Tittel retningslinjer:	**Retningslinjer for datavern**
Avsender retningslinjer:	**Juridisk rådgiver og SVP, HR** **Juridisk avdeling og HR**
Avdeling:	**24. mai 2018**
Innført:	
Revisjonsdato:	**24. mai 2019**
Neste dato for gjennomgang:	

RETNINGSLINJER FOR DATAVERN GENERELL REGEL

Ansatte i NEP-konsernet ("NEP" eller "selskapet") er ansvarlige for å beskytte NEPs selskapsinformasjon og informasjon om ansatte uansett medium.

Les brødteksten i disse retningslinjene for flere detaljer og mer informasjon.

INNHOLDSFORTEGNELSE:

FORKLARENDE MERKNAD OG STATUS FOR DISSE RETNINGSLINJENE

NEP Group, Inc. sammen med dets datterselskaper, refereres til i disse retningslinjene som "**NEP**"/, "**Selskapet/selskapene**" / "**vi**"/ "**oss**"/ "**vår**". NEP trenger å innhente visse opplysninger om personer for å kunne drive sin virksomhet på en effektiv måte. Denne informasjonen kommer fra, blant annet, nåværende, tidligere og potensielle ansatte, arbeidere, jobbsøkere, kunder, akkreditører, leverandører og andre personer som NEP kommuniserer og gjør forretninger med.

Dermed er vi ansvarlige overfor disse personene for å sørge for at vi bruker deres opplysninger med varsomhet og i samsvar med personvernlover og lover om databeskyttelse ("**datavernlover**"). Vårt merkes- og organisasjonsverdier krever at vi tar i bruk og overholder gode databehandlingsprosedyrer, inkludert de som er fastsatt i disse retningslinjene for datavern ("**retningslinjene**").

Disse retningslinjene fastsetter (i del A) hvordan NEP vil bruke opplysningene til sine ansatte, og (i del B) veiledning med tanke på noen av de viktige tiltakene NEP forventer sine ansatte vil ta når det gelder NEPs databehandling. Disse retningslinjene fastsetter våre regler om datavern og betingelsene som må oppfylles i forbindelse med anskaffelse, behandling, lagring, transport og destruksjon av personlige opplysninger.

Underlagt gjeldende lov gjelder disse retningslinjene for alle NEP-ansatte (fulltid og deltid), midlertidige arbeidere, entreprenører, frivillige, praktikanter, besøkende, forhandlere og andre tredjeparter.

For NEP-steder der gjeldende lov krever spesifikke retningslinjer og/eller prosedyrer i stedet for eller i tillegg til disse retningslinjene, kan det legges ved landsspesifikke vedlegg til disse retningslinjene.

DEL A –NEPs ANSVAR OVERFOR DEG UNDER DATAVERNLOVER

1. Personvernteam

NEP har utnevnt et team av datavernrepresentanter for å hjelpe selskapet med å overholde sine forpliktelser under datavernlovene. Nøkkelrollen til datavernsrepresentantene er som følger:

- å være et kontakt- og støttepunkt for ansatte;
- å utføre og støtte gjennomføringen av personvernrelaterte konsekvensutredninger;
- å gi opplæring til ansatte;
- å opprettholde kontakt med det lokale datatilsynet;
- å ta seg av forespørsler om tilgang til informasjon; og

Hvis du etter å ha lest disse retningslinjene på noe tidspunkt har spørsmål relatert til måten du bør behandle personopplysninger på, kontakter du din lokale datavernrepresentant.

Du finner din lokale datavernrepresentant ved å kontakte juridisk avdeling, HR eller IT-avdelingen.

2. Omfanget av datavernlover

Datavernlover styrer måten NEP kan behandle informasjon som identifiserer eller dreier seg om levende personer (personopplysninger) og gir også disse personene visse rettigheter og rettsmidler med tanke på den informasjonen. Lovene regulerer også markedsføringsaktiviteter og bruken av nettbaserte sporingsteknologier, som for eksempel informasjonskapsler. De dekker derfor et bredt omfang av aktiviteter som NEP (og dets samarbeidspartnere og leverandører på NEPs vegne) foretar.

Lovene påtvinger en høyere standard for forsiktighet i forbindelse med bruken av "**sensitive personopplysninger**" som omfatter informasjon om en persons rase eller etniske opphav, politiske meninger, religiøs eller filosofiske overbevisning, fagforeningsmedlemskap, helse, sexliv, seksuell legning, genetiske og biometriske data og, for formålene til disse retningslinjene, kriminelle dommer og lovovertredelser. I disse retningslinjene dekker henvisninger til "**personopplysninger**" handlinger foretatt med alle typer informasjon om personer, inkludert sensitive personopplysninger.

Datavernlover reguler informasjon som lagres av eller på vegne av NEP elektronisk eller, i visse situasjoner, som lagres som en del av visse typer velstrukturerte manuelle arkiveringssystemer. CCTV-video og lydopptak dekkes også.

