Persondatapolitik for Dansk Revision

- om behandling af personoplysninger

Version	Dato	Ændret af	Godkendt af
1.1	16. juli 2022	HACA/PHOE	Bestyrelsen

Indhold

Persondatapolitik for Dansk Revision

Denne persondatapolitik har to formål. For det første skal den tjene som et praktisk instrument i virksomhedens arbejde med beskyttelsen af persondata, for det andet skal den fungere som en skriftlig dokumentation af vores indsats for at overholde Persondataforordningen. Kunder, leverandører, medarbejdere, samarbejdspartnere og andre interessenter kan via dette dokument opnå sikkerhed for, at vi gør alt, hvad vi kan for at beskytte deres data og behandle disse data i overensstemmelse med både lovgivning og god databehandlingsskik.

Dansk Revisions persondatapolitik er udformet i sammenhæng med virksomhedens overordnede strategi, værdier og visioner og er på den måde en integreret del af, hvordan virksomheden arbejder. Politikken er godkendt af Dansk Revision A/S' bestyrelse, og ledelsen af det enkelte Dansk Revisions kontor har gjort alle medarbejdere bekendt med den og deres ansvar i forhold til persondata. Hvis der opstår mistanke om, at persondata ikke håndteres korrekt, skal man øjeblikkeligt kontakte sin nærmeste leder og informere denne om problematikken.

Persondatapolitikken bliver gennemgået og opdateret mindst én gang om året af Dansk Revision A/S' administrerende direktør og IT-chefen og efter høring af Dansk Revision A/S IT-udvalg. Ved ansættelse bliver alle nye medarbejdere gjort bekendt med persondatapolitikken, ligesom den indgår i medarbejdernes ansættelsesaftaler.

I tilknytning til persondatapolitikken er der udarbejdet en personalehåndbog IT og persondatapolitik, som omhandler de aspekter af persondatabehandlingen, der vedrører medarbejdernes konkrete håndtering af persondata i hverdagen, samt en sikkerhedsbrudsvejledning. Endvidere er der udarbejdet en fortegnelse over virksomhedens persondatabehandlinger. Fortegnelsen over persondatabehandlinger hos Dansk Revisions fælles IT-platform findes i Dansk Revision A/S' GDPR-gruppeportal fra GAPsolutions A/S (tidligere Persondatasupport). Dansk Revision inddrager ekstern rådgiver for at sikre fuld compliance med persondatalovgivningen.

1. Definitioner

Dansk Revision behandler persondata i forbindelse med køb, salg, samarbejde og HR-funktioner. I det følgende vil kernebegreber fra lovgivningen blive defineret for at lette forståelsen af persondatapolitikken.

Persondatalovgivningen/ databeskyttelseslovgivningen	Den persondataforordning/ databeskyttelsesforordning (forkortet GDPR) - som fra 25. maj 2018 regulerer behandlingen af persondata samt yderligere dansk lovgivning
Personoplysninger (data)	Enhver oplysning om en identificeret eller identificerbar fysisk person, eksempelvis navn, adresse, telefonnummer, billede, nummerplade, cpr-nummer eller lignende. Oplysninger om enkeltmandsfirmaer er derfor også personoplysninger.
Følsomme personoplysninger (data)	Eksempelvis oplysninger om helbred, fagforeningstilhørsforhold, race, etnicitet, politisk overbevisning eller om strafbare forhold med videre.
Registrerede	Alle personer, hvis oplysninger er registreret hos Dansk Revision, eksempelvis kunder, medarbejdere og leverandører.
Behandling af data	Alt, hvad virksomheden gør med data, inklusiv opbevaring og sletning.

Dataansvarlig	Den, der beslutter formål, omfang og metoder til behandling af persondata.
Databehandler	Den, der behandler data på vegne af den dataansvarlige, eksempelvis en cloudtjeneste eller et firma, som håndterer løn.

2. Organisation og ansvar

Dansk Revision er opdelt i en række forskellige afdelinger, der udøver revisions- og rådgivningsvirksomhed under selvstændige CVR-numre. Denne persondatapolitik gælder for alle afdelinger, men det kan være nødvendigt at indføre specifikke instrukser i specifikke afdelinger. I så fald skal disse instrukser være i overensstemmelse med persondatapolitikken, have en klar ansvarsfordeling og en fast plan for opdatering.

Ansvaret for medarbejdernes overholdelse af denne persondatapolitik hviler først hos medarbejderne selv, dernæst hos ledelsen af de enkelte afdelinger (i det følgende kaldet ledelsen). Kontrol med overholdelse af persondatapolitik skal dokumenteres skriftligt og opbevares på Dansk Revisions GDPR-gruppeportal. Hvis kontrollen viser, at der har været episoder, hvor persondatapolitikken ikke er blevet overholdt, er det lederens opgave at afhjælpe problemet. Dansk Revision A/S gennemfører hvert år interne kvalitetskontroller af afdelingernes arbejde, og overholdelse af persondatareglerne indgår i de interne kontroller.

