Persondatapolitik for Horsens Gymnasium & HF

Intern politik vedrørende behandling af personoplysninger

Version	Dato	Ændret af	Godkendt af
1.0	25.september 2025	HHD	HHD

Indhold

Persondatapolitik for Horsens Gymnasium & HF

Dette dokument har to formål:

1) At tjene som et praktisk instrument i Horsens Gymnasium & HF´s arbejde med beskyttelsen af personoplysninger.
2) Som skriftlig dokumentation af vores indsats for at overholde databeskyttelsesforordningen.

Horsens Gymnasium & HF´s persondatapolitik er udformet som led i Horsens Gymnasium & HF´s generelle arbejde med at efterleve databeskyttelsesforordningen og er på den måde en integreret del af, hvordan vi arbejder med GDPR. Politikken er godkendt af ledelsen, som er gjort bekendt med ansvaret. Hvis der opstår mistanke om, at persondata ikke håndteres korrekt, skal ledelsen straks tage hånd om dette.

Persondatapolitikken bliver gennemgået og opdateret løbende - minimum en gang om året.

1. Definitioner

Horsens Gymnasium & HF behandler personoplysninger i forbindelse med fx optagelse og gennemførelse af undervisning, køb, salg, samarbejde og HR-funktioner. Nedenfor vil kernebegreber fra lovgivningen blive defineret for at lette forståelsen af persondatapolitikken.

Databeskyttelsesforordningen	**Den lovgivning, som fra d. 25. maj 2018 regulerer behandlingen af personoplysninger (træder sammen med databeskyttelsesloven i stedet for persondataloven).**
Personoplysninger	Enhver oplysning om en identificeret eller identificerbar fysisk person, fx navn, adresse, telefonnummer, billede, nummerplade, eller lignende. Oplysninger om enkeltmandsfirmaer er derfor også personoplysninger.
Følsomme personoplysninger	Oplysninger om race og etnisk oprindelse, politisk overbevisning, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data med henblik på entydig identifikation, helbredsoplysninger og seksuelle forhold eller seksuel orientering.
Fortrolige oplysninger	Oplysninger, der betragtes som værende fortrolige oplysninger, fx CPR-nummer, oplysninger om indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold, oplysninger om interne familieforhold, herunder oplysninger om for eksempel ulykkestilfælde.
Registrerede	Alle personer, hvis oplysninger er registreret hos os, fx kunder, medarbejdere og leverandører.
Behandling af personoplysninger	Alt, hvad Horsens Gymnasium & HF gør med personoplysninger, inklusive opbevaring og sletning.
Dataansvarlig	Den, der beslutter formål, omfang og metoder til behandling af personoplysninger.

Databehandler	Den, der behandler personoplysninger på vegne af den dataansvarlige, fx et firma, som håndterer løn eller en cloudtjeneste.

2. Organisering og ansvar

Denne persondatapolitik gælder for hele Horsens Gymnasium & HF, men det kan være nødvendigt at indføre specifikke instrukser i relevante tilfælde. I så fald skal disse instrukser være i overensstemmelse med persondatapolitikken, have en klar ansvarsfordeling og en fast plan for opdatering.

Ansvaret for medarbejdernes overholdelse af persondatapolitikken påhviler ledelsen. Hvis der opstår episoder, som viser, at der fx har været uoverensstemmelse med persondatapolitikken, er Hans Henrik Danielsens opgave at afhjælpe problemet.

Databehandler

Vi er databehandler, når vi behandler personoplysninger på vegne af en dataansvarlig. Der skal etableres en databehandleraftale med den dataansvarlige, før behandlingen kan påbegyndes.