3. Typen informasjon NEP kan ha om sine ansatte

Typene personopplysninger NEP kommer til å behandle i løpet av sitt engasjement med deg omfatter:

- navn, adresser, telefonnumre og andre private kontaktopplysninger;
- kjønn, fødselsdato, personnummer, nasjonalt ID-nummer, immigrasjonsstatus, sivilstand, pårørende;
- personelldokumenter, inkludert opplæring, evalueringer, bilder, informasjon om ytelse og disiplinærforhold, informasjon om uførhet, CV-er og etterfølgerplanlegging;
- bankopplysninger, lønn, bonus, goder og pensjonsopplysninger;
- CCTV-bilder og telefonopptak;
- reisehistorikk, kopier av pass, kopier av førerkort, passordidentifikatorer og informasjon knyttet til visumberettigelse.
- Sensitive personopplysninger, som for eksempel informasjon om rasemessig eller etnisk opphav, religiøs eller filosofisk overbevisning, fagforeningsmedlemskap, helse, genetisk og biometriske data og kriminelle dommer eller lovovertredelser.

4. Måten NEP kan behandle ansattes personopplysninger

Personopplysninger om personer kan kun behandles for et legitimt formål. NEP kommer til å foreta seg mange handlinger med en ansatts personopplysninger, inkludert, men ikke begrenset til:

- lønns,- gode- og pensjonsadministrasjon;
- helse- og sikkerhetshistorikk og administrasjon;
- kriminelle bakgrunnssjekker, kredittsjekker og kredittklarering (der det er aktuelt);
- bekrefte informasjon på CV-er og følgebrev, gi referansebrev og utføre referansesjekker;
- opplæring og evaluering, inkludert ytelsesevaluering og disiplinærhistorikk;
- administrasjon av ansatte og forfremmelser;
- etterfølgerplanlegging;
- overvåkning av likestilling;
- eventuell potensiell endring av kontroll av et selskap i konsernet, eller eventuell overføring av ansettelse relatert til en forretningsoverføring eller endring av tjenesteleverandør (i Europa, "Acquired Rights Directive" (direktivet om erververde rettigheter"). Under slike omstendigheter kan personopplysninger offentliggjøres til den potensielle kjøperen eller investoren eller deres rådgivere i den grad loven tillater det;
- andre offentliggjøringer som kreves i sammenheng med en sysselsettingskampanje eller markedsføring av NEP, dets produkter eller tjenester;
- anskaffelse av informasjon om ansatte til kunder og byråer i løpet av anskaffelse av NEPs tjenester;
- CCTV-overvåkning av sikkerhetsmessige årsaker;
- drift av en etikk- eller varslerlinje som NEP kan drive nå eller i fremtiden;
- overholdelse av gjeldende prosedyrer, lover, forskrifter, inkludert eventuelle relaterte etterforskninger for å sørge for samsvar eller etterforskning av potensielle brudd;
- etablere, utøve og forsvare NEPs juridiske rettigheter;
- eventuelle andre rimelige formål i forbindelse med en persons ansettelse eller engasjement av NEP;
- tilby og administrere bruk av tjenester tilbudt av tredjeparter, som for eksempel reisebyråer, firmamobiler, firmakort og firmabiler samt fakturering for slike tjenester.

NEP kan også innhente og behandle personopplysninger om dine pårørende slik at de kan kontaktes i en nødssituasjon eller i forbindelse med bruk av en firmabil som leveres av NEP. Deres personopplysninger vil også bli behandlet i samsvar med datavernlovene og som beskrevet i disse retningslinjene.

For å kunne oppfylle disse formål, forbeholder NEP seg retten til å, etter eget skjønn, offentliggjøre en persons personopplysninger (eller sensitive personlige informasjon som hensiktsmessig) til politimyndigheter, tilsynsorganer, offentlige etater og andre tredjeparter som påkrevd av loven eller for administrasjonsmessige formål, i den grad lokal tillater og krever det.

NEP kan også gi personopplysninger spesielt for, men ikke begrenset til, de samme formål som fastsatt ovenfor, til entreprenører og leverandører som tilbyr tjenester til NEP og som kan bistå med behandlingene som fastsatt ovenfor. I et slikt tilfelle forplikter NEP seg til å inngå en databehandlingsavtale med entreprenørene og leverandørene som NEP gir personopplysninger til.

NEP kan overføre personopplysninger til andre selskaper i konsernet, til samarbeidspartnere, leverandører, politimyndigheter og til andre organisasjoner som befinner seg utenfor EØS ("**EEA**") (for disse formålene definert til å omfatte Storbritannia) for:

- HR-administrasjon (for eksempel personalrekruttering);
- lønnsadministrasjon for ansatte som jobber utenfor EØS;
- flytte ansatte fra et sted til et annet;
- visumsøknader;
- beskatning og registreringer for ansatte som jobber utenfor EØS;
- oppfylle NEPs juridiske krav;
- oppfylle kundekontrakter for anskaffelse av NEPs tjenester;
- rettssaker i utlandet; og
- utsetting av NEP-funksjoner.
- Akreditteringer og reisevisum.

