

Persondatapolitik for Dansk Revision

-vedrørende behandling af personoplysninger

Version	Dato	Ændret af	Godkendt af
1.0	11. april 2018	LOAN	Bestyrelsen

Indhold

Persondatapolitik for Dansk Revision..... 3

1. Definitioner..... 3

2. Organisering og ansvar 4

3. Medarbejderinstruks 4

 3.1 Sikring af lovligt grundlag/hjemmel..... 4

 3.2 Sikring af formål og at data er relevante 5

 3.3 Sikring af oplysningspligt 5

 3.4 Sikring af retten til indsigt 6

 3.5 Sikring af retten til berigtigelse 7

 3.6 Slettepligt og sikring af retten til at sletning 8

 3.7 Sikring af retten til begrænset behandling 9

 3.8 Sikring af retten til dataportabilitet..... 9

 3.9 Sikring af retten til indsigelse 9

 3.10 Databehandleraftaler 10

 3.11 Sikring af dokumentation 11

 3.12 Datasikkerhed 11

 3.13 Fysisk sikkerhed 12

 3.14 Gæster 12

 3.15 Print og dokumenter med personoplysninger 12

 3.16 Sikring af medarbejder awareness 13

 3.17 Notifikation ved brud på datasikkerheden..... 13

 3.18 Privacy by Design og Privacy by Default 14

 3.19 DPO 14

Persondatapolitik for Dansk Revision

Denne persondatapolitik har to formål. Den skal dels tjene som et praktisk instrument i virksomhedens arbejde med beskyttelsen af persondata, og dels 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 databehandlingskik.

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 straks kontakte sin nærmeste leder øjeblikkeligt og informere denne om problematikken.

Persondatapolitikken bliver gennemgået og opdateret mindst én gang om året af Dansk Revision A/S' administrerende direktør og IT-direktør 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 IT-politik, som omhandler de mere tekniske aspekter af persondatabehandlingen, inklusiv et beredskab ved nedbrud i sikkerheden. Endvidere er der udarbejdet en fortegnelse over virksomhedens persondatabehandlinger. Fortegnelsen over persondatabehandlinger hos Dansk Revision fælles IT-plattform findes i Dansk Revision A/S' GDPR Portal.

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.

Persondataforordningen	Den lovgivning, som pr. 25. maj 2018 regulerer behandlingen af persondata (træder i stedet for Persondataloven)
Personoplysninger (data)	Enhver oplysning om en identificeret eller identificerbar fysisk person, fx navn, adresse, telefonnummer, billede, nummerplade, cpr-nummer eller lignende. Oplysninger om enkeltmandsfirmaer er derfor også personoplysninger.
Følsomme personoplysninger (data)	Eksempelvis helbredsoplysninger, fagforeningstilhørsforhold, race, etnicitet, politisk overbevisning, oplysninger om strafbare forhold mv.
Registrerede	Alle personer, hvis oplysninger er registreret hos Dansk Revision, fx 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, i dette tilfælde Dansk Revision.
Databehandler	Den, der behandler data på vegne af den dataansvarlige, fx et firma, som håndterer løn eller en cloudtjeneste.

2. Organisering 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 S-drevet. 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-direktør ved eventuelle databrud.

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 Persondataforordningens krav 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-portal.

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

Kontrol:

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

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

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.

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, samt kontaktoplysninger på en eventuel Data Protection Officer,
- 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. Et link til denne tekst afgives elektronisk (fx 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. Én gang om måneden gennemgås alle åbne sager for at bekræfte, at oplysningspligten er opfyldt.

3.4 Sikring af retten til indsigt

Formål:

- Sikre at den 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 f.eks. være nødvendigt at stille kontrolspørgsmål, fx 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 registrerede på den registrerede 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 manglende indsigt 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 Slettepligt og sikring af retten til at sletning

Formål:

- Oplysninger slettes, når de ikke længere er nødvendige for formålet med behandlingen.
- Sikring af at kunne imødekomme den registreredes ret til sletning.

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 afidentificerer 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, bogføringsloven m.v..

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, fx hvis det ikke er muligt at servicere kunden uden personoplysningerne. Den registrerede skal til enhver tid kunne få slettet oplysninger, som er indsamlet baseret på samtykke. Den registreredes identitet bliver sikret, før oplysninger slettes, jf. afsnit 3.4.

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.

Hver måned gennemgås listen over fratrådte medarbejdere for at sikre, at personoplysninger, som ikke er nødvendige at opbevare i henhold til anden lovgivning, er slettet.

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.

3.7 Sikring af retten til begrænset behandling

Formål:

- Begrænse behandlingen af personoplysninger til opbevaring.

Procedure:

Når en registreret henvender sig og kræver, at behandlingen af vedkommendes oplysninger begrænses, skal den registrerede og medarbejderen oplyse lederen af den relevante Dansk Revision afdeling 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 indsigt 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 menneskelig indgreb i automatiske behandlinger af personoplysninger, såfremt en registreret ønsker dette.

Kontrol:

Se pkt. 3.4.

3.10 Databehandleraftaler

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.

Der udføres løbende kontrol med databehandlerne ved indhentning af erklæringer om, at databehandleraftalen overholdes.

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

Hvis en medarbejder i det daglige bliver opmærksom på fejl eller mangler i en databehandleres 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 at den gældende databehandleraftale stadig er tilstrækkelig.

Hvert år gennemfører en uafhængig 3. part en gennemgang af Dansk Revision A/S fælles IT-plattform, 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.

3.11 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:

Behandlingsaktiviteterne gennemgås årligt af en ekstern rådgiver 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 Datatilsynet konsulteres før behandlingen igangsættes. Risikovurdering og konsekvensanalyse opdateres hver gang, der er nye planlagte behandlingsaktiviteter eller ændringer til eksisterende behandlingsaktiviteter.

3.12 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.

Kontrol:

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

3.13 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 informationsikkerhedspolitik.

3.14 Gæster

Formål:

- Gæster skal håndteres i overensstemmelse med Personalehåndbogen vedr. IT- og persondata.

Procedure:

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

3.15 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.

3.16 Sikring af medarbejder awareness

Formål:

- 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:

Dansk Revision A/S opdaterer og udsender hvert år en persondatainstruks, som gennemgås i den enkelte afdeling.

3.17 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, om muligt, 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 Informationssikkerhedspolitikken.

Kontrol:

Det kontrolleres jævnligt, at situationer, som bør anmeldes til Datatilsynet, også bliver anmeldt indenfor 72 timer.

3.18 Privacy by Design og Privacy by Default

Formål:

- Imødekomme 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.

3.19 DPO

Formål:

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

Procedure:

Det vurderes årligt, hvorvidt virksomheden har behov for en DPO, baseret på EU Persondataforordningens kriterier for krav om DPO. I tvivlstilfælde kan Dansk Revision A/S administrerende direktør kontaktes.