Campus Bornholm

Persondataforordning

Lokale Regler og Procedurer

Version: 16. december 2020

Indholdsfortegnelse

Henvisninger:

- **Web-dokumentation**
  Samlet dokumentation foreligger på https://it.cabh.dk/Beredskab indeholdende:
  - Databehandlingsområder
  - Systembeskrivelser
  - Databehandleraftaler

Bilag:

1. Elektronisk opbevaring og arkivering
2. Dataoplysning
   - Underbilag 1 – Oplysningsbrev
3. Dataudlevering
   - Underbilag 1 – Erklæring for udlevering af egne personlige oplysninger
4. Datatilsynets minimumskrav til behandling af HR-oplysninger
5. Sikkerhedspersonale – Kontaktoplysninger
6. Datatilsynet om billeder
   - Underbilag 1 – Samtykkeerklæring for offentliggørelse af billeder og video
7. Samtykkeerklæring for personfølsomme oplysninger
8. Insident Response Plan

1 Virksomheden

Campus Bornholm er en selvejende institution inden for den offentlige forvaltning med hjemsted i Bornholms Regionskommune, Region Hovedstaden, og omfattet af lov om institutioner for erhvervsrettet uddannelse.

Campus Bornholms formål er i overensstemmelse med lovgivningen at udbyde erhvervsrettet grund- og efteruddannelse og anden uddannelse og undervisning. Campus Bornholm udbyder erhvervsuddannelser og arbejdsmarkedsuddannelser m.v. inden for primært det merkantile område og det tekniske område, gymnasiale uddannelser (hf, hhx, htx og stx) samt almen voksenundervisning og ordblindeundervisning for voksne.

1.1 Uddannelser

Campus Bornholm er er kombinationsskole, med følgende uddannelser:

- Gymnasium
  - STX ..... BEK nr 497 af 18/05/2017
  - HHX og HTX ..... LBK nr 871 af 27/08/2008
  - EUX ..... LBK nr 612 af 28/05/2019
  - HF ..... LBK nr 767 af 09/06/2015
- Erhvervsskole
  - Teknisk Skole
    - Erhvervsuddannelser ..... LBK nr 51 af 22/01/2020 og LBK nr 597 af 16/05/2019
    - Arbejdsmarkedsuddannelser ..... LBK nr 616 af 03/06/2019
    - Handelsuddannelse ..... BEK nr 421 af 15/04/2020
  - Mad til mennesker ..... BEK nr 312 af 21/03/2013
- Sprogskole ..... LBK nr 901 af 19/08/2019

1.2 Institutionsoplysninger

- CVR: 38442813
- Hjemmeside: https://www.campusbornholm.dk
- Adresse: Minervavej 1, 3700 Rønne
- Mail: post@cabh.dk
- Telefon: +45 5695 9700

2 Generelt

2.1 Begreber og definitioner

Der opereres med følgende begreber og definitioner:

- **"Need-to-know**" dækker – i modsætning til "nice-to-know" – over den adgang der er nødvendig for at kunne udføre opgaven.
- **Godkendt personale** er ansatte, eller ansatte i samarbejdende virksomheder, der er udpeget til behandling af klassificeret materiale, og som i kraft heraf, er underlagt tavshedspligt.
- **Uvedkommende** er enhver person der ikke er godkendt til indsigt i, eller behandling af, en given oplysning, sag eller område. Uvedkommende er også ellers godkendt personale, der ikke har brug for at vide noget om emnet.
- **Klassificeret materiale** er materiale der er underlagt særligt krav til beskyttelse. Klassificeret materiale må kun ses og behandles af godkendt personale.

2.1.1 Sikkerhedstyper.

- **Generel sikkerhed** omfatter krav til organisering og styring, herunder ansvarsfordeling, uddannelse og kontrolvirksomhed.
- **Personalesikkerhed** omfatter foranstaltninger, der har til formål at vurdere personellets sikkerhedsmæssige kvalifikationer med henblik på tavshedspligt, omgang med betroede midler og børn.
  Relevante oplysninger (strafbare forhold) og (børne-)attester indhentes ved ansættelse.
- **Materielsikkerhed** omfatter foranstaltninger til beskyttelse af materiel, herunder værktøjer, elektronisk udstyr og møblement.
- **Dokumentsikkerhed** omfatter foranstaltninger til beskyttelse af informationsbærende materialer (dokumenter og elektroniske lagermedier) mod hærværk, tyveri og tab.
- **Informationssikkerhed** omfatter foranstaltninger til beskyttelse af koncernens IT-systemer under behandling, lagring og transmission af informationer mod spionage, sabotage, kriminalitet og kompromittering samt under opretholdelse af fortrolighed, integritet, og tilgængelighed.
- **Fysisk sikkerhed** omfatter foranstaltninger i form af mekanisk sikring, elektronisk overvågning og fysisk tilstedeværelse til beskyttelse af virksomheden og dens materiel, dokumenter og informations- og kommunikationssystemer mod spionage, sabotage, kriminalitet og kompromittering.
- **Kontorsikkerhed** omfatter de foranstaltninger, der skal træffes på det enkelte kontor til imødegåelse af kompromittering af klassificeret materiale, mens det behandles og opbevares i kontorer, mødelokaler, arkiver m.v.
  Alle ansatte er ansvarlige for, at uvedkommende ikke får adgang til eller indsigt i klassificeret materiale.