Disse landene kan blant annet omfatte land hvor NEP har operasjoner, og lokasjonen til våre leverandører og deres datasentre, for eksempel Microsoft (USA), sammen med andre store leverandører av HR-programvare.

Vær oppmerksom på at lovene i noen jurisdiksjoner utenfor EØS kanskje ikke er like beskyttende som datavernlover innenfor EØS.

5. Dokumentoppbevaring

NEP har en lovpålagt plikt til å beholde visse dokumenter i en minimumsperiode. NEP skal ikke oppbevare personopplysninger lenger enn det som er nødvendig eller som kan kreves av gjeldende lov.

6. Overvåkning

<u>Overvåkning av NEPs systemer</u>

NEPs IT- og kommunikasjonssystemer skal fremme effektiv kommunikasjon og arbeidspraksis i organisasjonen vår.

Av forretningsmessige årsaker, og for å opprettholde IT-relaterte sikkerhetstiltak, blir bruken av NEPs systemer på en relevant plattform, inkludert telefonen (mobil og fasttelefon) og datasystemer (inkludert e-post og internettilgang), og eventuell privat bruk av dem, overvåket. Hvis du tar deg tilgang til tjenester gjennom bruk av passord og påloggingsnavn på NEPs IT- og kommunikasjonssystemer, kan dette bety at din private tilgangsinformasjon blir sett av NEP.

Overvåkning utføres kun hvis, og i den grad loven tillater det, eller det er påkrevd av loven og som nødvendig og berettiget for forretningsformål. Dette er påkrevd slik at tilfeller av misbruk og andre sikkerhetshendelser kan oppdages og at informasjon er tilgjengelig for å støtte eventuelle påfølgende etterforskninger og oppfølging. I den grad loven tillater det kan det, i tilfeller hvor det oppdages brudd på disse retningslinjene, fattes tiltak under disiplinærprosedyren.

NEP forbeholder seg retten til å hente innholdet i meldinger, sjekke søk som er gjort på Internett, kreve umiddelbar innlevering av enheter levert ut av NEP og ta seg tilgang til data lagret på slike enheter for følgende formål (denne listen er ikke uttømmende):

- for å overvåke om bruken av e-postsystemet eller Internett er legitimt og i samsvar med disse retningslinjene (og ansatte anerkjenner at NEP kan bruke programvare til å overvåke identiteten til sendere og mottakere av e-post);
- for å finne tapte meldinger eller for å hente meldinger som er gått tap på grunn av datafeil;
- for å bistå med etterforskning av ulovlige handlinger, inkludert disse som bryter våre andre retningslinjer eller gjeldende lov; og
- for å overholde eventuelle juridiske forpliktelser.

En betingelse for bruk av våre IT-systemer er at du opptrer på en yrkesmessig måte, ikke bringer vanry over selskapet og ikke opptrer på en upassende måte i tilknytning til kollegaene dine og andre du kontakter ved gjennom bruken av kommunikasjon mens du jobber for NEP. Hvis det oppdages beviser om et brudd på disse vilkårene eller misbruk av NEPs IT-systemer, kan NEP foreta en mer detaljert etterforskning i samsvar med NEPs disiplinærprosedyrer, som innebærer en undersøkelse og offentliggjøring av overvåkningsmateriell til de som er utpekt til å foreta en etterforskning samt eventuelle vitner eller ledere som er involvert i disiplinærprosedyren. Likeledes hvis NEP har rimelig mistanke om at ulovlig aktivitet eller handlinger som kan bryte med våre retningslinjer og prosedyrer har funnet sted.

Om nødvendig kan slik informasjon gis til politiet eller annen politimyndighet. Etterforskninger og offentliggjøring av informasjon til relevante myndigheter skal kun utføres i den grad loven tillater det.

CCTV

Noen av NEPs bygninger og anlegg bruker CCTV-systemer til å overvåke ytre og indre områder døgnet rundt av sikkerhetsmessige årsaker. Disse dataene tas opp. Bruk av CCTV og opptak av CCTV-data utføres kun i henhold til NEP-godkjente retningslinjer.

7. Dine datarettigheter

Under datavernlover kan ansatte ha rett til å be NEP om en kopi av sine personopplysninger, til å rette dem, slette dem eller begrense behandlingen av dem, eller til å be NEP om å overføre noe av denne informasjonen til andre organisasjoner. Ansatte kan også ha retten til å komme med innvendinger mot en viss behandling av sine personopplysninger og, der NEP har bedt om samtykket deres til å behandle data, til å trekke tilbake samtykket. Disse rettighetene skal i noen situasjoner være begrenset – for eksempel i de tilfeller hvor NEP demonstrerer at de har juridisk krav på å behandle dataene dine. I noen tilfeller kan dette bety at NEP kan oppbevare data selv om den ansatte trekker tilbake samtykket sitt.