Hver afdeling fører desuden en databrudslog, og ledelsen i den pågældende afdeling orienterer straks Dansk Revision A/S' administrerende direktør eller IT-chef ved eventuelle databrud.

Databehandler

Vi er databehandler for de personoplysninger, som vores dataansvarlige kunder overlader til os til behandling på deres vegne, når vi eksempelvis fungerer som revisor, rådgiver eller bogholder. Der skal derfor etableres en databehandleraftale med den dataansvarlige, før behandlingen kan påbegyndes.

Som databehandler har vi en række forpligtelser over for vores kunder:

- Vi må alene behandle de overladte personoplysninger efter instruksen indeholdt i databehandleraftalen.
- Vi skal føre en fortegnelse over behandlingen af personoplysninger.
- Vi skal følge sikkerhedsinstrukserne i databehandleraftalen og videreføre disse til vores underleverandører. Hvis der er forskel på sikkerhedskravene i vores databehandleraftaler med henholdsvis vores kunde og underleverandør, tager vi udgangspunkt i den aftale, der indeholder de strammeste krav til sikkerhed, så vi er sikre på, at alle aftaler, på trods af varierende udformning, bliver overholdt.
- Vi skal på opfordring fra kunden hjælpe med at opfylde kundens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra den registrerede om indsigt i egne oplysninger, udlevering af den registreredes oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af den registreredes oplysninger, underretning af den registrerede ved sikkerhedsbrud samt bistå kunden i forbindelse med dennes forpligtelser efter Databeskyttelsesforordningens artiklerne 32-36.
- Vi skal levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger, således at vores behandling af kundens personoplysninger opfylder kravene i Databeskyttelseslovgivningen samt sikrer beskyttelse af den registreredes rettigheder jævnfør personalehåndbog it og persondatapolitikken.
- Vi skal kunne oplyse, hvor kundens personoplysninger opbevares og ajourføre oplysningerne over for kunden ved enhver ændring.

3. Medarbejderinstruks

Det følgende er de konkrete regler og retningslinjer, som alle ansatte i Dansk Revision skal følge i forbindelse med behandling af persondata. Instruksen er baseret på kravene i Persondataforordningen samt yderligere dansk lovgivning og vil sammen med IT-politikken og den udarbejdede dokumentation sikre virksomhedens efterlevelse af forordningen. Hvert element i instruksen er delt op i formål (hvorfor gør vi det), procedure (hvordan gør vi det) og kontrol (har vi nu også gjort det).

3.1 Sikring af lovligt grundlag/hjemmel

Formål:

- Der er et lovligt grundlag for at behandle data.

Procedure:

Før en databehandling påbegyndes, skal der ske en afklaring af den lovlige hjemmel. Dette gøres af ejeren af processen i samarbejde med afdelingslederen. Persondataforordningen angiver seks gyldige grunde: Samtykke, opfyldelse af kontrakt, retlig forpligtelse, vitale interesser, opgaver i samfundets interesse og endelig interesseafvejning. Som hovedregel vil virksomheden i forbindelse med revisions- og assistanceopgaver anvende hjemlen retslig forpligtelse, og i forbindelse med bogholderiopgaver findes hjemlen i aftalen med den dataansvarlige kunde. Opstår der tvivl om den lovlige hjemmel, retter man henvendelse til ledelsen. Hvis et lovligt grundlag ikke kan identificeres, igangsættes behandlingen ikke.

Det lovlige grundlag for behandlingen dokumenteres i QWM sammen med den pågældende proces i fortegnelsen over behandlingsaktiviteter, som er angivet i Dansk Revision A/S' GDPR-gruppeportal.

Underskrevne/accepterede samtykkeerklæringer iht. nyhedsbreve opbevares på Dansk Revision A/S' S-drev, mens samtykkeerklæringer vedrørende medarbejdere opbevares i den enkelte Dansk Revisions afdeling sammen med øvrige fortrolige personaledokumenter.

Ansættelseskontrakter indeholder et afsnit og/eller tillæg om samtykke til at behandle følsomme oplysninger mv.

Kontrol:

Alle behandlingsaktiviteter og den lovlige hjemmel herunder aftalegrundlag, gennemgås hvert år af sekretariatet i Dansk Revision i forbindelse med de interne kvalitetskontroller.

3.2 Sikring af formål og at data er relevante

Formål:

- Oplysninger, som indsamles, er baseret på et klart formål og omfatter ikke mere, end hvad der kræves til opfyldelse af formålet med behandlingen.

