PRIVATLIVSPOLITIK FOR Hovedvejens Autocenter

1. INDLEDNING

Denne politik beskriver, hvordan vi anvender og beskytter persondata, og skal sikre, at medarbejderne har kendskab til de regler, der gælder for brug af de persondata, som de har adgang til som led i deres arbejde. Denne politik supplerer vores andre politikker om it-sikkerhed, internet og e-mail o.l.

Denne politik har til formål at opfylde kravene i Persondataforordningen, herunder særligt art. 13

Bente Petersen er ansvarlig for opdatering og kontrol af politikken.

Hvor der i politikken henvises til lovartikler refererer dette til Persondataforordningen, og hvor der er tale om paragraf-henvisninger, sker dette til Persondataloven.

2. GENERELT OM BEHANDLING AF PERSONDATA

Enhver behandling af persondata i vores virksomhed sker under henvisning til principperne om lovlighed, rimelighed og gennemsigtighed. Persondata indsamles alene til udtrykkeligt angivne og legitime formål, ligesom vi iagttager princippet om dataminering. Vi tilstræber, at alle oplysninger er korrekte og ajourførte, ligesom principperne om opbevaringsbegrænsning, integritet og fortrolighed og ikke mindst ansvarlighed er sat i højsædet.

Hvis du har spørgsmål til vores behandling af persondata og denne persondatapolitik, er du altid velkommen til at kontakte Bente Petersen, der har det interne overordnede ansvar herfor.

3. DATAANSVARLIG

Hovedvejens Autocenter er selv dataansvarlig, og vi sikrer, at dine persondata behandles i overensstemmelse med lovgivningen.

4. BEHANDLINGSFORMÅL; KATEGORIER AF OPLYSNINGER, DER BEHANDLES

Formålet med behandling af persondata kan være mangeartede, men følgende eksempler er de mest gængse. Hvis vi undtagelsesvist skal behandle persondata til formål, der er uforenelige med nedenstående, vil du blive orienteret herom. Tilsvarende gælder, såfremt vi indsamler eller behandler persondata fra andre end dig.

- gennemførelse af ordrer.
- registrering af køretøjer.
- håndtering af forsikrings- og finansieringsydelser.
- opfyldelse af reklamations- og garantiforpligtelser.
- opfølgning på salg, udlejning og værkstedsbesøg.
- kommunikation i forbindelse med din ordre eller andre forespørgsler til os.
- sikring af brugervenlighed og sikkerhed.
- optimering af vores digitale løsninger.
- mulighed for at deltage i kundeundersøgelser, konkurrencer, lodtrækninger, m.m. via digitale løsninger.

- Arkiv over registrerede produkter og tilhørende personlige oplysninger.

4.1 HVILKE DATA INDSAMLES

Vi anvender data om dig for at opfylde vores aftale med dig samt for at gøre vores service bedre og sikre kvalitet i vores produkter og tjenester. De persondata, vi behandler, omfatter:

4.1.1 Automatisk indsamlede data

Vi har en række digitale løsninger baseret på forskellige teknologier med det formål at sikre brugervenlighed og sikkerhed. Disse teknologier kan automatisk opsamle data for at kunne tilbyde den bedst mulige løsning, enten direkte af os eller af en tredjepart på vegne af os. Analyse af klikstrøms data og cookies er eksempler på dette. Det gælder eksempelvis vores kontaktfunktion på websiden.

Alle besøg til en digital løsning medfører, at der sendes oplysninger fra den browser, du benytter, til en server. Det er via analyse af disse data, at vi optimerer de digitale løsninger. Data opsamles via tredjepart på vegne af os. Der kan opsamles data om din browser for at administrere vores system og foretage interne, marketingsrelaterede analyser baseret på din adfærd. Eksempler på data, der opsamles og analyseres:

- dato og tidspunkt for besøg
- de sider, der besøges i løsningen
- IP-adressen, du benytter
- IP-adressens geografiske placering
- oplysninger om den anvendte browser og computer (type, version, operativsystem m.m.)
- URL fra henvisningssted (siden, hvorfra den besøgende er kommet til vores løsning)

Vi anvender Bilinfo A/S der fungerer som databehandlere for os. Vi er dataansvarlige for det indsamlede data, og de indsamlede data bliver ikke videregivet, medmindre der foreligger et samtykke eller der er tale om en retsligt krav. Databehandleraftale kan ses på www.bilinfo.dk/om-bilinfo/forretningsbetingelser/

Du kan læse mere om vores brug af cookies nedenfor i pkt. 4.

