IT- og informationssikkerheds-politik (GDPR)

For

Kontrapunkt Group

Versionshistorik

Version	Beskrivelse	Dato	Udarbejdet af
V. 0.1	Initiel draft	26 Oktober 2018	Kontrapunkt Group
V.0.2	1. Edition	13. November 2018	Kontrapunkt Group
V.0.3			
V.0.4			

Indholdsfortegnelse

IT- og informationssikkerhedspolitik for Kontrapunkt Group

Indledning

Kontrapunkt Group har en væsentlig rolle ved at tilbyde branding og identitetsservices. Kontrapunkt Group indsamler, behandler og opbevarer således en lang række informationer, hvorfor det er afgørende for såvel Kontrapunkt Groups omdømme som troværdighed, at disse beskyttes tilstrækkeligt.

For Kontrapunkt Group er det derfor vigtigt at sikre:

- Fortrolighed - en fortrolig behandling, herunder transmission og opbevaring af informationer, hvor kun autoriserede interne og eksterne brugere har adgang, og hvor brugernes adgang er begrænset til det nødvendige
- Integritet - en pålidelig og korrekt funktionalitet i vores IT-systemer, som minimerer risiko for ukorrekte informationer som følge af interne eller eksterne forhold
- Tilgængelighed - IT-systemernes tilgængelighed og kapacitet skal afspejle vores og kundernes behov for velfungerende IT-systemer og adgang til informationer.

Kontrapunkt Groups ledelse har derfor vedtaget denne IT- og informationssikkerhedspolitik (herefter "IT-sikkerhedspolitik"). IT-sikkerhedspolitikken udgør det samlede ledelsesgodkendte grundlag for IT-sikkerhedsarbejdet i Kontrapunkt Group.

IT-sikkerhed defineres i det følgende som værende alle sikringsforanstaltninger, der har til formål at beskytte elektroniske data, informationer og IT-relaterede aktiver, som Kontrapunkt Group anvender.

Formål
Formålet med denne IT-sikkerhedspolitik er, at:

- fastlægge de overordnede rammer for IT-sikkerheden under hensyn til Kontrapunkt Groups risikobillede
- beskrive en klar ansvarsfordeling og hensigtsmæssig styring og kontrol af IT-sikkerheden
- sikre, at Kontrapunkt Group-, forretningskritiske- og personhenførbare data indsamles, anvendes og opbevares i overensstemmelse med gældende lovgivning.

Opbygning
IT-sikkerhedsarbejdet er i Kontrapunkt Group opdelt i følgende kerneområder:

- *IT-sikkerhedspolitikken* beskriver de overordnede rammer for IT-politikken i Kontrapunkt Group.

- *IT-forretningsgange og procedurer* er de konkrete anvisninger, der skal følges af medarbejderne i det daglige arbejde, eksempelvis godkendelses-flow.
- *Drifts- og outsourcings retningslinjer* beskriver de detaljerede regler og kontroller, eksempelvis minimum sikkerhedskrav for opsætning af systemparametre. Dette vil være gældende i forhold til intern drift såvel som drift, der varetages af eksterne parter.

Risikostyring
For at kunne fokusere indsatsen af IT-sikkerhedsarbejdet hos Kontrapunkt Group, arbejdes der efter en struktureret tilgang til risikostyring. Resultatet af risikostyringen, herunder vurdering af risici, skal periodisk rapporteres til Kontrapunkt Groups ledelse.

Bestyrelsen orienteres straks om væsentlige afvigelser i det aktuelle trusselsbillede og den tilpasning, som dette afleder i forhold til indsatsområderne og kontrollerne. Almindelige afvigelser opsamles og rapporteres periodisk af direktionen.

Afvigelser
Som udgangspunkt skal IT-sikkerhedspolitikken, regelsættet og retningslinjerne altid efterleves. Situationer kan dog opstå, hvor særlige omstændigheder kræver en afvigelse fra de gældende sikkerhedsregler. En sådan afvigelse beror på en konkret vurdering og kræver en specifik dispensation. Dispensation skal godkendes af Kontrapunkt Groups direktion og skal være begrundet og understøttet af en risikovurdering. Dispensation er altid begrænset ift. en specifik begivenhed og periode.

