Persondatapolitik for Nordjyllands Landbrugsskole

til alle medarbejdere - vedrørende behandling af personoplysninger

Version	Dato	Ændret af	Godkendt af
1.0			

Indhold

Persondatapolitik for Nordjyllands Landbrugsskole

Dette dokument har to formål: Dels at tjene som et praktisk instrument i virksomhedens arbejde med beskyttelsen af persondata, dels som en skriftlig dokumentation af vores indsats for at overholde Databeskyttelsesforordningen.

Nordjyllands Landbrugsskoles persondatapolitik er udformet i sammenhæng med virksomhedens overordnede strategi, værdier og visioner og er på den måde en integreret del af, hvordan virksomheden arbejder. Politikken er godkendt af ledelsen og alle medarbejdere er gjort bekendt med den og deres ansvar i forhold til persondata. Hvis der opstår mistanke om, at persondata ikke håndteres korrekt, skal man straks kontakte sin nærmeste leder og informere denne om problematikken.

Persondatapolitikken bliver gennemgået og opdateret løbende, minimum hver andet år af administrationsleder, IT-afdeling og forstander. Ved ansættelse bliver alle nye medarbejdere gjort bekendt med persondatapolitikken og de skal ved underskrift på "Tillæg til ansættelseskontrakt vedrørende Persondatapolitik og Samtykkeerklæring" bekræfte deres kendskab til og forståelse af politikken.

1. Definitioner

Nordjyllands Landbrugsskole behandler persondata i forbindelse undervisning, eksamination, elevadministration og HR-funktioner. Nedenfor vil kernebegreber fra lovgivningen blive defineret for at lette forståelsen af persondatapolitikken.

Databeskyttelsesforordningen	Den lovgivning, som pr. 25. maj 2018 regulerer behandlingen af persondata (træder sammen med Databeskyttelsesloven i stedet for Persondataloven)
Personoplysninger	Enhver oplysning om en identificeret eller identificerbar fysisk person, fx navn, adresse, telefonnummer, billede, nummerplade, cpr-nummer eller lignende. Oplysninger om enkeltmandsfirmaer er derfor også personoplysninger
Følsomme personoplysninger	Eksempelvis helbredsoplysninger, fagforeningstilhørsforhold, race, etnicitet, politisk overbevisning, oplysninger om strafbare forhold mv.
Registrerede	Alle personer, hvis oplysninger er registreret hos Nordjyllands Landbrugsskole fx elever, medarbejdere og leverandører
Behandling af data	Alt hvad virksomheden gør med data, inklusiv opbevaring og sletning
Dataansvarlig	Den, der beslutter formål, omfang og metoder til behandling af persondata
Databehandler	Den, der behandler data på vegne af den dataansvarlige, fx et firma, som håndterer løn eller en cloudtjeneste

2. Organisering og ansvar

Denne persondatapolitik gælder for alle afdelinger, men det kan være nødvendigt at indføre specifikke instrukser i specifikke afdelinger. 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 denne persondatapolitik hviler først hos medarbejderne selv, dernæst hos afdelingslederne. Kontrol med overholdelse af persondatapolitik skal dokumenteres skriftlig og opbevares på Persondatasupports portal, samt i fysisk format i ringbind. Hvis kontrollen viser, at der

har været episoder, hvor persondatapolitikken ikke er blevet overholdt, er det afdelingslederens opgave at afhjælpe problemet.

3. Medarbejderinstruks

Det følgende er de konkrete regler og retningslinjer, som alle ansatte i Nordjyllands Landbrugsskole skal følge i forbindelse med behandling af persondata. Instruksen er baseret på Databeskyttelsesforordningens og Databeskyttelseslovens krav og vil sammen med IT-politikken og den udarbejdede dokumentation sikre skolens efterlevelse af forordningen. Hvert element i instruksen er delt op i formål (hvorfor gør vi det), procedure (hvordan gør vi det) og kontrol (har vi nu også gjort det).

