KELLPOS INTERNE PERSONDATAPOLITIK

(REVIDERET 8. MAJ 2018)

Indhold

1. Forord

Denne politik henvender sig til alle medarbejdere hos Kellpo, der som led i deres arbejde behandler personoplysninger om kunder, samarbejdspartnere, leverandører og medarbejdere. Politikken omfatter således medarbejdere, som har adgang til personoplysninger til brug for deres arbejde.

Politikken beskriver, hvordan persondata skal behandles i en række typisk forekommende situationer i Kellpo. Politikken er udarbejdet som led i Kellpos bestræbelser på at overholde gældende lovgivning, herunder EU-forordningen om persondata (herefter kaldet "GDPR") samt databeskyttelsesloven, der forventes vedtaget af Folketinget omkring 1. maj 2018.

Da overtrædelse af persondatareglerne kan være forbundet med meget betydelige bødesanktioner samt påføre Kellpo betydelig imagemæssig skade, er det vigtigt, at alle medarbejdere, som behandler persondata, læser denne politik og erklærer at ville følge den samt evt. yderligere instrukser, der måtte blive udstedt af Kellpo eller en af denne udpeget persondataansvarlig person. Såfremt du i forbindelse med behandlingen af persondata overtræder politikken, kan det få ansættelsesretlige konsekvenser – i yderste konsekvens i form af afskedigelse eller bortvisning.

Politikken omfatter indledningsvis en beskrivelse af de gældende regler og dernæst en nærmere beskrivelse af de væsentligste forhold, du skal være opmærksom på i din hverdag hos Kellpo.

2. Hvad er personoplysninger? – almindelige og følsomme oplysninger

GDPR indeholder i artikel 4 en række vigtige definitioner, som her omtales.

2.1 Definitioner

Personoplysninger er oplysninger, som vedrører en identificeret eller identificerbar fysisk person (den registrerede). Det vil sige, at man enten umiddelbart ud fra oplysningerne eller via andre tilgængelige oplysninger kan knytte oplysningerne til en bestemt fysisk person.

Behandling af persondata er omfattet af persondatalovgivningen, uanset om det sker elektronisk eller manuelt som led i en systematisk behandling. Ved behandling forstås både indsamling, registrering, systematisering, søgning, bearbejdning, opbevaring, videregivelse og sletning af personoplysninger.

Både elektronisk lagrede oplysninger, og oplysninger, der er udskrevet på papir, er omfattet af reglerne (undtaget er alene løsrevne papirbaserede oplysninger, f.eks. håndskrevne notater, der ikke indgår i en systematisk behandling). Når du har en pligt til at slette personoplysninger (mere herom senere), er det vigtigt, at der både sker sletning af de elektronisk lagrede oplysninger og de der er udskrevet på papir – disse skal makuleres.

Udover den registrerede – som er den fysiske person, oplysningerne vedrører – opererer lovgivningen med 2 andre "aktører":

- Den dataansvarlige, som er den, der bestemmer formålene med behandlingen samt midlerne hertil, herunder hvilke oplysninger, der skal indsamles samt hvilke (it)-værktøjer der skal anvendes til at behandle disse.
- Databehandleren, der kan være antaget af den dataansvarlige til at foretage en behandling af persondata på den dataansvarliges vegne og efter dennes instruks.

Se mere om sondringen mellem rollen som dataansvarlig og databehandler samt kravene til databehandleraftaler nedenfor i pkt. 5.

2.2 Følsomme oplysninger

De følsomme oplysninger - i GDPR, artikel 9, kaldet "særlige kategorier af persondata", er oplysninger om:

- Race eller etnisk oprindelse
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold
- Genetiske og biometriske data
- Helbredsoplysninger (herunder handicap)
- Seksuelle forhold eller seksuel orientering

Der er skrappere krav til behandling af følsomme oplysninger. Som udgangspunkt må de kun behandles efter udtrykkeligt og specifikt samtykke fra den registrerede i forbindelse med den konkrete behandling, men der kan dog være grundlag for at behandle følsomme oplysninger i andre situationer, jf. pkt. 4.2.