2.2 Sikkerhedsstruktur

Følgende indgår i håndtering af sikkerheden:

- **Dataansvarlig** er Campus Bornholms Direktør.

  Den dataansvarlige indfører regler og gennemfører passende foranstaltninger med henblik på at sikre og være i stand til at påvise, at behandlingen af personoplysninger foretages i overensstemmelse med forordningen (”Compliance”).

  Foranstaltningerne omfatter navnlig:

  - Opbevaring af dokumentation.
  - Gennemførelse af datasikkerhedskrav.
  - Gennemførelse af konsekvensanalyser vedrørende databeskyttelse.
  - Overholdelse af kravene om forudgående godkendelse eller høring af tilsynsmyndigheden.
  - udpegning af en DPO.

  Den dataansvarlige gennemfører mekanismer, der har til formål at kontrollere effektiviteten af de trufne foranstaltninger.

- **Databehandler** er eksterne virksomheder/administrative fællesskaber med hvilke der er tegnet aftale om udførelse af databehandling på Campus Bornholms vegne.
  Det er den dataansvarliges ansvar at sikre, at databehandleren træffer de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.

- **Data Protection Officer** (DPO) er en, over for Campus Bornholm, uafhængig person, hvis opgave det er, at føre tilsyn med Persondataforordningens bestemmelser. Anvisninger og påbud fra denne, skal følges.
- **Uddannelsesansvarlige** sikrer efterlevelse af de fastlagte bestemmelser inden for uddannelsesområdet.
- **IT-ansvarlige** sikrer efterlevelse af de fastlagte bestemmelser inden for IT-området.
- **HR-ansvarlige** sikrer efterlevelse af de fastlagte bestemmelser inden for personaleområdet.

3 Databehandling

3.1 Databehandlere

Campus Bornholm anvender databehandlere til persondatabehandling i centrale systemer. Sikkerhed for databeskyttelse er (af Campus Bornholm) pålagt databehandlerne.

Oversigt og status fremgår af "web-dokumentation".

Persondatabehandling foretages også lokalt, men gemmes på EFIF's filserver.

3.2 Oplysningstyper

Oplysninger, der som standard behandles (og registreres), fremgår af bilag 2.

Derudover foretages der behandling af personfølsomme oplysninger på følgende områder og systemer:

- LØN
  - Fagforeningsmæssige tilhørsforhold (SLS)
- HR
  - Helbredsoplysninger (personalearkiv)
  - Straffe- og børneattester (personalearkiv)
- Uddannelsesadministration
  - Helbredsoplysninger (Lectio, EASY)
- Mentor
  - Helbredsoplysninger (fil-arkiv)
  - Straffe- og børneattester (fil-arkiv)
- Studievejledning
  - Helbredsoplysninger (fil-arkiv)
  - Straffe- og børneattester (fil-arkiv)

For detaljeret oversigt, henvises til web-dokumentationen.

3.3 Rollevurdering

Campus Bornholm er:

- Dataansvarlig, og
- Databehandler for FGU Bornholm vedrørende:
  - Løn (SLS)
  - Bogholderi (Navision STAT)
  - Controllerfunktion

For så vidt angår Facebook (som kan implicere databehandlerrollen) anvendes det ikke officielt i undervisningsøjemed. Der er udtrykkeligt udstedt forbud mod anvendelse af det.

4 Risici

"Privacy Impact Assessment"

4.1 Risikovurdering

Risiko for datalæk er altid til stede. Der skal til stadighed drages omsorg for at gældende regler overholdes.

4.1.1 Generelt

Datalæk sker typisk på følgende måder:

1. Medarbejder udsender klassificerede oplysninger til uautoriseret. Det kan ske:
    a. Tilsigtet (ved undladelse af overholdelse af gældende regler)
        1) Ukrypteret mailafsendelse (uautoriserede kan få adgang).
        2) Bevidst skadelig handling (whistleblowing).
    b. Utilsigtet (fremsendelse til forkert modtager)
2. Utilstrækkelig fysisk beskyttelse af klassificeret materiale og oplysninger, på grund af:
    a. Manglende overholdelse af gældende bestemmelser (sløseri eller ikke indførte fastlagte beskyttelsesforanstaltninger).
    b. Dårlige fysiske installationer (som ikke yder nok beskyttelse)
3. Hacking
    a. Centrale systemer (indtrængen).
    b. Overtagelse af medarbejders computer ved
        1) Phising (klik på skadeligt link i mail eller på webside)
        2) Fysisk installation af agent – enten ved indbrud eller under manglende opsyn.
4. Blotlæggelse (forkert eller manglende sikkerhed på servere)

4.1.2 Sårbarhed og omfang ("impact")

Hvor der risiko for datalæk, skal konsekvensanalyse foretages.

Da risiko altid foreligger, er der fortaget sårbarhedsanalyse for alle områder og anvendte systemer. (se "web-dokumentation").

4.2 Brud på datasikkerheden

Brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet udbredelse af eller adgang til personoplysninger, der er videregivet, lagret eller på anden måde behandlet, skal anmeldes Datatilsynet senest efter 72 timer fra sikkerhedsbruddets opdagelse.

Sikkerhedsbruddets omfang skal i første omgang vurderes lokalt (IT-ansvarlige, HR-ansvarlige, DPO) inden sagen indberettes.

