Persondatapolitik for Arbejdernes-Andelsboligforening Varde

Intern politik vedrørende behandling af personoplysninger

Version	Dato	Ændret af	Godkendt af
1.1	14-07-2022	MK	LB

Indhold

Persondatapolitik for Arbejdernes Andelsboligforening Varde

Dette dokument har to formål:

1) At tjene som et praktisk instrument i virksomhedens arbejde med beskyttelsen af persondata
2) Som skriftlig dokumentation af vores indsats for at overholde Databeskyttelsesforordningen.

Arbejdernes Andelsboligforening Varde' 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 de er gjort bekendt med deres ansvar i forhold til persondata. Hvis der opstår mistanke om, at persondata ikke håndteres korrekt, skal man straks kontakte øverste ledelse.

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

1. Definitioner

Arbejdernes Andelsboligforening behandler persondata i forbindelse med køb, salg, samarbejde 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	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 som virksomheden og samfundet betragter som værende fortrolige oplysninger, f.eks. CPR-nummer, oplysninger om indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold, oplysninger om interne familieforhold, herunder for oplysninger om for eksempel selvmordsforsøg og ulykkestilfælde.
Registrerede	Alle personer, hvis oplysninger er registreret hos os, fx kunder, medarbejdere og leverandører
Behandling af data	Alt hvad virksomheden gør med data; inklusive 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 i Arbejdernes Andels-Boligforening, 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 hos ledelsen. Hvis der opstår episoder som viser, at der f.eks. har været uoverensstemmelse med Persondatapolitikken, er det afdelingslederens opgave at afhjælpe problemet.

3. Retningslinjer

Det følgende er de konkrete regler og retningslinjer, som Arbejdernes Andels-Boligforening Varde skal følge i forbindelse med behandling af persondata. Instruksen er baseret på Databeskyttelsesforordningens og Databeskyttelseslovens krav.

Hvert element i instruksen er delt op i:

- **Formål** (hvorfor gør vi det)
- **Procedure** (hvordan gør vi det)
- **Kontrol** (har vi nu også gjort det)

3.1 Sikring af lovlig grundlag/hjemmel

Formål: Sikre at 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 ledelsen i samarbejde med den ansvarshavende i den relevante afdeling. Som hovedregel vil virksomheden i forbindelse med data ang. kunder og leverandører anvende hjemlen "opfyldelse af kontrakt" og ved data ang. medarbejdere hjemlerne "samtykke", "interesseafvejning" eller "retlig forpligtelse". Opstår der tvivl om den lovlige hjemmel henvender man sig til 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.

Underskrevne/accepterede samtykkeerklæringer opbevares i personalemappen, der står i et aflåst rum, hvor kun direktør og HR-medarbejder har kode til døren.

Kontrol: Alle arbejdsprocesser gennemgås årligt, hvor den lovlige hjemmel revurderes.

3.2 Sikring af formål og at data er relevante

Formål: Kun at indsamle oplysninger baseret på et klart defineret formål, og at de ikke omfatter mere end hvad der kræves til opfyldelse af formålet med behandlingen.

Procedure: For hver arbejdsproces 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 arbejdsproces, er defineret og beskrevet under "arbejdsprocesser" i virksomhedens GDPR-portal.

For arbejdsprocesser hvor vi er databehandlere, er formålet med disse arbejdsprocesser 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

Formål: Sikre gennemsigtigheden af virksomhedens behandling af personoplysninger samt de registreredes viden om deres rettigheder.

Procedure: Ved ansættelsen får medarbejderen udlevet "persondatapolitikken" og "samtykkeerklæring", som informerer 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.

Kontrol:

Hvert år sendes en mail til alle medarbejdere med henblik på at sikre, at de alle har link til privatlivspolitikken i deres signatur og at linket stadig er til den gældende privatlivspolitik.

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 og 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 en indsigtsanmodning skal hurtigt muligt kontakte ledelsen

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 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 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 ledelsen involveres.

Kontrol:

Henvendelser vedrørende indsigt bliver gennemgået hver måned for at sikre, at alle henvendelser er blevet imødekommet uden unødigt 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 korrigeres dette hurtigst muligt. Den registreredes identitet bliver sikret før oplysninger rettes, jf. afsnit 3.4.