Oplysninger om strafbare forhold er omfattet af GDPR artikel 10 og databeskyttelseslovens § 8. Sådanne oplysninger må som udgangspunkt kun behandles efter samtykke fra den registrerede eller hvor det er nødvendigt til varetagelse af en berettiget interesse, der klart overstiger hensynet til den registrerede.

Oplysninger om CPR-numre har sin egen bestemmelse i databeskyttelseslovens § 11. Oplysning om cpr-nummer må behandles, hvor det kræves af lov, af en offentlig myndighed eller for at sikre entydig identifikation, eller hvor der er et grundlag, som tillader behandling af følsomme oplysninger - men uanset dette må cpr-numre ikke offentliggøres, herunder i dokumenter, som uvedkommende tredjemand har adgang til.

2.3 De almindelige personoplysninger

Personoplysninger, som ikke er enten følsomme oplysninger (artikel 9), oplysninger om strafbare forhold eller cpr-numre, er omfattet af reglerne for almindelige personoplysninger i GDPR artikel 6. Det kan f.eks. være adresse, kontaktoplysninger, (telefon, e-mail, profilnavne på sociale medier etc.), oplysninger om uddannelsesbaggrund, erhvervserfaring, lønforhold, familieforhold mv.

De almindelige oplysninger kan godt være fortrolige i den forstand, at man ikke uden videre kan behandle dem – og særligt ikke kan videregive dem.

Visse personoplysninger betragtes som ikke-fortrolige. Det er f.eks. almindelige kontaktoplysninger (med mindre personen har adressebeskyttelse) samt stilling, civilstatus osv.

Det bemærkes, at karakteren af personoplysninger har betydning for, hvornår vi må behandle dem, jf. afsnit 3 og 4, og de sikkerhedsforanstaltninger, vil skal bruge for at beskytte dem (mere herom i afsnit 4).

3. Grundlæggende behandlingsprincipper

Når man vil behandle personoplysninger, er der både nogle generelle principper, man altid skal følge, og derudover skal man have et konkret grundlag – en såkaldt "hjemmel" til at foretage netop den konkrete behandling. Begge dele skal være opfyldt. Man kan f.eks. ikke basere en behandling af personoplysninger på, at man har "hjemmel" i form af et samtykke fra den berørte person, hvis man ikke samtidig kan argumentere for, at der er et sagligt behov for behandlingen. Nedenfor beskrives disse principper og grundlag mere generelt.

Principperne for behandling af personoplysninger går ud på følgende:

- Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede.
- Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål.
- Personoplysningerne skal være tilstrækkelige og relevante for den givne behandling, men der må heller ikke indsamles flere oplysninger end nødvendigt.
- Personoplysninger skal være korrekte og ajourførte, og fejlagtige oplysninger skal slettes eller berigtiges.
- Personoplysninger må ikke opbevares i en længere periode end nødvendigt for at opfylde det formål, hvortil de er indsamlet, med mindre der foreligger grundlag for en videre behandling.
- Personoplysninger skal – gennem anvendelse af passende tekniske og organisatoriske foranstaltninger – opbevares og behandles på en måde, der skaber tilstrækkeligt sikkerhed for, at der ikke sker uautoriseret eller ulovlig behandling, samt at der ikke sker tab, tilintetgørelse eller beskadigelse af oplysninger.

Ansvaret for, at de anførte principper overholdes, ligger hos den **dataansvarlige** (se nærmere i pkt. 5). Ansvaret påhviler Kellpo som sådan, men enhver medarbejder, der behandler personoplysninger, har en pligt til at sætte sig ind i disse regler og i tvivlstilfælde at søge tvivlen afklaret hos den person, der i det daglige har det overordnede ansvar for behandlingen af persondata og sikkerheden i forbindelse med denne.