Revision og opfølgning
Det er den IT-sikkerhedsansvarliges opgave at sikre, at der mindst en gang årligt, med afsæt i risikobilledet, foretages en systematisk gennemgang og vurdering af, om IT-sikkerhedspolitikken skal opdateres. Den IT-sikkerhedsansvarlige skal om nødvendigt opdatere IT-sikkerhedspolitikken og underliggende retningslinjer og procedurer.

Publikation
IT-sikkerhedspolitikken er tilgængelig for alle ansatte i Kontrapunkt Group via intranettet. Retningslinjer og procedurer er tilgængelig for de medarbejdere og IT-underleverandører, som har et arbejdsbetinget behov herfor.

Persondatabeskyttelse

Persondatapolitik
Kontrapunkt Group behandler vores kunders og medarbejderes personoplysninger i henhold til denne datapolitik.

Den registreredes rettigheder
Kontrapunkt Group respekterer fuldt ud den registreredes ret og ønske om hemmeligholdelse af personlige oplysninger, som udleveres /indsamles ifm. Kontrapunkt Groups arbejde og behandling. Vi er opmærksomme på behovet for beskyttelse og forsvarlig behandling af alle personlige oplysninger, som vi får udleveret/indsamler.

Personoplysninger dækker over alle oplysninger, der kan bruges til at identificere en person, herunder, men ikke begrænset til, vedkommendes for- og efternavn, alder, køn, privatadresse eller anden fysisk adresse, e-mailadresse eller andre kontaktoplysninger, lønoplysninger, evt. helbredsoplysninger, mv.

Kontrapunkt Group behandler vores kunders og medarbejderes information i forbindelse med arbejdet og vi vil slette alle udleverede oplysninger udover kontaktoplysning som navn, telefon og e-mail. Disse oplysninger gemmes i 6 måneder eller så længe som vores forpligtigelser / samarbejde er gældende.

Det er kun Kontrapunkt Groups medarbejdere, eller samarbejdspartnere, som specifikt er tilknyttet en specifik opgaver, der får adgang til personoplysninger og kun i det omfang det er nødvendigt for at kunne løse de arbejdsopgaver som vi har aftalt eller på anden vis er forpligtiget til.

Dokumentation af persondatabehandling
Da vi i Kontrapunkt Group skal kunne dokumentere vores behandling af persondata, så er det vigtigt at vi til enhver tid følger de arbejdsgange og procedurer, der beskriver vores behandling af persondata. Ligeledes må persondatabehandling kun foretages i de it-systemer, der er godkendt hertil.

Risikoanalyse og krav til sikkerhed
Såfremt vi som led i vores arbejde indfører nye arbejdsgange eller it-systemer, der potentielt kan behandle persondata, så skal vi gennemføre og dokumentere en risikoanalyse. Denne risikoanalyse skal tydeligt vise hvilken potentiel konsekvens den pågældende behandling kan have på den registrerede.

Såfremt en risikovurdering påviser en forhøjet risiko for den registrerede, så skal der implementeres kontroller, der medvirker til at nedbringe risikoen til et acceptabelt niveau.

Sikkerhedsbrud
Vi skal rapportere sikkerhedsbrud uden forsinkelse til tilsynsmyndigheder, indenfor maksimalt 72 timer. Såfremt et sikkerhedsbrud kan have konsekvens for den registrerede, så skal vi ligeledes underrette denne indenfor samme tidsfrist.

Udveksling af persondata
Vi videregiver kun oplysninger til Myndigheder som vi er forpligtet til ift. lovgivningen fx cpr. og lønoplysninger.

IT-sikkerhedskrav

Der er fastlagt en række overordnede krav til IT-sikkerheden, der skal medvirke til, at der er et grundlag for at kunne opretholde det forventede sikkerhedsniveau. Sikkerhedsniveauet sikres ved, at:

- der er en ledelsesmæssig forankring af IT-sikkerhed
- det er præcist fastlagt, hvordan Kontrapunkt Group lever op til alle lovgivnings- og myndighedskrav
- der er placeret et entydig ansvar i organisationen for alle områder omfattet af IT-sikkerhedspolitikken, og der gennemføres løbende oplysningsaktiviteter
- alle medarbejdere er instrueret i de dele af IT-sikkerhedspolitikken, IT-forretningsgange, procedurer mv., som er relevante for deres arbejdsområde
- grænseflader og ansvarsfordeling med driftsleverandører er fastlagte
- eksterne parter er bekendt med og forpligter sig til at efterleve de til enhver tid gældende IT-sikkerhedspolitikker, forretningsgange, regler og retningslinjer i samarbejdet med Kontrapunkt Group
- der udføres løbende kontrol med væsentlige IT-underleverandører om overholdelse af de krav, som Kontrapunkt Group har opstillet, ligesom der løbende foretages en vurdering af disses kompetencer til at kunne varetage den konkrete opgave.

