Grønbyg Entreprise ApS

Virksomheds Rapport

Oprettet: 03.oktober 2018

Indholdsfortegnelse

Administration

Bogføring

Generelt

Formålet er at kunne imødekomme og påvise overholdelse af bogføringsloven.. Det vurderes derfor, at behandlingen er nødvendig for, at overholde en retlig forpligtelse, jf. artikel 6, stk. 1, litra c).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder bankoplysninger, CPR-nummer, kontaktoplysninger om kunder, ansatte, leverandører, debitorer, kreditorer, tidligere ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, samarbejdsparter, kunder, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes tidligst 5 år efter det regnskabsår, hvortil de er tilknyttet.

Videregivelse

Oplysningerne videregives til samarbejdspartnere, offentlige myndigheder, revisorer.

Databehandlere

Aktiviteten håndteres med ekstern bistand. Der er indgået datahandleraftaler med de eksterne parter

Fakturering

Generelt

Formålet er at kunne imødekomme og påvise overholdelse af bogføringsloven.. Det vurderes derfor, at behandlingen er nødvendig for, at overholde en retlig forpligtelse, jf. artikel 6, stk. 1, litra c).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger, bankoplysninger om kunder. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes tidligst 5 år efter det regnskabsår, hvortil de er tilknyttet.

Videregivelse

Oplysningerne videregives til revisorer, samarbejdspartnere, offentlige myndigheder.

Databehandlere

Aktiviteten håndteres med ekstern bistand. Dog uden der behandles personplysninger deri

Håndtering af databehandlere

Generelt

Formålet er at kunne imødekomme og påvise overholdelse af databeskyttelsesforordningen. Det vurderes derfor, at behandlingen er nødvendig for, at overholde en retlig forpligtelse, jf. artikel 6, stk. 1, litra c).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger om samarbejdsparter. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes senest 5 år efter samarbejdets ophør.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af de registreredes rettigheder

Generelt

Formålet er at kunne imødekomme og påvise overholdelse af databeskyttelsesforordningen. Det vurderes derfor, at behandlingen er nødvendig for, at overholde en retlig forpligtelse, jf. artikel 6, stk. 1, litra c).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder CPR-nummer, kontaktoplysninger, ansættelses- og lønforhold om registrerede generelt. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger, personoplysninger om fagforeningsmæssigt tilhørsforhold om, kreditorer, debitorer, ejere, ansøgere, pårørende til de øvrige registrerede , leverandører, klienter, kunder, samarbejdsparter, ansatte, tidligere ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter sagens afslutning.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af forpligtelser overfor tilsynsmyndigheder

Generelt

Formålet er at kunne imødekomme en myndigheds påbud. Det vurderes derfor, at behandlingen er nødvendig for, at overholde en retlig forpligtelse, jf. artikel 6, stk. 1, litra c).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder CPR-nummer, ansættelses- og lønforhold om registrerede generelt. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes tidligst 5 år efter det regnskabsår, hvortil de er tilknyttet.

Videregivelse

Oplysningerne videregives til offentlige myndigheder.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

IT-administration

Generelt

Formålet er at kunne opretholde den daglige drift. Det vurderes derfor, at behandlingen er nødvendig for at forfølge en legitim interesse, jf. artikel 6, stk. 1, litra f).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger, ansættelses- og lønforhold om ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Kvittering

Generelt

Formålet er at kunne imødekomme og påvise overholdelse af bogføringsloven.. Det vurderes derfor, at behandlingen er nødvendig for, at overholde en retlig forpligtelse, jf. artikel 6, stk. 1, litra c).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder bankoplysninger, kontaktoplysninger om kunder, debitorer, kreditorer, leverandører. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes tidligst 5 år efter det regnskabsår, hvortil de er tilknyttet.

Videregivelse

Oplysningerne videregives til samarbejdspartnere, revisorer, offentlige myndigheder.

Databehandlere

Aktiviteten håndteres med ekstern bistand. Dog uden der behandles personplysninger deri

Opretholdelse af databeskyttelsesforpligtelser

Generelt

Formålet er at kunne opretholde den daglige drift, beskytte forretningshemmeligheder og personoplysninger, samt at værne mod angreb. Det vurderes derfor, at behandlingen er nødvendig for, at overholde en retlig forpligtelse, jf. artikel 6, stk. 1, litra c).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger, ansættelses- og lønforhold om samarbejdsparter, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger, personoplysninger om fagforeningsmæssigt tilhørsforhold om, ansatte, kunder. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Revision

Generelt

Formålet er at kunne imødekomme og påvise overholdelse af selskabsloven.. Det vurderes derfor, at behandlingen er nødvendig for, at overholde en retlig forpligtelse, jf. artikel 6, stk. 1, litra c).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder lønoplysninger, CPR-nummer, ansættelses- og lønforhold, kontaktoplysninger, bankoplysninger om kunder, leverandører, debitorer, kreditorer, samarbejdsparter, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansatte, kunder, leverandører, samarbejdsparter, debitorer, kreditorer. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes tidligst 5 år efter det regnskabsår, hvortil de er tilknyttet.