Selv om Kellpo måtte benytte sig af eksterne samarbejdspartnere til behandling eller opbevaring af personoplysninger påhviler det endelige ansvar fortsat Kellpo som dataansvarlig. Det er et lovkrav, at der laves skriftlige databehandleraftaler i sådanne tilfælde. Selvom udkast til databehandleraftaler i mange tilfælde leveres af leverandøren, er det i sidste ende den dataansvarliges ansvar at sikre, at aftalen indgås og lever op til de gældende krav. Vær opmærksom på, at kravene til indholdet af databehandleraftaler skærpes, når forordningen træder i kraft (Art. 28). Det er den persondataansvarlige medarbejder på kontoret, der har ansvar for at sikre, at databehandleraftaler indgås.

Ved spørgsmål omkring den praktiske behandling af personoplysninger er den ansvarlige Ole Petersen.

Ved spørgsmål omkring it-sikkerhed er den ansvarlige Ole Petersen.

4. Grundlag (hjemmel) for behandling af personoplysninger

4.1 Almindelige personoplysninger

Der skal altid være et grundlag for at behandle personoplysninger. Almindelige oplysninger kan efter GDPR artikel 6 behandles efter et af følgende grundlag:

- Hvor behandlingen er nødvendig for at opfylde en kontrakt, som den registrerede er part i.

- Hvor behandlingen er nødvendig for at opfylde en retlig forpligtelse, som påhviler den dataansvarlige. Ved retlig forpligtelse forstås forpligtelser, der følger af lovgivningen. Det følger herunder af ansættelsesbevisloven, at arbejdsgivere har pligt til at udarbejde en ansættelseskontrakt til dennes medarbejdere indeholdende den ansattes navn, adresse, stilling, lønforhold og pensionsforhold.

- Hvor den registrerede har givet samtykke til behandlingen af personoplysningerne. Et samtykke skal som udgangspunkt gives udtrykkeligt, men i nogle sammenhænge – hvor oplysningerne kommer fra den registrerede selv – kan samtykket ligge implicit i overgivelsen af oplysningerne, men i så fald kun til behandling i det omfang, den registrerede klart måtte forudse. Et sådant samtykke kan f.eks. foreligge, når Kellpo modtager henvendelser fra kontaktpersoner hos leverandører eller kunder, hvor det er nødvendigt for at kommunikere omkring ordrer.

- Hvor behandling er nødvendig, for at arbejdsgiveren eller tredjemand kan forfølge en legitim interesse, med mindre den registreredes interesser eller grundlæggende rettigheder går forud herfor. Dette er den såkaldte "interesseafvejningsregel", som kan anvendes i en lang række sammenhænge. Kellpo forfølger bl.a. en legitim interesse, når der indhentes personoplysninger om kontaktpersoner hos samarbejdspartnere, leverandører eller kunder, idet Kellpo har en legitim interesse i at tage kontakt til disse personer, hvor relationen giver anledning dertil.

4.2 Følsomme personoplysninger

GDPR artikel 9 indeholder som udgangspunkt et forbud mod at behandle disse. De relevante undtagelser er:

- Hvor den berettigede har givet et udtrykkeligt og specifikt samtykke. Det vil sige, at samtykket skal gå specifikt på den konkrete behandling af de konkrete, følsomme oplysninger.

- Hvor behandlingen vedrører oplysninger, som den berettigede selv allerede har offentliggjort, kan oplysningerne behandles (naturligvis forudsat de i pkt. 2 omtalte behandlingsprincipper overholdes). Bemærk, at oplysningerne ikke må behandles, hvis det er andre end den berettigede selv, der har offentliggjort oplysningen. Oplysninger på sociale medier skal derfor behandles med stor varsomhed, idet der ikke er sikkerhed for, at det er den registrerede selv, der har offentliggjort dem.

- Hvor behandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares.

- Hvor behandlingen er nødvendig for at overholde den dataansvarliges eller den registreredes arbejds-, sundheds- og socialretlige forpligtelser og specifikke rettigheder, for så vidt den har

hjemmel i EU-retten eller medlemsstaternes nationale ret eller en kollektiv overenskomst i medfør af medlemsstaternes nationale ret, som giver fornødne garantier for den registreredes grundlæggende rettigheder og interesser. Denne hjemmel er relevant i tilfælde hvor Kellpo anmelder arbejdsskader på vegne af medarbejdere, idet denne forpligtelse følger af lovgivningen.