Som databehandler har vi en række forpligtelser over for vores kunder:

- Vi må alene behandle de overladte personoplysninger efter instruksen indeholdt i databehandleraftalen.
- Vi skal føre en fortegnelse over behandlingen af personoplysninger.
- Vi skal følge sikkerhedsinstrukserne i databehandleraftalen og videreføre disse til vores underleverandører. Hvis der er forskel på sikkerhedskravene i vores databehandleraftaler med vores kunde og underleverandør, tager vi udgangspunkt i den aftale, der indeholder de strammeste krav til sikkerhed. På den måde er vi sikre på, at alle aftaler, på trods af varierende udformning, bliver overholdt.
- Vi skal på opfordring fra kunden hjælpe med at opfylde kundens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra registrerede om indsigt i egne oplysninger, udlevering af den registreredes oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af den registreredes oplysninger, underretning af den registrerede ved sikkerhedsbrud, samt bistå kunden i forbindelse med dennes forpligtelser efter databeskyttelsesforordningens art. 32-36.
- Vi skal levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger, således at vores behandling af kundens personoplysninger opfylder kravene i databeskyttelsesforordningen samt sikrer beskyttelse af den registreredes rettigheder, jf. de implementerede sikkerhedsforanstaltninger
- Vi skal kunne oplyse, hvor kundens personoplysninger opbevares og ajourføre oplysningerne for kunden ved enhver ændring.

3. Retningslinjer

Det følgende er de konkrete regler og retningslinjer, som Horsens Gymnasium & HF skal følge i forbindelse med behandling af personoplysninger. Behandlingen er baseret på databeskyttelsesforordningens og databeskyttelseslovens krav og vil, sammen med den øvrige udarbejdede dokumentation, sikre Horsens Gymnasium & HF´s efterlevelse af forordningen.

Hvert element i politikken er delt op i:

- **Formål** (hvorfor vi gør det)
- **Procedure** (hvordan vi gør det)
- **Kontrol** (at vi faktisk også gør det)

3.1 Sikring af lovligt grundlag

Formål: At sikre, at der er et lovligt grundlag for at behandle personoplysninger.

Procedure: Før en behandling af personoplysninger påbegyndes, skal der ske afklaring af det lovlige behandlingsgrundlag. Opstår der tvivl om det lovlige grundlag, vil dette blive afklaret af ledelsen. Hvis et lovlig grundlag ikke kan identificeres, igangsættes behandlingen ikke.

Det lovlige grundlag for behandlingen dokumenteres sammen med den pågældende proces i fortegnelsen over arbejdsprocesser for Horsens Gymnasium & HF.

For de arbejdsprocesser, hvor vi er databehandler, er det lovlige grundlag for behandlingen af personoplysninger baseret på databehandleraftalen, der er indgået med den dataansvarlige.

Kontrol: Alle arbejdsprocesser gennemgås årligt, hvor det lovlige behandlingsgrundlag revurderes.

3.2 Sikring af formål og at personoplysninger er relevante

Formål: At sikre, at der kun indsamles oplysninger baseret på et klart defineret formål, og at de ikke omfatter mere, end der kræves til opfyldelse af formålet med behandlingen.

Procedure: For hver arbejdsproces bliver det klart defineret, hvilke personoplysninger der er relevante for formålet. Det sikres, at der ikke indsamles flere oplysninger end nødvendigt. Formålet med behandlingen af personoplysninger, samt hvilke typer personoplysninger der behandles for hver arbejdsproces, er defineret og beskrevet i fortegnelsen for arbejdsprocesserne på Horsens Gymnasium & HF.

For behandling af personoplysninger, hvor vi er databehandlere, er formålet med behandlingen defineret i den aftale, der er indgået med den dataansvarlige.

Kontrol: Alle arbejdsprocesser gennemgås årligt, hvor kategorierne af de indsamlede oplysninger sammenholdes med formålet, med henblik på at sikre, at oplysningerne stadig er nødvendige for formålet.

3.3 Sikring af oplysningspligt – internt

Formål: At sikre gennemsigtigheden Horsens Gymnasium & HF´s behandling af personoplysninger samt de registreredes (medarbejdernes) viden om deres rettigheder.