Procedure:

For hver behandlingsaktivitet bliver det klart defineret hvilke personoplysninger, som er relevante for formålet, og det sikres, at der ikke indsamles flere oplysninger end nødvendigt for at understøtte dette formål. Formålet med behandlingen af personoplysninger samt hvilke typer personoplysninger, der behandles for hver behandlingsaktivitet, er defineret i "Fortegnelsen over behandlingsaktiviteter" i Dansk

Revision A/S' GDPR-portal.

I tilfælde, hvor det kan være i virksomhedens interesse at indsamle flere oplysninger end nødvendigt, skal der udarbejdes en samtykkeerklæring jf. afsnit 3.1.

Kontrol:

Alle behandlingsaktiviteter gennemgås årligt, hvor kategorier af indsamlede oplysninger sammenholdes med formålet, med henblik på at sikre, at oplysningerne stadig er nødvendige for formålet. Kontrollen foretages af Dansk Revisions sekretariat og sker i forbindelse med de interne kvalitetskontroller.

3.3 Sikring af oplysningspligt

Formål:

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

Procedure:

Ved ansættelsen bliver medarbejderne via deres ansættelseskontrakt på en letforståelig måde informeret om:

- Hvem der er dataansvarlig og dennes kontaktoplysninger
- Formålet med behandling af data
- Hjemmel for behandling samt legitime interesser, som forfølges af virksomheden
- Eventuelle andre modtagere af data, herunder overførsel til tredjelande
- Opbevaringsperiode for data
- Den registreredes rettigheder i forhold til data (indsigt, berigtigelse, sletning, begrænset behandling og dataportabilitet).
- Retten til at tilbagekalde et eventuelt afgivet samtykke
- Retten til at klage til Datatilsynet
- At de har pligt til at afgive oplysninger og konsekvenser ved ikke at gøre det
- Hvor oplysningerne er indhentet, hvis dette ikke er direkte fra den registrerede selv
- Omfanget af automatiske afgørelser, herunder profilering og logikken bag

Hvis virksomheden senere ønsker at behandle oplysninger til et andet formål end oplyst til den registrerede, bliver den registrerede oplyst om dette, før den nye behandling igangsættes.

For at oplyse kunder og samarbejdspartnere er der udformet en tekst, indeholdende de ovenstående punkter, der er tilgængelig på www.danskrevision.dk/legal. Et link til denne tekst afgives elektronisk (Eksempelvis pr. mail) eller via telefon til den registrerede ved første kontakt. Oplysningsteksten angives også i kundeaftaler.

Kontrol:

Det er ledelsens ansvar at kontrollere, at reglen om oplysningspligt bliver overholdt. Langt det meste sikres elektronisk via hjemmesiden, men når en henvendelse kommer direkte via mail/telefon, skal der udsendes en mail med link til oplysningerne. Den afsendte mail er dokumentation for overholdelse af

oplysningspligten og skal gemmes på den relevante sag under navnet oplysningspligt.

En gang om året gennemgår Dansk Revisions Sekretariat, at den eksterne oplysningspligt overholdes. Dette inkluderer en kontrol af oplysningspligten på hjemmesiden og i kundekontrakter samt, at det eksisterende link til privatlivspolitikken fortsat er til den gældende privatlivspolitik.

I forbindelse med kontrollen om procedurens efterlevelse udføres der årligt stikprøver, i form af en e-mail sendt til de HR -ansvarlige i udvalgte afdelinger af Dansk Revision med henblik på at sikre, at alle medarbejdere har læst og underskrevet dokumentet "Oplysning og samtykke medarbejdere".

3.4 Sikring af retten til indsigt

Formål:

- Sikre at de registrerede kan få indsigt i de oplysninger, som behandles om dem.

Procedure:

Ved henvendelse skal den registrerede, uden unødigt ophold, på en let forståelig måde have indsigt i de oplysninger, som er registreret om den pågældende, herunder:

- Formålet med behandling af data
- Hvilke kategorier af oplysninger, som behandles
- Eventuelle andre modtagere af data, herunder overførsel til tredjelande
- Opbevaringsperiode for data
- Den registreredes rettigheder i forhold til data (indsigt, berigtigelse, sletning, begrænset behandling og dataportabilitet)
- Retten til at klage til datatilsynet
- Hvor oplysningerne er indhentet, hvis dette ikke er direkte fra den registrerede selv
- Omfanget af automatiske afgørelser, herunder profilering og logikken bag

En medarbejder, der modtager et ønske om indsigt skal hurtigst muligt kontakte ledelsen i den relevante Dansk Revision afdeling. Oplysninger udleveres i papirform eller almindeligt anvendt elektronisk form, baseret på hvilket format, den registrerede ønsker.