5. Dataansvarlig ctr. databehandler

Kellpo behandler alene personoplysninger i tilfælde, hvor det er relevant og bestemmer formålet med behandlingen. Kellpo er ikke underlagt instruks fra andre i forhold til hvilke personoplysninger, der skal behandles, eller hvorledes disse skal behandles. Når Kellpo behandler oplysninger om vores samarbejdspartnere, kunder, leverandører eller medarbejdere, er vi således utvivlsomt dataansvarlige.

Sondringen mellem databehandlere og dataansvarlige er yderligere forklaret af datatilsynet i deres vejledning herom:
https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_om_dataansvarlige_og_databehandlere_-_endelig_version.pdf

Det er den dataansvarlige, der har ansvaret for at sikre, at der er lovligt grundlag for behandling af personoplysningerne, jf. pkt. 3 og 4, også hvor databehandlingen helt eller delvist overlades til en databehandler.

Det er også den dataansvarlige, der har pligt til at sikre, at den registreredes rettigheder, jf. pkt. 6, overholdes, uanset om den praktiske opfyldelse af disse måtte blive overladt til en databehandler efter aftale med denne.

6. De registreredes rettigheder

Det almindelige princip om gennemsigtighed indebærer en række konkrete pligter over for de registrerede, som er beskrevet i EU-forordningens kapitel III. Generelt indebærer bestemmelserne heri, at den dataansvarlige skal assistere den registrerede med at udnytte sine rettigheder.

6.1 Oplysningspligt

Der gælder efter GDPR artikel 13-14 en oplysningspligt ved enhver indsamling af personoplysninger, uanset om disse indsamles fra den registrerede selv eller tredjemand. Der skal altid gives oplysning om:

- Den dataansvarliges identitet og kontaktinformation – herunder på en person, der i Kellpo er udpeget som ansvarlig for persondata
- Formålet med og grundlaget for behandlingen
- Den legitime interesse, hvis grundlaget er interesseafvejningsregel
- Eventuelle modtagere af personoplysningerne eller kategorier af modtagere (herunder eksterne lønbureauer og koncernforbundne virksomheder)
- Om der sker overførsel til tredjelande (udenfor EU/EØS)
- Hvor længe oplysningerne opbevares (frist eller kriterier for sletning)
- Retten til at kræve indsigt i egne oplysninger (art. 15)

- Retten til at kræve berigtigelse (art. 16) eller sletning (art. 17) af oplysninger, begrænsning af behandling (art. 18) samt retten til dataportabilitet (art. 20).
- Eksistensen af evt. profilering og automatiserede afgørelser (art. 21-22)
- Muligheden for at trække et evt. samtykke tilbage
- Muligheden for at klage til Datatilsynet

Ved oplysninger indhentet fra den registrerede selv, skal der yderligere afgives oplysning om:

- Hvorvidt den registreredes afgivelse af oplysningerne er nødvendige for at opfylde en kontrakt eller lovmæssige forpligtelser
- Hvorvidt oplysningerne kan forventes anvendt til et andet formål, end de er indhentet

Ved oplysninger indhentet fra tredjemand, skal der yderligere afgives oplysning om:

- Hvilken tredjemand, der har givet oplysningerne
- Hvilke kategorier af oplysninger, der er indhentet (fra tredjemand)

Den nævnte oplysningspligt skal opfyldes i forbindelse med indsamling af oplysningerne hos den registrerede eller senest en måned efter indsamlingen, hvor denne sker hos tredjemand. Oplysningerne skal gives i et let forståeligt sprog og bør gives på skrift.

Kellpo opfylder oplysningspligten over for kunder og samarbejdspartnere ved at fremsende en skrivelse indeholdende de relevante oplysninger til den registrerede, pr. e-mail straks ved indsamlingen af oplysningerne.

