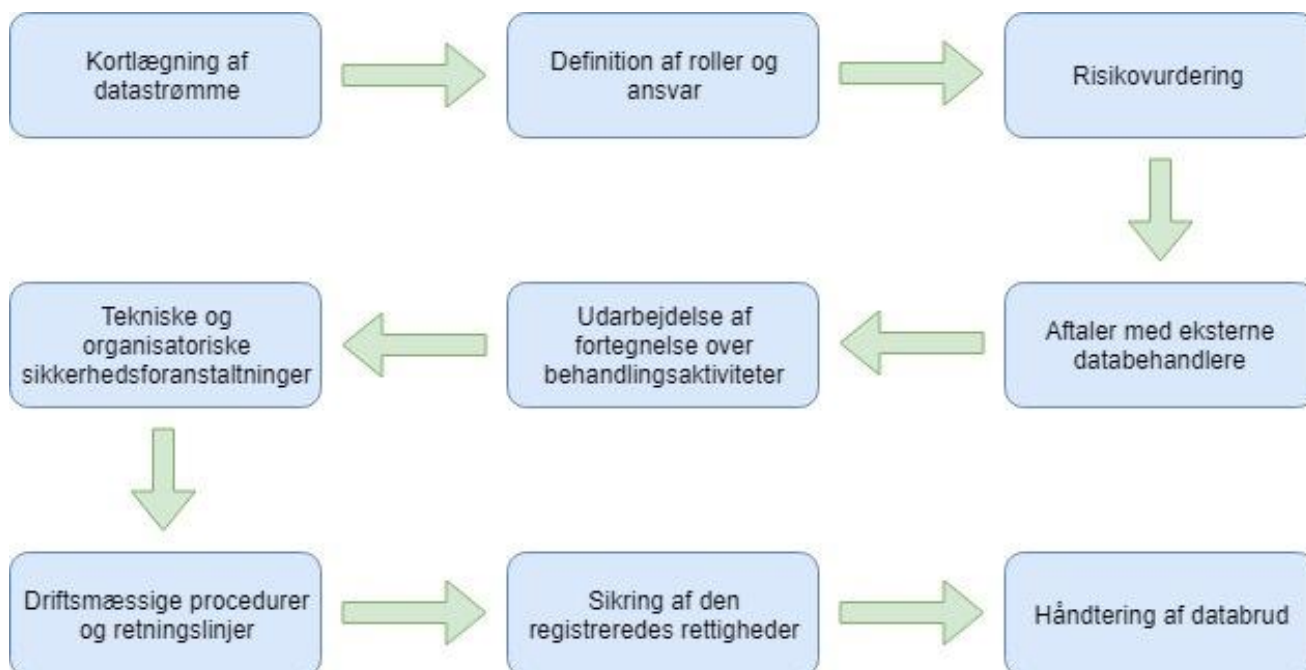
Datapolitikken for Haslev Privatskole har til formål at sikre og dokumentere, at al behandling af personoplysninger på Haslev Privatskole sker med udgangspunkt i EU's databeskyttelsesforordning og den danske databeskyttelseslov.

For Haslev Privatskole er det vigtigt at sikre, at følgende principper overholdes i hele organisationen:

- Al behandling af personoplysninger sker på en lovlige, rimelig og gennemsigtig måde
- Behandling af personoplysninger sker kun til saglige formål
- Mængden af persondata begrænses ved at slette løbende eller ved at anonymisere data, og ved ikke at indhente flere oplysninger end højst nødvendigt
- Alle personoplysninger er korrekte og ajourførte
- Alle personoplysninger beskyttes for at sikre integritet og fortrolighed

### 2.2 Opbygning

Datapolitikken er opbygget i følgende hovedelementer:



### 2.3 Fysiske og digitale publikationer af Datapolitikken

Datapolitikken er dynamisk og ændres løbende i tilfælde af ændringer i organisationens virkeområde og databehandlingsområde, eller ændringer i databeskyttelseslovgivningen eller fortolkningen heraf.

Datapolitikken er til enhver tid tilgængelig i en digital udgave, der er placeret i Administrationsmappen på Clouden og i en fysisk udgave, der er placeret i en mappe på kontoret.

### 2.4 Årshjul

En stor del af arbejdet med at overholde databeskyttelsesforordningen og databeskyttelsesloven består i opfølgning på, at Datapolitikken fortsat er i overensstemmelse med den behandling af personoplysninger, der foregår i organisationen, samt kontrol af, at alle medarbejdere i organisationen, der behandler personoplysninger, overholder de retningslinjer og procedurer, der er fastsat i Datapolitikken.