4.1.2 Oplysninger du selv afgiver

Vi noterer naturligvis de oplysninger, du selv giver os i forbindelse med et fysisk besøg eller et besøg på vores webside.

Eksempler på data, som du aktivt afgiver, er som oftest almindelige og omfatter navn, adresse, telefonnummer, e-mailadresse m.v. og stammer oftest fra:

- Oplysninger du deler med os via sociale medier
- Oplysninger sendt på e-mail
- Oplysninger vi modtager fra dig i forbindelse med gennemførelse af ordre
- Oplysninger du deler med os, når du deltager i undersøgelser, events og konkurrencer

Listen er ikke udtømmende.

5 BEHANDLINGSGRUNDLAG

Persondata behandles hovedsagelig med hjemmel i art. 6.1.b, idet behandling er nødvendig af hensyn til opfyldelse af kontraktretslige forpligtelser mellem os.

Visse oplysninger, herunder følsomme, behandles i videst muligt omfang på baggrund af et samtykke, jf. straks nedenfor.

6 MODTAGERE OG VIDEREGIVELSE AF PERSONDATA

Vi videregiver udelukkende persondata til tredjepart i overensstemmelse med, hvad der er anført i denne privatlivspolitik.

Vi kan videregive dine oplysninger, såfremt vi er forpligtet til at videregive eller dele disse, for at overholde en retslig forpligtelse. Videregivelse kan også ske efter anvisning fra en domstol eller en anden myndighed, eller for at beskytte varemærker, rettigheder eller ejendom. Dette indebærer udveksling af oplysninger med andre virksomheder og organisationer med henblik på beskyttelse mod svindel.

Vi anvender tjenesteudbydere og databehandlere, der udfører arbejde på vores vegne. Tjenesterne kan fx være serverhosting og systemvedligeholdelse, analyse, betalingsløsninger, adresse- og soliditetskontrol, e-mail service samt grossister i forbindelse med bestilling af reservedele m.m. Disse samarbejdspartnere kan få adgang til data i det omfang, det er nødvendigt for at levere deres tjenester og services. Samarbejdspartnerne vil være kontraktligt forpligtet til at behandle alle data strengt fortroligt, og har dermed ikke tilladelse til at anvende data til andet end, hvad der er omfattet af den kontraktuelle forpligtelse overfor os. Vi kontrollerer, at vores samarbejdspartnere indenfor databehandling overholder deres forpligtelser. Såfremt vi videregiver dine oplysninger til en tjenesteudbyder eller databehandler udenfor EU, sikrer vi, at vi overholder de krav lovgivningen stiller til sådanne overførsler.

Vi indsamler som udgangspunkt ikke persondata, uden at du selv har givet os disse oplysninger ved registrering, køb eller deltagelse i en undersøgelse m.v.

7 OPBEVARINGSTIDS OG SLETTEPOLITIK

Vi gemmer oplysninger om dig, så længe vi har et legitimt og sagligt grundlag herfor, herunder så vi har mulighed for at betjene dig og din bil bedst muligt.

Som udgangspunkt vil alle persondata blive slettet efter 5 år efter afslutning af kundeforholdet, hvorved der menes sidste aktive transaktion. Persondata kan blive gemt længere, såfremt der er et sagligt behov herfor, eksempelvis hvis et retskrav skal fastlægges, gøres gældende eller forsvares, jf. art. 17.3.e.

Cookies, jf. pkt. 4 slettes dog senest 12 måneder efter brug.

8 INDSIGTSRET, BERIGTIGELSE OG SLETNING (ART. 13.2.B, jf. ART. 15.)

Du har en ret til at anmode om indsigt i forhold til de oplysninger, som vi behandler. De oplysninger, du kan anmode om er i hvert fald:

- at der behandles persondata
- hvad der behandles
- formålene med behandlingen
- de berørte kategorier af persondata (almindelige eller følsomme)
- tidsrummet, hvori de behandles, herunder opbevares
- retten til at
    - anmode om berigtigelse eller sletning
    - indgive klage til Datatilsynet

Du har ret til at få urigtig oplysninger om dig selv korrigeret uden unødig forsinkelse. Du må selv tage initiativet til en sådan berigtigelse.

Du kan ligeledes anmode om at blive slettet ("retten til at blive glemt"), dog først efter udløbet af vores lovgivningsmæssige opbevaringspligt i medfør af bogføringsloven. Du kan også kontakte os, hvis du mener, at dine persondata bliver behandlet i strid med lovgivningen eller andre retlige forpligtelser.