6.2 Indsigtsret

Den registrerede har efter GDPR artikel 15 desuden en indsigtsret, dvs. vedkommende har til enhver tid ret til at kræve de oplysninger, som er anført i pkt. 6.1, også selv om Kellpo har opfyldt sin oplysningspligt.

Anmodninger om indsigt skal besvares skriftligt inden 1 måned efter, de fremsættes.

Indsigtsanmodninger skal fremsættes over for Kellpos persondataansvarlige Ole Petersen.

6.3 Ret til berigtigelse

Den registrerede har efter GDPR artikel 16 ret til at få berigtiget urigtige oplysninger uden unødig forsinkelse. Kellpo besvarer berigtigelsesanmodninger inden for en måned.

6.4 Retten til at blive glemt

Den registrerede har efter GDPR artikel 17 endvidere ret til at få slettet personoplysninger, som ikke længere er nødvendige for det formål, de er indsamlet til, eller hvor der ikke længere er et lovligt grundlag for at behandle dem, herunder hvor et meddelt samtykke, som behandlingen baseres på, trækkes tilbage. Dette kaldes "retten til at blive glemt". Sletning bør ske inden for en 1 måned, forudsat anmodningen er berettiget og sletning ikke strider mod andre regler.

Ved modtagelse af en begæring om sletning, skal du kontakte Kellpos persondataansvarlige Ole Petersen, som skal tage stilling til eventuel sletning forinden den gennemføres. Der kan således være hensyn, som betyder, at en begæring om sletning ikke skal imødekommes eller kun imødekommes delvist.

6.5 Ret til begrænsning af behandling

Den registrerede kan efter GDPR artikel 18 endvidere kræve, at behandlingen af personoplysninger begrænses til de formål, der er lovlige, ligesom det kan kræves, at behandlingen suspenderes, mens rigtigheden af personoplysninger undersøges, en interesseafvejning foretages, eller et retskrav fastlægges. I sidstnævnte tilfælde må oplysningerne ikke slettes, men skal opbevares, mens den anførte afklaring finder sted.

6.6 Underretningspligt overfor tredjemand ved berigtigelse, sletning eller begrænsning.

Når vi berigtiger, sletter eller begrænser behandlingen af personoplysninger, jf. pkt. 6.3 - 6.5, har vi efter GDPR artikel 19 pligt til at orientere de tredjemænd, hvortil oplysningerne måtte være videregivet, herom, med mindre en sådan orientering er umulig eller uforholdsmæssig vanskelig.

6.7 Ret til dataportabilitet

GDPR artikel 20 giver den registrerede ret til at modtage de oplysninger, som vedkommende selv har forsynet os med på et elektronisk medie i et almindeligt læsbart format. Denne ret gælder, hvor behandlingen er baseret på samtykke eller en kontrakt/aftale med den registrerede.

6.8 Forbud mod profilering og automatiske afgørelser

Der gælder efter GDPR artikel 21 – 22 et forbud mod at træffe rent automatiserede afgørelser baseret på personoplysninger, som har væsentlig retsvirkning for den pågældende. Dette rammer f.eks. automatisk screening af jobansøgere alene ud fra karaktergennemsnit. Beslutningsprocessen kan godt være understøttet af delvis automatisering, men der er altså krav på en menneskelig vurdering.

7. Adgangsbegrænsning af sager

GDPR's principper om fortrolighed indebærer, at adgangen til sagsoplysninger i et vist omfang bør begrænses. Dette gælder i sager, hvor der behandles følsomme oplysninger, eller oplysninger der i øvrigt anses for fortrolige, jf. indledningen.

Kellpo behandler alene følsomme oplysninger i personalesager. Der er udarbejdet en særskilt persondatapolitik for så vidt angår personalesager, som der henvises til i den forbindelse.

Kellpo behandler ikke følsomme oplysninger om vores kunder, leverandører eller samarbejdspartneres medarbejdere.