Datapolitikken suppleres af et årshjul (vedlagt Datapolitikken som **bilag 1**), der oplister de opgaver, Haslev Privatskole skal igennem i løbet af et år med henblik på sikring af, at Datapolitikken altid er opdateret samt at føre kontrol med overholdelse af Datapolitikken.

Årshjulet består endvidere af en oversigt over de ad hoc-opgaver Haslev Privatskole skal igennem i tilfælde af, at Haslev Privatskole indfører nye arbejdsområder i organisationen, hvor der sker en væsentlig anden eller ny form for behandling af personoplysninger.

Hver gang en opgave i årshjulet er udført, signeres opgaven i årshjulet af den person, der har udført opgaven. Årshjulet opbevares i udskrevet form i mappen med Datapolitikken på kontoret, så det til enhver tid kan dokumenteres overfor Datatilsynet, at opgaverne løbende er udført.

### **3 ROLLER**

#### **3.1 Rolledefinition**

Med henblik på en sikring af en stærk forankring af arbejdet med beskyttelse og korrekt behandling af personoplysninger på Haslev Privatskole fastsættes de individuelle roller, når det kommer til behandling af personoplysninger, i nærværende afsnit.

#### **3.2 Ledelsen**

Det er ledelsen/bestyrelsen på Haslev Privatskole, der har det overordnede, primære og endelige ansvar for, at EU's databeskyttelsesforordning og den danske databeskyttelseslov overholdes i hele organisationen.

Det er blandt andet ledelsens/bestyrelsens ansvar, at:

- forestå udarbejdelsen og implementeringen af en IT-sikkerheds- og databeskyttelsespolitik i organisationen
- sikre, at der er de fornødne rammer og ressourcer til rådighed for overholdelse af databeskyttelsesreglerne
- sikre, at alle politikker overholdes i organisationen, og at der løbende undervises i og følges op på alle politikker om IT-sikkerhed og databeskyttelse

Slutteligt er det ledelsens/bestyrelsens ansvar, at der udpeges en person i organisationen – i eller uden for ledelsen – der har primære og overordnede ansvar for IT-sikkerhed og databeskyttelse i organisationen.

### 3.3 Medarbejdere

Alle medarbejdere, der er ansat på Haslev Privatskole uddannes og testes i Datapolitikken.

En stor del af den behandling af personoplysninger, der foregår på Haslev Privatskole foretages af medarbejderne. Det er dermed vigtigt, at medarbejderne har stort kendskab til de regler for IT-sikkerhed og databeskyttelse, der er fastsat i Datapolitikken.

Alle nye medarbejdere introduceres grundigt til Datapolitikken indenfor én måned efter, at ansættelsesforholdet er tiltrådt.

Gentagen overtrædelse af Datapolitikken kan have ansættelsesretlige konsekvenser for en medarbejder.

### 3.4 Eksterne samarbejdspartnere

I det omfang, der bruges eksterne samarbejdspartnere (eksempelvis rengøringspersonale, reparatører m.v.), der ikke er defineret som eksterne databehandlere (jf. punkt 5 herom), men som fortsat får adgang til Haslev Privatskoles interne personoplysninger,

indgås der fortrolighedserklæringer mellem Haslev Privatskole og den eksterne leverandør.

Haslev Privatskoles fortrolighedserklæring er vedlagt Datapolitikken som **bilag 2**.

### 3.5 Data Protection Officer (DPO)

Det vurderes, at Haslev Privatskole ikke er forpligtet til at udpege en DPO jf. databeskyttelsesforordningens artikel 37, idet behandling af personoplysninger på Haslev Privatskole *ikke* er organisationens kerneaktivitet, og der *ikke* behandles personoplysninger i et stort omfang.

Det vurderes én gang årligt i forbindelse med den ordinære gennemgang af Datapolitikken, hvorvidt Haslev Privatskole er forpligtet til at udpege en DPO.

### 3.6 Dataansvarlig/databehandler

Haslev Privatskole er **dataansvarlig** i medfør af databeskyttelsesforordningens artikel 26 i forhold til de personoplysninger, der indsamles og behandles i organisationen om Haslev Privatskole s medarbejdere, om elever, der er tilknyttet skolen eller SFO'en på Haslev Privatskole.