Kontrol: Henvendelser vedrørende berigtigelse bliver gennemgået i et interval af 30 dage, hvor det kontrolleres at oplysninger er blevet rettet i systemet.

3.6 Sletteplig og sikring af retten til at sletning

Formål: Sikre at oplysninger bliver slettet, når de ikke længere er nødvendige for formålet med behandlingen, samt sikring af den registreredes ret til sletning.

Procedure: I "Fortegnelsen over arbejdsprocesser" er der taget stilling til opbevaringsperioder for hver arbejdsproces.

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 afidentificerer løbende oplysninger, som ikke længere er nødvendige for formålet med behandlingen.

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

Kontrol: Opbevaringsperioden på arbejdsprocesser revurderes årligt.

Procedure: *Medarbejderoplysninger*
Persondata på medarbejdere skal slettes når der ikke længere er et formål med opbevaring.

- Kriterier for sletning af medarbejderens personoplysninger
  - Når en medarbejder fratræder, lukkes medarbejderens adgange til virksomhedens systemer.
  - Ved fratrædelse gennemgår HR personalemappen, og sletter ikke-relevante dokumenter og oplysninger.
  - Senest 5 år efter medarbejderens fratrædelse slettes alle oplysninger vedr. medarbejderen, dog kan der være undtagelser og/eller en retlig forpligtelse til opbevaring af disse oplysninger.

Kontrol:

Det kontrolleres kvartalsvis at oplysninger som skulle slettes ved medarbejderens fratrædelse også er slettet, og det sikres hvorvidt oplysninger der skal opbevares efter fratrædelsen grundet juridiske forpligtelser iht. kontrakt el. lovgivning er arkiveret/journaliseret korrekt.

Procedure: *Oplysninger om lejere*
Kundeoplysninger skal slettes når de ikke længere har et formål med opbevaring.

- Personoplysninger på vores tidligere lejere slettes efter indeværende år + 5 år efter fraflytning, medmindre der er en aktuel sag.
  -

Kontrol:

Det kontrolleres og revurderes årligt om de pågældende kundeoplysninger skal slettes eller opbevares i længere tid.

Procedure: *Samarbejdspartnere- og leverandøroplysninger*

Oplysninger på leverandører og samarbejdspartnere skal slettes når de ikke længere har et formål med opbevaring.

- Kriterier for sletning af leverandørdata:
  - Når der ikke har været samhandel i 5 år
  - Bliver vi opmærksom på at der er en ny kontaktperson opdateres dette så snart vi er blevet bekendt med ændringerne

Kontrol:

Det kontrolleres og revurderes årligt om de pågældende leverandøroplysninger skal slettes eller opbevares i længere tid.

Procedure: *Ansøgere*

Ansøgning og CV skal slettes når de ikke længere er relevante at gemme, og senest 6 måneder efter modtagelse.

Hvis det vurderes at kandidaten kan bruges senere, indhentes samtykke fra kandidaten til yderligere opbevaring i max 6 måneder.

Retten til at blive glemt:
Når en registreret henvender sig med et ønske om at blive slettet skal dette oplyses til ledelsen, 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.

Kontrol:

Hver måned gennemgås gemte ansøgninger og CV'er. Hvis de 6 måneder nærmer sig udløb, vurderes det om ansøgning/CV skal slettes, eller om samtykke til yderligere opbevaring skal indhentes.

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 ledelsen 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 månedligt 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 ledelsen, 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 månedligt 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.

Procedure: Når en registreret oplyser at denne ikke ønsker at vedkommendes oplysninger behandles, skal der straks rettes henvendelse til ledelsen som derefter vurderer anmodningen og igangsætter relevante handlinger baseret på udfaldet af vurderingen. Den registreredes identitet bliver sikret før behandlingen eventuelt stoppes, jf. afsnit 3.4.

Kontrol: Henvendelser, som resultererede i indsigelse gennemgås månedligt for at kontrollere, at virksomheden eksporterer data korrekt og at det bliver gjort indenfor rimelig tid.