I forhold til persondatareglerne anbefaler Datatilsynet i dag, at private virksomheder anvender kryptering, når der sendes e-mails indeholdende følsomme oplysninger eller CPR-nummer. For at efterleve dette, er der iværksat tiltag for at oprette en sikkermailkonto hvorfra cpr. numre og øvrigt følsomme oplysninger kan sendes til og fra.

7.1 Adgangsbegrænsning i sagssystemet

Kellpo har vedtaget følgende;

Det er alene de medarbejdere, hvis ansvarsområde tilsiger adgang til kunde- leverandør- og samarbejdspartneres medarbejderoplysninger, som har adgang til oplysningerne. Oplysningerne er registrerede i Microsoft Dynamics Navision, som Kellpos direktion, produktionsansvarlige, økonomiansvarlige, salgsansvarlige samt administrationsmedarbejder har adgang til.

Der er begrænset adgang til HR-sager. Begrænsningen er som anført i fortegnelsen vedrørende personaleadministration.

7.2 Fysiske sagsakter

Så vidt det er muligt skal du undgå at have fysiske dokumenter indeholdende personoplysninger. Såfremt du har fysiske dokumenter med sådanne oplysninger, er det vigtigt, at du sørger for, at sagsmapperne håndteres fortroligt, hvilket f.eks. indebærer, at du – når forlader dit skrivebord i længere tid – skal sikre, at sager med sådanne oplysninger er pakket sammen og lagt til side.

7.3 Arkivering af kommunikation

Al kommunikation skal gemmes i Microsoft Dynamics Navision, og herefter slettes i mailindbakken såvel i indbakke, sendt post og slettet post.

Kellpo har vedtaget følgende politik vedrørende sletning af mails:

Du skal sørge for at gemme mails i Microsoft Dynamics Navision, og herefter slette mails i indbakke, sendt post og slettet post. Dette bør så vidt muligt ske hver dag, således at indbakke og sendt post hele tiden er reduceret til at indeholde helt nye mails, og gerne således, at der ikke ligger mails, som er mere end 1 måned gamle.

8. Håndtering af indsigtsanmodninger mv.

Såfremt du modtager en indsigtsbegæring fra en kontaktperson eller en medarbejder, skal Kellpos persondataansvarlige kontaktes med henblik på at tage stilling til henvendelsen og bistå med den praktiske besvarelse i henhold til særskilt instruks herom.

Indsigtsbegæringer skal fremsættes over for Ole Petersen, mail: ope@kellpo.dk.

I forbindelse med modtagelse af en indsigtsbegæring, er det vigtigt at sikre sig, vedkommende er den, han / hun giver sig ud for at være. Det er særligt vigtigt, at der ikke udleveres oplysninger om medarbejdere, før vi har sikret os, at den indsigtsbegærende er den, som personen giver ud for at være.

Såfremt der er tale om en medarbejder, og henvendelsen har en karakter, der giver anledning til nærmere overvejelse, skal den pågældende kontaktes telefonisk med henblik på at sikre, at henvendelsen reelt stammer fra den pågældende. Eksempler på forhold, der kan give anledning til nærmere overvejelse:

- Hvis pågældende skriver fra en anden e-mail end sædvanligt
- Hvis pågældende skriver fra en e-mail, som giver udtryk for at være en fællesmail, f.eks. "familienjensen@gmail.com"

Det følger af GDPR, at en dataansvarlig ikke skal besvare indsigtsbegæringer, hvis besvarelsen krænker andres rettigheder og frihedsrettigheder eller en lovbestemt tavshedspligt.

9. Sagsafslutning samt sletning og makulering af sager

Der henvises til persondatapolitikken for rekruttering vedrørende slettefrister for medarbejderoplysninger.

Personoplysninger må ikke opbevares i en længere periode end nødvendigt for at opfylde det formål, hvortil de er indsamlet, med mindre der foreligger grundlag for en videre behandling.