Indberetning skal indeholde følgende:

- Beskrivelse af karakteren af bruddet på persondatasikkerheden, herunder kategorierne og antallet af berørte registrerede samt kategorierne og antallet af berørte registreringer.
- Angivelse af identitet og kontaktoplysninger for DPO'en eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
- Anbefaling af foranstaltninger, der kan afhjælpe de mulige skadevirkninger af bruddet på persondatasikkerheden.
- Beskrivelse af konsekvenserne af bruddet på persondatasikkerheden.
- Beskrivelse af de foranstaltninger, som den dataansvarlige foreslår eller har iværksat for at afhjælpe bruddet på persondatasikkerheden.

4.2.1 Sanktioner

Overtrædelsestype	Bødeniveau
• Ingen fastlæggelse af ordninger for registreredes anmodninger • Ej rettidig besvarelse heraf	Op til € 250.000
• Ikke giver relevante oplysninger ved indsigtsanmodning • Ikke sletter oplysninger • Manglende ajourføring af dokumentation	Op til € 500.000
• Behandler oplysninger uden hjemmel • Ikke respekterer en indsigelse • Ikke varsler tilsynet om brud på sikkerheden • Ikke gennemfører konsekvensanalyser • Ikke udpeger en DPO • Overfører oplysninger til tredjelande uden hjemmel	Op til € 1.000.000

5 Databeskyttelse

5.1 Fysisk beskyttelse

5.1.1 Kontorsikkerhed

I kontorer hvor klassificeret databehandling finder sted, skal almindelig kontorsikkerhed opretholdes.

- Adgang til lokalet skal begrænses til autoriseret personale.
- Når en computer forlades, skal man logge af eller slukke den.
- Når kontoret efterlades ubemandet, skal det aflåses.
- Der skal holdes øje med, om computere har undergået fysiske forandringer eller om der er blevet tilsluttet ekstra udstyr (USB-penne eller lignende).

I kontorer og områder hvor der er adgang hele tiden[1], skal der være truffet særlige foranstaltninger mod uautoriseret adgang til computere og klassificeret materiale.

5.1.2 Opbevaring

Materiale (mapper, ringbind o.l.) skal opbevares i aflåst lokale og/eller aflåst skab. Personfølsomt eller andet følsomt materiale skal opbevares i aflåst skab.

5.1.3 IT-installationer

Fysisk adgang til netværksudstyr og servere giver sårbarhed over for ødelæggelse eller mulighed for uautoriseret adgang. Udstyret er vitalt for IT-driften, og skal derfor ydes særlig beskyttelse.

Serverrum skal til stadig holdes aflåst. Kun adgang for IT-personale. Ikke-autoriserede personer (håndværkere o.a.) gives kun adgang ledsaget af IT-personale. Pedeller har adgang, men skal aftale/melde adgang. Der føres besøgslog (ophængt i serverrum).

Netværksskabe er knudepunkter for netværket. Kun IT-personale har adgang hertil.

5.1.4 Bygnings- og rumadgang

Bygningerne M1, M2 og M10 er åbne på hverdage 06:00 – 17:00. Derefter kun adgang med brug af låsekort. Uden for anførte tidsrum, er alarm aktiveret. Vagtselskab møder op ved alarm.

Rum har elektroniske låse, og der er defineret låsegrupper, for hvilke der er gradueret adgang.

5.2 Elektronisk beskyttelse

Der må udelukkende anvendes godkendte systemer til opbevaring af persondata.

[1] Lager, bibliotek o.a.

Fordi persondata ikke må forlade EU-området, må (bl.a.) følgende systemer ikke anvendes (til behandling af persondata):

- Flickr
- Gdrive
- DropBox
- FaceBook
- M.fl.

5.2.1 Mail

I forbindelse med mail-korrespondance skal følgende foranstaltninger træffes:

- **Intern mail**: Ingen begrænsninger
- **Ekstern mail**: Personoplysninger indeholdende CPR og/eller person- og personfølsomme oplysninger, eller andre følsomme oplysninger skal krypteres

Det skal – i videst mulig udstrækning – undlades at anvende mail til personoplysninger.

5.2.2 Udskrivning

For næsten al udskrivning anvendes en "Follow-Me"-løsning, hvor udskrifter først udskrives, når man på én af de kopimaskiner, der er med i løsningen, "swiper" sit låsekort. Det betyder, at udskrifter ikke kommer uvedkommende til indsigt, og højner derved generelt dokumentsikkerheden.

5.3 Opbevaring

5.3.1 Systemer og tjenester

Opbevaring må kun ske på godkendte systemer og tjenester

5.3.2 Arkivering

Alle dokumenter skal fremadrettet arkiveres elektronisk, og det skal også tilstræbes for papirarkiv. Den elektroniske arkivering imødekommer disse formål:

- Dokumenterne kan tilgås, eksternt[2] (fx når der arbejdes hjemmefra).
- Dokumenterne kan tilgås på tværs af organisationen.
- Der er udpegede godkendte placeringer/systemer for hvilke der er specifikke adgangsbegrænsning.
- Giver samlet overblik over hvor mange og hvilke typer oplysninger der arkiveres.
- Der er regelmæssig backup.
- Udtræk af oplysninger kan automatiseres, og oplysningspligten kan nemme opfyldes.
- Sletning kan automatiseres.