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 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.

Der udføres løbende kontrol med databehandlerne ved at udøve revisionsbeføjelsen.

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. Den øverste IT-ansvarlige i virksomheden inddrages i nødvendigt omfang, men orienteres som minimum.

Kontrol: Hvert år gennemgås listen over databehandlere og matches med den tilhørende databehandleraftale og det vurderes, om den gældende databehandleraftaler stadig er dækkende.

Hvert år udøves revisionspligten med databehandlerne vedrørende behandling af persondata, hvor eventuelle observationer gennemgås og vurderes.

3.11 Sikring af dokumentation

Formål: Imødekomme Databeskyttelsesforordningens krav om fortegnelse over arbejdsprocesser og konsekvensanalyse.

Procedure: Virksomheden har etableret en fortegnelse over arbejdsprocesser som kan findes i GDPR portalen. Fortegnelsen opdateres løbende når der sker ændringer i virksomhedens arbejdsprocesser.

Medarbejderne er instrueret i at opdatere fortegnelsen i tilfælde af ændringer til deres 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 1 gang årligt og for højrisiko-områder udarbejdes der en handlingsplan for nedsættelse af risiko. Hvis risikoen ikke kan nedsættes, konsulteres Datatilsynet.

Kontrol: Arbejdsprocesserne gennemgås årligt med henblik på at vurdere, om arbejdsprocesser 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 arbejdsproces eller ændringer til eksisterende arbejdsprocesser.

3.12 Datasikkerhed

Formål: Sikre de 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, så det kun er de medarbejdere, der har behov for adgangen til at udføre deres arbejde, der har adgang til systemer/drev med personoplysninger.

Mails med personoplysninger
Mails med personoplysninger er begrænset til et absolut minimum. Følsomme og fortrolige personoplysninger der skal sendes via mail, skal sendes krypteret.

Kontrol: Hvert Kvartal gennemgår ledelsen 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.

3.13 Fysisk sikkerhed

Formål: Sikre forholdsregler imod 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. Dette sker ved at opbevare personoplysninger i aflåste skabe, når lokalet ikke er under opsyn. Løbende, afhængigt 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 skal de 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 skal hvert år i forbindelse med aflæggelse af årsregnskab sikres, at gemte dokumenter er maks. 5 år gamle. Ældre dokumenter destrueres.

Ledelsen skal ved løbende stikprøver tjekke, om aflåste skabe med personoplysninger faktisk er aflåste, og at det kun er relevante medarbejdere som er i besiddelse af nøglen til skabene.

Ledelsen skal løbende være opmærksomme på, om medarbejderne husker at låse deres PC, når arbejdsstationen forlades.

3.14 Print og dokumenter med personoplysninger

Formål: Personlige oplysninger må ikke ligge frit tilgængeligt i papirform.

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

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 makuleres.

Kontrol:

Hvert kvartal skal ledelsen foretage en stikprøve runde og tjekke om der ligger frit tilgængeligt personoplysninger i papirform i virksomheden.

3.15 Sikring af medarbejder awareness

Formål: Sikre at medarbejdere er bekendt med reglerne for behandling af persondata.

Procedure: Samtlige medarbejdere i Arbejdernes Andels boligforening skal underskrive en tavshedserklæring ved deres ansættelse.

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

Kontrol:

Hvert år skal samtlige medarbejdere genlæse Informationssikkerhedspolitikken og Persondatapolitikken.

3.16 Notifikation ved brud på datasikkerheden

Formål: Rettidig advisering af Datatilsynet, og under visse omstændigheder den registrerede, ved brud på datasikkerheden.

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 ledelsen, som indenfor 72 timer, om muligt, skal have overblik over bruddet. Dette overblik indebærer at ledelsen i samarbejde med de eventuelt implicerede medarbejdere samler alle 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 de 72 timer via hjemmesiden.

Brud, der sandsynligvis medfører 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.

3.17 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 ledelsen ikke har godkendt, herunder bl.a. private mail-applikationer, egen cloudløsning eller programmer, som downloades fra nettet.

3.18 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.