Når du henvender dig med en anmodning om at få rettet eller slettet dine persondata, undersøger vi, om betingelserne er opfyldt, og gennemfører i så fald ændringer eller sletning så hurtigt som muligt.

Hvis du ønsker adgang til de oplysninger, som er registreret om dig hos os via vores cookies, skal du rette henvendelse på mail bente@hovedvejensauto.eu. Er der registreret forkerte data, eller har du andre indsigelser, kan du rette henvendelse samme sted. Du har mulighed for at få indsigt i, hvilke informationer der er registreret om dig, og du kan gøre indsigelse mod en registrering heroverfor.

9 DATAPORTABILITET OG PROFILERING

Du har ret til at modtage de persondata, du har stillet til rådighed for os, og dem, vi har indhentet om dig hos andre aktører på baggrund af dit samtykke. Hvis vi behandler data om dig som led i en kontrakt, hvor du er part, kan du også få tilsendt dine data. Du har også ret til at overføre disse persondata til en anden tjenesteudbyder.

Hvis du ønsker at bruge din ret til data-portabilitet, vil du modtage dine persondata fra os i et almindeligt anvendt format.

Vi foretager i almindelighed ikke profilering, dvs. automatiserede afgørelser til brug for analyser eller lignende.

10 SAMTYKKE

Hvor samtykke er nødvendigt som behandlingsgrundlag, skal vi kunne dokumentere, at der foreligger et sådant. Derfor kræver vi altid et samtykke skriftligt.

Et samtykke er en frivillig, specifik, informeret og utvetydig viljestilkendegivelse omkring en behandling af personoplysninger. Du kan til enhver tid trække dit samtykke tilbage, og såfremt det er eneste behandlingsgrundlag, vil fremtidig behandling ophøre. Vores opbevaringspligt og -ret ændres dog ikke heraf.

Samtykket kan trækkes tilbage ved at rette henvendelse til os på de kontaktoplysninger, der er anført under pkt. 1.

11 COOKIES

11.1 Hvad er cookies?

Cookies er små tekstfiler, der indeholder bogstaver og tal, som sættes på din computer eller anden enhed. Cookies sættes, når du besøger et websted, der bruger cookies og de kan bruges til at holde styr på hvilke sider du har besøgt, de kan hjælpe dig til at fortsætte, hvor du slap eller de kan huske dine sprogindstillinger eller andre præferencer. Der er ingen personlige oplysninger gemt i vores cookies, og de kan ikke indeholde virus.

Hvis vi placerer cookies, bliver du informeret om anvendelsen og formålet med at indsamle data via cookies. Samtidig bliver du bedt om at afgive dit samtykke. Nødvendige cookies til sikring af funktionalitet og indstillinger kan dog anvendes uden dit samtykke.

11.2 Cookietyper og deres formål

Formålet med cookies er at foretage trafikmåling og lette din brugeroplevelse af websiden. Websiden bruger cookies fra Google Analytics til at måle trafikken på websitet.

Du kan fravælge cookies fra Google Analytics her: http://tools.google.com/dlpage/gaoptout

11.3 Slet eller slå cookies fra i browseren

Du kan altid afvise cookies på din computer ved at ændre indstillingerne i din browser. Hvor du finder indstillingerne afhænger af, hvilken browser du anvender. Du skal dog være opmærksom på, at hvis du gør det, er der mange funktioner og services på internettet, du ikke kan bruge.

Alle browsere tillader, at du sletter dine cookies samlet eller enkeltvis. Hvordan du gør det afhænger af, hvilken browser du anvender. Husk, at bruger du flere browsere, skal du slette cookies i dem alle.

Læs mere om sletning og håndtering her: http://minecookies.org/cookiehandtering

12 SIKKERHED

Vi beskytter dine persondata og har et sæt interne regler om informations- og IT-sikkerhed.

Vores interne sikkerhedsregler indeholder instrukser og foranstaltninger, der beskytter dine persondata mod at blive tilintetgjort, gå tabt eller blive ændret, mod uautoriseret offentliggørelse, og mod at uvedkommende får adgang eller kendskab til dem.

Vi har fastlagte procedurer for tildeling af adgangsrettigheder til de af vores medarbejdere, der behandler persondata, herunder følsomme. Vi kontrollerer deres faktiske adgang gennem logning, koder og tilsyn. For at undgå datatab tager vi løbende back up af vores datasæt.