Arkivering sker i følgende systemer:

- IMS Arkiv
- Netværksdrev (se bilag 1 – "Elektronisk opbevaring og arkivering")
- EASY filarkiv
- PersSys

Detaljeret beskrevet i "web-dokumentation".

5.4 Forældede data

Elektroniske og trykte data skal løbende kasseres, i takt med deres forældelse.

[2] Kun fra udleverede arbejdscomputer.

5.4.1 Forældelsesfrister

- **Ansatte**
  Data kasseres umiddelbart efter ansættelsens ophør. Hvor operative hensyn i enkelttilfælde taler for det, kan visse oplysninger gemmes i op til 1 år – fx en leders mailboks.
- **Elever**
  Data kasseres 1 år efter ophørt uddannelse[3].
  Eksamensbeviser gemmes i 30 år.

5.5 Kassering

5.5.1 Sletning

Sletning foregår automatisk, hvor det er muligt. Hvor det ikke er muligt, sker det manuelt.

Ved anskaffelse af nye systemer – eller revidering af eksisterende – skal det prioriteres, at de har indbygget funktionalitet for automatisk sletning.

Sletteprocedurer fremgår af "web-dokumentation".

5.5.2 Destruering

Klassificeret papirmateriale skal destrueres ved makulering[4] eller kontrolleret afbrænding[5]. Hvor det ikke på stedet er muligt at destruere materialet, skal det afleveres centralt, for videre destruering.

Øvrigt materiale bortskaffes som almindeligt affald.

6 Dataoplysning

Ansatte og elever har krav på at få oplyst, hvilke data der som standard registreres.

Oplysningsmetoder fremgår af bilag 2 – "Dataoplysning".

7 Dataudlevering

Ansatte og elever har krav på – efter ønske – at få udleveret de oplysninger der er på dem[6]. Såfremt nogen måtte have ønske herom, skal anmodning fremsendes således:

- **Ansatte**:
  Via Økonomi- og Administrationschef
- **Elever**:
  Via Uddannelsesadministrationen

Dataudlevering fremgår af bilag 3 – "Dataudlevering".

8 Ajourføring af oplysninger

Oplysninger skal altid holdes ajour. Hvor det er muligt, skal systemer opsættes til automatisk CPR-register validering[7].

---

[3] Det sker ofte at eleven kommer ind igen kort tid efter.

[4] Makulering er itu-skæring af papir. Der bør anvendes "krydsskærsmakulering" der skærer papiret ud i millimeterstykker, og ikke strimmelmakulering der skærer papiret ud i strimler. Sidstnævnte er for nemme at sætte sammen igen.

[5] Med kontrolleret afbrænding menes en overvåget afbrænding hvor der efterfølgende ikke er læsbare rester tilbage af materialet.

[6] LT: På EFIF's 5. Sikkerhedsgruppemøde af 17-01-2019 anførte DPO at det ikke skal forveksles med aktindsigt. Der skal lægges mere vægt på *hvilke typer af data der er registreret*. Der skal fx ikke udleveres samtlige mails hvor personen er nævnt.

[7] Derved opdateres bl.a. navne- og adresseoplysninger automatisk.

Såfremt en ansat eller elev konstaterer fejlagtige eller forældede oplysninger på sig selv, skal de ved henvendelse til HR eller Uddannelsesadministrationen, umiddelbart rettes/slettes.

9 Portering af data

Hvis en medarbejder eller elev skifter uddannelsessted, og udtrykker ønske at eksisterende relevante data medflyttes, skal anmodningen efterfølges. Dette vil ofte kræve assistance fra IT-administrationen og evt. eksterne databehandlere.

10 Håndtering af fotos og videos

Samtykkeerklæring er nødvendig ved portræt- og holdbilleder (f.eks. nyudlærte, vinderhold, klassebilleder), men ikke ved situationsbilleder. Samtykkeerklæring skal indhentes inden foto-seancen.

(se bilag 7 – ” Datatilsynet om billeder”)

11 Godkendte systemer og programmer

Kun godkendte systemer og programmer må anvendes.

EFIF har lavet spærring for installation, så kun administratorer kan godkende installation. Det betyder, at de fysisk skal indtaste brugernavn og adgangskode i hvert enkelt tilfælde.

EFIF anvender et overvågningssystem (”SecTeer”), der holder øje med skadelige programmer på den enkelte workstation. Skedige programmer deaktiveres.
Ikke-skadelige programmer fra 3.-partsleverandør (Adobe, Google, m.fl.) opdateres automatisk.

Softwarecenteret indeholder godkendte programmer, og godkendt ønske om anvendelse af et programmer, optages hér.

IT-administrationen fører desforuden en liste på: https://it.cabh.dk/Home/Indhold/105

11.1 Godkendelse af nye systemer og programmer

Systemer og programmer der behandler personoplysninger, skal risicivurderes i forhold til, hvordan personoplysningerne behandles. Proceduren hedder DPIA (Data Protection Impact Assessment).

12 Kontrolmekanismer

For til stadighed at opretholde høj persondatabeskyttelse samt overholdelse af gældende EU-forordning og egne regler (”Compliance”), iværksættes nednævnte kontrolmekanismer:

12.1 Løbende kontrol

Alle ansatte skal bidrage til:

- Kontrol af om regler inden for eget område overholdes.
- Melde om uregelmæssigheder.
- Bidrage til forslag til forbedringer.

