BALLERUP KOMMUNE

Til: Chefgruppen

POLITIK OG ORGANISATION
Digitalisering og Forretningsudvikling

Dato: 23. juni 2022

E-mail: gdpr-ballerup@balk.dk
Kontakt: GDPR-Team

GDPR handleplan 2022/23

Indledning
Denne handleplan beskriver indsatsområder og planlagte aktiviteter på GDPR-området i Ballerup Kommune i 2022 og 2023. Handleplanen er udarbejdet på baggrund af DPO'ens (Databeskyttelsesrådgiverens) rapport 2021 og dennes anbefalinger. GDPR-teamet indstiller handleplanens indsatsområder til godkendelse hos Chefgruppen.

Organisering af GDPR-opgaven
Det overordnede ansvar for GDPR ligger hos den øverste politiske ledelse. GDPR-teamet er en rådgivende funktion, som har til opgave at understøtte GDPR-compliance i organisationen.

GDPR-teamet består af et årsværk fordelt på to medarbejdere, som er placeret i Afsnit for Digitalisering og Forretningsudvikling i Center for Politik og Organisation.

GDPR-teamets arbejde kan inddeles i følgende områder:

1) Beredskab ved brud på persondatasikkerheden (sikkerhedsbrud)
2) Indgåelse af databehandleraftaler
3) Understøtte GDPR-compliance i organisationen, herunder sikre, at dokumentation, såsom fortegnelser over behandlingsaktiviteter, risikovurderinger, handleplaner og retningslinjer, er tilstrækkelige og ajourførte
4) Rådgive og skabe awareness om GDPR i organisationen

DPO rapport 2021
DPO'en rådgiver og fører tilsyn med Ballerup Kommune og udarbejder hvert år en rapport om efterlevelsen af persondataforordningen. I sin rapport for 2021 konkluderer DPO'en følgende:

"Ballerup Kommune har robuste processer, der sikrer tilstrækkelig og rettidig inddragelse af DPO'en i alle spørgsmål vedrørende beskyttelse af personoplysnin-

ger. Der er gode rammer for GDPR i Ballerup Kommune og et acceptabelt modenhedsniveau i organisationen. Det er dog vigtigt at fastholde fokus på den gode og tilstrækkelig databeskyttelse i alle behandlingsaktiviteter."

DPO'en anbefaler dog, på baggrund af sin gennemgang af Ballerup Kommunes GDPR-compliance, fire indsatsområder, som kræver opmærksomhed:

1. Opdatering af fortegnelser over behandlingsaktiviteter
2. Udarbejdelse af risikovurderinger for it-systemer
3. Tilsyn med logning og brugeradgange
4. Styring og ansvarsfordeling af GDPR arbejdet samt awareness-kampagner

Handleplaner:

På baggrund af DPO'ens anbefalinger og GDPR-teamets igangværende arbejde er følgende indsatsområder planlagt i hhv. 2022 og 2023. De fire anbefalede indsatser er pga. opgavernes omfang spredt ud over 2022 og 2023. Dertil har GDPR-teamet udvalgt nogle indsatsområder, som anses for væsentlige for organisationens compliance, og som kan løses sideløbende med DPO'ens anbefalede indsatser.

For hver indsats beskrives opgaven, samt planlagte eller igangsatte aktiviteter med et overslag over ressourceforbruget per hvert center.

2022:

Indsats	**Styring og ansvarsfordeling af GDPR-arbejdet samt awareness-kampagner**
Beskrivelse	DPO'en har som del af sine anbefalinger at "skabe endnu bedre ledelsesmæssig forankring af GDPR opgaven". "[der] ligger fortsat en vigtig opgave for ledelsen i at minde medarbejder om retningslinjer og god praksis for den korrekte databehandling, der gælder lokalt. Der er igangsat et godt program for awarenes, som bør suppleres af et ledelsesmæssigt fokus."
Aktiviteter	*Afrapportering til Centerchefer:* Formålet med afrapporteringen er at anskueliggøre konkrete emner og indsatsområder inden for GDPR med henblik på, at øge ledelsens kendskab til GDPR-opgaverne i deres center og understøtte GDPR-ambassadørernes rolle. GDPR-teamet vil udarbejde en årlig rapport per center. Rapporten giver en status på igangværende, tværgående indsatser, samt udpeger anbefalede indsatsområder specifikt for centeret, på baggrund af hvilke centeret udarbejder en lokal handleplan. For at styrke den lokale forankring og opgaveløsning i centrene, opstartede GDPR-teamet i efteråret 2021 et GDPR-ambassadørnetværk. Netværket er et frivilligt tilbud om sparring, videndeling og rådgivning i GDPR-relaterede opgaver. Indtil nu har netværket beskæftiget sig med udformningen af SMS-retningslinjer samt forebyggelse af sikkerhedsbrud. GDPR er forankret ledelsesmæssigt hos digitaliseringslederne, som derfor vil være modtager af afrapporteringen og have ansvar for at uddelegere opfølgning i form af eksempelvis handleplaner og tiltag i deres center, fx til GDPR-ambassadøren. Første afrapportering vil finde sted ved udgangen af 2022.