Haslev Privatskole defineres som dataansvarlig, idet Haslev Privatskole alene bestemmer, hvilket formål oplysningerne indsamles til, og hvordan oplysningerne behandles.

## 4 **DATASTRØMSANALYSER**

Med henblik på en kortlægning af alle de personoplysninger, der strømmer ind og ud af organisationen, har Haslev Privatskole udarbejdet en visuel datastrøms analyse, der viser, hvilke data, der strømmer ind i organisationen, hvor der databehandles internt i organisationen, samt hvortil data strømmer ud af organisationen.



Haslev Privatskole er bekendt med, at det ikke er en forpligtelse i henhold til databeskyttelsesforordningen eller databeskyttelsesloven at udarbejde en datastrømsanalyse.

Der er udarbejdet en datastrømsanalyse for hver af de hovedgrupper af personer, Haslev Privatskole behandler personoplysninger om.

Datastrømsanalyse for medarbejdere, der er tilknyttet Haslev Privatskole, er vedlagt Datapolitikken som **bilag 3**.

Datastrøms analyse for elever, der er tilknyttet skolen og SFO'en på Haslev Privatskole, er vedlagt Datapolitikken som **bilag 5**.

## **5 GENEREL RISIKOVURDERING FOR HASLEV PRIVATSKOLE**

### **5.1 Formål**

I forbindelse med udarbejdelsen af Datapolitikken, har Haslev Privatskole udarbejdet en generel risikovurdering for al behandling af personoplysninger, der foregår i organisationen.

Som **bilag 6** til Datapolitikken vedlægges Haslev Privatskole s risikovurderingen.

Formålet med, at Haslev Privatskole foretager en generel risikovurdering i forbindelse med al behandling af personoplysninger, er at måle risikoen for behandlingen ved at bedømme, hvor stor sandsynlighed der er for, at en hændelse indtræffer, samt hvor store konsekvenser hændelsen kan have for den registrerede person og Haslev Privatskole.

Ud fra den foretagne risikovurdering har Haslev Privatskole gennemført de nødvendige tekniske og organisatoriske foranstaltninger (jf. Datapolitikkens punkt 8) for at sikre et sikkerhedsniveau, der passer til de identificerede risici.

Risikovurderingen benyttes endvidere ved indgåelse af aftaler med data behandlere med henblik på en sikring af, at de data behandlere Haslev Privatskole har indgået databehandleraftaler med iagttager et passende sikkerhedsniveau på baggrund af de identificerede risici.

Risikovurderingen skal altid gennemføres af en person, der har den nødvendige faglige indsigt i de personoplysninger, der behandles på Haslev Privatskole

## 5.2 Gennemførelse af risikovurderingen

Risikovurderingen gennemføres ud fra Haslev Privatskoles synspunkt, men det er den/de registrerede person(er), der er hovedfokus i risikovurderingen.

Ved risikovurderingens gennemførelse tages der udgangspunkt i:

- 1) Hvad er sandsynligheden for forekomsten af et databrud i forbindelse med behandlingen
- 2) Hvad er konsekvensen for den registrerede ved databrud

## 5.3 Håndtering af identificerede risici

Hvis Haslev Privatskole vurderer, at der kan være risici forbundet med en behandling af personoplysninger, skal det efterfølgende afgøres, hvordan de identificerede risici håndteres. Dette gøres ved udarbejdelse af handlingsplan herfor.

Haslev Privatskole har besluttet fire muligheder for håndtering af kortlagte risici i risikovurderingen:

- 1) **Accept af risiko** – risikoen accepteres, og der foretages ikke yderligere
- 2) **Flyt** – den pågældende behandling flyttes – eksempelvis til et andet system

- 3) **Undgå** – risikoen undgås ved at stoppe eller ændre den aktivitet, som er årsag til risikoen
- 4) **Kontrollér** – risikoen kontrolleres ved at indføre foranstaltninger, som fjerner eller reducerer sandsynligheden eller konsekvenserne

## 6 DATABEHANDLERE

### 6.1 Identifikation af databehandlere

I datastrøms analyserne, der er vedlagt Datapolitikken som bilag 3-5, er det kortlagt, at Haslev Privatskole har indgået samarbejde med en række data behandlere, der behandler personoplysninger efter instruks fra Haslev Privatskole. Disse databehandlere vil til enhver tid fremgå af **bilag 7** til Datapolitikken (Liste over databehandlere).