I tilfælde af et sikkerhedsbrud, der resulterer i en høj risiko for dig for diskrimination, ID-tyveri, økonomisk tab, tab af omdømme eller anden væsentlig ulempe, vil vi underrette dig om sikkerhedsbruddet så hurtigt som muligt, ligesom vi har en lovbestemt anmeldelsespligt.

13 KLAGER (ART. 77)

Enhver registreret har ret til at indgive klage til Datatilsynet over vores behandling af persondata.

Klage sker ved henvendelse til

Datatilsynet
Borgergade 28, 5.
1300 København K
e-mail: dt@datatilsynet.dk
tlf: 3319 3200

14 VERSION OG OPDATERING

Den hurtige udvikling af internettet betyder, at ændringer i vores privatlivspolitk kan blive nødvendige. Vi forbeholder os derfor ret til at opdatere og ændre nærværende retningslinjer for behandling af persondata. Gør vi det, retter vi selvfølgeligt datoen for "sidst opdateret" nederst på siden. I tilfælde af væsentlige ændringer giver vi dig besked i form af en synlig meddelelse på vores webside.

Denne privatlivspolitik er senest ændret den 11. juni 2018

IT-SIKKERHEDSPOLITIK FOR Hovedvejens Autocenter

1. INDLEDNING

Sikkerhedspolitikken skal til enhver tid understøtte virksomhedens værdigrundlag og vision samt demonstrere, at virksomheden har en seriøs holdning til sikkerhed for persondata, systemer og andre IT-aktiver.

Hensigten med sikkerhedspolitikken er endvidere at tilkendegive over for alle, som har en relation til virksomhed, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer.

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at virksomheden fremstår troværdig, og for at fastholde denne troværdighed skal det sikres, at al information behandles med fornøden fortrolighed og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer betragtes, næst efter medarbejderne, som virksomhedens mest kritiske ressource. Der lægges derfor vægt på driftsikkerhed, kvalitet, overholdelse af lovgivningskrav og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at vores image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Beskyttelsen skal være vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Alle personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

Tilsidesættelse af denne IT-politik kan få aftaleretlige, herunder ansættelsesretlige, konsekvenser for såvel medarbejdere, ledelse som leverandører. Ledelsen er pligtig at påse overholdelsen.

2. FORMÅL

Målene for virksomhedens IT-politik er at

- opnå høj driftsikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab - TILGÆNGELIGHED
- opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer - INTEGRITET
- opnå fortrolig behandling, transmission og opbevaring af data - FORTROLIGHED
- opnå en gensidig sikkerhed omkring de involverede parter - AUTENTICITET
- opnå en sikkerhed for gensidig og dokumenterbar kontakt - UAFVISELIGHED

alt under skyldig hensyntagen til den til enhver tid værende persondatalovgivning.

3. VIGTIGE GRUNDPRINCIPPER

3.1 FUNKTIONSADSKILLELSE

Funktionsadskillelse er det bærende kontrolprincip på såvel personligt som organisationsplan. Dette er sjældent praktisk fuldt ud muligt, blandt andet af hensyn til medarbejderens IT-færdigheder og -kompetencer. I det omfang, det er muligt, og opgaven således ikke er outsourcet til en databehandler, herunder et lønbureau eller en IT-supporteringsvirksomhed, er det ledelsens pligt at sikre, at alle nødvendige behandlingsskridt noteres med navn, dato og beskrivelse af behandlingen.

3.2 SIKKERHEDSFORANSTALTNINGER

Ledelsen beslutter omfang og styrke af de sikkerhedsforanstaltning, der findes nødvendige at installere. Sådanne installeres af den IT-ansvarlige, hvilken funktion kan være outsourcet. Ledelsen varetager og formulerer administrative foranstaltninger ved nye tiltag og foranstaltninger, herunder udarbejdelse af retningslinjer og instrukser.

3.3 STYRING AF SIKKERHEDSHÆNDELSER

Ledelsen skal løbende sikre og monitere eventuelle hændelser, der kan true sikkerheden, således at risikoen for databrud kan minimeres eller undgås. Ledelsen skal holdes orienteret fra medarbejderne, jf. pkt. 5.

Ledelsen er opmærksom på pligten til at foretage indberetning af databrud. Ved databrud skal følgende iagttages.

Virksomheden skal foretage anmeldelse af sikkerhedsbruddet til Datatilsynet uden unødig forsinkelse, dog senest 72 timer efter, vi er blevet bekendt med bruddet.