Arbejde med en risikostyringsmodel

For at sikre Kontrapunkt Group mod negative konsekvenser ved IT-trusler skal IT-sikkerhedsarbejdet tage afsæt i en risikovurdering af de trusler, som Kontrapunkt Group har identificeret, ved at:

- der foregår en struktureret indsamling og vurdering af potentielle trusler. Disse skal analyseres periodisk, og der skal løbende tages stilling til, hvordan disse risici og trusler imødegås.
- driftsleverandører har en primær rolle i at udarbejde risikovurderinger ift. udviklingsprojekter og drift, som de har ansvaret for. Leverandører har dermed ansvar for at indsamle og reagere på ændrede risici og nye sikkerhedshændelser, og kommunikere dette til Kontrapunkt Group.
- Kontrapunkt Group skal stille krav til samarbejdspartnere og leverandører om, at der er udarbejdet og dokumenteret IT-beredskabsplaner, og at disse er testet i samarbejde med Kontrapunkt Group. Tests skal godkendes af Kontrapunkt Groups IT-sikkerhedsansvarlig
- der er etableret beredskabsplaner, der indeholder forholdsregler for at kunne genskabe forretningssystemerne. Disse forholdsregler gælder også for brud på fortrolighed og brud på integritet.

Beskyttelse af informationer og aktiver
Kontrapunkt Group skal fremstå som en pålidelig organisation, der sikrer, at IT-services er tilgængelige, og at informationer er beskyttet. Det sikres ved, at:

- nye indkøb af betydning for informationssikkerheden er baseret på forretningsbetingede behov og underlagt en indledende risikovurdering.
- udvikling og ændring af IT-systemer sker efter en dokumenteret proces, hvor Kontrapunkt Groups behov og krav beskrives. Processen skal sikre driftsstabilitet, sporbarhed og testbarhed af systemet. Derudover skal processen sikre udarbejdelse af system-, drifts- og brugerdokumentation.
- alle personfølsomme, forretningskritiske og fortrolige informationer, der IT-behandles, er identificeret og bliver behandlet lovgivnings-, forretningsmæssigt og etisk korrekt. Informationerne er vurderet i en livscyklus fra registrering, behandling og opbevaring til bortskaffelse.
- der er en systemejer, som sikrer, at systemer er specificerede, bliver testet og implementeret, samt at der er implementeret kontroller, der modsvarer risikobilledet.
- IT-miljøet sikres mod uønskede hændelser som fysisk skade, driftsforstyrrelser, tab, uautoriserede ændringer og anvendelse.
- der ikke opnås uautoriserede adgang til IT-miljøet, og at der opretholdes betryggende funktionsadskillelse.

Rolle- og ansvarsfordeling

For at sikre en funktionsadskillelse og forankringer af ansvar omkring IT-sikkerheden i Kontrapunkt Group er de primære roller og ansvar for informationssikkerheden beskrevet herunder:

Direktionens ansvar
Direktionen sikrer, at IT-sikkerhedspolitikken efterleves. Direktionen har i den sammenhæng ansvaret for at:

- der stilles de fornødne rammer og ressourcer til rådighed for at opnå det ønskede IT-sikkerhedsniveau
- det sikres, at en relevant IT-sikkerhedspolitik er implementeret
- der drages nødvendige konsekvenser ved væsentlige sikkerhedsbrud.
- sikre, at IT-sikkerhedspolitikken overholdes og er tilstrækkeligt implementeret igennem forretningsgange, procedurer og retningslinjer
- skabe fælles organisatorisk forståelse for, at IT-sikkerhed er et fælles ansvar, og at retningslinjer, forretningsgang mv. gælder for alle parter internt som eksternt
- sikre, at roller og ansvar er beskrevet og tildelt både internt i Kontrapunkt Group og over for samarbejdspartnere og leverandører
- iværksætte IT-sikkerhedsinitiativer

- godkende og prioritere alle forretningskritiske IT-systemer i en beredskabssituation
- udarbejde afvigelsesrapporter til bestyrelsen.