Databehandlere

Aktiviteten håndteres med ekstern bistand. Der er indgået datahandleraftaler med de eksterne parter

Human Resources

Afslag på jobansøgninger

Generelt

Formålet er at oplyse ansøgerne om, at rekrutteringsrunden er afsluttet, og at en anden kandidat er blevet tilbudt stillingen. Det vurderes derfor, at behandlingen er nødvendig for at forfølge en legitim interesse, jf. artikel 6, stk. 1, litra f).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger om ansøgere. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes straks efter rekrutteringen er afsluttet.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Gennemførsel af arbejdspladsvurderinger

Generelt

Formålet er at efterleve og kunne påvise overholdelse af arbejdsmiljøloven. Det vurderes derfor, at behandlingen er nødvendig for at overholde en arbejdsretlige forpligtelser, som har hjemmel i medlemsstatens nationale ret, jf. artikel 9, stk. 2, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger, ansættelses- og lønforhold om ansatte. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes senest 3 år efter vurderingen er gennemført.

Videregivelse

Oplysningerne videregives til offentlige myndigheder.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af afskedigelsesbreve fra arbejdsgiver

Generelt

Formålet er at afslutte ansættelsesforløbet rettidigt og i overensstemmelse med ansættelseskontrakten. Det vurderes derfor, at behandlingen er nødvendig for at opfylde en kontrakt, som den registrerede er part i, jf. artikel 6, stk. 1, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder ansættelses- og lønforhold, kontaktoplysninger om ansatte. Oplysningerne er indsamlet fra de registrerede.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansatte. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af afvænningstilbud, psykologhjælp, massage o.l.

Generelt

Formålet er at sørge for at de ansatte har mulighed for at få hjælp og støtte i det omfang, der måtte være behov for det, for derigennem at sikre en sund, rask og produktiv arbejdsstyrke. Det vurderes derfor, at den registrerede har givet sit samtykke til behandlingen, jf. artikel 6, stk. 1, litra a).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger, CPR-nummer om klienter, patienter, pårørende til de øvrige registrerede. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, samarbejdsparter, læger, pårørende til de øvrige registrerede , ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Videregivelse

Oplysningerne videregives til forsikringsselskaber, offentlige myndigheder.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af arbejdsskadesager

Generelt

Formålet er at efterleve og kunne påvise overholdelse af sygedagpengeloven. Det vurderes derfor, at behandlingen er nødvendig for at overholde en arbejdsretlige forpligtelser, som har hjemmel i medlemsstatens nationale ret, jf. artikel 9, stk. 2, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder CPR-nummer, kontaktoplysninger, lønoplysninger, ansættelses- og lønforhold om ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Videregivelse

Oplysningerne videregives til forsikringsselskaber, offentlige myndigheder.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af barselssager

Generelt

Formålet er at efterleve og kunne påvise overholdelse af barselsloven og sygedagpengeloven. Det vurderes derfor, at behandlingen er nødvendig for at overholde en arbejdsretlige forpligtelser, som har hjemmel i medlemsstatens nationale ret, jf. artikel 9, stk. 2, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder ansættelses- og lønforhold, lønoplysninger, CPR-nummer, kontaktoplysninger om ansatte, pårørende til de øvrige registrerede. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, pårørende til de øvrige registrerede , ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Videregivelse

Oplysningerne videregives til offentlige myndigheder.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af deltagerlister til interne sociale arrangementer

Generelt

Formålet er at kunne administrere økonomien i forbindelse med afholdelse af eventet og løbende informere deltagerne. Det vurderes derfor, at behandlingen er nødvendig for at forfølge en legitim interesse, jf. artikel 6, stk. 1, litra f).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger om eventdeltagere, respondenter, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes dagen for afholdelse af arrangement.