Anmeldelsen skal foretages af direktøren som kontaktperson, og anmeldelsen skal mindst

- beskrive karakteren af bruddet, herunder forventet antal berørte og kategorierne af oplysninger,
- sandsynlige konsekvenser af sikkerhedsbruddet, og
- de foretagne foranstaltninger, der er truffet.

Derudover dokumenterer ledelsen alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne, afhjælpende foranstaltninger.

Hvis bruddet indebærer en høj risiko for fysiske personer, underretter vi som udgangspunkt den unødig forsinkelse de registrerede om bruddet. Ledelsen har ansvaret herfor.

3.4 DOKUMENTATION

Såfremt der skal udføres særlige, væsentlige sikkerhedsaktiviteter, skal disse planlægges, risikovurderes og dokumenteres.

4 ORGANISERING AF SIKKERHEDSARBEJDET

Ledelsen har det overordnede ansvar for det IT-mæssige sikkerhedsarbejde. Ledelsen kan og skal i fornødent omfang inddrage medarbejdere og samarbejdspartnere, der fungerer som databehandlere.

Ledelsen har ansvaret for udformningen af IT-politikken, herunder opdateringer heraf, ligesom ledelsen udpeger den eller de personer, der skal have adgang til især følsomme persondata.

5 MEDARBEJDERE - SIKKERHEDSBEVIDSTHED

Den enkelte medarbejder har pligt til at gøre sig bekendt med IT-sikkerhedspolitikken, herunder reglerne for opkobling udefra, hjemmearbejde m.v. således at vedkommende opnår en sikkerhedsbevidsthed. Den enkelte medarbejdere har yderligere pligt til straks ved mistanke eller konstatering af eventuelle sikkerhedsbrud at foretage indberetning heraf til ledelsen.

Medarbejderne skal løbende informeres om IT-sikkerhedspolitikken, herunder om deres pligter og rettigheder og om nødvendigt undervises nærmere heri.

6 STYRING AF AKTIVER

Virksomhedens IT-aktiver (software, data og fysiske enheder) skal identificeres og registreres med en ejer, der typisk vil være den daglige bruger heraf. Er der tale om en hosted løsning, skal der tages hensyn hertil i aftalegrundlaget med samarbejdspartneren, afhængigt af, om vedkommende optræder som databehandler.

Den registrerede ejer af aktivet har ansvaret for

- at aktivet til stadighed ved placering, brug og forandring m.v. opfylder IT-politikken,
- at aktivet ikke udsættes for særlig risiko, eksempelvis særlig usikre offentlige netværk m.v.
- at aktivet til stadighed er forsynet med en af den registrerede ejer selvvalgt og hemmelig kode, der SKAL fornys mindst hver 3. måned,
- at aktivet til stadighed er forsynet med tilstrækkelig og opdateret firewall og viruskontrol.
- at sensitive koder ikke lagres automatisk

Den registrerede ejer skal føre en logbog over sine forpligtelser, herunder tidspunkter for forandring af koder. Ledelsen kan kræve dokumentationen fremvist med mindst 6 måneders mellemrum, medmindre der foreligger en konkret begrundet mistanke om misbrug eller sikkerhedshændelser.

Ethvert aktiv skal sikre og beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport eller ved opbevaring. Dette gælder også – og især – bærbare computere, tablets og mobiltelefoner.

Enhver medarbejder har pligt til at sikre, at alle fysiske dokumenter, der indeholder persondata, almindelige eller følsomme, opbevares utilgængelige for uvedkommende, herunder i skabe eller andre arkivalier, og at sådanne makuleres, når disse ikke længere benyttes eller der foreligger en sletteplig i øvrigt iht. virksomhedens persondata- og privatlivspolitik.

Bortskaffelse af aktiver, som indeholder eller kan give adgang til persondata og andre følsomme oplysninger, herunder fortrolig information af hvad art tænkes kan, skal ske efter aftale med og instruks fra ledelsen, der skal sikre, at aktivet lagres og dokumenteres, hvorefter bortskaffelse kan ske forsvarligt, eksempelvis ved destruktion, makulering eller definitiv sletning af data.

Det er tilladt for medarbejderne at benytte virksomhedens aktiver til privat brug.

7 STYRING AF ADGANG – ELEKTRONISK

Enhver elektronisk adgang til virksomhedens systemer kræver log-on-koder. Alle fysiske aktiver kræver korrekt indtastet kode indenfor 5 forsøg. Herefter blokeres der for adgang indtil Bente Petersen har godkendt ny opsætning af adgang.