3.1 Sikring af lovligt grundlag/hjemmel

Formål:

- Der er et lovligt grundlag for at behandle data

Procedure:

Før en databehandling påbegyndes skal der ske en afklaring af den lovlige hjemmel. Dette gøres af ejeren af processen i samarbejde med afdelingslederen. Som hovedregel vil virksomheden i forbindelse med kunder og leverandører anvende hjemlen opfyldelse af kontrakt og ved medarbejdere hjemlerne samtykke, interesseafvejning eller retlig forpligtelse. Opstår der tvivl om den lovlige hjemmel retter man henvendelse til administrationsleder eller IT-afdeling. Hvis et lovlig grundlag ikke kan identificeres, igangsættes behandlingen ikke.

I tilfælde hvor der indhentes samtykke til at behandle oplysninger om børn under 13 år, bliver samtykket afgivet eller godkendt af indehaverne af forældremyndigheden over barnet.

Det lovlige grundlag for behandlingen dokumenteres sammen med den pågældende proces i fortegnelsen over behandlingsaktiviteter.

Underskrevne/accepterede samtykkeerklæringer opbevares i sikret elektronisk IMS-arkiv

Kontrol:

Alle behandlingsaktiviteter gennemgås årligt, hvor den lovlige hjemmel revurderes.

3.2 Sikring af formål og at data er relevante

Formål:

- Oplysninger, som indsamles, er baseret på et klart formål og omfatter ikke mere, end hvad der kræves til opfyldelse af formålet med behandlingen.

Procedure:

For hver behandlingsaktivitet bliver det klart defineret hvilke personoplysninger, som er relevante for formålet, og det sikres, at der ikke indsamles flere oplysninger end nødvendigt for at understøtte dette formål. Formålet med behandlingen af personoplysninger, samt hvilke typer personoplysninger, der behandles for hver behandlingsaktivitet er defineret i ”Fortegnelsen over behandlingsaktiviteter”

I tilfælde hvor det kan være i virksomhedens interesse at indsamle flere oplysninger end nødvendigt, skal der med hjælp fra juridisk afdeling udarbejdes en samtykkeerklæring jf. afsnit 3.1.

Kontrol:

Alle behandlingsaktiviteter gennemgås årligt, hvor kategorier af indsamlede oplysninger sammenholdes med formålet, med henblik på at sikre, at oplysningerne stadig er nødvendige for formålet.

Afdelingsledere kan udføre stikprøvevis kontrol af registreringer i databehandlingssystemer for at tjekke, om der er registeret mere end, hvad der er relevant for at servicere kunden. Hvis dette er tilfældet, skal der foreligge en samtykkeerklæring fra den registrerede.

3.3 Sikring af oplysningspligt

Formål:

- Sikre gennemsigtigheden af virksomhedens behandling af personoplysninger, samt de registreredes viden om deres rettigheder.

Procedure:

Ved ansættelsen bliver medarbejderne via deres ansættelseskontrakt på en letforståelig måde informeret om:

- hvem der er dataansvarlig og dennes kontaktoplysninger, samt kontaktoplysninger på en eventuel Data Protection Officer,
- formålet med behandling af data
- hjemmel for behandling, samt legitime interesser som forfølges af virksomheden
- eventuelle andre modtagere af data, herunder overførsel til tredjelande
- opbevaringsperiode for data
- den registreredes rettigheder i forhold til data (indsigt, berigtigelse, sletning, begrænset behandling og dataportabilitet).
- retten til at tilbagekalde et eventuelt afgivet samtykke
- retten til at klage til Datatilsynet
- at de har pligt til at afgive oplysninger og konsekvenser ved ikke at gøre det
- hvor oplysningerne er indhentet, hvis dette ikke er direkte fra den registrerede selv
- omfanget af automatiske afgørelser, herunder profilering og logikken bag

Hvis virksomheden 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.

For at oplyse kunder og samarbejdspartnere udformes der en tekst, indeholdende de ovenstående punkter, til firmaets hjemmeside. Et link til denne tekst afgives elektronisk (fx pr. mail) eller via telefon til den registrerede ved første kontakt.

Kontrol:

Det er afdelingsledernes ansvar at kontrollere, at reglen om oplysningspligt bliver overholdt. Langt det meste sikres elektronisk via hjemmesiden, men når en henvendelse kommer direkte via mail/telefon, skal der udsendes en mail med link til oplysningerne. Den afsendte mail er dokumentation for overholdelse af oplysningspligten og skal gemmes på den relevante sag under navnet oplysningspligt.