Det følger af produktansvarsloven, at der gælder en 10-årig forældelsesfrist for erstatningskrav i anledning af produktskade. Kellpo har derfor konkret besluttet, at der skal gælde en 10 årig slettefrist for al dokumentation og korrespondance i forbindelse med kundeordrer, således at Kellpo kan varetage sine interesser i tilfælde af, at en kunde rejser et krav mod Kellpo for produktskade idet det kan blive nødvendigt at gennemgå korrespondance i forbindelse med ordren, for at kunne afgøre et eventuelt ansvar. Forældelsesfristen/slettefristen regnes fra tidspunktet, hvor produktet er blevet bragt i omsætning af producenten, dvs. tidspunktet for overlevering af varen til kunden.

Det er ligeledes besluttet, at der gælder en 10-årig slettefrist for al dokumentation og korrespondance i forbindelse med Kellpos aflæggelse af ordrer ved leverandører for at sikre, at Kellpo kan varetage sine interesser i tilfælde af, at det bliver nødvendigt at videreføre eller selvstændigt rette et krav mod en leverandør af materialer/dele, som indgår i Kellpos produktion af varer som følge af produktskade. Forældelsesfristen/slettefristen regnes fra tidspunktet, hvor produktet er blevet bragt i omsætning af producenten, dvs. tidspunktet for modtagelsen af delene/materialerne fra leverandøren.

Det er i relation til Kellpos samarbejdspartnere besluttet, at personoplysninger skal slettes 10 år efter afslutning af korrespondancen. Kellpos samarbejdspartnere består af et advokatselskab og et revisorselskab. Advokater og revisorer er underlagt et rådgiveransvar, og der gælder i henhold til forældelsesloven en absolut forældelsesfrist på 10 år i anledning af et evt. rådgiveransvar. For at Kellpo kan varetage sine interesser i tilfælde af, at det måtte blive nødvendigt at rejse et sådant krav mod dets samarbejdspartnere, er det afgørende, at relevant korrespondance gemmes indtil forældelsesfristens udløb.

I tilfælde af, at Kellpo har kontakt til samarbejdspartnere, som ikke leverer en rådgivningsydelse, må personoplysninger som indgår i sådan korrespondance ikke gemmes længere end formålet med behandlingen af oplysningerne tilsiger.

Du skal i forbindelse med afslutningen af en ordre eller korrespondance følge nedenstående fremgangsmåde:

1. I forbindelse med afslutning af en ordre (med en kunde eller leverandør) eller korrespondance (med en samarbejdspartner), skal alle dokumenter, mails mv. gemmes i Microsoft Na-

vision. Fysiske dokumenter skal scannes ind på sagen, således at der ikke gemmes fysiske dokumenter. De fysiske dokumenter skal makuleres så snart de er scannet ind med undtagelse af originale dokumenter hvis opbevaring er nødvendig. Elektroniske dokumenter skal ligeledes lægges på sagen, og slettes fra mailindbakken, sendt post og slettet post.

2. Umiddelbart efter afslutningen af en korrespondance med en samarbejdspartner, modtagelse af bekræftelse på, at ordren er leveret til kunden, henholdsvis ved modtagelse af en ordre fra en leverandør, skal det noteres i Microsoft Dynamics Navision og medarbejderens kalender, at sagen alle personoplysninger på sagen skal slettes 10 år efter den pågældende dato.

Sletning af korrespondance vedrørende en ordre foretages af den til enhver tid værende økonomiansvarlige medarbejder.

Retningslinjer for makulering af fysiske sager:
Det anbefales generelt at undgå opbevaring af fysiske sager. Alle oplysninger bør således ligge elektronisk, hvilket gør det noget lettere at imødekomme indsigtsanmodninger mv.

Har kontoret imidlertid fysiske arkivsager, skal det sikres, at disse makuleres, hvis slettefristen er overskredet.

Retningslinjer for sletning af elektroniske sager:
For at sikre, at gamle sager ikke opbevares efter sletningsfristen, vil en af Kellpo udpeget betroet medarbejder hvert år i januar måned gennemgå alle afsluttede ordrer med henblik på at slette dokumenter mv. indeholdende personoplysninger, som er afsluttede for mere end 10 år siden.