I de tilfeller hvor NEP krever at personopplysninger samsvarer med juridiske eller kontraktsmessige forpliktelser, er tilveiebringelse av slike data obligatorisk: hvis slike data ikke tilveiebringes, vil NEP ikke lenger være i stand til å administrere ansettelsesforholdet, eller til å oppfylle forpliktelser som er pålagt oss. I alle andre tilfeller er tilveiebringelse av forespurte personopplysninger valgfritt.

For eventuelle bekymringer eller spørsmål om hvordan NEP behandler ansattes personopplysninger, kontakter du datavernteamet.

8. Klager

En individuell arbeider som mener at en annen person har krenket hans/hennes datavernrettigheter, oppfordres til å ta dette opp med sin linjeleder eller en annen person som er utpekt innenfor forretningsenheten/lokal klageprosedyre.

Ansatte med uløste bekymringer har også rett til å klage direkte til datavernmyndigheter. Den relevante datavernmyndigheten vil være den overordnede myndigheten i det samme landet som enheten som sysselsetter deg.

DEL B – Ditt ansvar overfor andre under datavernlover

Denne delen av retningslinjene har til hensikt å informere ansatte om hvordan de skal behandle personopplysninger under visse omstendigheter. Alle ansatte har en forpliktelse til å overholde datavernlovene. Det er viktig at personer er klar over sine egne datavernansvar overfor andre under datavernlovene, som omfatter behovet for å følge retningslinjene og prosessen fastsatt nedenfor. Her er noen viktige punkter å huske:

- Vurder ansvaret ditt under datavernlovene og disse retningslinjene og hvordan de påvirker dine daglige aktiviteter.
- Del kun personopplysninger (eller kommersielt sensitive opplysninger) på et behov for å vite-grunnlag. Ikke del en hel database når det kun er behov en del av den.
- Dobbeltsjekk mottakerens opplysninger før du deler data. Sender du data som tiltenkt eller utsetter du selskapet for risiko?
- Bruk passordbeskyttelse for dokumenter og filer når det er passende.
- Bruk kun personopplysninger på den måten personen som opplysningene gjelder har godtatt eller som fastsatt i disse retningslinjene.
- Bruk en fornuftig tilnærming når du bestemmer hvordan du skal beskytte, bruke og kvitte deg med personopplysninger. Tenk på hvordan du vil at dine personopplysninger skal behandles.

Denne delen er tiltenkt å gi generell veiledning og er ikke en omfattende eller uttømmende veiledning. Avhengig av den nøyaktige karakteren av jobben din, kan du ha ytterligere ansvar overfor andre under datavernlover.

Ditt generelle ansvar er som følger:

9. Datavernprinsipper

Ved behandling av personopplysninger, må NEP og selskapets ansatte følge visse datavernprinsipper som finnes i datavernlovene. Disse omfatter at personopplysninger må:

- behandles på en rettferdig og lovlig måte;

- behandles kun for ett eller flere spesifiserte og lovlige formål, og ikke behandles ytterligere på noen måte som er uforenlig med slike formål, med mindre det er uttrykkelig tillatt under gjeldende lover;
- være tilstrekkelige, relevant og ikke urimelig i relasjon til formålene de blir behandlet for;
- være nøyaktige og, der det er nødvendig, holdes oppdatert;
- ikke oppbevares lenger enn det som er nødvendig for formålene de ble behandlet for;
- behandles i samsvar med en persons rettigheter, deriblant under visse omstendigheter: til tilgang til personopplysninger, til å få dem overført til en tredjepart, eller til at de slettes hvis de er feil eller ikke lenger er nødvendige, og at de ikke skal være gjenstand for betydelige automatiserte beslutningstakingsprosesser;
- holdes sikre; og
- kun overføres til eller tas tilgang til fra et land eller territorium utenfor EØS hvis det landet eller territoriet sørger for et tilstrekkelig nivå av beskyttelse for rettighetene og friheten til personer i forbindelse med behandling av personopplysninger, eller hvor det finnes tilstrekkelige kontraktsmessige forholdsregler for å beskytte opplysningene.

10. Holde data sikre

Bestemmelsene i denne delen og del 11 (Rapportere mistenkte datasikkerhetsbrudd) gjelder ikke bare for personopplysninger, men for all informasjon, IT- og kommunikasjonssystemer som du er ansvarlig for sikkerheten til, eller utstyr som er tildelt eller brukes av deg, og du må ikke la det blir brukt av noen andre i samsvar med disse retningslinjene.