Sikkerhedspersonale skal ved fysisk rundering kontrollere:

- Faktisk efterlevelse af gældende regler og procedurer.
- Ændring i fysiske, personalemæssige og andre forhold, der kan, eller medfører brud sikkerheden.
- IT-systemers fortsatte opretholdelse af fastlagte sikkerhed.
- Databehandleraftaler for nye leverandører.

12.2 Årshjul

Der fastlægges årligt tilbagevendende tidspunkter, hvor udpeget sikkerhedspersonale udfører følgende rutiner:

- Kontrol af regelsæt gennemgås
  - Nye systemer/procedurer vurderes
  - Gamle systemer/procedurer revurderes.
- Revision af tilknyttet revisionsfirma
- Information af ansatte
  - Ny regler oplyses
  - Nyt personale grundinformeres.
- Deltagelse i ERFA-gruppe sammen med andre (EFIF-)skoler.

13 Sikkerhedsbrud

Ref.: Bilag 5 – "Sikkerhedspersonale - Kontaktoplysninger"

13.1 Hændelse ("Incident")

En hændelse er en uregelmæssighed, der kan medføre – eller har medført – følgende:

Utilsigtet eller forsætlig destruering, sletning, tab, ændring, uautoriseret adgang eller offentliggørelse af personlige data.

Mistanke om – eller en konstateret hændelse – skal ufortøvet meldes til nærmeste leder, der melder videre til den lokale datakontaktperson. Datakontaktpersonen kontakter det øvrige relevante sikkerhedspersonale.

13.2 Vurdering

Sikkerhedspersonalet vil vurdere hændelsens alvor. Vurderes hændelsen at have afstedkommet uvedkommendes adgang til persondata, er der tale om et sikkerhedsbrud.

13.3 Iværksættelse af "Incident Response Plan"

I tilfælde af sikkerhedsbrud, skal "Incident Response Plan" (jf. bilag 8) omgående iværksættes.

Elektronisk opbevaring og arkivering

Følgende netværksstruktur skal anvendes i det omfang der er behov for lagring af de anførte kategorier.

Kategori	Mappeplacering	Type	Navn	Filtype	Note
Foto – Låsekort	P:\Foto\Låsekort	Enkeltfil	<cpr>	.jpg .png	
Foto – Portræt – Ansatte	P:\Foto\Portræt\Ansatte	Enkeltfil	<brugernavn> - <navn>	.jpg .png	
Foto – Portræt – Elever	P:\Foto\Portræt\Elever	Enkeltfil	<brugernavn> - <navn>	.jpg .png	
Foto – Gruppe	P:\Foto\Gruppe	Enkeltfil	<dato> - <gruppe>	.jpg .png	Gruppe- eller holdnavn. (1)
Foto – Situation	P:\Foto\Situation	Mappe pr. situation	<dato> - <situation>		Fx: ”2018-05-04 Gallafest STX” (1)
		– med enkeltfiler	<valgfri>	.jpg .png	
Samtykkeerklæringer	P:\Samtykke	Mappe pr. person	<brugernavn> - <navn>		
		– med enkeltfiler	<valgfri>	.pdf	
Persondata – Ansatte	P:\PersonData\Ansat	Mappe pr. person	<brugernavn> - <navn>		= Personalearkiv
		– med enkeltfiler	<valgfri>	.pdf	
	IMS Arkiv	Record	<cpr>	.pdf	
Persondata – Elever	P:\PersonData\Elev	Mappe pr. person	<brugernavn> - <navn>		
		– med enkeltfiler	<valgfri>	.pdf	
	IMS Arkiv	Record	<cpr>	.pdf	
Kvitteringer – Nøgler/låsekort	P:\Kvittering\NøgleLås	Enkeltfil	<brugernavn>	.pdf	
Kvitteringer – Computerudstyr	P:\Kvittering\Computer	Enkeltfil	<brugernavn>	.pdf	
Kvitteringer – Mobiltelefon	P:\Kvittering\Mobil	Enkeltfil	<brugernavn>	.pdf	

Alle mapper er beskyttet med Active Directory gruppesikkerhed.

Noter:

1. Skal behandles manuelt.

Dataoplysning

Oplysninger og metoder

Underbilag:

1. Velkomstmeddelelse

Følgende data registreres som standard, og disse metoder anvendes for løft af oplysningspligt:

Ansatte	Elever
Oplysninger: • CPR, Navn, Adresse, mailadresse og telefon afdeling og hold • Brugernavn til netværk, UNI-login og Lectio • Fravær • Uddannelse • CV • Situationsbilleder • Fagforeningsmæssige tilhørsforhold (betaling via løn) • Helbredsoplysninger • Straffeattest + børneattest	Oplysninger: • CPR, Navn, Adresse, mailadresse og telefon afdeling og hold • Brugernavn til netværk, UNI-login og Lectio • Foto til studiekort • Fravær • Karakterer, vurderinger • Situationsbilleder • Helbredsoplysninger • Straffeattest + børneattest
Metoder: • Oplyses på INTRA	Metoder: • Lectio forside • Oplysningsmeddelelse medsendes velkomstbrev i e-boks.

Velkommen som studerende på Campus Bornholm

Vi glæder os over at du har valgt at tage din uddannelse hos os.