Det sikres, at den, der meddeles oplysninger til, er rette person. Der må kun udleveres oplysninger, når vedkommende har legitimeret sig, eller når der på anden måde er skabt sikkerhed for, at den, der fremsætter en indsigtsbegæring, er identisk med den person, som oplysningerne vedrører eller er i besiddelse af en fuldmagt fra denne.

Telefoniske henvendelser

Ved telefoniske henvendelser skal det sikres, at der kun gives oplysninger til rette person. Det kan være nødvendigt at stille kontrolspørgsmål, eksempelvis spørge efter adresse og CPR-nr. eller foretage en kontrolopringning til et telefonnummer for at sikre, at det er den rette person, som anmoder om oplysningerne. Hvis medarbejderen ikke kan få den nødvendige sikkerhed, må oplysningerne i stedet sendes pr. post til den adresse, der er registreret på vedkommende.

Henvendelser via brev og e-mail

Hvis navn og adresse i brevet/e-mailen er identisk med de oplysninger, som i forvejen fremgår af systemet, kan oplysningerne normalt sendes til den registreredes post- eller e-mailadresse. Er dette ikke tilfældet, bør forholdet undersøges nærmere.

Indsigt for børn under 18 år

Forældremyndighedens indehaver kan begære indsigt på barnets vegne. Barnet kan også selv få indsigt.

Indsigt på andres vegne (fuldmagt)

Den registrerede kan give en anden fuldmagt til at få indsigt i egne oplysninger. Fuldmagten kan være specifik eller generel. Er der tale om en advokat, er det normalt ikke nødvendigt at efterspørge en fuldmagt.

Kontrol:

Henvendelse vedrørende indsigt bliver løbende gennemgået i de enkelte Dansk Revision afdelinger. Ved modtagelse af en anmodning om indsigt fra en registreret, skal ledelsen i de enkelte Dansk Revision afdelinger fremsende besked om anmodningen til den administrerende direktør for Dansk Revision. Dansk Revisions sekretariat foretager løbende kontroller med, at de enkelte Dansk Revision afdelinger besvarer de registreredes anmodninger inden for den af loven fastsatte tidsfrist.

Hvis den registrerede, ikke modtager en rettidig tilbagemelding vedrørende sin anmodning fra den relevante Dansk Revision afdeling, kan Dansk Revision A/S' administrerende direktør kontaktes. Den administrerende direktørs kontaktdata fremgår af hjemmesiden www.danskrevision.dk.

3.5 Sikring af retten til berigtigelse

Formål:

- Sikre, at de registrerede kan få berigtiget deres oplysninger.

Procedure:
Ved henvendelse fra den registrerede skal virksomheden berigtige/rette eventuelle forkerte eller vildledende oplysninger om den pågældende.

En medarbejder, der modtager besked om, at der behandles forkerte oplysninger, henvender sig til lederen af den relevante Dansk Revision afdeling, som sørger for at korrigere oplysningerne. Den registreredes identitet bliver sikret, før oplysninger rettes, jf. afsnit 3.4.

Kontrol:

Se under pkt. 3.4.

3.6 sikring af retten til at sletning

Formål:

- Sikre den registreredes ret til sletning på den registreredes anmodning herom (”Retten til at blive glemt”)

Procedure:

Retten til at blive glemt. Når en registreret henvender sig med et ønske om at blive slettet, skal dette oplyses til lederen af den relevante Dansk Revision afdeling, som foretager sletningen uden unødigt ophold efter at have sikret sig, at formålet med behandlingen af oplysningerne ikke længere er til stede.

Det skal hermed sikres, at den registrerede ikke har nogle udeståender med virksomheden, før sletningen foretages.

Medarbejderne, som håndterer anmodningen om sletning, orienterer den pågældende registrerede om årsagen til, at anmodningen om sletning ikke kan imødekommes helt eller delvist, eksempelvis hvis det ikke er muligt at servicere kunden uden personoplysningerne eller den fortsatte behandling af disse er nødvendig for at opfylde krav i lovgivningen. Den registrerede skal til enhver tid kunne få slettet oplysninger, som er indsamlet baseret på samtykke. Den registreredes identitet bliver sikret, før oplysninger slettes, jævnfør afsnit 3.4

I henhold til virksomhedens backup-strategi bliver backups overskrevet hver uge, så alle sletninger i systemet bliver overskrevet i backuppen ugentligt. Hvis der bliver behov for at indlæse en backup, sikres det, at oplysninger, der er slettet i live-miljøet bliver slettet igen, efter at backuppen indlæses.

Kontrol:

Se under pkt. 3.4.