Videregivelse

Oplysningerne videregives til samarbejdspartnere.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af jobansøgninger

Generelt

Formålet er at vurdere, hvorvidt ansøgerne er kvalificerede. Det vurderes derfor, at behandlingen er nødvendig af hensyn til foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt, jf. artikel 6, stk. 1, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder CPR-nummer, kontaktoplysninger, lønoplysninger, portrætbillede om ansøgere. Oplysningerne er indsamlet fra andre end de registrerede.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansøgere. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes senest 3 måneder efter rekrutteringsrunden er afsluttet.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af lønsedler

Generelt

Formålet er at overholde reglerne i kildeskatteloven og bogføringsloven. Det vurderes derfor, at behandlingen er nødvendig for at overholde en arbejdsretlige forpligtelser, som har hjemmel i medlemsstatens nationale ret, jf. artikel 9, stk. 2, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder bankoplysninger, ansættelses- og lønforhold, kontaktoplysninger, lønoplysninger om ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Videregivelse

Oplysningerne videregives til banker, offentlige myndigheder, revisorer, samarbejdspartnere.

Databehandlere

Aktiviteten håndteres med ekstern bistand. Der er indgået datahandleraftaler med de eksterne parter

Håndtering af opsigelsesvarsel fra ansat

Generelt

Formålet er at afslutte ansættelsesforløbet rettidigt og i overensstemmelse med ansættelseskontrakten. Det vurderes derfor, at behandlingen er nødvendig for at opfylde en kontrakt, som den registrerede er part i, jf. artikel 6, stk. 1, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder ansættelses- og lønforhold, kontaktoplysninger om ansatte. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af sundhedsforsikringer

Generelt

Formålet er at kunne tilbyde de ansatte arbejdspladsens sundhedsforsikring. Det vurderes derfor, at behandlingen er nødvendig for at forfølge en legitim interesse, jf. artikel 6, stk. 1, litra f).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder CPR-nummer, kontaktoplysninger, ansættelses- og lønforhold om ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Videregivelse

Oplysningerne videregives til samarbejdspartnere, offentlige myndigheder, forsikringsselskaber.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af sygedagpenge

Generelt

Formålet er at efterleve og kunne påvise overholdelse af sygedagpengeloven. Det vurderes derfor, at behandlingen er nødvendig for at overholde en arbejdsretlige forpligtelser, som har hjemmel i medlemsstatens nationale ret, jf. artikel 9, stk. 2, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder CPR-nummer, kontaktoplysninger om ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Videregivelse

Oplysningerne videregives til offentlige myndigheder.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af sygesamtaler

Generelt

Formålet er at efterleve og kunne påvise overholdelse af sygedagpengeloven. Det vurderes derfor, at behandlingen er nødvendig for at overholde en arbejdsretlige forpligtelser, som har hjemmel i medlemsstatens nationale ret, jf. artikel 9, stk. 2, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder ansættelses- og lønforhold, CPR-nummer, kontaktoplysninger om ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Håndtering af tilsynsmyndigheder

Generelt

Formålet er at kunne imødekomme et myndighedspåbud. Det vurderes derfor, at behandlingen er nødvendig for at forfølge en legitim interesse, jf. artikel 6, stk. 1, litra f).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger, CPR-nummer, ansættelses- og lønforhold om registrerede generelt, kunder, samarbejdsparter, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes 5 år.

Videregivelse

Oplysningerne videregives til offentlige myndigheder.

Databehandlere

Aktiviteten håndteres med ekstern bistand. Der er indgået datahandleraftaler med de eksterne parter

Indgåelse af ansættelseskontrakter

Generelt

Formålet er at opfylde kravene i ansættelsesbevisloven. Det vurderes derfor, at behandlingen er nødvendig for, at overholde en retlig forpligtelse, jf. artikel 6, stk. 1, litra c).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder bankoplysninger, ansættelses- og lønforhold, lønoplysninger, CPR-nummer, kontaktoplysninger om ansatte. Oplysningerne er indsamlet fra de registrerede.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansatte. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Indkaldelse til jobsamtaler

Generelt

Formålet er at vurdere, hvorvidt ansøgerne er kvalificerede. Det vurderes derfor, at behandlingen er nødvendig af hensyn til foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt, jf. artikel 6, stk. 1, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder ansættelsesforhold, lønoplysninger, kontaktoplysninger om ansøgere. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes straks efter rekrutteringen er afsluttet.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Logning af brug af IT på arbejdspladsen

Generelt

Formålet er at beskytte erhvervshemmeligheder i overensstemmelse med markedsføringsloven, samt generelt at beskytte virksomheden. Det vurderes derfor, at behandlingen er nødvendig for at forfølge en legitim interesse, jf. artikel 6, stk. 1, litra f).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger, browseroplysninger, IP-adresse om ansatte. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes senest 10 år efter ansættelsesforholdets ophør.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Logning af brug af IT uden for arbejdspladsen