Fotografering

Ved skolestart, skal der tages et portrætfoto til dit låse- og printkort og det studieadministrative system Lectio. Det er obligatorisk.

Ved forskellige begivenheder og enkelte undervisningsaktiviteter vil der bliver taget situationsbilleder, som vi i nogle tilfælde offentliggør (fx hjemmeside, FaceBook og presse). Inden situationsbillederne tages, får klassen besked om det.

Studie- og printkort

Du får udleveret et studie- og printkort til brug på skolen, som gælder så længe du går her. Det er personlig og må ikke udlånes til andre. Hvis du måtte miste det, skal du omgående melde det. Kortet skal afleveres når du stopper.

Kortet har påtrykt foto, da det er din legitimation. Du skal forevise det på forlangende af skolens ansatte, vagter o.a.

Ud over at fungere som legitimation, anvendes det også til print og kopiering.

Computersystemer

Du får udleveret en computerkonto til brug på skolen, som gælder så længe du går her. Den er personlig og må ikke oplyses til andre eller lånes ud. Hvis andre får adgang til dit password, skal du omgående skifte det.

Hvis det er muligt, bedes du medbringe din egen computer. Ellers kan du, efter behov, anvende én af skolens computere.

Registreringer

- For at kunne håndtere dig som studerende, er du registreret med følgende oplysninger:
- CPR, Navn, Adresse, mailadresse og telefon
- Afdeling og hold
- Brugernavn til vores netværk, UNI-login og Lectio
- Fravær
- Eksamenskarakterer
- Portrætfoto

Vi opbevarer oplysningerne i 1 år efter endt uddannelsesforløb, hvorefter de automatisk slettes.
Vi opbevarer dine kursus-/eksamensbeviser i 30 år (jf. gældende lov herfor).

Dataudlevering

Underbilag:

1. Erklæring for udlevering af egne personlige oplysninger

Udlevering sker kun ved personligt fremmøde, idet modtageren skal:

- Identificere sig
- Kvittere for modtagelsen

Afhængig af, hvad der aftales mellem skolen og anmodende person, kan dataudlevering ske på følgende måder:

- Fremvisning – via skærm eller
- Skriftlig udlevering
- Kombination af ovennævnte

Ansatte	**Elever**
Oplysninger: • CPR, Navn, Adresse, mailadresse og telefon afdeling • Brugernavn til netværk, UNI-login og Lectio • Fravær • Uddannelse • Fagforeningsmæssige tilhørsforhold • Helbredsoplysninger • Oplysninger om strafbare forhold – herunder børneattest	Oplysninger: • CPR, Navn, Adresse, mailadresse og telefon afdeling og hold • Brugernavn til netværk, UNI-login og Lectio • Foto til studiekort • Fravær • Eksamenskarakterer • Helbredsoplysninger • Oplysninger om strafbare forhold – herunder børneattest
System fremskaffelsemetode: • PersSys (webopslag) • Personalearkiv (manuelt) • Filmapper (manuelt) • IMS Arkiv (manuelt) • Cicero (manuelt) • SLS (manuelt) • Navision	System fremskaffelsemetode: • UMS (webopslag) • IMS Arkiv (manuelt) • Filmapper (manuelt) • Lectio (manuelt) • EASY – AMU og Praktik (manuelt) • Elevplan (webopslag) • Svejsepas (manuelt) • Cicero (manuelt) • Navision

Erklæring

– for udlevering af egne personlige oplysninger

Jeg erklærer hermed at:

☐ *Jeg har set mine personlige oplysninger.*
☐ *Jeg har fået udleveret mine personlige oplysninger i skriftlig form.*

Modtager	Campus Bornholm
_____	_____
Dato	Dato
_____	_____
Navn	Navn
_____	_____
Underskrift	Underskrift

Datatilsynets minimumskrav til behandling af HR-oplysninger

1. Beskrivelse af hvordan personaleoplysninger beskyttes.
2. Autorisation af personer, der har et sagligt behov for adgang til oplysningerne – så få personer som muligt.
3. Instruktion og oplæring af medarbejdere, der håndterer personaleoplysninger.
4. Personaleoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug.
5. Adgangskontrol til systemer – personlige koder.
6. Forgæves forsøg på at få adgang til IT-systemer med følsomme personaleoplysninger skal registreres.
7. Beskyttelse af bærbare datamidler (USB-nøgler mv.) med adgangskode og kryptering.
8. PC'ere koblet til internettet skal have en opdateret firewall og viruskontrol installeret.
9. Kryptering af hjemmesideformularer, hvor følsomme personaleoplysninger og personnummer kan indtastes og fremsendes.
10. Kryptering af e-mails, der indeholder følsomme personaleoplysninger og personnummer.
11. Sikkerhedsforanstaltninger i forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, og når datamedier skal sælges eller kasseres.
12. Indgåelse af databehandleraftaler med databehandlere.