Bilag 7 opdateres hver gang, der sker en ændring i til- eller fragangen af databehandlere samt i de tilfælde, hvor eksisterende databehandlere sender en opdatering ud af den nugældende databehandleraftale mellem Haslev Privatskole og databehandleren.

### 6.2 Fysisk placering af databehandleraftaler

Alle de til enhver tid gældende databehandleraftaler fremgår af mappen ”Databehandleraftaler” i den digitale mappe for Datapolitikken og i en fysisk mappe i arkivet.

### 6.3 Indgåelse af nye databehandleraftaler

Som **bilag 8** til Datapolitikken vedlægges Haslev Privatskoles procedure for indgåelse af databehandleraftaler og kontrol med data behandlere, som Haslev Privatskole samarbejder med.

Hver gang der skal indgås en ny databehandleraftale mellem Haslev Privatskole og en ny ekstern databehandler, eller hvis der skal indgås en ny databehandleraftale med en ekssi-

sterende databehandler, gennemgås proceduren for indgåelse af nye databehandleraftaler med henblik på sikring af, at de databehandlere, der indgås databehandleraftaler med, har et passende teknisk og organisatorisk sikkerhedsniveau.

#### 6.4 Tilsyn med databehandlere

Jf. Datatilsynets vejledning "Vejledende tekst om tilsyn med databehandlere og underdatabehandlere" fra maj 2018, er det Datatilsynets opfattelse, at man skal påse behandlingssikkerheden hos sine databehandlere for at leve op til kravet, der stilles til den dataansvarlige, om ansvarlighed for overholdelse af reglerne i databeskyttelsesforordningen.

Det er endvidere Datatilsynets opfattelse, at den dataansvarlige ikke vil kunne leve op til ovenstående krav ved blot at indgå en databehandleraftale med databehandleren. Den dataansvarlige skal også føre et (større eller mindre) tilsyn med, at de databehandleraftaler, man har indgået, overholdes, herunder at databehandleren har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger.

Med baggrund i, at der ikke er tale om komplekse databehandlerforhold mellem Haslev Privatskole og de databehandler, Haslev Privatskole har databehandleraftaler med, foretager Haslev Privatskole selv kontrol af alle data behandlere med eventuel bistand fra Haslev Privatskoles advokat/revisor/IT-konsulent med henblik på at sikre, at databehandleren har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger.

Alle data behandlere Haslev Privatskole har indgået databehandleraftaler med kontrolleres én gang årligt med udgangspunkt i proceduren for kontrol med data behandlere, der vedlagt Datapolitikken i bilag 8.

#### 6.5 Håndtering af underdatabehandlere

Det er Haslev Privatskoles ansvar at data behandles brug af underdatabehandlere kun sker efter forudgående aftale/accept fra Haslev Privatskoles side.

Alle dokumenter/aftaler vedrørende underdatabehandlere gemmes tillige i mappen "Databehandleraftaler" i den digitale mappe for Datapolitikken.

Det er databehandlerens ansvar at sikre sig, at de tekniske og organisatoriske sikkerhedsforanstaltninger, der pålægges databehandleren i databehandleraftalen mellem Haslev Privatskole og databehandleren, tillige pålægges eventuelle underdatabehandlere, der gøres brug af. Det er også databehandlerens opgave og ansvar at føre tilsyn med eventuelle underdatabehandlere.

Det er derimod Haslev Privatskoles opgave at kontrollere, at alle databehandlere har ført det fornødne tilsyn med eventuelle underdatabehandlere. Dette gøres én gang årligt i forbindelse med, at Haslev Privatskole kontrollerer alle data behandlere jf. procedure herom i bilag 8.

## **7 FORTEGNELSE OVER BEHANDLINGSAKTIVITETER**

### **7.1 Fortegnelsen**

Jf. databeskyttelsesforordningens artikel 30 er den dataansvarlige forpligtet til at lave en fortegnelse over behandlingsaktiviteter

### **7.2 Fortegnelse over behandlingsaktiviteter – medarbejdere**

Som **bilag 9** til Datapolitikken er vedlagt en fortegnelse over behandlingsaktiviteter for medarbejdere, der er tilknyttet Haslev Privatskole.