3.4 Sikring af retten til indsigt

Formål:

- Sikre at den registrerede kan få indsigt i de oplysninger, som behandles om dem

Procedure:

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

- formålet med behandling af data
- hvilke kategorier af oplysninger, som behandles
- eventuelle andre modtagere af data, herunder overførsel til tredjelande
- opbevaringsperiode for data
- den registreredes rettigheder i forhold til data (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 et ønske om indsigt skal hurtigt muligt kontakte administrationsleder eller IT-afdeling. Oplysninger udleveres i papirform eller almindelige anvendt elektronisk form, baseret på hvilket format, den registrerede ønsker.

Det sikres, at den, der meddeles oplysninger til, er rette person. 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 f.eks. være nødvendigt at stille kontrolspørgsmål, fx spørge efter adresse og CPR-nr., 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 til den adresse, der er registeret på vedkommende eller sendes til E-boks.

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
Forældremyndighedens indehaver kan begære indsigt på barnets vegne. Barnet kan også selv få indsigt.

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, er det normalt ikke nødvendigt at efterspørge en fuldmagt.

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

Kontrol:

Henvendelser vedrørende indsigt bliver gennemgået hver måned for at sikre, at henvendelser er blevet imødekommet uden unødig ophold.

3.5 Sikring af retten til berigtigelse

Formål:

- Sikre, at de registrerede kan få berigtiget deres oplysninger

Procedure:

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

En medarbejder, der modtager besked om at der behandles forkerte oplysninger, henvender sig til administrationsleder eller IT-afdeling, som sørger for at korrigere oplysningerne. Den registreredes identitet bliver sikret før oplysninger rettes, jf. afsnit 3.4.

Kontrol:

Henvendelser vedrørende berigtigelse bliver gennemgået hver måned, hvor det tjekkes at oplysninger er blevet rettet i systemet.

3.6 Sletteplig og sikring af retten til at sletning

Formål:

- Oplysninger slettes, når de ikke længere er nødvendige for formålet med behandlingen
- Sikring af at kunne imødekomme den registreredes ret til sletning

Procedure:

I "Fortegnelsen over behandlingsaktiviteter" er der taget stilling til opbevaringsperioder for hver behandlingsaktivitet.

Personoplysninger opbevares centralt på dertil indrettede drev og systemer for at mindske spredning af personoplysninger i organisationen og effektivisere sletteprocessen. Hvis medarbejderne har behov for midlertidigt at have personoplysninger liggende lokalt på deres maskiner eller skriveborde, skal disse fjernes så snart arbejdet er udført.

Det sikres, at oplysninger også slettes hos eventuelle databehandlere.

Oplysninger slettes løbende:
Medarbejdere sletter løbende e-mails indeholdende personoplysninger, når disse er arkiveret andre steder, eller ikke længere er nødvendige for formålet med behandlingen.

Medarbejderne makulerer løbende fysiske dokumenter med personoplysninger, når disse ikke længere er nødvendige for formålet med behandlingen.

De ansvarlige for systemer indeholdende personoplysninger sletter/uigenkaldeligt af-identificere løbende oplysninger i systemerne, som ikke længere er nødvendige for formålet med behandlingen.

IT-afdelingen sikrer centralt, at der sker en manuel eller automatisk sletning/uigenkaldelig af-identificering af oplysninger i de enkelte systemer, når den aftalte opbevaringsfrist er nået.

Før oplysninger slettes, sikres det, at oplysningerne ikke er nødvendige at opbevare i henhold til andre lovgivninger, herunder bl.a. bogføringsloven.

Retten til at blive glemt:
Når en registreret henvender sig med et ønske om at blive slettet skal dette oplyses IT-afdelingen eller administrationslederen], 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 virksomheden, 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 servicere kunden uden personoplysningerne. 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 3.4.

Sletning i backup:
I henhold til virksomhedens backup-strategi bliver backups overskrevet dagligt så alle sletninger i systemet bliver overskrevet i backuppen dagligt.

Hvis der bliver behov for at indlæse en backup, sikres det, at oplysninger, der er slettet i live-miljøet bliver slettet igen efter at backuppen indlæses. Dette gøres manuelt

Kontrol:

Opbevaringsperioden på behandlingsaktiviteter revurderes årligt.

Hver måned gennemgås listen over fratrådte medarbejdere for at sikre, at personoplysninger som ikke er nødvendige at opbevare for anden lovgivning, er slettet.