Sikkerhedspersonale

Kontaktoplysninger

Rolle	Navn, titel	Email	Telefon
Dataansvarlige	Inge Prip, Direktør	ipr@cabh.dk	6012 1801
Dataansvarlige – stedfortræder	Lisbeth Hvid Christensen, Vicedirektør	sso@cabh.dk	6012 1803
Uddannelsesansvarlige	Lisbeth Hvid Christensen, Uddannelseschef GYM Claus Jørgensen, Uddannelseschef EUD	lhc@cabh.dk clj@cabh.dk	5364 2676 6012 1831
HR-ansvarlige	Signe Saabye Ottosen, Ressourcechef	sso@cabh.dk	6012 1803
IT-ansvarlige	Lars Thisted, IT-koordinator	lt@cabh.dk	6012 1822
Lokale Datakontaktperson	Lars Thisted, IT-koordinator	lt@cabh.dk	6012 1822
Data Protection Officer (DPO)	Flemming Rasmussen	fr@efif.dk	2060 1942
Data Protection Officer (DPO) - stedfortræder	Arild Ehrenskjöld	ague@efif.dk	2541 3506

Datatilsynet om billeder

Ref.: https://www.datatilsynet.dk/offentlig/internettet/billeder-paa-internettet

1. Situationsbilleder

Situationsbilleder defineres i denne sammenhæng som billeder, hvor en aktivitet eller en situation er det egentlige formål med billedet. Det kunne f.eks. være gæster til en rockkoncert, legende børn i en skolegård eller besøgende i en zoologisk have.

Modsætningen hertil er portrætbilleder, hvor formålet er at afbilde en eller flere bestemte personer, jf. mere herom nedenfor.

Udgangspunktet er, at situationsbilleder kan offentliggøres *uden samtykke* med hjemmel i interesseafvejningsreglen i persondatalovens § 6, stk. 1, nr. 7.

Da der er tale om en helhedsvurdering af formålet med offentliggørelsen, skal offentliggørelse ske under skyldig hensyntagen til karakteren af billedet, herunder den sammenhæng, hvori billedet optræder og formålet med offentliggørelsen. Det afgørende kriterium er, at den afbildede ikke med rimelighed må kunne føle sig udstillet, udnyttet eller krænket, f.eks. i markedsførings eller andet kommercielt øjemed. Billederne skal således være *harmløse*.

Eksempler på situationsbilleder der som udgangspunkt kan offentliggøres uden samtykke:

- Billeder optaget under en fritidsklubs udfoldelse af aktiviteter.
- Billeder optaget af unges ophold på en efterskole eller anden privat skole.
- Billeder optaget ved en kommunal skoles juleafslutning.

Billeder kan dog være af en sådan beskaffenhed, at det må antages at virke krænkende for de afbildede. Dette kunne f.eks. være hvis to genkendelige personer afbildes i intime situationer.

En indsigelse mod et offentliggjort billede vil derudover konkret kunne bevirke, at interesseafvejningen falder ud til fordel for den registreredes interesse.

Følgende situationsbilleder vil normalt *ikke* kunne offentliggøres uden samtykke:

- Billeder optaget af ansatte på arbejde i en privat virksomhed eller en offentlig myndighed.
- Billeder af kunder i en forretning, i banken, på posthuset m.v.
- Besøgende på en bar, natklub, diskotek eller lignende.

2. Portrætbilleder

Som altovervejende udgangspunkt kræver det et samtykke at offentliggøre portrætbilleder på internet.

Dette er begrundet i, at en sådan offentliggørelse vil kunne medføre ulemper for de registrerede, idet nogle mennesker vil kunne føle ubehag ved, at sådanne billeder, eventuelt sammen med oplysninger om navn m.v., gøres offentligt tilgængeligt for alle, der har adgang til internet, og at denne ulempe vejer tungere end interessen i offentliggørelsen, jf. interesseafvejningsreglen i persondatalovens § 6, stk. 1, nr. 7.

Hvis en skole f.eks. ønsker at offentliggøre portrætbilleder eller klassebilleder af eleverne på sin hjemmeside, må det kun ske, hvis der inden offentliggørelsen indhentes et udtrykkeligt samtykke fra hver enkelt elev, eller dennes forældre afhængig af elevens alder.

Ansatte portrætfotos må kun offentliggøres efter den ansattes *udtrykkelige samtykke*.

3. Klassebilleder

Er at betragte som portrætfotos.

Samtykkeerklæring

– for offentliggørelse af billeder og video

Formål: At profilere CB.

Jeg giver hermed samtykke til, at følgende må offentliggøres:

☐ *Jeg giver tilladelse til at portrætfotos offentliggøres.*
☐ *Jeg giver tilladelse til at klassebilleder offentliggøres.*
☐ *Jeg giver tilladelse til at situationsbilleder/video anvendes til markedsføring*
☐ *Jeg giver tilladelse til at materialet må anvendes efter mit ophør på skolen*

Formål: _____

Mit samtykke gælder indtil: _____
(samtykket kan altid trækkes tilbage)

Dato: _____

Navn: _____

Underskrift: _____

Samtykkeerklæring

– for personfølsomme oplysninger

Til brug for _____

giver jeg hermed samtykke til, at lade mig registrere med følgende personfølsomme oplysninger:

- ☐ *Race eller etnisk oprindelse*
- ☐ *Politisk, religiøs eller filosofisk overbevisning*
- ☐ *Fagforeningsmæssige tilhørsforhold*
- ☐ *Genetiske data (DNA)*
- ☐ *Biometriske data med formål at foretage identifikation*
- ☐ *Fagforeningsmæssige tilhørsforhold*
- ☐ *Helbredsoplysninger*
- ☐ *Seksuel tilhørsforhold*
- ☐ *Oplysninger om strafbare forhold – herunder børneattest*

Den registrerede	Registrant
_____	_____
Dato	Dato
_____	_____
Navn	Navn
_____	_____
Underskrift	Underskrift

Incident Response Plan

Denne plan iværksættes ved konstateret sikkerhedsbrud.