Fortegnelsen omfatter personoplysninger om følgende kategorier af medarbejdere:

- Ansatte medarbejdere
- Vikarer
- Praktikanter
- Bestyrelsesmedlemmer

### 7.3 Fortegnelse over behandlingsaktiviteter – børn/elever

Som **bilag 10** til Datapolitikken er vedlagt en fortegnelse over behandlingsaktiviteter for børn/elever, der er tilknyttet Haslev Privatskole herunder skolens SFO'en.

### 7.4 Ændringer i fortegnelsen

Fortegnelsen gennemgås minimum én gang årligt i forbindelse med, at Datapolitikken gennemgås jf. årshjulet vedlagt i bilag 1.

Ved indførelse af nye arbejdsområder i organisationen, hvor der sker en væsentlig ny behandlingsaktivitet af personoplysninger, skal der tillige udarbejdes en ny fortegnelse over behandlingsaktiviteter jf. årshjulet vedlagt i bilag 1.

## 8 **TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER**

### 8.1 Generelt om tekniske og organisatoriske sikkerhedsforanstaltninger

Det fremgår af databeskyttelsesforordningens artikel 5, stk. 1, litra f, at personoplysninger skal *"behandles 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".*

Det slås hermed fast, at organisationen skal iagttage en række tekniske og organisatoriske sikkerhedsforanstaltninger ved behandling af personoplysninger.

Det tekniske og organisatoriske sikkerhedsforanstaltninger, der iværksættes i organisationen, hænger i høj grad sammen med de risici, der er identificeret i organisationens risikovurdering jf. punkt 5.

## 8.2 Tekniske og organisatoriske sikkerhedsforanstaltninger på Haslev Privatskole

Haslev Privatskole er en organisation af en mindre størrelse, hvorfor det er besluttet fra ledelsens side, at der på tidspunktet for Datapolitikens udarbejdelse ikke er ressourcer til at tiltræde en godkendt certificeringsordning (eksempelvis ISO 27001).

Haslev Privatskole har derfor, på baggrund af udarbejdet risikovurdering, selv fastsat de tekniske og organisatoriske sikkerhedsforanstaltninger, der som minimum skal iagttages i organisationen med henblik på en sikker behandling af personoplysninger.

Haslev Privatskole vurderer løbende, hvorvidt Haslev Privatskole skal tiltræde en godkendt certificeringsordning eller om brancheorganisationen, der er på området for frie skoler, har udarbejdet et adfærdskodeks for tekniske og organisatoriske sikkerhedsforanstaltninger ved behandling af personoplysninger.

Af **bilag 11** til Datapolitikken fremgår de til enhver tid gældende tekniske og organisatoriske sikkerhedsforanstaltninger for Haslev Privatskole.

## 9 **DRIFTMÆSSIGE RETNINGSLINJER OG PROCEDURER**

Med henblik på sikring af, at Datapolitikken og de databeskyttelsesretlige regler overholdes i forbindelse med de enkelte driftsmæssige opgaver i organisationen, har Haslev Privatskole udarbejdet en række driftsmæssige retningslinjer og procedurer.

Haslev Privatskole s driftsmæssige retningslinjer og procedurer er vedlagt Datapolitikken som **bilag 12**.

## **10 DEN REGISTREREDES RETTIGHEDER/ORIENTERING TIL DE REGISTREREDE**

### **10.1 Generelt om de registreredes rettigheder**

Alle personer, hvis personoplysninger behandles på Haslev Privatskole, har en række rettigheder, der er fastslået i Databeskyttelsesforordningens artikel 13 – 22. Disse rettigheder er Haslev Privatskole forpligtet til at overholde som dataansvarlig.

Følgende rettigheder håndteres af Haslev Privatskole på eget initiativ:

- Den registreredes ret til at blive oplyst om behandlingen
- Den registreredes ret til sletning
- Den registreredes ret til ikke at blive underlagt afgørelser, der alene er baseret på automatisk behandling eller profilering

Følgende rettigheder håndteres af Haslev Privatskole ved anmodning fra den registrerede:

- Den registreredes ret til indsigt i de oplysninger, der behandles samt hvilke behandlinger, der foretages
- Den registreredes ret til berigtigelse af urigtige oplysninger
- Den registreredes ret til at anmode om begrænsning i behandlingen, så behandlingen alene består i opbevaring
- Den registreredes ret til at modtage oplysninger i et struktureret, almindelig anvendt og maskinlæsbart format
- Den registreredes ret til at få flyttet sine oplysninger til en anden dataansvarlig



- Den registreredes ret til at gøre indsigelse mod behandlingen af oplysninger

## 10.2 Processuelle krav ved håndtering af den registreredes rettigheder

I databeskyttelsesforordningens artikel 12 stilles der en række processuelle krav til den dataansvarlige, der skal iagttages, når den registreredes rettigheder håndteres.