3.7 Sikring af retten til begrænset behandling

Formål:

- Begrænse behandlingen af personoplysninger til opbevaring alene

Procedure:

Når en registreret henvender sig og kræver, at behandlingen af vedkommendes oplysninger begrænses, skal lederen af den relevante Dansk Revision afdeling oplyses herom. Behandlingen af personoplysningerne begrænses til blot at opbevare oplysningerne, indtil forholdet, som er grundlag for den begrænsede behandling, løses. Den registreredes identitet bliver sikret, før behandlingen begrænses, jf. afsnit 3.4.

Kontrol:

Se pkt. 3.4.

3.8 Sikring af retten til dataportabilitet

Formål:

- At personlysninger, som behandles automatisk, kan udleveres eller overføres i et struktureret, almindeligt anvendt og maskinlæsbart format.

Procedure:

Når en registreret henvender sig med et ønske om at få udleveret eller overført personlysninger, rettes der straks henvendelse til lederen af den relevante Dansk Revision afdeling, som, baseret på den registreredes ønske, enten udleverer materialet i et struktureret, almindeligt anvendt, maskinlæsbart format eller, hvis teknisk muligt, overfører oplysningerne til en ny dataansvarlig, ønsket af den registrerede. Den registreredes identitet bliver sikret, før oplysninger udleveres eller overføres, jf. afsnit 3.4.

Kontrol:

Se pkt. 3.4.

3.9 Sikring af retten til indsigelse

Formål:

- Imødekomme den registreredes ret til indsigelse mod profilering og direkte markedsføring.

Procedure:

Når en registreret oplyser, at denne ikke ønsker, at vedkommendes oplysninger benyttes til profilering eller direkte markedsføring, skal der straks rettes henvendelse til lederen af den pågældende Dansk Revision afdeling, som derefter sørger for, at behandlingen af oplysningerne i forbindelse med profilering og direkte markedsføring stoppes. Den registreredes identitet bliver sikret, før behandlingen stoppes, jf. afsnit 3.4.

Det er sikret, at der er mulighed for menneskelige indgreb i automatiske behandlinger af personoplysninger, såfremt en registreret ønsker dette.

Kontrol:

Se pkt. 3.4.

3.10 Sikring af løbende sletning af oplysninger

Formål:

- Sikre at oplysninger bliver slettet, når de ikke længere er nødvendige for formålet med behandlingen.

Procedure:

I "Fortegnelsen over behandlingsaktiviteter" i Dansk Revision A/S' GDPR-portal er der taget stilling til opbevaringsperioder for hver behandlingsaktivitet. Personoplysninger opbevares i QVM og dertil indrettede drev for at mindske spredning af personoplysninger i organisationen og effektivisere sletteprocessen. Hvis medarbejderne har behov for midlertidigt at have personoplysninger liggende lokalt på deres maskiner eller skriveborde, skal disse fjernes så snart arbejdet er udført. Det sikres, at oplysninger også slettes hos eventuelle databehandlere.

Oplysninger slettes løbende:

Medarbejdere sletter løbende e-mails indeholdende personoplysninger, når disse er arkiveret andre steder, eller ikke længere er nødvendige for formålet med behandlingen.
Medarbejderne makulerer løbende fysiske dokumenter med personoplysninger, når disse ikke længere er nødvendige for formålet med behandlingen. De ansvarlige for systemer indeholdende personoplysninger sletter/uigenkaldeligt og af identificerer løbende oplysninger i systemerne, som ikke længere er nødvendige for

formålet med behandlingen. Før oplysninger slettes, sikres det, at oplysningerne ikke er nødvendige at opbevare i henhold til anden lovgivning, herunder bl.a. hvidvaskregler og bogføringsloven.

Sletning i backup:

I henhold til virksomhedens backup-strategi bliver backups overskrevet hver uge, så alle sletninger i systemet bliver overskrevet i backuppen ugentligt.
Hvis der bliver behov for at indlæse en backup, sikres det, at oplysninger, der er slettet i live-miljøet, bliver slettet igen efter, at backuppen indlæses.

Kontrol:

Opbevaringsperioden på behandlingsaktiviteter revurderes årligt af Dansk Revision Sekretariatet.

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

Kontrol: Det kontrolleres månedligt af de enkelte Dansk Revision afdelinger, at oplysninger, som skulle slettes ved medarbejderens fratræden, også er slettet, og det sikres, at oplysninger der skal opbevares efter fratrædelsen grundet juridiske forpligtelser iht. kontrakt el. lovgivning er arkiveret/journaliseret korrekt.
Eksempelvis skal billeder af fratrådte medarbejdere slettes på S-drevet, men oplysninger op arbejdsskader skal opbevares i minimum 30 år, også selvom medarbejderen er fratrådt.