Procedure: Ved ansættelsen bliver medarbejderne informeret om:

- Hvem der er dataansvarlig og dennes kontaktoplysninger, samt kontaktoplysninger på en eventuel Data Protection Officer (DPO).
- Formålet med behandling af personoplysningerne.
- Det lovlige grundlag for behandlingen samt legitime interesser, som forfølges af Horsens Gymnasium & HF.
- Eventuelle andre modtagere af personoplysningerne, herunder overførsel til usikre tredjelande.
- Opbevaringsperioden for personoplysningerne.
- Den registreredes (medarbejderens) rettigheder i forhold til personoplysningerne (indsigt, berigtigelse, sletning, begrænset behandling og dataportabilitet).
- Retten til at tilbagekalde et eventuelt afgivet samtykke.
- Retten til at klage til Datatilsynet.
- Hvorfra oplysningerne er indhentet, hvis dette ikke er direkte fra den registrerede (medarbejderen) selv.
- Omfanget af automatiske afgørelser, herunder profilering og logikken bag.

Hvis Horsens Gymnasium & HF senere ønsker at behandle oplysninger til et andet formål end oplyst til den registrerede (medarbejderen), bliver den registrerede oplyst om dette, før den nye behandling igangsættes.

Kontrol: Det kontrolleres årligt at alle eksisterende medarbejdere har modtaget oplysningsdokumentet, og at alle nye medarbejdere har modtaget og oplysningsdokumentet.

3.4 Sikring af oplysningspligt - eksternt

Formål: At sikre gennemsigtigheden af Horsens Gymnasium & HF´s behandling af personoplysninger samt de registreredes viden om deres rettigheder.

Procedure: Når Horsens Gymnasium & HF eksternt indhenter personoplysninger om den registrerede, sikres det gennem vores privatlivspolitik, at den registrerede på en letforståelig måde informeres om:

- Hvem der er dataansvarlig og dennes kontaktoplysninger, samt kontaktoplysninger på en eventuel Data Protection Officer (DPO).
- Formålet med behandling af personoplysningerne.
- Det lovlige grundlag for behandling samt legitime interesser, som forfølges af Horsens Gymnasium & HF.
- Eventuelle andre modtagere af personoplysningerne, herunder overførsel til tredjelande.
- Opbevaringsperioden for personoplysningerne.
- Den registreredes rettigheder i forhold til personoplysningerne (indsigt, berigtigelse, sletning, begrænset behandling og dataportabilitet).

- Retten til at tilbagekalde et eventuelt afgivet samtykke.
- Retten til at klage til Datatilsynet.
- Hvor oplysningerne er indhentet, hvis dette ikke er direkte fra den registrerede selv.
- Omfanget af automatiske afgørelser, herunder profilering og logikken bag.

Hvis vi senere ønsker at behandle oplysninger til et andet formål end oplyst til den registrerede, bliver den registrerede oplyst om dette, før den nye behandling igangsættes.

Kontrol: Det gennemgås årligt, at linket til privatlivspolitikken, som er indsat i mailsignaturen, stadig er den gældende på hjemmesiden.

Herudover kontrolleres det årligt, at links til privatlivspolitikken på hjemmesiden fortsat er til den gældende privatlivspolitik.

3.5 Sikring af retten til indsigt

Formål: At sikre, at de registrerede kan få indsigt i de oplysninger, som behandles om dem.

Procedure: Ved henvendelse skal den registrerede uden unødigt ophold og på en let forståelig måde have indsigt i de oplysninger, som er registreret om den pågældende, herunder:

- Formålet med behandling af personoplysningerne.
- Hvilke kategorier af oplysninger, som behandles.
- Eventuelle andre modtagere af personoplysningerne, herunder overførsel til usikre tredjelande.
- Opbevaringsperioden for personoplysningerne.
- Den registreredes rettigheder i forhold til personoplysningerne (indsigt, berigtigelse, sletning, begrænset behandling og dataportabilitet).
- Retten til at klage til Datatilsynet.
- Hvor oplysningerne er indhentet, hvis dette ikke er direkte fra den registrerede selv.
- Omfanget af automatiske afgørelser, herunder profilering og logikken bag.

En medarbejder, der modtager en indsigtsanmodning, skal hurtigst muligt kontakte ledelsen eller Horsens Gymnasium & HF´s GDPR-ansvarlige.