Generelt

Formålet er at beskytte erhvervshemmeligheder i overensstemmelse med markedsføringsloven, samt generelt at beskytte virksomheden. Det vurderes derfor, at behandlingen er nødvendig for at forfølge en legitim interesse, jf. artikel 6, stk. 1, litra f).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger, browseroplysninger, IP-adresse om ansatte. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes senest 10 år efter ansættelsesforholdets ophør.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Oprettelse af personalesager

Generelt

Formålet er at have samling på alle relevante dokumenter og information om de enkelte ansatte. Det vurderes derfor, at behandlingen er nødvendig for at forfølge en legitim interesse, jf. artikel 6, stk. 1, litra f).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder CPR-nummer, kontaktoplysninger, ansættelses- og lønforhold om ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger, personoplysninger om fagforeningsmæssigt tilhørsforhold om, samarbejdsparter, tidligere ansatte, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Videregivelse

Oplysningerne videregives til samarbejdspartnere, advokater.

Databehandlere

Aktiviteten håndteres med ekstern bistand. Der er indgået datahandleraftaler med de eksterne parter

Tidsregistrering

Generelt

Formålet er at sikre opfyldelse af ansættelseskontrakten. Det vurderes derfor, at behandlingen er nødvendig for at opfylde en kontrakt, som den registrerede er part i, jf. artikel 6, stk. 1, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger, ansættelses- og lønforhold, CPR-nummer om ansatte. Oplysningerne er indsamlet fra de registrerede.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, ansatte. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes senest 5 år efter ansættelsesforholdets ophør.

Videregivelse

Oplysningerne videregives til offentlige myndigheder.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Kernevirksomhed

Afdelingen behandler ikke personhenførbar data

Public Relations

Drift af hjemmeside

Generelt

Formålet er at kunne markedsføre produkter, services og informere om nyheder og arrangementer til de registrerede, der besøger hjemmesiden. Det vurderes derfor, at den registrerede har givet sit samtykke til behandlingen, jf. artikel 6, stk. 1, litra a).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder oplysninger om forbrugsvaner, IP-adresse, browseroplysninger, kontaktoplysninger om kunder, ansatte. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes den besøgende er informeret om privatlivs- og cookiepolitik og informeret om at de selv skal slette samt oplysning om rettigheder.

Databehandlere

Aktiviteten håndteres med ekstern bistand. Dog uden der behandles personplysninger deri

Håndtering af sociale medier

Generelt

Formålet er at kunne markedsføre produkter, services og informere om nyheder og arrangementer til de registrerede på de sociale medier. Det vurderes derfor, at behandlingen er nødvendig for at opfylde en kontrakt, som den registrerede er part i, jf. artikel 6, stk. 1, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder købsvaner, oplysninger om forbrugsvaner, kontaktoplysninger om eksterne parter generelt, respondenter. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 10 år efter samtykkets afgivelse.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

Salg

Generelt

Formålet er at sælge ydelser.. Det vurderes derfor, at behandlingen er nødvendig for at opfylde en kontrakt, som den registrerede er part i, jf. artikel 6, stk. 1, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder kontaktoplysninger, bankoplysninger om kunder. Oplysningerne er indsamlet fra de registrerede.

Aktiviteten indebærer behandling af artikel 9-oplysninger, herunder helbredsoplysninger om, kunder. Oplysningerne er indsamlet fra de registrerede.

Oplysningerne slettes 5 år efter fakturering.

Databehandlere

Alle dele af aktiviteten håndteres internt, uden bistand fra eksterne.

SEO

Generelt

Formålet er at optimere søgeresultaterne i søgemaskiner. Det vurderes derfor, at behandlingen er nødvendig for at opfylde en kontrakt, som den registrerede er part i, jf. artikel 6, stk. 1, litra b).

Aktiviteten indebærer behandling af artikel 6-oplysninger, herunder browseroplysninger, kontaktoplysninger, IP-adresse om klienter, kunder, samarbejdsparter, leverandører, eksterne parter generelt. Oplysningerne er indsamlet fra både de registrerede og andre.

Oplysningerne slettes senest 3 år efter samtykkets afgivelse.