Ansøgninger, hvor der ikke er afgivet samtykke til at gemme, er placeret i den relevante Dansk Revision afdeling og slettes, når den ansøgte stilling er besat. Denne kontrol udføres af de enkelte Dansk Revision afdelinger

Procedure: *Kundeoplysninger*
Kundeoplysninger skal slettes, når der ikke længere er et formål med opbevaring.

Kontrol: Det kontrolleres og revurderes årligt af de enkelte Dansk Revision afdelinger, om de pågældende kundeoplysninger skal slettes eller opbevares i længere tid.

Procedure: *Samarbejdspartnere- og leverandøroplysninger*
Oplysninger på leverandører og samarbejdspartnere skal slettes, når der ikke længere er et formål med opbevaring.

Kontrol: Det kontrolleres og revurderes årligt, om de pågældende leverandøroplysninger skal slettes eller opbevares i længere tid. Kontrollen hermed foretages af de enkelte afdelinger i Dansk Revision.

Procedure: *Sociale Medier, Hjemmeside, Messenger og lign.*
Oplysninger på medarbejdere, kunder samt andre personer i opslag på sociale medier og lignende slettes når der ikke længere har et formål med behandlingen.

Kontrol: Det kontrolleres og revurderes hvert 2. år om de pågældende personoplysninger fortsat er relevante på de forskellige opslag, i samtaler mv. Hvis det vurderes, at opslaget eller samtalen ikke længere er relevant for Dansk Revision A/S, skal de slettes. Kontrollen foretages af Dansk Revisions sekretariat.

3.11 Databehandleraftaler

Databehandleraftaler, når vi er dataansvarlig

Formål:

- Sikring af, at der etableres databehandleraftaler med andre juridiske enheder, som behandler personoplysninger på vegne af os.

Procedure:

Der er indgået databehandleraftaler med samtlige juridiske enheder, der behandler personoplysninger på vegne af os. Hver gang, der indgås en ny aftale med en samarbejdspartner, vurderes det, om ydelsen involverer behandling af personoplysninger på vegne af os. Hvis dette er tilfældet, indgås der en databehandleraftale.

Databehandleraftaler, der omfatter Dansk Revision A/S fælles IT-platform gemmes centralt hos Dansk Revision A/S på S:/IT afd/GDPR og lægges ind på GDPR-gruppeportalen. Øvrige databehandleraftaler opbevares af ledelsen.

Hvis en medarbejder i det daglige bliver opmærksom på fejl eller mangler i en databehandlers håndtering af personoplysninger, skal medarbejderen gøre nærmeste leder opmærksom på problemet. Lederen skal herefter undersøge problemet og eventuelt foretage den nødvendige opfølgning. Dansk Revision A/S IT-afdeling inddrages i fornødent omfang.

Kontrol:

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

Der skal udføres kontrol en gang årligt med databehandlerne ved indhentning af erklæringer om, at databehandleraftalen overholdes. Kontrollerne foretages af Dansk Revisions sekretariat (IT-chefen) og forelægges for Dansk Revisions IT-udvalg.

Hver enkelt afdeling gennemgår sin egen liste over eventuelle databehandlere, som der er indgået aftale med lokalt, og vurderer ligeledes om disse databehandleraftaler fortsat er tilstrækkelige.

Databehandleraftaler, når vi er databehandler

Formål:

- Sikring af, at der etableres databehandleraftaler med dataansvarlige, som vi behandler data på vegne af.

Procedure:

Der er indgået databehandleraftale med alle relevante eksterne og interne parter. Såfremt der ønskes et skift af leverandør (underdatabehandler) for de behandlinger der involverer de dataansvarlige, skal skiftet godkendes i henhold til godkendelsesproceduren i databehandleraftalen.

Hvis en medarbejder bliver opmærksom på fejl eller mangler i den dataansvarliges håndtering af personoplysninger, skal medarbejderen ligeledes gøre den relevante leder opmærksom på problemet, således

at problemet kan blive undersøgt og eventuelt foretage den nødvendige opfølgning. IT-chefen inddrages i nødvendigt omfang, men orienteres som minimum.

Kontrol:

Hvert år gennemfører Dansk Revisions sekretariat en gennemgang af Dansk Revision A/S fælles IT-platform, herunder IT-systemer og -processer med henblik på at identificere eventuelle forbedringer i forhold til håndtering af persondata. Dokumentation herfor samt opdateringer kan ses i Dansk Revision A/S GDPR-portal.

3.12 Sikring af dokumentation

Formål:

- Imødekomme EU persondataforordningens krav om fortegnelse over behandlingsaktiviteter og konsekvensanalyse.

Procedure:

Virksomheden har etableret en fortegnelse over behandlingsaktiviteter, som kan findes i Dansk Revision A/S GDPR-portal. Fortegnelsen opdateres løbende, når der sker ændringer i virksomhedens behandlingsaktiviteter.