Der må kun udleveres oplysninger, når vedkommende har legitimeret sig, eller når der på anden måde er skabt sikkerhed for, at den, der fremsætter en indsigtsbegæring, er identisk med den person, som oplysningerne vedrører, eller er i besiddelse af en fuldmagt fra denne.

Telefoniske henvendelser

Ved telefoniske henvendelser skal det sikres, at der kun gives oplysninger til rette person. Det kan fx være nødvendigt at stille kontrolspørgsmål for at identificere personen eller foretage en kontrolopringning til et telefonnummer for at sikre, at det er den rette person, som anmoder om oplysningerne. Hvis medarbejderen ikke kan få den nødvendige sikkerhed, må oplysningerne i stedet sendes pr. post eller e-mail til den adresse, der er registeret på vedkommende.

Henvendelser via brev og e-mail

Hvis navn og adresse i brevet/e-mailen er identisk med de oplysninger, som i forvejen fremgår af systemet, kan oplysningerne normalt sendes til den registrerede på den registrerede post- eller e-mailadresse. Er dette ikke tilfældet, bør forholdet undersøges nærmere.

Indsigt for børn under 18 år

Forældremyndighedsindehaver kan begære indsigt på barnets vegne. Barnet kan også selv få indsigt. Der skal ved en begæring om indsigt i oplysninger om personer, der er under 18 år, foretages en konkret vurdering af, hvorvidt den registrerede er i stand til selv at modtage oplysningerne, eller om oplysningerne skal gives til en værge.

Indsigt på andres vegne (fuldmagt)

Den registrerede kan give en anden fuldmagt til at få indsigt i egne oplysninger. Fuldmagten kan være specifik eller generel. Er der tale om en advokat eller tilsvarende stillingsfuldmagt, som henvender sig med en indsigtsanmodning på vegne af den registrerede, er det ikke nødvendigt at efterspørge en fuldmagt.

Hvis der opstår tvivl om, hvorvidt fuldmagten er tilstrækkelig, skal juridisk afdeling involveres.

Kontrol: Henvendelser vedrørende indsigt bliver gennemgået i et interval af én måned for at sikre, at alle henvendelser er blevet imødekommet uden unødigt ophold.

3.6 Sikring af retten til berigtigelse

Formål: At sikre, at de registrerede kan få berigtiget deres oplysninger.

Procedure: Ved henvendelse fra den registrerede skal vi berigtige/rette eventuelle forkerte eller vildledende oplysninger om den pågældende.

En medarbejder, der modtager besked om, at der behandles forkerte oplysninger, henvender sig til den GDPR-ansvarlige, som sørger for at korrigere og/eller supplere oplysningerne. Den registreredes identitet bliver sikret, før oplysninger rettes, jf. afsnit 3.5.

Kontrol: Henvendelser vedrørende berigtigelse bliver gennemgået i et interval af én måned, hvor det kontrolleres, at oplysninger er blevet rettet i systemet.

3.7 Sikring af den registreredes ret til sletning

Formål: At sikre den registreredes ret til sletning på den registreredes anmodning herom (”Retten til at blive glemt”)

Procedure: Når en registreret henvender sig med et ønske om at blive slettet, skal dette oplyses til GDPR-ansvarlige, som foretager sletningen uden unødigt ophold efter at have sikret sig, at formålet med behandlingen af oplysningerne ikke længere er til stede.

Det skal hermed sikres, at den registrerede ikke har nogle udeståender med os, før sletningen foretages. Medarbejderne, som håndterer anmodningen om sletning, orienterer den pågældende registrerede om årsagen til, at anmodningen om sletning ikke kan imødekommes helt eller delvist, fx hvis det ikke er muligt at efterkomme vores kontraktretlige forpligtelser

overfor den registrerede, herunder kunder, leverandører eller andre samarbejdspartnere, eller hvis man ikke må slette oplysningerne i henhold til gældende lovgivning eller andre retlige forpligtelser. Den registrerede skal til enhver tid kunne få slettet oplysninger, som er indsamlet baseret på samtykke. Den registreredes identitet bliver sikret, før oplysninger slettes, jf. afsnit 3.5.