Datamaskin/-bærbar datamaskin-sikkerhet:

- Alle IT-brukere vil ha mottatt unike kontodetaljer. Du må ikke dele kontoer eller passord. Du må ikke bruke kontoer som er tilordnet til deg eller avsløre kontodetaljene dine til andre.
- Du bør alltid låse, logge av eller slå av din datamaskin eller bærbare datamaskin eller håndholdte enhet i perioder hvor du vil la dem ligge uten ubevoktet (f.eks. for å delta på møter eller under matpauser). NEPs IT-systemer er utviklet, der det er mulig, til å automatisk låses eller stenges ned etter en gitt periode uten aktivitet.
- På slutten av hver arbeidsdag bør du sørge for at datamaskinen og skjermen er slått av. Hvis du har en bærbar datamaskin, bør den lagres på en sikker måte, for eksempel i et låst skap eller i en skuff.
- Sørg for at forretningsmessig sensitiv og konfidensiell informasjon som vises på en skjerm ikke lett kan sees fra utenfor eiendommen vår.
- Du må bruke et sterkt passord (f.eks. en blanding av store og små bokstaver, tall og spesielle tegn) og holde det konfidensielt. Du bør endre det regelmessig, og hvis du tror at noen kjenner til passordet ditt bør du endre det med én gang.
- Endringer til eller vedlikehold av datamaskinen din eller IT-utstyr eller installasjon av eventuelle maskinvare eller programvare på NEP-støttede ressurser skal kun gjøres av NEPs Informasjon

Services-team eller dets assosierte eller godkjente personer med tillatelse fra Information Services-teamet.

Tilgang til data som lagres elektronisk:

- Bruk passord for å begrense tilgang til sensitive filer.
- Ikke omgå etablerte sikkerhetsgrupperinger eller godkjenningsnivåer.
- Opprettholde et revisjonsspor for endringer som gjøres til databaser eller dokumenter som inneholder sensitiv informasjon.
- Ikke forhindre noen planlagte IT-sikkerhetskopieringsprosesser.

Sikkerheten til bærbare enheter:

- Hvis du er blitt gitt tilgang til NEP-støttede IT-systemer eller infrastruktur, er du ansvarlig for å beskytte den og ta rimelige forholdsregler og varsomhet for å sørge for at den ikke blir brukt av uautoriserte parter, mistes, stjeles eller skades, spesielt når du reiser eller når du er borte fra kontoret.
- Bærbare enheter må ikke legges igjen i biler på noe tidspunkt, spesielt over natten, men hvis det er absolutt nødvendig må du sørge for at de holdes utenfor åsyn.
- Hvis du bruker bærbare enheter på, for eksempel, offentlig transport eller på offentlige steder som en hotellfoajé, må du sørge for at skjermen ikke kan leses av andre passasjerer, og du bør ta passende forholdsregler i lys av den risikoen.
- Hvis du bruker din bærbare enhet på noen eksterne eller tredjepartsnettverk, for eksempel på et hotell eller en flyplass, må du ta rimelige forholdsregler for å sikre at nettverket er sikkert, for eksempel ved å bruke et nettverk som leveres av et vel ansett selskap og som fortrinnsvis er låst i stedet for tilgjengelig uten begrensning. Hvis du er tvil om sikkerheten til nettverket, bør du ikke koble enheten din til det.
- Du må ikke prøve å omgå krypteringsprogramvare eller sikkerhetsfunksjoner på de bærbare enhetene.
- NEP bruker en kombinasjon av følgende sikkerhetsfunksjoner på bærbare enheter for å sørge for at de holdes sikre:
    - brukernavn/passord og PIN-numre;
    - virusbeskyttelse;
    - datakryptering;
    - låsing av konto ved mislykkede tilgangsforsøk;
    - låsing av enhet/applikasjon etter manglende aktivitet;
    - låsing av konto eller enhet etter tyveri/tap;
    - overvåkning av bruk; og

- sletting av innhold på mistede eller stjålne enheter.

Sikkerhet for papirkopier av personopplysninger på stedet:

- Hold pulten din fri for personopplysninger og forretningsmessig sensitiv konfidensiell informasjon.
- Ikke la personopplysninger eller forretningsmessig sensitiv konfidensiell informasjon ligge uten tilsyn på pulter på noe tidspunkt.
- Hvis du skriver ut sensitive personopplysninger eller forretningsmessig sensitiv konfidensiell informasjon, må du sørge for at du står ved skriveren for å ta imot dem og unngå at noen andre plukker dem opp.
- Ikke etterlat personopplysninger eller forretningsmessig sensitiv konfidensiell informasjon på møterom eller andre områder på kontoret. Ta dem med deg og kvitt deg med dem på en sikker måte hvis du ikke lenger trenger dem. Tørk av tavler før du forlater møterom med mindre du blir tydelig fortalt ikke å tørke av dem.
- Lås/lagre personopplysninger og forretningsmessig sensitiv konfidensiell informasjon på et sikkert sted over natten, slik som i et låsbart arkivskap, skuff eller i område/rom som er låst eller som det er begrenset tilgang til.
- Følg eventuelle spesifikke retningslinjer som gjelder for ditt sted eller avdeling.