For hver behandlingsaktivitet er der foretaget en risikovurdering baseret på sandsynligheden for, at personoplysninger mister fortrolighed, integritet eller tilgængelighed, samt hvilken konsekvens det har for den registrerede. Risikovurderingen revurderes 1 gang årligt, og for højrisikoområder udarbejdes der en handlingsplan for nedsættelse af risiko. Hvis risikoen ikke kan nedsættes, konsulteres Datatilsynet.

Kontrol:

Dansk Revision sekretariat kontrollerer årligt risikoen for alle behandlingsaktiviteter med henblik på at vurdere, om behandlingsaktiviteter er af høj risiko og dermed, om der skal etableres en konsekvensanalyse og handlingsplan for at nedsætte risikoen. Hvis det ikke er muligt at nedsætte risikoen, skal det vurderes, om ekstern rådgiver Datatilsynet skal konsulteres, før behandlingen igangsættes. Risikovurdering og konsekvensanalyse opdateres hver gang, der er nye planlagte behandlingsaktiviteter eller ændringer til eksisterende behandlingsaktiviteter.

3.13 Datasikkerhed

Formål:

- Der er etableret fornødne organisatoriske og tekniske foranstaltninger mod at personoplysninger kommer til uvedkommendes kendskab eller går tabt.

Procedure: Begrænsning af adgangen til elektronisk persondata

Alle systemer/drev, der indeholder personoplysninger er omfattet af begrænset adgang, således at det kun er de medarbejdere, der har behov for adgangen til at udføre deres arbejde, der har adgang til systemer/drev med personoplysninger.

Procedure: Mails med personoplysninger

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

Generel sikkerhed i IT miljøet. Der henvises til virksomhedens personalehåndbog for IT og persondata i Dansk Revision. Procedure: Mobile enheder

Behandlingen af data på mobile enheder er begrænset til et absolut minimum. Der er vedtaget retningslinjer for brugen af mobile enheder, herunder at det udelukkende er tilladt at behandle data herpå i den udstrækning, det er nødvendigt for udførelsen af brugernes arbejde.

Kontrol:

Hvert år gennemgår den IT-ansvarlige på hvert kontor listen over medarbejdere med adgang til systemer og mapper med personoplysninger med henblik på at verificere, at kun de nødvendige medarbejdere har adgang til systemer og mapper indeholdende personoplysninger.

3.14 Fysisk sikkerhed

Formål:

- Der er forholdsregler, der sikrer mod uvedkommendes adgang til lokaler, hvor der foregår behandling af personoplysninger.

Procedure:

Områder med adgang til personoplysninger sikres således, at uvedkommende ikke kan få adgang til disse. Det sker ved at opbevare personoplysninger i aflåst skab, når lokalet ikke er under opsyn. Løbende, afhængig af mængden af bilag, kan personoplysninger fra aflåst skab arkiveres i et aflåst arkiveringsrum.

Alle medarbejdere skal låse deres PC, når arbejdsstationen forlades, også kortvarigt. Medarbejdere er underlagt en clean desk politik, som indebærer, at medarbejderne skal fjerne alle dokumenter fra deres skrivebord, når de forlader arbejdspladsen. Derudover skal de følge en face down politik, som indebærer, at dokumenter med personoplysninger vendes med den blanke side op eller på anden måde afdækkes, når medarbejderen efterlader dokumenter på arbejdsstationen.

For yderligere oplysninger om fysisk sikkerhed henvises til Dansk Revisions Personalehåndbog IT og persondata.

Kontrol:

En gang om året kontrolleres det, via de interne tjeklister for fysisk sikkerhed på de enkelte revisionskontorer, at de fysiske sikkerhedsforanstaltninger på kontoret efterleves og er tilstrækkelige. Kontrollen foretages af Dansk Revisions sekretariat.

3.15 Gæster

Formål:

- Gæster skal håndteres i overensstemmelse med Personalehåndbogens afsnit; "IT- og persondata for Dansk Revision".

Procedure:

Gæster må ikke færdes alene. Bliver en medarbejder opmærksom på, at en gæst færdes alene, skal gæstens ærinde afklares og relevant eskorte etableres.

3.16 Print og dokumenter med personoplysninger

Formål:

- Personlige oplysninger må ikke ligge frit tilgængeligt i papirform.

Procedure:

Print i Dansk Revision foregår med Follow Me Print. Print med personoplysninger må ikke efterlades i printerrummet.

Papirdokumenter, der indeholder personoplysninger, må i arbejdstiden ikke opbevares uden opsyn af en medarbejder.

Alle henvendelser (breve i papirformat, print af e-mails, papirlapper m.v.), som indeholder personoplysninger, skal efter endt brug makuleres eller smides ud i en særlig aflåst papircontainer. Indholdet af papircontainer bliver makuleret, når containeren er fyldt.