Kontrol: Henvendelser vedrørende den registreredes ret til sletning bliver gennemgået i et interval af én måned for at kontrollere, at vi har besvaret den registreredes anmodning, og såfremt anmodningen resulterede i sletning af oplysninger, kontrolleres det også, at vi har slettet alle oplysninger, og at det blev gjort indenfor rimelig tid.

3.8 Sikring af retten til begrænset behandling

Formål: At sikre, at behandlingen af personoplysninger begrænses til kun opbevaring.

Procedure: Når en registreret henvender sig og kræver, at behandlingen af vedkommendes oplysninger begrænses, skal den GDPR-ansvarlige straks oplyses herom. Behandlingen af personoplysningerne begrænses til opbevaring, indtil forholdet, som er grundlag for den begrænsede behandling, løses. Den registreredes identitet bliver sikret, før behandlingen begrænses, jf. afsnit 3.5.

Kontrol: Henvendelser vedrørende den registreredes ret til begrænset behandling bliver gennemgået i et interval af én måned for at kontrollere, at vi har besvaret den registreredes anmodning, og såfremt anmodningen har resulteret i, at vi skal begrænse behandlingen, kontrolleres det også, at behandlingen er blevet begrænset til udelukkende at omfatte opbevaring, og at dette er blevet gjort indenfor rimelig tid.

3.9 Sikring af retten til dataportabilitet

Formål: At sikre, at personoplysninger, som behandles automatisk eller er baseret på en kontrakt, kan udleveres eller overføres i et struktureret, almindeligt anvendt og maskinlæsbart format.

Procedure: Når en registreret henvender sig med et ønske om at få udleveret eller overført personoplysninger, rettes der straks henvendelse til den GDPR-ansvarlige, som - baseret på den registreredes ønske - enten udleverer materialet i et struktureret, almindeligt anvendt, maskinlæsbart format eller, hvis teknisk muligt, overfører oplysningerne til en ny dataansvarlig, ønsket af den registrerede. Den registreredes identitet bliver sikret før oplysninger udleveres eller overføres, jf. afsnit 3.5.

Kontrol: Henvendelser om dataportabilitet bliver gennemgået i et interval af én måned for at kontrollere, at vi har svaret den registrerede indenfor den lovbestemte tidsfrist på en måned, og for at kontrollere, at vi eksporterer personoplysningerne korrekt, og at det bliver gjort indenfor rimelig tid.

3.10 Sikring af retten til indsigelse

Formål: At sikre imødekommelse af den registreredes ret til indsigelse.

Procedure: Når en registreret oplyser, at denne ikke ønsker, at vedkommendes oplysninger behandles, skal der straks rettes henvendelse til den GDPR-ansvarlige, som derefter vurderer anmodningen og igangsætter relevante handlinger baseret på udfaldet af vurderingen. Den registreredes identitet bliver sikret før behandlingen eventuelt stoppes, jf. afsnit 3.5.

Kontrol: Henvendelser om indsigelser bliver gennemgået i et interval af én måned for at kontrollere, at anmodningen om indsigelse blev behandlet indenfor en måned, og at vi er ophørt med behandlingen.

3.11 Sletteplig

Formål: At sikre, at oplysninger bliver slettet, når de ikke længere er nødvendige ift. formålet med behandlingen.

Procedure: I Horsens Gymnasium & HF´s kortlægning af personoplysninger er det angivet, hvor personoplysninger opbevares, og der er taget stilling til opbevaringsperioder. Dette er gjort for at effektivisere sletteprocessen.

Personoplysninger opbevares centralt på dertil indrettede drev og systemer for at mindske spredning af personoplysninger i Horsens Gymnasium & HF og effektivisere sletteprocessen.

Kontrol: Opbevaringsperioden i alle arbejdsprocesser revurderes årligt.

3.12 Databehandleraftaler, når vi er dataansvarlige

Formål: At sikre, at der etableres databehandleraftaler med andre juridiske enheder, som behandler personoplysninger på vegne af os.