	Ressourcetræk i centrene: <10 timer Status: Indstilling til godkendelse

Indsats	**Opdatering af fortegnelser over behandlingsaktiviteter**
Beskrivelse	DPO'en anbefaler: "Fortegnelserne skal opdateres efter de seneste anbefalinger og skabeloner. Det anbefales at der etableres en proces, der sikre en løbende vedligeholdelse." Databeskyttelsesforordningen stiller krav om, at alle dataansvarlige og databehandlere fører interne fortegnelser over deres behandling af personoplysninger (jf. GDPR, artikel 30). Fortegnelser er en kortlægning af, hvilke personoplysninger kommunen behandler, og om hvem. Konsekvensen for manglende fortegnelser kan føre til alvorlig kritik fra Datatilsynet og mulighed for bøde. Kommunens nuværende fortegnelser blev udarbejdet i 2018 og er ikke blevet ajourført. I 2020 udkom Datatilsynet med en ny vejledning, som sætter nye, højere krav til detaljeniveauet i fortegnelserne. Disse forhold gør, at kommunens nuværende fortegnelser ikke lever op til lovgivningen. Opdateringen af fortegnelserne ift. de nye krav er en omfattende opgave. Dog forventes det, at den indsats, der udføres i 2022 ikke skal gentages, hvis centrene sikrer løbende ajourføring af deres fortegnelser fremover.
Aktiviteter	*1) Udarbejdelse af nye fortegnelser over behandlingsaktiviteter:* Formålet med aktiviteten er at bringe kommunens fortegnelser op på et tilstrækkeligt niveau til at overholde lovgivningen med udgangspunkt i Datatilsynets vejledning. Opgaven kræver en tværfaglig indsats mellem GDPR-teamet og centrene, da kortlægningen bygger på et indgående kendskab til de konkrete behandlinger af personoplysninger, der finder sted i løsningen af opgaverne. Opgaven forankres hos digitaliseringslederne, som kan uddelegere udførelsen, fx til GDPR-ambassadørerne. GDPR-teamet udarbejder grundige vejledninger til opgaven og vil løbende stå til rådighed for sparring og rådgivning. Der er indkøbt et it-værktøj (Wired Relations) til indtastning af fortegnelserne, der sikrer bedre overblik og vil lette arbejdsgange og uddelegering. GDPR-ambassadørerne vil modtage fælles oplæring i både værktøj og opgaven til netværksmøder i efteråret. Ressourcetræk i centrene: 30-40 timer Status: igangsat

Indsats	**Procedurer for billed-/video-samtykke**
Beskrivelse	For at indhente og behandle personoplysninger skal der altid være et retligt behandlingsgrundlag. Billeder og video er iht. GDPR personoplysninger. Ved brug af billeder/video til fx markedsføring, kommunikation og rekruttering er behandlingsgrundlaget samtykke fra den eller de personer, der optræder på billederne. Samtykke er frivilligt, eksplicit, konkret og tidsbegrænset (Jf. GDPR artikel 6). Billeder/video må kun bruges og opbevares, så længe samtykket er gældende. Procedurer og tilhørende it-tekniske løsninger for indhentning og håndtering af samtykke til brug af billeder/video skal sikre, at billedmateriale kun bruges, når der er et gyldigt samtykke fra personer på billedet, at samtykke kan trækkes tilbage, og at data slettes rettidigt.

	På nuværende tidspunkt eksisterer der ikke procedurer for systematisk og juridisk vandtæt håndtering af billed-/videosamtykke på tværs af organisationen. Dette kan medføre alvorlig kritik eller bøder fra Datatilsynet.
Aktiviteter	En kortlægning af behov og arbejdsgangene omkring billeder og video-materiale på tværs af organisationen med henblik på at sikre den nødvendige organisatoriske og tekniske understøttelse af indhentning, opbevaring og sletning, så samtykkeerklæringer udfyldes juridisk korrekt, og billeder opbevares sikkert og kun i den tilladte periode. Ressourcetræk i centrene: internt i C-PO Status: Procedure for indhentning og håndtering af samtykke er færdiggjort. Procedure for opbevaring og sletning afventer.