Ansøgninger og henvendelser, hvor der ikke er afgivet samtykke til at gemme, er placeret centralt og gennemgås månedligt med henblik på sletning, når den ansøgte stilling er besat.

Det kontrolleres månedligt, om de centrale sletninger er gennemført.

De enkelte afdelingsledere og IT-afdeling kontrollerer ved stikprøvekontrol, om medarbejderne sletter data på deres computere og i deres mail.

3.7 Sikring af retten til begrænset behandling

Formål:

- begrænse behandlingen af personoplysninger, til kun opbevaring

Procedure:

Når en registreret henvender sig og kræver at behandlingen af vedkommendes oplysninger begrænses, skal IT-afdelingen og administrationslederen straks oplyses herom. Behandlingen af personoplysningerne begrænses til blot at opbevare oplysningerne indtil forholdet som er grundlag for den begrænsede behandling løses. Den registreredes identitet bliver sikret før behandlingen begrænses, jf. afsnit 3.4.

Kontrol:

Henvendelser, som resulterede i begrænset behandling gennemgås løbende for at kontrollere, at virksomheden har begrænset behandlingen til blot opbevaring og at det blev gjort indenfor rimelig tid.

3.8 Sikring af retten til dataportabilitet

Formål:

- At personlysninger som behandles automatisk 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 personlysninger, rettes der straks henvendelse til IT-afdeling eller administrationsleder, 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 3.4.

Kontrol:

Henvendelser om dataportabilitet gennemgås løbende for at kontrollere, at virksomheden eksporterer data korrekt og at det bliver gjort indenfor rimelig tid.

3.9 Sikring af retten til indsigelse

Formål:

- Imødekomme den registreredes ret til indsigelse mod profilering og direkte markedsføring

Procedure:

Når en registreret oplyser, at denne ikke ønsker at vedkommendes oplysninger benyttes til profilering eller direkte markedsføring, skal der straks rettes henvendelse IT-afdeling eller administrationsleder, som derefter sørger for, at behandlingen af oplysningerne i forbindelse med profilering og direkte markedsføring stoppes. Den registreredes identitet bliver sikret før behandlingen stoppes, jf. afsnit 3.4.

Det er sikret at der er mulighed for menneskelig indgreb i automatiske behandlinger af personoplysninger, såfremt en registreret ønsker dette.

Kontrol:

Henvendelser om indsigelse gennemgås løbende for at kontrollere, at virksomheden ikke længere benytter den registreredes oplysninger til profilering eller direkte markedsføring.

3.10 Databehandleraftaler

Formål:

- Sikring af, at der etableres databehandleraftaler med andre juridiske enheder, som behandler

personoplysninger på vegne af os.

Procedure:

Der er indgået databehandleraftaler med samtlige juridiske enheder, der behandler personoplysninger på vegne af os.

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.

Databehandleraftalerne gemmes centralt på Persondatasupports elektroniske portal samt i fysisk form i ringbind

Hvis en medarbejder i det daglige bliver opmærksom på fejl eller mangler i en databehandlers håndtering af personoplysninger, skal medarbejderen gøre nærmeste leder opmærksom på problemet. Lederen skal herefter undersøge problemet og eventuelt foretage den nødvendige opfølgning. Forstanderen inddrages i fornødent omfang, men orienteres som minimum.

Kontrol:

Hvert år gennemgås listen over databehandlere og matches med den tilhørende databehandleraftale og det vurderes, om at den gældende databehandleraftale stadig er tilstrækkelig.

Hvert år indhenter forstanderen en revisorerklæring fra databehandlerne vedrørende behandling af persondata, hvor eventuelle observationer gennemgås og vurderes.

Hvert år udsendes der kontrolskemaer som omhandler håndteringen af personoplysninger til databehandlerne. Disse skal besvares og vil indikere om databehandleren lever op til de krav, der er i databehandleraftalen.

3.11 Sikring af dokumentation

Formål:

- Imødekomme Databeskyttelsesforordningens krav om fortegnelse over behandlingsaktiviteter og konsekvensanalyse

Procedure:

Virksomheden har etableret en fortegnelse over behandlingsaktiviteter, som kan findes på Persondatasupports elektroniske portal samt opbevares i fysisk form i ringning. Fortegnelsen opdateres løbende, når der sker ændringer i virksomhedens behandlingsaktiviteter.