Kontrol:

Lederne skal løbende være opmærksomme på, at der ikke ligger print med personoplysninger i printrummet, eller at der ligger dokumenter og papir ved arbejdspladserne indeholdende personoplysninger. Det foretages en gang årligt en kontrol med at disse punkter er overholdt. Kontrollen foretages af Dansk Revisions sekretariatet i forbindelse med de interne revisioner.

3.17Sikring af medarbejdernes awareness

Formål:

- Sikre og demonstrere at medarbejdere er bekendt med reglerne for behandling af persondata

Procedure:

Samtlige medarbejdere i Dansk Revision er underlagt tavshedserklæring ved deres ansættelse.

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

Kontrol:

Hvert år kontrollerer den enkelte afdeling i Dansk Revision, at samtlige medarbejdere genlæser Personalehåndbog it og at relevante medarbejdere har kendskab til Persondatapolitikken.

Hvert år kontrollerer den enkelte afdeling i Dansk Revision, at samtlige medarbejdere genlæser sikkerhedsbrudsvejledningen.

3.18 Notifikation ved brud på datasikkerheden

Formål:

- Datatilsynet, og under visse omstændigheder, den registrerede, bliver ved brud på datasikkerheden notificeret om muligt indenfor 72 timer efter, at brud er konstateret.

Procedure:

Brud på datasikkerheden er defineret som en hændelse, som resulterer i, at der sandsynligvis er en risiko

for, at personoplysninger er blevet udsat for uautoriseret adgang eller er gået tabt.

Hvis en medarbejder opdager brud på datasikkerheden, meddeles dette straks til lederen af den relevante Dansk Revision afdeling samt Dansk Revision A/S' IT-afdeling. Ledelsen vil i samarbejde med IT-afdelingen indenfor 72 timer, have overblik over bruddet. Ledelsen samler i samarbejde med de eventuelt implicerede medarbejdere oplysninger omkring hændelsen, berørte datakategorier, antal lækkede data records, sandsynlige konsekvenser og hvilke tiltag, der er iværksat for at imødegå bruddet, som anmeldes til Datatilsynet indenfor 72 timer via deres hjemmeside.

Brud, der sandsynligvis medfører en risiko for, at personoplysninger er blevet udsat for uautoriseret adgang eller er gået tabt, anmeldes til Datatilsynet.

Alle brud på sikkerheden noteres i en databrudslog, som føres i alle Dansk Revision afdelinger af lederen af den relevante afdeling.

Hvis sikkerhedsbruddet er af sådan karakter, at det er nødvendigt at informere de registrerede, gøres dette via mail.

Hvis virksomheden ikke har kontaktoplysningerne på de registrerede, sker orienteringen offentligt via Datatilsynets hjemmeside.

For virksomhedens procedurer omkring sikring mod og identificering af brud henvises til Personalehåndbog IT og persondata.

Kontrol:
Det kontrolleres jævnligt ved kontrol af sikkerhedsbrudsloggen, at situationer, som skal anmeldes til Datatilsynet, også bliver anmeldt indenfor 72 timer.

3.19 Privacy by Design og Privacy by Default

Formål:

- Imødekommelse af EU Persondataforordningens krav om Privacy by design and default.

Procedure:

Ved udvikling eller anskaffelse af nye it-systemer er virksomheden opmærksom på, at systemerne er sikre og at de understøtter opdeling af adgangsrettigheder, således at personoplysninger kan beskyttes mod uautoriseret adgang og tab.

Medarbejderne må ikke benytte tjenester til behandling af personoplysninger, som ledelsen ikke har godkendt, herunder bl.a. private mail-applikationer, sin egen cloudløsning eller programmer, som kan downloades fra nettet til behandling af personoplysninger.

Kontrol:

Dansk Revision A/S IT-afdeling har sin egen tjekliste i forhold til opsætning af eksisterende og udvikling og opsætning af nye IT-systemer. IT-afdelingen foretager løbende en revision af de eksisterende systemer og afsøger netværket for brug af uautoriserede programmer. Dansk Revisions sekretariat foretager en årlig kontrol med tjeklisten, og tjeklisten skal i den forbindelse fremlægges for IT-udvalget.

3.20 DPO

Formål:

- Vurdering af, om det er et krav, at virksomheden har en DPO.

Procedure:

Dansk Revision har vurderet, at virksomheden ikke har behov for en DPO. Vurderingen er baseret på EU Persondataforordningens kriterier for krav om en DPO. Dansk Revision vil foretage en vurdering heraf igen, hvis virksomheden undergår signifikante ændringer i sit arbejde med personoplysninger. I tvivlstilfælde kan Dansk Revision A/S administrerende direktør kontaktes.