Som **bilag 13** til Datapolitikken vedlægges procedure for Haslev Privatskoles overholdelse af de processuelle krav i forbindelse med modtagelse af en anmodning fra en registreret.

## 10.3 Håndtering af oplysningspligten

Jf. Databeskyttelsesforordningens artikel 13 og 14 skal den dataansvarlige give den registrerede skriftlig besked om, at der behandles oplysninger om vedkommende.

Oplysningspligten skal iagttages på eget initiativ.

Haslev Privatskole iagttager oplysningspligten på følgende måder:

Medarbejdere	Privatlivspolitik for medarbejdere ved Haslev Privatskole ( <b>bilag 14</b> )
Børn/elever	Privatlivspolitik for børn/elever ved Haslev Privatskole ( <b>bilag 15</b> )
Hjemmeside	Privatlivspolitik for besøgende på Haslev Privatskole s hjemmeside ( <b>bilag 16</b> )

## 11 DATABRUD

### 11.1 Ansvar ved databrud

Haslev Privatskole er, som led i driften, dataansvarlig for en række personoplysninger om medarbejdere og børn/elever, som Haslev Privatskole på egne vegne behandler, herunder indsamler, registrerer og opbevarer.

Retningslinjerne i punkt 11 har til formål at beskrive, hvordan Haslev Privatskole vil agere i tilfælde af, at der konstateres et brud på datasikkerheden i organisationen, dvs. et sikkerhedsbrud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til de personoplysninger, som Haslev Privatskole behandler, eksempelvis:

- Hackerangreb
- Offentliggørelse af personoplysninger på internettet ved en fejl
- Videregivelse af personoplysninger ved en fejl
- Personoplysninger går hændeligt til grunde (eksempelvis brand eller vandskade)
- Bærbart medie mistes
- Uvedkommende adgang til IT-systemer

### 11.2 Konstatering af brud på datasikkerheden

Haslev Privatskole har indført en række tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre, at eventuelle brud på persondatasikkerheden opdages. Der henvises til Datapolitikens punkt 8 herom.

Alle medarbejdere hos Haslev Privatskole er desuden forpligtet til omgående at underrette ledelsen, såfremt man bliver opmærksom på et muligt brud på datasikkerheden på Haslev Privatskole. Underretningen skal ske skriftligt til skolens ledelse.

Haslev Privatskoles data behandlere (og disses eventuelle underdatabehandlere) har via de indgåede databehandleraftaler forpligtet sig til at orientere Haslev Privatskole om enhver mistanke om eller konstatering af brud på datasikkerheden.

I tilfælde af brud på persondatasikkerheden følges den procedure, der er beskrevet nedenfor.

### 11.3 Dokumentation af brud på persondatasikkerheden

Haslev Privatskole har oprettet et dokument, der er vedlagt som **bilag 17** til Datapolitikken, hvori eventuelle brud på datasikkerheden på Haslev Privatskole løbende noteres.

Alle konstaterede brud på datasikkerheden noteres i dokumentet – også brud, der ikke nødvendigvis fører til en anmeldelse til Datatilsynet og efterfølgende underretning af den eller de berørte registrerede, jf. punkterne nedenfor.

For hvert brud på datasikkerheden beskrives i dette dokument de faktiske omstændigheder ved bruddet, dets virkninger og de afhjælpende foranstaltninger, som Haslev Privatskole har truffet i anledning af bruddet. Desuden tages for hvert brud stilling til, om der skal ske anmeldelse til Datatilsynet samt underretning af den eller de registrerede, der er berørt af bruddet, punkterne nedenfor. Endelig foretages en evaluering med henblik på at vurdere, om bruddet giver grundlag for at igangsætte nye organisatoriske, administrative og/eller tekniske løsninger på Haslev Privatskole, således at samme type hændelse fremover undgås.

Ledelsen er ansvarlig for dokumentet, herunder at dette løbende opdateres.

Dokumentet udleveres til Datatilsynet, hvis tilsynet anmoder herom.

#### 11.4 Anmeldelse til Datatilsynet om brud på datasikkerheden

For hvert enkelt konstateret brud på datasikkerheden vurderer ledelsen om der er grundlag for at foretage en anmeldelse af bruddet til Datatilsynet. Vurderingen dokumenteres skriftligt i skemaet i bilag 17.