Relevante medarbejdere er instrueret i at opdatere fortegnelsen i tilfælde af ændringer til deres behandlingsaktiviteter.

For hver behandlingsaktivitet er der foretaget en risikovurdering baseret på sandsynligheden for at personoplysninger mister fortrolighed, integritet eller tilgængelighed, samt hvilken konsekvens det har for den registrerede. Risikovurderingen revurderes 1 gang årligt og for høj risiko områder udarbejdes der en handlingsplan for nedsættelse af risiko. Hvis risikoen ikke kan nedsættes konsulteres Datatilsynet.

Kontrol:

Behandlingsaktiviteterne gennemgås årligt med henblik på at vurdere, om behandlingsaktiviteter er af høj risiko og dermed, om der skal etableres en konsekvensanalyse og handlingsplan for at nedsætte risikoen. Hvis det ikke er muligt at nedsætte risikoen skal Datatilsynet konsulteres før behandlingen igangsættes. Risikovurdering og konsekvensanalyse opdateres hver gang der er nye planlagte behandlingsaktiviteter eller ændringer til eksisterende behandlingsaktiviteter

3.12 Datasikkerhed

Formål:

- Der er etableret fornødne organisatoriske og tekniske foranstaltninger mod at personoplysninger

kommer til uvedkommendes kendskab eller går tabt.

Procedure:

Begrænsning af adgangen til elektronisk persondata
Alle systemer/drev, der indeholder personoplysninger er omfattet af begrænset adgang, således at det kun er de medarbejdere, der har behov for adgangen til at udføre deres arbejde, der har adgang til systemer/drev med personoplysninger.

Kontrol:

Hvert kvartal gennemgår afdelingsledere liste 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.

Mails med personoplysninger
Mails med personoplysninger er begrænset til et absolut minimum. Følsomme personoplysninger der skal sendes via mail, skal sendes krypteret eller via E-boks

Kontrol:

IT-afdeling og afdelingsledere kan foretage stikprøvekontrol i mails, virksomhedens onedrive og sharepoint og lignende for at sikre, at datasikkerheden overholdes

3.13 Fysisk sikkerhed

Formål:

- Der er forholdsregler, der sikrer mod uvedkommendes adgang til lokaler, hvor der foregår behandling af personoplysninger.

Procedure:

Områder med adgang til personoplysninger sikres således, at uvedkommende ikke kan få adgang til disse. Det sker ved at opbevare personoplysninger i aflåste rum, og aflåste skabe, når lokalet ikke er under opsyn. Løbende, afhængig af mængden af bilag, kan personoplysninger fra aflåste skabe arkiveres i et aflåst arkiveringsrum.

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. Derudover er skal de følge en front 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,

For yderligere oplysninger om fysisk sikkerhed henvises til virksomhedens informationssikkerhedspolitik

Kontrol:

Regnskabsmedarbejderen skal hvert år i forbindelse med aflæggelse af årsregnskab sikre, at der er maks. 5 år gamle dokumenter i kælderen. Ældre dokumenter destrueres.

Nærmeste afdelingsleder skal 1 gang årligt gennemgå de aflåste skabe med medarbejderne.

Afdelingsledere tjekker løbende stikprøvevist, at aflåste skabe med personoplysninger faktisk er aflåste og at det kun er relevante medarbejdere, som er i besiddelse af nøglen til skabene.

Afdelingsledere skal løbende være opmærksomme på, om medarbejderne husker at låse deres PC, når arbejdsstationen forlades, samt at regler omkring fysiske dokumenter på skrivebordet indeholdende personfølsomme data overholdes

3.14 Gæster

Formål:

- Gæster skal håndteres sikkert.

Procedure:

Gæster må ikke færdes alene, og møder medarbejderen en ukendt gæst, skal denne kontaktes med henblik på at afdække gæstens ærinde

3.15 Print og dokumenter med personoplysninger

Formål:

- Personlige oplysninger må ikke ligge frit tilgængeligt i papirform.

Procedure:

Print med personoplysninger må ikke efterlades i printerrummet.