IT-sikkerhedsansvarlig
Den IT-sikkerhedsansvarlig har det daglige og operationelle ansvar for IT-sikkerheden, herunder:

- det kontinuerlige arbejde med og videreudvikling af IT-sikkerhedsniveauet hos Kontrapunkt Group, så det er i overensstemmelse med kravene i IT-sikkerhedspolitikken. Dette omfatter alle tilhørende forretningsgange og retningslinjer samt overensstemmelse med gældende lovgivning, herunder bekendtgørelser og vejledninger på området.
- at sikre at leverandører efterlever de stillede krav i outsourcing-aftaler, herunder at aftalegrundlag med leverandører er i overensstemmelse med IT-sikkerhedspolitikken for så vidt angår kontrol, opfølgning og rapportering
- løbende at monitorere og rapportere på eventuelle IT-sikkerhedsmæssige hændelser i overensstemmelse med denne IT-sikkerhedspolitiks fastsatte regelsæt.
- at iværksætte egne undersøgelser eller tests i det omfang, der vurderes behov herfor.
- varetagelse af en overordnet IT-sikkerhedskoordinator rolle.
- at fungere som kontaktperson til den eksterne revision i forbindelse med IT-revision.

Forretningsejer, systemejer og dataejer

I Kontrapunkt Group er der tre centrale roller i relation til IT-anvendelsen.

Forretningsejer: Forretningsejer er forretningens repræsentant mod IT, og er ansvarlig for at forretningen og IT er afstemt.

Systemejer: Varetager driften og udviklingen af systemet, herunder godkender niveau for sikkerhedsmæssig overvågning, niveau for logning af sikkerhedsrelevante områder samt niveau for backup ift. forretningens krav.

Dataejer: Har ansvaret for, at behandling af data i systemet behandles sikkerhedsmæssigt forsvarligt, herunder at der er udarbejdet risikovurdering og klassifikation. Dataejer er også ansvarlig for at fastlægge rammerne for adgangstildeling, som IT-driftsleverandøren eller systemadministratoren varetager/udfører.

Medarbejderne
Medarbejderne er den vigtigste udviklings- og driftsressource for Kontrapunkt Group og dermed også den største individuelle trussel for informationssikkerheden. Fokus på efterlevelse af IT-sikkerhedspolitikken og

udarbejdelse af medarbejderinstrukser for de enkelte områder er derfor afgørende for sikkerhedsniveauet i Kontrapunkt Group.

Enhver medarbejder i Kontrapunkt Group har et medansvar for IT-sikkerheden og er forpligtet til at efterleve de regler, der er fastlagt af IT-sikkerhedspolitikken med tilhørende forretningsgange, retningslinjer, procedurer mv.

På baggrund af en konkret vurdering i hvert enkelt tilfælde kan overtrædelser blive anset som en misligholdelse af ansættelsesforholdet.

Outsourcing

Kontrapunkt Group kan beslutte at outsource aktiviteter, herunder anvende cloud-løsninger. Outsourcing af væsentlige aktivitetsområder kan kun ske ved en bestyrelsesbeslutning under hensyntagen til alle relevante lovgivningsmæssige krav og reguleringer i øvrigt.

Outsourcing-kontrakten
Kontrakten skal indeholde en IT-sikkerhedsinstruks, der beskriver det ønskede IT-sikkerhedsniveau for Kontrapunkt Groups systemer og data, samt krav om, at driftsleverandøren til enhver tid overholder Kontrapunkt Groups IT-sikkerhedspolitik og -regelsæt. Kontrapunkt Group skal sikre løbende kontrol og opfølgning på efterlevelse heraf.

IT-leverancen
IT-leverandøren sikrer, at IT-leverancen foregår efter anerkendt "god IT-skik" for de relevante områder, herunder daglig administration, system-planlægning, overvågning, ændringsstyring, rapportering etc.

Kontrapunkt Group har ansvaret for opfølgning på, at IT-ydelsen modsvarer de krav og forventninger, som Kontrapunkt Group har opstillet.

IT-revision
Ved outsourcing af væsentlige aktivitetsområder skal IT-leverandøren sikre, at deres eksterne IT-revision mindst en gang om året rapporterer om det aktuelle niveau for IT-sikkerhed hos IT-leverandøren til Kontrapunkt Group.