Procedure: Der er indgået databehandleraftaler med alle relevante eksterne og interne parter.

Hver gang, der indgås en ny aftale med en samarbejdspartner, vurderes det, om ydelsen involverer behandling af personoplysninger på vegne af os. Hvis dette er tilfældet, indgås der en databehandleraftale, og det kontrolleres, at databehandleraftalen lever op til Datatilsynets gældende standard.

Der udføres løbende kontrol med databehandlerne ved at udøve revisionsbeføjelsen.

Kontrol: Listen over databehandlere gennemgås og matches med den tilhørende databehandleraftale årligt, og det vurderes, om databehandleraftalen fortsat lever op til Datatilsynets gældende standard.

Revisionspligten med databehandlerne, hvor eventuelle observationer gennemgås og vurderes, udøves årligt.

3.12.1 Databehandleraftaler, når vi er databehandler

Formål: At sikre, at der etableres databehandleraftaler med dataansvarlige, som vi behandler personoplysninger på vegne af.

Procedure: Der er indgået databehandleraftale med alle relevante eksterne og interne parter.

Såfremt der ønskes et skift af leverandør (underdatabehandler) for de behandlinger, der involverer de dataansvarlige, skal skiftet godkendes i henhold til godkendelsesproceduren i databehandleraftalen.

Kontrol: Det tjekkes årligt, om vi efterlever vores forpligtelser i databehandleraftalen.

Listen over leverandører (underdatabehandlere) gennemgås tillige årligt med henblik på at tjekke op på, om der er sket udskiftning eller ændring i anvendelsen af leverandører (underdatabehandlere). Hertil sikres det, at udskiftning af eller ændring i anvendelsen af leverandører (underdatabehandlere), underrettes til den dataansvarlige.

3.12.2 Fælles dataansvar

Formål: At sikre at begge parter lever op til forpligtelserne som fælles dataansvarlig.

Procedure: Der skal indgås en aftale om fælles dataansvar med disse kunder/partnere til fastlæggelse af forholdene imellem os og dem.

Kontrol: Det skal kontrolleres årligt at ansvaret for ovenstående forpligtelser fortsat er delegeret korrekt mellem de fælles dataansvarlige, og at alle lever op til deres forpligtelser.

3.12.3 Leverandørforhold uden for databehandlerkonstruktioner

Formål: At sikre en tilstrækkelig sikkerhed for databehandling, som ikke kan varetages af en databehandleraftale.

Procedure: Hvis det vurderes at være nødvendigt, indgås der fortrolighedsaftaler med relevante eksterne parter.

Dette er til de situationer, hvor en leverandør/samarbejdspartner måske får adgang til personoplysninger, men ikke skal have en databehandleraftale. Dette kan fx være eksternt rengøringspersonale.

Kontrol: Det kontrolleres årligt, at ovenstående leverandører har indgået relevante fortrolighedsaftaler.

3.13 Sikring af risikovurderinger og eventuelle konsekvensanalyser

Formål: At imødekomme databeskyttelsesforordningens krav om en risikobaseret tilgang til databehandling.

Procedure: Horsens Gymnasium & HF har etableret en fortegnelse over arbejdsprocesser. Fortegnelsen opdateres løbende, når der sker ændringer i vore arbejdsprocesser.

For hver arbejdsproces er der foretaget en risikovurdering baseret på sandsynligheden for, at personoplysninger mister fortrolighed, integritet eller tilgængelighed, samt hvilken konsekvens det må have for den registrerede. Risikovurderingen revurderes én gang årligt og for højrisiko-områder udarbejdes der en handlingsplan for nedsættelse af risiko. Hvis risikoen ikke kan nedsættes, konsulteres Datatilsynet.