Sikkerhet for papirkopier av personopplysninger på et eksternt arbeidssted:

- Ta kun personopplysninger eller forretningsmessig sensitiv konfidensiell informasjon utenfor kontoret eller til et eksternt arbeidssted hvis det er absolutt nødvendig.
- Vær klar over risikoen for tap eller tyveri og ta passende forholdsregler for å sørge for at personopplysninger eller forretningsmessig sensitiv konfidensiell informasjon holdes sikker.
- Ikke la personopplysninger eller forretningsmessig sensitiv konfidensiell informasjon ligge uten tilsyn på noe tidspunkt på tog eller andre former for offentlig transport eller på andre offentlige steder. Sørg for at forretningsmessig sensitiv informasjon ikke enkelt kan overvåkes når du er på et offentlig sted.
- Arkiver eller lagre kun personopplysninger eller forretningsmessig sensitiv informasjon på eksterne arbeidssteder ved å bruke en NEP-godkjent leverandør hvor det foreligger en skriftlig kontrakt.

Bruk av mobile lagringsmedier:

Bærbare/flyttbare medium ("**medium**") omfatter alle bærbare enheter som er i stand til å lagre, overføre, manipulere eller fjerne data omfatter (men er ikke begrenset til) mobile enheter, Flash-disker/minnepinner, flyttbare harddisker og optiske medium (CD-er, DVD-er osv.).

- Data kan kun overføres fra NEPs IT-systemer til andre medium når det finnes en genuin forretningsmessig grunn til det, og når bestemmelsene i disse retningslinjene samt direktiver fra Information Services-teamet er fulgt.
- NEP overvåker alle data som kopieres fra nettverket for å oppdage uautorisert dataoverføring og hindre sikkerhetsbrudd.
- Utvekslingen av data enten internt eller med eksterne parter bør alltid foregå via NEPs informasjonssystemer, som for eksempel e-post eller felles dataområder. Bruk av media for dataoverføring skal kun brukes når alle andre alternativer er oppbrukt.
- Eventuelle media som fysisk overføres mellom NEP og/eller en kunde skal sendes som spesialleveranse (for å sikre at mediet kan spores og skaffes tilbake hvis det går tapt).

- Før du bruker et medium, må du være oppmerksom på at:
    - du kun kan bruke medium som er kjøpt gjennom eller godkjent av NEPs Information Services og som er kryptert;
    - mediet må kunne spores for å sikre at det ankommer tiltenkt destinasjon;
    - mediet må skannes for skadelig programvare/virusinfeksjon ved hjelp av et antivirusprogram levert av NEPs Information Services-team før bruk, og må ikke brukes hvis det oppdages at det finnes en mulig infeksjon;
    - kun lagre data som er absolutt nødvendig, dvs. ikke last ned en hel database hvis det kun er behov for små deler av den;
    - sjekk at det mobile lagringsmediet kan kryptere personopplysninger;
    - sørg for at filer som oppbevares på mediet er passordbeskyttet, og at passordet sendes separat til det krypterte mediet;
    - slett umiddelbart data fra mediet når de ikke lenger er nødvendig; og
    - media som ikke kan brukes på ny blir riktig avhendet/destruert på slutten av sin livssyklus i samsvar med anbefalingene fra Information Services-teamet.

<u>Restriksjoner for bruk av uautoriserte enheter eller programvare</u>:

- Du må ikke laste ned ulisensiert programvare, tredjeparts programvare, fritt tilgjengelig programvare eller liknende programvare til datamaskinen din eller annet IT-utstyr fordi de kan inneholde virus eller annen skadelig kode som kan bryte sikkerheten til NEPs systemer.

<u>Tredjepartstilgang</u>:

- NEP er ansvarlig for handlingene og utelatelsene til entreprenører og entreprenører som kan ta seg tilgang til eller behandle personopplysninger på NEPs vegne. Hvis du engasjerer entreprenører, konsulenter eller midlertidig ansatte som har tilgang til NEPs systemer og/eller personopplysninger, må de først skrive under på en avtale som inneholder bestemmelser som tilstrekkelig beskytter NEPs personopplysninger, for eksempel konfidensialitet og sikkerhet. Du bør kontakte din datavernrepresentant for veiledning om bestemmelsene som kreves.

- Spesifikt vil alle prosjekter som innebærer tilkobling av en tredjepart/leverandør til NEPs systemer, kreve en spesifikk vurdering av risikoen og ytterligere kontraktsmessige vilkår knyttet til sikkerhet.
- Alle endringer til tredjeparters/leverandørers tilgang til NEPs nettverk må gjennomgås og dokumenteres for å sikre at sikkerheten opprettholdes.
- Hvis en tredjeparts/entreprenørs tilgang ikke lenger kreves, må tilkoblingen avsluttes og eventuelle personopplysninger innhentet av tredjeparten/entreprenøren må returneres eller destrueres i samsvar med det kontraktsmessige vilkårene.
- Alle tredjepartsleverandører og entreprenører må pålegges å varsle NEP, via deres hovedkontakt, om alle informasjonssikkerhetshendelser de selv eller kundene deres opplever.