Henvisning: Bilag 5 – ”Sikkerhedspersonale - Kontaktoplysninger”

Overordnet plan:

1. **Dan overblik**

   Hvor er skaden sket. Er det lokalt eller hos en databehandler? Er det sket på web, mail, tyveri, USB-pen?

2. **Start logning**

   Start log op på https://it.cabh.dk/LogHændelse og begynd registrering.

3. **Stands ulykken**
   - Frakobl angrebet udstyr
   - Kontakt databehandleren, og få denne til at isolere det ramte.
   - Få evt. assistance fra EFIF.

4. **Konstatér omfanget**
   - Find ud af skadens omfang.
   - Er det hos en databehandler, skal denne foretage vurderingen.

5. **Anmeld**

   Afhængig af omfanget skal sikkerhedsbruddet rapporteres.

   a. **Advicér sikkerhedspersonalet**

      Skal ske, hvis det ikke allerede er sket. Dette inkluderer DPO. Se bilag 6.

   b. **Rapportér til Datatilsynet**

      Hvis DPO vurderer, at sikkerhedsbruddet skal indrapporteres til Datatilsynet, skal dette ske inden 72 timer – regnet fra det tidspunkt hvor sikkerhedsbruddet blev opdaget.

   c. **Politianmeldelse**

      Politiet inddrages om nødvendigt med henblik på evt. opklaring.

6. **Analyser og reparér skaden**
   - Interview personer involveret i hændelsen.
   - Fjern plantet information på evt. ”defaced” webside.
   - Pas på ikke at komme til at slette spor eller beviser.
   - Anvend ekspertbistand.

7. **Evaluér og informer**

   På baggrund af hændelsen, skal der dannes en viden om hvordan det kunne ske, og hvorledes det kan undgås fremover.

   Informér ud i organisation, så alle kan tage ved lære.

Specifik plan:

1. **Ransomware angreb** (kryptering af alle filer på netværket - pengeafpresning)

   HØJRISIKO. En inficeret computer krypterer alle netværksfiler. Skal omgående stoppes. Alarmér IT-administrationen eller EFIF, der vil isolere netværket, indtil smittekilden er fundet. Derefter rulles backup tilbage. Der må forudses datatab[8].

   Global udskiftning af adgangskoder kan være nødvendig.

   Alle medarbejdere skal informeres – både om hændelsen og datatabet.

2. **Stjålet/mistet ansat computer**

   Mister en ansat sin computer, eller har mistanke om at der har være autoriseret adgang via den, skal det omgående meldes.

   - Der skal som minimum skiftes adgangskode.
   - Computeren skal fjernes fra listen over indmeldte computere i Active Directory.

   På grund af den indbyggede "Direct Access" kan en stjålet computer være potentielt "meget farlig" i uvedkommendes hænder.

3. **Hacking**

   Sker ofte mod servere og sjældnere mod personlige computere. Svær at spore og opdage. Server- og netværkspersonale skal være meget opmærksomme på uregelmæssigheder.

   - Inficeret server(e) skal ofte geninstalleres.
   - Global udskiftning af adgangskoder kan være nødvendig.

   Ved konstatering eller mistanke kontaktes IT-administrationen.

4. **Keylogger installeret**

   Meget alvorligt. En keylogger kan optage al tastatur- og museaktivitet og derved opsnappe brugernavne og adgangskoder.

   Computeren skal geninstalleres fra grunden af.

   Ved konstatering eller mistanke kontaktes IT-administrationen

5. **Overtagelse af computer** ("Zombie")

   Meget alvorligt. Computeren kan fjernstyres og indgå i flere typer koordinere angreb, så som DDoS-angreb.

   Computeren skal geninstalleres fra grunden af.

   Ved konstatering eller mistanke kontaktes IT-administrationen

6. **DDoS angreb** ("Distributed Denial of Service")

   Er efterhånden almindeligt forekommende. DDoS er et angreb fra flere tusind computere rundt om i verden, som lammer ens internetforbindelse. Selvom et angreb kan virke voldsomt og ofte lammer al ekstern trafik, går der ikke data tabt.

[8] Noget af dagens arbejde vil gå tabt. Den inficerede computer skal reinstalleres.

7. **Tab af (følsomme) data**

   Ved indbrud (fysisk/elektronik) eller mistet opbevaringsmedie, meldes til IT-administrationen, der vurderer omfanget. På baggrund heraf, kan indberetning til Datatilsynet komme på tale.

8. **Tab af låse-/studiekort**

   Giver fysisk adgang til bygningen, og mulighed for uretmæssig personidentifikation.

   Meld straks til Teknisk Service, der spærrer kortet, og udsteder et nyt.

9. **Mailafsendelse af personfølsomme oplysninger til uvedkommende**

   Der er foretaget afsendelse til forkerte adressat eller via ikke godkendt system.

   Meld til IT-administrationen der vurderer omfanget og de videre tiltag.

10. **Misbrug af personoplysninger**

    Hvis nogen opdager, at andres personoplysninger (data eller billeder/video) bliver brugt uretmæssigt, kan det være ulovligt. Politianmeldes kan komme på tale. Kontakt IT-administrationen for vurdering af situationen.