Kontrol: Arbejdsprocesserne og de dertilhørende risikovurderinger gennemgås årligt med henblik på at fastslå, om vurderingen er retvisende, og om der eventuelt skal etableres en konsekvensanalyse (DPIA) og handlingsplan for at nedsætte risikoen ved arbejdsprocesser af høj risiko. Hvis det ikke er muligt at nedsætte risikoen, skal Datatilsynet konsulteres, før behandlingen igangsættes. Risikovurdering og eventuelle konsekvensanalyser opdateres, hver gang der er nye planlagte arbejdsprocesser eller ændringer i eksisterende arbejdsprocesser.

3.14. Sikring af dokumenter og procedurer

Formål: At sikre, at de fornødne dokumenter og procedurer er opdateret.

Procedure: Samtlige GDPR-dokumenter og IT-relevante procedurer gennemgås og opdateres.

Kontrol: Hvert år gennemgår den GDPR-ansvarlige alle dokumenter og politikker med henblik på opdatering og revidering heraf.

3.15 Datasikkerhed

3.15.1 Organisatoriske foranstaltninger

Formål: At sikre de fornødne organisatoriske og tekniske foranstaltninger mod, at personoplysninger kommer til uvedkommendes kendskab eller går tabt.

Procedure: Begrænsning af adgangen til elektroniske personoplysninger.
Alle systemer/drev, der indeholder personoplysninger, er omfattet af begrænset adgang, så det kun er de medarbejdere, som har behov for adgangen for at udføre deres arbejde, der har adgang til systemer/drev med personoplysninger.

Kontrol: Ledelsen gennemgår årligt listen over medarbejdere med adgang til systemer og mapper med personoplysninger med henblik på at verificere, at kun de nødvendige medarbejdere har adgang til systemer og mapper indeholdende personoplysninger.

Det kontrolleres årligt at der ikke er installeret applikationer uden retmæssig tilladelse på mobile enheder eller sker uretmæssig synkronisering af mailboks.

3.15.2 Tekniske foranstaltninger - informationsaktiver

Formål: At vurdere, om de tekniske sikkerhedsforanstaltninger, der er implementeret, fortsat er korrekte, og om de sikrer en passende behandlingssikkerhed.

Procedure: For hvert informationsaktiv er det klart defineret, hvilke relevante sikkerhedsforanstaltninger der er implementeret for at sikre en tilstrækkelig behandlingssikkerhed. Det sikres, at de opsatte sikkerhedsforanstaltninger stadig er retvisende, og implementeret korrekt.

Kontrol: Alle tekniske sikkerhedsforanstaltninger gennemgås årligt, hvor det kontrolleres, om de stadig er retvisende og implementeret korrekt.

3.15.3 Fysisk sikkerhed

Formål: At sikre forholdsregler imod uvedkommendes adgang til lokaler, hvori der sker behandling af personoplysninger.

Procedure: Områder med adgang til personoplysninger sikres således, at uvedkommende ikke kan få adgang til disse. Dette sker ved at opbevare personoplysninger i aflåste skabe, når lokalet ikke er under opsyn.

Alle medarbejdere skal låse deres PC, når arbejdsstationen forlades, også kortvarigt.

Medarbejdere er underlagt en clean desk politik, som indebærer, at medarbejderne skal fjerne alle dokumenter fra deres skrivebord, når de forlader arbejdspladsen.

Medarbejderne skal følge en face down politik, som indebærer, at dokumenter med personoplysninger vendes med den blanke side op eller på anden måde afdækkes, når medarbejderen efterlader dokumenter på arbejdsstationen.

Kontrol: Det kontrolleres løbende og mindst årligt ved stikprøver, at skabe med personoplysninger aflåses, og at det kun er relevante medarbejdere, som er i besiddelse af nøglen til skabene.

Det kontrolleres tillige løbende og mindst årligt, om medarbejderne husker at låse deres PC, når arbejdsstationen forlades, samt at de overholder clean desk- og face down-politikken.

3.15.4 Print og dokumenter med personoplysninger

Formål: At sikre, at personlige oplysninger ikke ligger frit tilgængeligt i papirform.

Procedure: Print med personoplysninger må ikke efterlades i printerrummet og skal hentes, så snart de er printet.

Papirdokumenter, der indeholder personoplysninger, må i arbejdstiden ikke opbevares uden opsyn af en medarbejder.