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

Alle henvendelser (breve i papirformat, print af e-mails, papirlapper m.v.), som indeholder personoplysninger skal efter endt brug smides ud i en særlig aflåst papircontainer, som står i kopirummet eller makuleres. Indholdet af papircontainer bliver makuleret, når containeren er fyldt.

Kontrol:

Afdelingslederne skal løbende være opmærksomme på, at der ikke ligger print med personoplysninger i printrummet, eller at der ligger dokumenter og papir ved arbejdspladserne indeholdende personoplysninger.

3.16 Sikring af medarbejder awareness

Formål:

- Demonstrere at medarbejdere er bekendt med reglerne for behandling af persondata.

Procedure:

Samtlige medarbejdere på Nordjyllands Landbrugsskole skal kvittere for at have modtaget og forstået skolens politikker vedrørende persondata og informationssikkerhed.

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

Kontrol:

I forbindelse med ansættelsen skriver medarbejderen under på, at vedkommende har modtaget og forstået skolens regler og politikker vedrørende persondata og informationssikkerhed.

Samtlige medarbejdere skal deltage i CyberPilots e-learning-moduler vedrørende behandling af persondata.

3.17 Notifikation ved brud på datasikkerheden

Formål:

- Datatilsynet, og under visse omstændigheder, den registrerede, bliver ved brud på datasikkerheden notificeret om muligt indenfor 72 timer efter et brud er konstateret

Procedure:

Brud på datasikkerheden er defineret som en hændelse, der resulterer i, at der sandsynligvis er en risiko for, at personoplysninger er blevet udsat for uautoriseret adgang eller er gået tabt.

Hvis en medarbejder opdager brud på datasikkerheden, meddeles dette straks til IT-afdelingen, som indenfor 72 timer, om muligt, skal have overblik over bruddet. IT-afdelingen samler i samarbejde med de eventuelt implicerede medarbejdere oplysninger omkring hændelsen, berørte datakategorier, antal lækkede data records, sandsynlige konsekvenser og hvilke tiltag, der er iværksat for at imødegå bruddet, som anmeldes til datatilsynet indenfor 72 timer via deres hjemmeside.

Brud der sandsynligvis medføre en risiko for, at personoplysninger er blevet udsat for uautoriseret adgang eller er gået tabt anmeldes til Datatilsynet.

Alle brud på sikkerheden noteres i Databrudsloggen.

Hvis sikkerhedsbruddet er af sådan karakter, at det er nødvendigt at informere de registrerede, gøres dette via mail.

Hvis virksomheden ikke har kontaktoplysningerne på de registrerede sker orienteringen offentligt via datatilsynets hjemmeside.

Kontrol:

Det kontrolleres jævnligt, at situationer, som bør anmeldes til datatilsynet, også bliver anmeldt indenfor 72 timer.

3.18 Privacy by Design og Privacy by Default

Formål:

- Imødekommelse af Databeskyttelsesforordningens krav om Privacy by design and default

Procedure:

Ved udvikling eller anskaffelse af nye it-systemer er virksomheden opmærksom på, at systemerne er sikre og at de understøtter opdeling af adgangsrettigheder, således at personoplysninger kan beskyttes mod uautoriseret adgang og tab.

Medarbejderne må ikke benytte tjenester til behandling af personoplysninger som [IT-afdelingen] ikke har godkendt, herunder bl.a. private mail-applikationer, sin egen cloudløsning eller programmer, som kan downloades fra nettet til behandling af personoplysninger.

Kontrol:

IT-afdelingen har sin egen tjekliste i forhold til opsætning af eksisterende og udvikling og opsætning af nye IT-systemer. IT-afdelingen foretager en gang årligt en revision af de eksisterende systemer og afsøger netværket for brug af uautoriserede programmer.

3.19 DPO

Formål:

- Vurdering af, om det er et krav, at virksomheden har en DPO

Procedure:

Det vurderes årligt, hvorvidt virksomheden har behov for en DPO, baseret på Databeskyttelsesforordningens kriterier for krav om DPO. Vurderingen er dokumenteret i Persondatasupports elektroniske portal samt opbevaret fysisk i ringbind.

Virksomhedens DPO er:

Anne-Lene Pugholm

IT-center Nord

c/o Tech College

Øster Uttrupvej 1

9000 Aalborg

tlf. 72 50 59 99

mail: dpo@itcn.dk