Sikkerhetskopiere personopplysninger:

- Der det er mulig skal data oppbevares i nettverkslagring, siden dette enkelt kan sikkerhetskopieres ved hjelp av automatiserte prosesser. Flyttbare medium, som for eksempel USB-flash-enheter og CD-er skal ikke brukes til lagring av forretningskritisk informasjon, siden de ikke vil bli sikkerhetskopiert og derfor ikke vil kunne gjenopprettes ved tap, ødeleggelse eller hvis de blir utilsiktet slettet.

Avhending av personopplysninger:

Personopplysninger i papirformat skal der det er mulig avhendes ved bruk av søppelbøtter for konfidensielle eller makuleringsmaskiner.

- Sørg for at all IT-programvare, mobile enheter, mobile lagringsmedium eller annet utstyr renses riktig for alle personopplysninger før avhending. Media som ikke kan brukes på nytt, som for eksempel CD-ROM-er, må avhendes riktig eller destrueres på slutten av mediets livssyklus. Kontakt Information Services-teamet for å sørge for at dette gjøres riktig.

E-post og systembruk:

- Du må ikke prøve å omgå antivirus-programvare, for eksempel ved å deaktivere den.
- Ansatte bær være forsiktige når de åpner e-post fra ukjente eksterne kilder eller når, av en hvilken som helst grunn, en e-post virker mistenkelig (for eksempelet hvis e-postnavnet ender på .exe).
- Information Services-teamet skal informeres umiddelbart hvis et mistenkt virus mottas eller identifiseres.
- NEP forbeholder seg retten til å blokkere tilgang til vedlegg til e-poster for å sikre effektiv bruk av NEPs IT-systemer og for samsvar med disse retningslinjene.
- NEP forbeholder seg også retten til å ikke overføre (inngående eller utgående) noen e-postmeldinger hvis det finnes mistanke om at et virus kan være vedlagt.

- NEP tillater tilfeldig bruk av Internett, e-post og telefonsystemer for sending av privat e-post, surfing på Internett og private telefonsamtaler, underlagt visse betingelser som er fastsatt nedenfor. Privat bruk er et privilegium og ikke en rettighet. Det må hverken misbrukes eller brukes for mye og NEP forbeholder seg retten til å tekke tilbake tillatelsen når som helst. NEP forbeholder seg også retten til å begrense eller hindre tilgang til visse telefonnumre eller nettsteder hvis NEP anser det slik at den private bruken er urimelig stor. Følgende betingelser må oppfylles for at privat bruk skal kunne fortsette:
    - bruken må være minimal og i hovedsak skje utenom arbeidstiden;
    - bruken må ikke komme i veien for forretninger eller kontorforpliktelser; og
    - bruken må ikke forplikte NEP til noen grensekostnader.
- All e-post-trafikk relatert til forretningsaktiviteter må skje gjennom et godkjent bedriftssystem for e-post.

Kontaktopplysninger til kunder:

- Du må hverken la adressebøker i fast kopi eller andre dokumenter eller enheter som inneholder forretningskontakter ligge ubevoktet.
- Hvis du lagrer forretningskontakter elektronisk, må du lagre dem i et sikkert område på NEP-nettverket.

11. Rapportere mistenkte datasikkerhetsbrudd

Et datasikkerhetsbrudd kan skje i forbindelse med eller som en følge av en hvilken som helst av følgende hendelser (denne listen er ikke uttømmende):

- tyveri av data (inkludert fysiske kopier) eller utstyr (bærbare datamaskiner, mobiltelefoner, minnepinner, CD-ROM-er osv.) som det er lagret data på;
- uvitenhet hos brukeren/mangel på opplæring;
- uautorisert tilgang/kopiering;
- feil sikkerhetsklassifisering/markering/merking;
- usikker metode for overføring;
- bruk av ukontrollerte eller uautoriserte medium;
- tap, eller mulig tap, av medium, enheter eller utstyr;
- tap eller mulig tap av sikkerhetskopieringsmedier;
- upassende oppbevaring av informasjon;
- feiladressering/feilruting;

- feil metode for avhending av data eller media;
- hacking/oppsnapping;
- tyvlytting/spionasje;
- upassende offentliggjøring til allmennheten;
- tilgang av opprettholdere/entreprenører som det ikke føres tilsyn med;
- upassende tilgangskontroller som muliggjør uautorisert bruk av medlemmer eller ansatte eller andre; eller
- informasjon som er anskaffet ved å villede NEP.

Hvis du blir klar over et datasikkerhetsbrudd i forbindelse med personopplysninger (eller andre opplysninger) eller du har mistanke om at et slikt brudd har skjedd, må du umiddelbart rapportere dette til din datavernrepresentant og linjelederen din, som kan varsle den rettmessige datavernmyndigheten og personen som er berørt av datavernbruddet. Det er ditt ansvar å sørge for at rapporten mottas og at datavernrepresentanten og linjelederen din er klar over at den er blitt sendt (det er ikke sikkert det er tilstrekkelig å sende en e-post eller legge igjen en talepostmelding hvis du ikke kan være sikker på at mottakeren har mottatt meldingen – alltid sjekk).