10. Kellpos markedsføring/CRM

Behandling af personoplysninger som led i markedsføring, herunder opretholdelse af CRM-database skal ske i henhold til følgende retningslinjer:

Selve registreringen af en fysisk person med tilhørende kontaktoplysninger i en CRM-database med henblik på markedsføring er i orden ud fra en interesseafvejningsregel, men husk oplysningspligten - der skal orienteres om registreringen senest en måned efter registreringen eller ved første kontakt – afhængig af, hvad der kommer først.

Hvad du så kan bruge registreringen til i form af markedsføring, afhænger af, hvilken form for markedsføring du påtænker, jf. nedenfor.

Husk i denne sammenhæng, at såkaldt imagemarkedsføring - herunder udsendelse af nyhedsbreve eller indbydelse til gratis arrangementer – sidestilles med markedsføring, hvor der reklameres for en konkret ydelse.

Direkte markedsføring via fysisk post:

- Vi må gerne sende direkte markedsføring til navngivne personer med fysisk post, forudsat at vi forinden har tjekket, at de pågældende modtagere ikke har tilmeldt sig Robinsonlisten (forbrugere).
- Vi skal respektere, hvis modtagerne frabeder sig at modtage yderligere henvendelser fra os (gælder både forbrugere og erhverv). Dette skal således registreres i CRM-databasen.

Direkte markedsføring via telefon til erhvervsdrivende:

- Vi må gerne ringe og tilbyde en konkret ydelse eller markedsføre os mere generelt overfor erhvervsdrivende.
- Den vi ringer op, kan dog frabede sig yderligere henvendelser, og vi skal i så fald registrere dette i CRM-databasen, så de ikke bliver ringet op igen.
- Vi må ikke benytte telefonopkald til markedsføring overfor forbrugere.

Direkte elektronisk markedsføring (e-mail, SMS, messenger m.v.):

Elektronisk markedsføring må som udgangspunkt kun ske overfor personer efter forudgående samtykke fra modtageren. Er der tidligere indhentet samtykke til udsendelse af nyhedsbreve, er det tilladt at markedsføre tilsvarende produkter og services, hvis den pågældende er gjort opmærksom på, at denne kan modsætte sig markedsføring.

11. Rekruttering af medarbejdere

Deltager du i rekruttering af nye medarbejdere til Kellpo, skal du sætte sig ind i den særskilte persondatapolitik for rekruttering, som findes på Kellpos hjemmeside. Link

12. Personoplysninger om Kellpo medarbejdere – under og efter ansættelsen

Vil du som medarbejder i Kellpo vide hvordan Kellpo behandler dine personoplysninger, kan du læse nærmere herom i Kellpos medarbejderoplysning om persondata, som kan fås udleveret på kontoret.

13. Overførsel af oplysninger til udlandet

Kellpo benytter sig af følgende databehandlere uden for EU:

- Microsoft Outlook
- Microsoft Dynamics Navision

Det er vurderet, at databehandlerne har etableret et tilstrækkeligt sikkerhedsniveau til at beskytte personoplysninger fordi det af databehandleraftalerne fremgår, at de har truffet foranstaltninger for at sikre, at dine oplysninger ikke hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Datatilsynet har udtalt, at personoplysninger sikkert kan overføres til tredjelande, herunder USA i det omfang virksomhederne har tilsluttet sig EU-U.S. Privacy Shield, hvilket samtlige databehandlere har gjort.[1] Det vurderes derfor tillige på denne baggrund, at databehandlerne har etableret den fornødne sikkerhed.

14. Tvivlsspørgsmål

Er du i tvivl om forståelse af denne instruks, så spørg den person, der i Kellpo er udpeget som persondataansvarlig. Endvidere kan der henvises til vejledninger og udtalelser udstedt af Datatilsynet på følgende hjemmeside:

[1] Jf. Datatilsynets vejledning om overførsel af personoplysninger til tredjelande

- Datatilsynet www.datatilsynet.dk.