Databehandlere

Aktiviteten håndteres med ekstern bistand. Dog uden der behandles personplysninger deri

Udvikling

Afdelingen behandler ikke personhenførbar data

Databehandler fortegnelser

Databehandleraftale

Dataansvarlig	**Databehandler**	**Kontrakt Uploadet**
Grønbyg Entreprise ApS Vestre Gade 6H 2605 Brøndby Danmark 34612269	LD Regnskab Kringholmen 19A 2730 Herlev Danmark 39105837	Nej: Der er ikke uploadet en kontrakt
Grønbyg Entreprise ApS Vestre Gade 6 H 2605 Brøndby Danmark 34612269	RA Entreprise A/S Stubberupvej 6 4140 Borup Danmark 32836194	Nej: Der er ikke uploadet en kontrakt

Databeskyttelsespolitikker

Databeskyttelsespolitikker

Politik	Status	Point
Har I en opgørelse over hvilke enheder, der er autoriseret til anvendelse i firmaet?	**Under udarbejdelse**	**25/55**
Har I en opgørelse over hvilken software, der er autoriseret til anvendelse i firmaet?	**Nej**	**0/40**
Har I en politik for konfigurering af hardware og software på mobile enheder, bærbare computere, arbejdsstationer og servere?	**Nej**	**0/70**
Har I en politik for løbende sårbarhedsvurdering og -håndtering?	**Nej**	**0/25**
Har I en opgørelse over hvem, der har administrative rettigheder til hardware, software og netværk?	**Nej**	**0/50**
Har I en politik for vedligeholdelse, gennemgang og analyse af audit logs?	**Nej**	**0/35**
Har I en politik for e-mail og webbrowser-beskyttelse?	**Nej**	**0/60**
Har I en politik for malware-beskyttelse?	**Nej**	**0/35**
Har I en politik for begrænsning af og kontrol med netværksporte, protokoller og services?	**Nej**	**0/30**
Har I en politik for backup?	**Nej**	**0/40**
Har I en politik for konfiguration af netværksenheder, såsom firewalls, routere og switche?	**Nej**	**0/30**
Har I en politik for beskyttelse af netværksgrænseflader?	**Nej**	**0/30**
Har I en politik for kryptering af data, der opbevares og sendes?	**Nej**	**0/50**
Har I en politik for adgangsstyring baseret på et need to know princip?	**Nej**	**0/30**
Har I en politik for adgangsstyring på det trådløse netværk?	**Nej**	**0/25**
Har I en politik for overvågning og kontrol af brugerkonti?	**Nej**	**0/50**
Har I en politik for metoder til vurdering af, og passende træning til forbedring af, medarbejdernes sikkerhedsfærdigheder?	**Nej**	**0/25**
Har I en politik for håndtering af sikkerhedsniveauet i egenudviklede applikationer?	**Nej**	**0/30**
Har I en politik for hændelseshåndtering?	**Nej**	**0/25**
Har I en politik for penetrationstest?	**Nej**	**0/15**

Enhedspolitik

Internet Hackere/Angribere, befinder sig overalt i verden, de kan uanset hvor de er fra kontinuerligt scanne et IP adresserum for de firmaer/organisationer de ønsker tilgang til. Ofte venter de på, at nye og ubeskyttede systemer bliver knyttet til netværket, for så at benytte disse til at komme videre ind i organisationen..
Angriberne kigger også efter enheder (især bærbare computere), som kommer og går fra virksomhedens netværk, og derfor kommer de ud af synkroniseringen omkring patches og sikkerhedsopdateringer.
En angriber kan udnytte hardware, der er installeret på netværket, men som ikke endnu er konfigureret og patched med passende sikkerhedsopdateringer. Selv enheder, der ikke er synlige fra internettet, kan bruges af angribere, der allerede har fået intern adgang og søger efter interne IP adresser eller eksisterende kompromitterede ofre.
Der skal også tænkes på midlertidige systemer, der er på virksomhedens netværk (f.eks. Demonstrationssystemer, midlertidige testsystemer, gæstetjenester) disse bør også forvaltes omhyggeligt og være isoleret for at forhindre adgang udefra.
I forbindelse med at BYOD (medbring din egen enhed) - hvor medarbejdere bringer personlige computere/enheder til arbejde og forbinder dem med virksomhedsnetværket - bliver mere og mere almindeligt kan disse enheder allerede være kompromitteret og bruges til at inficere interne ressourcer.

Der kan med fordel implementeres et automatiseret værktøj der kan finde og identificerer de IT Devices der via IPv4 eller IPv6 er forbundet til netværket.
Hvis organisationen tildeler IP adresser ved hjælp af DHCP, skal du aktivere serverloggning af den dynamiske hostkonfiguration (DHCP), check loggen for de registrerede men ukendte systemer.