Du bør prøve å oppgi så mye informasjon som mulig (inkludert, men ikke begrenset til, følgende informasjon):

- typen data som var involvert (om den var sensitiv eller ikke);
- når sikkerhetsbruddet skjedde;
- hvordan bruddet skjedde (f.eks. om data er mistet eller stjålet eller om det er mistanke om uautorisert tilgang);
- om dataene er skadet eller ødelagt, på hvilken måte de er skadet eller ødelagt;
- hvor mange personers personopplysninger som sannsynligvis vil berøres av bruddet;
- hvem personene er hvis data er mistet (dvs. er det ansatte, kunder, klienter eller leverandører);
- skritt som er tatt eller som vil tas for å hindre flere problemer, enten bruddet er gjentakende eller om ytterligere data er berørt; og
- eventuelle kjente kontraktsmessige forpliktelser gitt til tredjeparter angående sikkerheten til personopplysningene (f.eks. NEPs kunder).

Du bør deretter hjelpe dem med å stoppe eller redusere datasikkerhetsbruddet.

12. **Sørge for at personer vet hvordan NEP** vil bruke dataene deres

Under visse omstendigheter vil det kreves samtykke fra personer. NEP har standard personvernerklæringer- og klausuler som selskapet har innarbeidet i sine standardkontrakter for å sørge for at dette kravet oppfylles, og for å gi veiledning til de som trenger å vite når det må innhentes samtykke.

13. Sørg for at personopplysninger er nøyaktige og holdt oppdatert

Eventuelle unøyaktigheter i personopplysninger som oppbevares av NEP skal rettes av ansatte i alle relevante systemer. Eventuelle oppdateringer eller endringer til informasjon som er oppgitt av en person på noe tidspunkt skal også gjøres i NEPs oppføringer.

Datasubjekter må informeres om sin rett til tilgang, til å rette, slette eller begrense behandlingen av deres innsamlede personopplysninger.

14. Avhende personopplysninger på en sikker måte

Hvis du ikke lenger trenger personopplysninger, må du sørge for at de avhendes med aktsomhet og på en sikker måte.

Hvis noen ansatt mottar en forespørsel om informasjon som refererer til noen datavernlov, må du umiddelbart kontakte din datavernrepresentant for å sørge for at forespørselen tas hånd om på riktig måte innen de gitte tidsgrensene.

15. **Konsekvensutredninger**i forbindelse med personvern (Privacy impact assessment/PIA)

Hvis du oppretter en ny prosess, retningslinjer eller prosedyrer, går i gang med et nytt prosjekt eller kjøper nye systemer som kan involvere håndtering eller overføring av store mengder personopplysninger, eller som kan ha en vesentlig effekt på personvernet eller sikkerheten til personopplysninger som behandles av eller på vegne av NEP, bør du utføre en konsekvensutredning i forbindelse med personvern ("**PIA**"). Se NEPs PIA-retningslinjer. Dette kan også forekomme hvis du setter ut en spesiell funksjon eller tjeneste eller i sammenheng med en betydelig anskaffelse.

16. Opplæring

Du må delta på alle kurs angående beskyttelse og behandling av personopplysninger som NEP ber deg om å delta på. Dette kan omfatte eksterne kurs og nettbasert opplæring.

17. Ekstern veiledning fra din lokale datavernmyndighet

Det finnes en rekke nyttige veiledningsnotater på nettstedene til European Data Protection Board, Storbritannias ICO og andre datavernmyndigheter.

18. Datavern og disiplinærtiltak

Hvis noen person bryter (eller er mistenkt for å ha brutt) noe aspekt av disse retningslinjene, kan det tas passende disiplinærtiltak i samsvar med den relevante disiplinærprosedyren.

Avhengig av hvor alvorlig atferden er, kan disiplinærtiltak føre til oppsigelse uten varsel.

NEP forbeholder seg også retten til å ta andre tiltak mot en person utenom oppsigelse (inkludert å fjerne retten til autorisert tilgang til personopplysninger) som kan være passende, omstendighetene tatt i betraktning.

Hvis noen person har noen tvil om han eller hun behandler personopplysninger på en rettferdig og lovlig måte, skal de kontakte datavernteamet før de utfører noen behandling.

19. Overvåkning og gjennomgang av disse retningslinjene

Disse retningslinjene gjennomgås regelmessig. Du vil bli varslet om eventuelle betydelige endringer til retningslinjene via NEPs nettsted.

GODKJENNELSE

Godkjennelse for implementering av disse retningslinjene er gitt av:

_____ _____
Administrerende direktør Dato

_____ _____
Juridisk rådgiver og compliance-direktør Dato

_____ _____
Direktør personalavdeling/HR Dato

Revidert

Dato	**Revisjons-sammendrag** (begynn med seksjonsnummer/-tittel)
1. mai 2018	Retningslinjene er i kraft