Anmeldelse kan kun undlades, hvis det vurderes *usandsynligt*, at bruddet på datasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Følgende forhold skal altid inddrages i denne risikovurdering:

- Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse
- Oplysningernes art og omfang
- Risikoen for at registrerede kan identificeres
- Konsekvenser bruddet kan have for de registrerede
- Hvorvidt bruddet omfatter særlige registrerede (f.eks. børn)
- Antallet af berørte fysiske personer

Der skal være en rimelig høj grad af sikkerhed, før anmeldelse til Datatilsynet undlades.

Vurderingen skal foretages hurtigst muligt, og således at en eventuel anmeldelse til Datatilsynet så vidt muligt kan ske inden 72 timer efter, at bruddet på persondatasikkerheden er blevet konstateret.

Såfremt der skal ske anmeldelse til Datatilsynet, foretages denne via den digitale indgang på [www.virk.dk](http://www.virk.dk).

Anmeldelsen skal indeholde følgende:

- En beskrivelse af karakteren af bruddet på datasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
- Den relevante kontaktperson hos Haslev Privatskole
- En beskrivelse af de sandsynlige konsekvenser af bruddet på datasikkerheden
- En beskrivelse af, hvordan Haslev Privatskole har håndteret eller forventer at håndterer bruddet på datasikkerheden, herunder en beskrivelse af de foranstaltninger, der er truffet, for at begrænse dets mulige skadevirkninger

#### 11.5 Underretning af den registrerede om brud på persondatasikkerheden

For hvert enkelt konstateret brud på datasikkerheden vurderer ledelsen, om der er grundlag for at underrette den eller de registrerede, der er berørte af bruddet. Vurderingen dokumenteres skriftligt i skemaet i bilag 17.

Underretning skal som udgangspunkt ske, hvis det vurderes sandsynligt, at det pågældende brud på datasikkerheden vil medføre en høj risiko for fysiske personers rettigheder. Ved denne risikovurdering skal alle de mulige konsekvenser og negative virkninger for den eller de berørte registrerede inddrages.

Vurderingen skal foretages hurtigst muligt, og således at en eventuel underretning kan ske uden unødigt forsinkelse efter, at bruddet på datasikkerheden er blevet konstateret.

Vurderes det, at bruddet er af en sådan karakter, at det sandsynligvis vil indebære en høj risiko for den eller de berørte registrerede, kan underretning kun undlades, hvis en af undtagelserne i databeskyttelsesforordningens artikel 34, stk. 3, er til stede, herunder hvis der på Haslev Privatskole er gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger (f.eks. kryptering) og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden.

Såfremt der skal ske underretning, foretages denne via e-mail eller pr. brev i et klart og forståeligt sprog. Underretningen skal indeholde følgende:

- En beskrivelse af karakteren af bruddet på persondatasikkerheden
- Kontaktperson hos Haslev Privatskole
- Beskrivelse af de sandsynlige konsekvenser, som bruddet på persondatasikkerheden har for den registrerede
- Beskrivelse af, hvordan Haslev Privatskole har håndteret eller forventer at håndtere bruddet på datasikkerheden, herunder en beskrivelse af de foranstaltninger, der er truffet, for at begrænse dets mulige skadevirkninger

Underretningen sendes til hver enkelt af de berørte registrerede.

## **12 OPFØLGNING OG OPDATERING**

### **12.1 Årlig gennemgang af Datapolitikken**

Ledelsen bærer ansvaret for at sikre, at der mindst én gang årligt med afsæt i årshjulet, der er vedlagt Datapolitikken som bilag 1 foretages en systematisk gennemgang og vurdering af, om Datapolitikken skal opdateres med henblik på at sikre, at politikken altid er opdateret og i overensstemmelse med den seneste praksis fra Datatilsynet og fortolkninger af EU's Persondataforordning.

Alle tilrettede dokumenter (Datapolitikken samt tilhørende underbilag) påføres en dato for seneste ændring.

### **12.2 Nye arbejds- og driftsområder i organisationen**

I årshjulet, der er vedlagt Datapolitikken som bilag 1 fremgår det ligeledes, hvordan organisationen skal forholde sig i relation til Datapolitikken i de tilfælde, hvor der indføres helt nye arbejds- eller driftsområder i organisationen.

*Marts 2019*