Implementér netværksniveauautentificering via 802.1x for at begrænse og styre, hvilke enheder der kan sluttes til netværket.
Benyt klientcertifikater til at validere og godkende IT Devices/Systemer forud for tilslutning til virksomhedens private netværk.

Har du en oversigt over det hardware i organisationen, der tilgår dit netværk?

Svaret: Nej

Såfremt i har en oversigt over alle enheder der kan tilgå jeres netværk kan i bedre finde de enheder der ikke skal have adgang til netværket.
En generel god ide er at påtrykke jeres Devices et prefix, således kan jeres computere alle starte med samme 3 bogstavs koder – således kan der oprettes en DHCP regel der kun uddeler IP Adresser til disse klienter/Devices/servere etc.

Mindre virksomhed:
Sørg for at der på DHCP Serveren bliver tastet en MAC adresse ind for de devices der skal tilgå jeres netværk.
Etabler regler der sikre at jeres devices skal have modtaget en IP-adresse fra DHCP serveren for at kommunikerer med Active Directory.

Mellem Virksomhed
Såfremt i benytter Microsoft Windows servere, kan i ved hjælp af DHCP, NAP og NPS kontrollerer hvilke enheder der modtager en IP Adresse og derved kommunikerer mod Active directory.
Sæt et ejernavn evt en rolle på virksomhedens netværksudstyr og computer, denne person kan aktivt kan håndterer og opdateret enheder.

Større virksomhed:
Såfremt i benytter Microsoft Windows servere, kan i ved hjælp af DHCP, NAP og NPS kontrollerer hvilke enheder der modtager en IP Adresse og derved kommunikerer mod Active Directory. Benyt VLAN funktionalitet for at dirigerer og/eller isolerer enheder der har påtrykt en manuel IP Adresse.
Der kan implementeres en NPS server der via certifikater ligeledes kan hjælpe med at højne sikkerheden på netværket.

Bliver firmaets data gemt andre steder end på firmaets computere og servere?

Svaret: Ja

Det kan være svært at sikre firmaets data forbliver indenfor firmaets IT sikkerheds rammer. Det vil altid være at foretrække at firmaet har fuldstændig kontrol over hvor egne data befinder sig. Ud over at lovgivningen foreskriver at firmaet skal have styr på de personhenførbare data, er det også set ud fra firmaets omdømme et internt krav at sikre data ikke ”flyder” rundt uden kontrol.

Etabler et sikkert område hvor data gemmes, dette kan være et drev i skyen, eller et lokalt drev der deles via VPN. Vær sikker på at ingen ud over administratoren har rettigheder til at ændre rettigheder for andre.
Sørg for at de drev/devices der benyttes til at håndterer data er krypteret – USB drev, laptops, telefoner kan nemt krypteres.

Benytter du netværksservices så som DNS og DHCP internt?

Svaret: Nej

Det anbefales at der benyttes netværksservices til at kontrollere og styre kommunikationen på netværket. Såfremt der ikke benyttes netværks services som DNS og DHCP, hvortil der kan aktiveres logning kan det være meget svært at finde spor efter hacking eller at der har været ubudne gæster.

Har du etableret logning på disse?

Svaret: Nej

Såfremt der ikke er aktiveret logning på hverken DNS og DHCP, bør der aktiveres logning på den server der uddeler IP-adresser, endvidere vil logning på DNS muliggøre at der kan findes mistænkelig adfærd tilbage i tiden.
Aktiver DNS Analytical Services samt aktiver Log på klienter – under DNS Client Events og Microsoft-Windows-Dhcp-Client/Operational.

Har du isoleret dine netværk, således at kun firmaets ansatte kan komme på det interne netværk?

Svaret: Ja

Det tilstræbes at benytte sikre isolerede fysiske eller logiske netværk. Sørg for at i har en basis logning der kan forbinde en IP-adresse med en MAC adresse og evt med navn på udstyr og evt bruger navn.

Har dine gæster mulighed for at komme på et midlertidigt Wi-Fi?

Svaret: Nej

Det kan overvejes at etablerer en WIFI Router med et sim kort fra en teleudbyder der kan benyttes til at lade gæster få Internet adgang.

Giver midlertidig adgang til Wi-Fi adgang til interne systemer?

Svaret: Nej

Lad altid gæster der forbinder via Wifi være isoleret ift de interne systemer.

Benytter du automatisk opdatering af klientmaskiner- og servere?