Forgæves log-on-forsøg med spærring skal registreres manuelt af Bente Petersen med angivelse af dato, ejer af aktivet, jf. pkt. 6, samt de faktiske omstændigheder ved hændelsen.

7.1 HR-OPLYSNINGER

Alle persondata, herunder følsomme, kan alene tilgås af Bente Petersen, der har ansvaret for lønbogholderi henholdsvis virksomhedens daglige ledelse. Disse oplysninger kan alene tilgås af de pågældende efter indtastning af en af dem valgt kode til systemet.

7.2 KUNDEDATA

Alene de medarbejdere, der har behov for persondata på kunder, eksempelvis den medarbejder, der konkret udfører arbejde for pågældende kunde, har adgang til disse data. Principielt set har alle medarbejdere dog adgang hertil i erkendelse af, at en medarbejder kan blive nødsaget til at overtage en konkret opgave for en anden medarbejder.

7.3 PRIVAT BRUG AF AKTIVER OG E-MAILS

Private e-mails skal være forsynet med emnefeltet "PRIVAT" og slettes straks ved arbejdsforholdets ophør, såfremt medarbejderen ikke forud herfor selv har gjort dette.

Arbejdsrelaterede, nødvendige, e-mails fra *tidligere* medarbejdere, der ikke i forvejen er arkiveret, overføres til virksomhedens hovedpostkasse og arkiveres i overensstemmelse med virksomhedens generelle håndterings- og privatlivspolitik. Øvrige e-mails slettes samtidig med arbejdsforholdets ophør, dog senest 1 måned herefter.

Enhver håndtering af fratrådte medarbejderes e-mail skal være færdiggjort senest 12 måneder efter fratræden. Selve e-mailadressen skal nedlægges senest 1 måned efter fratræden med henvisning til en anden.

8 STYRING AF ADGANG – FYSISK

Alle følsomme persondata opbevares hos den herfor ansvarlige i aflåste skabe. Almindelige oplysninger opbevares på virksomhedens kontor, der låses af udenfor normal arbejdstid.

9 E-MAIL- OG KOMMUNIKATIONSSIKKERHED

Ingen e-mails må indeholde persondata i emnefeltet, ligesom e-mail indeholdende følsomme persondata i videst muligt omfang skal fremsendes krypteret. Lønsedler og andre HR-relaterede oplysninger skal altid fremsendes krypteret, kodet eller med sikker post.

Al overførsel af information, herunder via e-mail, skal klassificeres i forhold til persondatalovgivningen, ligesom der skal foretages en konkret risikovurdering. Om nødvendigt kan brugen af begrebet "fortroligt" eller "hemmeligt" benyttes i emnefeltet til forsendelse og overførsel.

10 DRIFTSSIKKERHED, ANSKAFFELSE OG VEDLIGEHOLDELSE

Driftssikkerhed drejer sig om at opnå korrekt og sikker drift af de faciliteter og systemer, der behandler, herunder opbevarer, information og persondata. Heri indgår dokumentation af procedurer for drift, softwareinstallation samt styring af ændringer, der løbende forekommer, herunder opdateringer, som kan påvirke sikkerheden.

Der skal indføres sikkerhedsforanstaltninger, der kan opdage og forhindre data- og sikkerhedsbrud, eksempelvis forårsaget af malware. Ligeledes skal der foretages løbende backup af data, ligesom der skal udarbejdes en backup-plan til brug for større sikkerhedsbrud.

Enhver anskaffelse med tilhørende installation og vedligeholdelse må alene ske fra en leverandør, der opfylder betingelserne i pkt. 11.

11 OUTSOURCING

Leverandører, der helt eller delvist står for drift af virksomhedens aktiver og systemer skal overholde virksomhedens IT-sikkerhedspolitik. Der skal være mulighed for at udøve effektiv kontrol hermed, ligesom leverandører skal kunne dokumentere deres overholdelse.

I forbindelse med outsourcing kan det blive nødvendigt at udarbejde en databehandleraftale, der i detaljer skal beskrive de sikkerhedskrav, som leverandøren skal leve op til.

12 VERSION OG OPDATERING

Den hurtige udvikling af internettet betyder, at ændringer i IT-sikkerhedspolitikken kan blive nødvendige. Derfor kan og skal ledelsen foretage ændringer heri, såfremt det er nødvendigt. Enhver ændring skal meddeles de berørte pligtsubjekter, eksempelvis medarbejderene.

Denne IT-sikkerhedspolitik er senest ændret den 11. juni 2018