Kontrol: Det kontrolleres løbende og mindst kvartalsvist ved stikprøver, om der ligger frit tilgængelige personoplysninger fremme i papirform.

3.16 Gæster

Formål: At sikre, at gæster bliver håndteret sikkert.

Procedure: Alle gæster skal efter registrering i gæstelog tildeles gæstekort og hentes i receptionen. Gæster må ikke færdes alene, medmindre de har fået specifik tilladelse hertil.

Faste gæster over en længere periode (fx eksternt tilknyttede konsulenter, gymnasiepraktikanter eller lign.) skal underskrive en tavshedserklæring.

Kontrol: Det kontrolleres årligt, at proceduren for håndtering af gæster overholdes, herunder at de underskriver evt. tavshedserklæringer.

3.17 Sikring af medarbejder-awareness

Formål: At sikre, at medarbejdere er bekendt med reglerne for behandling af personoplysninger.

Procedure: Alle nye medarbejdere skal i forbindelse med deres ansættelse gøres bekendt med regler for behandling af personoplysninger og IT-sikkerhed.

Kontrol: Samtlige medarbejdere skal årligt deltage i og bestå en e-learning eller andre kurser vedrørende behandling af personoplysninger.

Herudover skal samtlige medarbejdere genlæse håndbogen og sikkerhedsbrudsvejledningen årligt.

3.18 Notifikation ved brud på datasikkerheden

Formål: At sikre, at alle sikkerhedsbrud dokumenteres i sikkerhedsbrudsloggen, og at det vurderes, hvorvidt de skal anmeldes til Datatilsynet.

Procedure: Et brud på sikkerheden er defineret som en hændelse, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Hvis en medarbejder opdager brud på datasikkerheden, meddeles dette straks den GDPR-ansvarlige, som danner sig et overblik over bruddet og – om muligt - indenfor 72 timer indberetter dette til Datatilsynet. Dette overblik indebærer, at den GDPR-ansvarlige og ITafdelingen i samarbejde med de eventuelt implicerede medarbejdere samler alle oplysninger omkring hændelsen, berørte datakategorier, antal lækkede personoplysningerne, sandsynlige konsekvenser og hvilke tiltag, der er iværksat for at imødegå bruddet.

Brud på processer der involverer en dataansvarlig, skal hurtigst mulig anmeldes til den dataansvarlige (senest efter 48 timer), hvorefter det er den dataansvarliges pligt at indberette bruddet. Bruddet skal noteres i Sikkerhedsbrudsloggen.

Alle brud på sikkerheden noteres i sikkerhedsbrudsloggen.

Det er kun brud, der sandsynligvis medfører en risiko for en fysisk persons rettigheder eller frihedsrettigheder, der skal anmeldes til Datatilsynet.

Hvis sikkerhedsbruddet er af en sådan karakter, at det skal anmeldes til Datatilsynet, skal der som hovedregel tillige foretages underretning af de registrerede, hvis personoplysninger indgår i bruddet.

Hvis vi ikke har kontaktoplysningerne på de registrerede, sker orienteringen offentligt via vores hjemmeside.

Kontrol: Det kontrolleres årligt, at sikkerhedsbrudsproceduren fungerer. I den forbindelse gennemgås sikkerhedsbrudsloggen med henblik på at identificere, om vurderingerne af sikkerhedsbrud er foretaget korrekt, og at der er indberettet rettidigt til Datatilsynet.

3.19 DPO

Formål: At sikre en vurdering af, om det er et krav, at Horsens Gymnasium & HF har en DPO

Procedure: Det vurderes ved ændringer af kerneydelser eller ved organisatoriske ændringer, hvorvidt Horsens Gymnasium & HF har behov for en DPO, baseret på databeskyttelsesforordningens kriterier for krav om DPO.

Kontrol: Det revurderes årligt, om virksomhedens behov for en DPO har ændret sig.

Det revurderes, når det findes nødvendigt, fx ved skift af DPO, om DPO'en lever op til de krav, som loven og praksis fastsætter.