Svaret: Ja

Sørg for at Jeres netværks udstyr bliver opdateret ligesom Jeres Computere. Lav en manuel stikprøve en gang i måneden hvor i checker en given Computer for at se opdateringsstatus.

Såfremt i benytter BYOD/Adgang fra telefoner skal i sikre at disse ligeledes er opdateret.
Hold øje med andet software end det fra Microsoft – er det ligeledes opdateret.

Benytter du automatisk opdatering af hardwareudstyr?

Svaret: Nej

De fleste nyere HW Devices kan sættes til automatisk opdatering direkte fra HW udbyderen. Endvidere kan i sætte automatisk genstart til. Sørg for at der checkes mindst en gang om ugen samt at udstyret genstartes en gang ugenligt.

Er der mulighed for at dine medarbejdere kan benytte egne maskiner hjemmefra?

Svaret: Nej

Såfremt der er medarbejdere der ønsker adgang udefra med eget IT udstyr skal i tilsikre at disse ikke kommer direkte ind i interne systemer. Sørg for at de tilkobles via VPN og endvidere kommer på et isoleret del af netværket der skal betragtes som en DMZ. Her kan man på den interne Firewall specificerer om der skal tilgåes Mail, CRM, ERP etc.

Kan man benytte egen maskine i virksomhedens IT netværk, skal firmaet sikre at maskinen er opdateret, har Personlig Firewall aktiveret, Kører Defender etc. Der kan etableres en DHCP Policy hvor virksomheden specificerer de minimums sikkerheds regler der skal være aktive for at kunne få tildelt en IP adresse.

Er der i denne forbindelse taget højde for status på medarbejderes egne maskiner?

Svaret: Nej

Sørg for at i kan indsamle informationer omkring hvilke maskiner der blev tilsluttet hvornår således at i altid kan gå tilbage i tiden og kontrollerer aktiviteten. Opret en politik for minimums krav til at få en IP-adresse via DHCP. Download evt SCM fra Microsoft for at etablere en minimums baseline for jeres sikkerhed. Det er muligt via SCM at tildele sikkerheds indstillinger til ikke Domain Computere.

Er der etableret sikkerhed for at en hvilken som helst maskine ikke kan tilsluttes netværksstik i væggen, evt ved hjælp af sikkerhedscertifikater?

Svaret: Ja

Sørg for at der er etableret VLANs således at ikke autoriserede maskiner bliver routet ud på et isoleret netværk. Der finden en række sikkerheds muligheder afhængig af hvilken type netværksudstyr der er investeret i således at i kan sikre at ikke autoriserede Devices ikke får adgang til virksomhedes LAN.

Benytter i VPN til at tilgå firmaets data hjemmefra/udefra?

Svaret: Nej

Såfremt der tilgås virksomheden data via et RDP værktøj, etabler da hellere en VPN løsning som kan benyttes som grundlag for RDP, Netop, TeamViewer, VNC, PC Anywhere, GotMyPC etc.

Softwarepolitik

Internet Angribere scanner løbende firmaer/organisationer på udkig efter sårbare versioner af software, der kan udnyttes udefra. Nogle angribere distribuerer ligeledes fjendtlige websider, dokumentfiler, mediefiler og andet indhold via deres egne websider eller umiddelbare troværdige tredjepartswebsteder.
Såfremt en sårbar browser tilgår disse websteder, er det muligt at kompromittere PC'ere/computere, og der kan herved installeres bagdørsprogrammer eller robotter, der giver angriberen kontrol over systemet.
Nogle sofistikerede angribere kan bruge Zero-day-exploits, der udnytter tidligere ukendte sårbarheder, for hvilke der ikke er blevet udgivet nogen sikkerhedsopdatering fra softwareleverandøren.
Uden ordentlig viden eller kontrol over den software, der implementeres i en organisation, kan firmaerne ikke sikre deres netværk og applikationer korrekt.

Er en PC'ere blevet kompromitteret kan den anvendes som et startpunkt for adgang til hele netværket og evt servere eller tilknyttede organisationer. På denne måde kan angriberne hurtigt benytte en kompromitteret maskine til at kompromittere flere.
En central styring af Software på servere og klienter vil også sikre en korrekt backup, opdatering og vedligeholdelse af virksomhedens software. Endvidere er det set fra en økonomisk vinkel fordelagtigt at vide hvilke licenser virksomheden har.

Konfigurationspolitik – Hardware og software

Som standard leveret af producenter og forhandlere, er konfigurationerne af operativsystemer og applikationer normalt gearet til brugervenlighed og brugervenlighed - ikke sikkerhed. Grundlæggende kontroller, åbne tjenester og porte, standardkonti eller adgangskoder, ældre (sårbare) protokoller, forudinstallation af unødvendig software; kan måske udnyttes i deres default tilstand.
Udvikling af konfigurationsindstillinger med gode sikkerhedsegenskaber er en kompleks opgave ud over individuelle brugeres evne, der kræver analyse af potentielt hundredvis eller tusindvis af muligheder for at træffe gode valg. Selvom en stærk indledende konfiguration er udviklet og implementeret, skal der løbende kontrolleres og styres for at undgå sikkerheds"forfald", da software opdateres eller patches, nye sikkerhedsproblemer rapporteres, og konfigurationerne er "tweaked" for at tillade installation af ny software eller support nye operationelle krav. Hvis ikke, vil angriberne finde muligheder at udnytte både netværkstilgængelige tjenester og klientsoftware på.

Sårbarhedspolitik

Cyber-forsvarere skal operere i en konstant strøm af nye oplysninger: softwareopdateringer, patches, sikkerhedsrådgivning, trusselspil osv. Forståelse og håndtering af sårbarheder er blevet en kontinuerlig aktivitet, der kræver betydelig tid, opmærksomhed og ressourcer. Angribere har adgang til de samme oplysninger og kan udnytte huller mellem udsendelse af ny viden og afhjælpning. For eksempel, når forskere rapporterer om nye sårbarheder, starter et kapløb mellem angribere og forsvarere (for at vurdere risiko, regressionsteste patches, installere/opdatere).
Organisationer, der ikke scanner efter sårbarheder og proaktivt adresserer opdagede fejl, står over for en betydelig sandsynlighed for at få deres computersystemer kompromitteret. Forsvarere står over for særlige udfordringer i forbindelse med håndtering af dette på tværs af hele virksomheden og prioritere handlinger med modstridende effekter samt nogle gange usikre følgevirkninger.

Administratorpolitik

Misbrug af administrative privilegier er en primær metode for angribere til at sprede sig inden for en målvirksomhed. To meget almindelige angriberteknikker udnytter ukontrollerede administrative rettigheder. I den første lokkes en arbejdsstationsbruger, der kører som en privilegeret bruger, til at åbne en ondsindet email vedhæftning, downloade og åbne en fil fra et ondsindet websted eller blot surfe på et websted, der besidder angriberens indhold, der automatisk kan udnytte browsere. Filen eller udnyttelsen indeholder eksekverbar kode, der enten afvikles på offerets maskine automatisk eller ved at narre brugeren til at udføre angriberens indhold. Hvis offerets brugerkonto har administrative rettigheder, kan angriberen overtage offerets maskine fuldstændigt og installere keyloggere, sniffere og fjernbetjeningssoftware for at finde administrative adgangskoder og andre følsomme data. Lignende angreb sker med e-mail. En administrator åbner utilsigtet en e-mail, der indeholder en inficeret vedhæftning, og dette bruges til at opnå et pivot-punkt i netværket, der bruges til at angribe andre systemer.
Den anden almindelige teknik, som angriberne bruger, er forhøjelse af privilegier ved at gætte eller knække et kodeord for en administrativ bruger for at få adgang til en målmaskine. Hvis administrative rettigheder er løst og bredt fordelt, eller identiske adgangskoder benyttes flere steder, har angriberen meget lettere ved at få fuld kontrol over systemer, fordi der er mange flere konti, der kan fungere som veje for, at angriberen kan kompromittere administrative rettigheder.

Logningspolitik

Mangler i sikkerhedslogging og analyse gør det muligt for angriberne at skjule deres placering, ondsindet software og aktiviteter på ofrenes maskiner. Selv hvis ofrene ved, at deres systemer er blevet kompromitteret, er de er blinde for detaljerne i angrebet og efterfølgende handlinger taget af angriberne uden beskyttede og fuldstændige logbogsposter. Uden solide audit logs, kan et angreb gå ubemærket hen og de skader der forvoldes kan være irreversible. Nogle gange er log optegnelser det eneste bevis for et angreb.
Mange organisationer opbevarer revisionsjournaler med henblik på overholdelse, men angriberne er afhængige af, at sådanne organisationer sjældent ser på revisionslogbøgerne, så de ikke ved, at deres systemer er blevet kompromitteret. På grund af dårlige eller ikke-eksisterende loganalyseprocesser styrer angriberne nogle gange offermaskine i måneder eller år uden at nogen i målorganisationen ved det, selv om beviset for angrebet er blevet registreret i (ikke-undersøgte) logfiler.

Indrapporteringer

Bilag