Indsats	**E-læring & GDPR-onboarding**
Beskrivelse	DPO'en skriver: "Det anbefales at få e-læringsværktøjet op og køre og fortsæt med at være tilstede i organisationen og formidle GDPR på en nærværende måde. Det skal dokumenteres at der er gennemført undervisning/e-læring af alle medarbejdere." Der er desuden, i dialog med GDPR-ambassadørnetværket, afdækket behov for systematisk og ensartet on-boarding for nye medarbejdere. E-læringsværktøjet kan blive en vigtig del af on-boardingen, suppleret af Ballerup-specifikke retningslinjer.
Aktkiviteter	Der er allerede indkøbt et LMS-system med 2 kurser; 1) GDPR og 2) informationssikkerhed. Der lægges en udrulningsplan, hvori det afdækkes, hvilke medarbejdergrupper, der skal omfattes i e-lærings-systemet. I forbindelse med udviklingen af det nye INTRA bliver alle GDPR-relaterede vejledninger og undervisningsmaterialer gennemgået, og GDPR-netværket inddraget i tilrettelæggelse af en on-boarding-pakke. Ressourcetræk i centrene: ? Status: udrulning planlægges

2023:

Indsats	**Udarbejdelse af retningslinjer for brug af Outlook**
Beskrivelse	Der har i 2021 og 2022 været flere brud på persondatasikkerheden som følge af forkert brug af Outlook e-mails og kalender og manglende sletning af personoplysninger. Der findes ikke pt. GDPR-retningslinjer for brugen af Outlook på tværs af hele organisationen.
Aktiviteter	GDPR-teamet lægger op til at udarbejde nye retningslinjer for korrekt og datasikker brug af Outlook, herunder hvordan medarbejderne skal indstille deres Outlook kalender, samt frister for sletning af e-mails med personoplysninger. Ressourcetræk i centrene: <10 Status: igangsættes efter sommerferien

Indsats	**Udarbejdelse af risikovurderinger for it-systemer**
Beskrivelse	DPO'en anbefaler "at få udarbejdet risikovurderinger for de behandlingsaktivitet og it-løsninger der indeholder persondata. Det anbefales at der skabes et overblik over, om der

	mangler at blive udarbejdet konsekvensanalyser (DPIA) på behandlingsaktiviteter og it-løsninger." Iht. Databeskyttelsesforordningen skal den dataansvarlige udarbejde risikovurderinger for behandlingsaktiviteter med henblik på at foretage passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de identificerede risici (Artikel 32). Der er på nuværende tidspunkt udarbejdet et begrænset antal risikovurderinger for it-systemer i Ballerup Kommune. Risikovurderingerne skal ajourføres årligt, eller når ændringer påkræver det, men ajourføring er endnu ikke implementeret tilstrækkeligt hos systemadministratorerne.
Aktiviteter	GDPR-teamet har udarbejdet en model for risikovurderinger for it-systemer, som kan udarbejdes for alle systemer, der behandler personoplysninger. Opgaven kræver et tværfagligt samarbejde mellem GDPR-teamet og en it-tekniske kompetence og/eller en fagperson, som kan beskrive, hvordan data behandles i det pågældende it-system. Ressourcetræk i centrene: uafklaret Status: igangsættes i 2023

Indsats	**Interne tilsyn med logning og brugeradgange**
Beskrivelse	DPO'en anbefaler: "Det anbefales at der indføres en struktureret og dokumenteret proces for logning af it-brugere i kommunens it-systemer der behandler personoplysninger. Datatilsynet anbefaler tilsyn på udvalgte bruger 3-4 gange om året, for systemer der behandler mange følsomme persondata om borgerne" Iht. princippet om integritet og fortrolighed i GDPR må personoplysninger kun tilgås af de medarbejdere, der har behov for at se dem for at løse deres opgave over for borgeren. Hvis personoplysninger tilgås af uvedkommende, herunder medarbejdere i kommunen, der ikke har et formål med at tilgå oplysningerne, er der tale om brud på persondatasikkerheden.
Aktiviteter	Der foretages årligt stikprøver af brugeradgange og adgangskontrol. Det er centrene selv, der udfører tilsynet med understøttelse af GDPR-teamet. Ressourcetræk i centrene: <10 timer Status: igangsættes i 2023

Indsats	**Gennemgang af sletteprocedurer og retningslinjer**
Beskrivelse	Den registreredes personoplysninger kan alene behandles, hvis der er et lovligt grundlag. Den dataansvarlige må vurdere, hvor lang en periode det vil være relevant at opbevare oplysningerne (Jf. Artikel 5 om opbevaringsbegrænsning og 6 om formålsbegrænsning). Det forventes, at arbejdet med fortegnelser vil synliggøre eventuelle huller i sletteprocedurer eller retningslinjer for behandling af personoplysninger, som vil kræve handling i det nye år.
Aktiviteter	Der igangsættes en systematisk gennemgang af sletteprocedurer, der sikrer rettidig sletning af alle personoplysninger. GDPR-teamet faciliterer eventuelle manglende lokale retningslinjer, som arbejdet med fortegnelser måtte afdække. Ressourcetræk i centrene: uafklaret Status: igangsættes i 2023

Opgaver i pipeline:
Følgende indsatsområder er i GDPR-teamets pipeline, da de anses for væsentlige for organisationens compliance og persondatasikkerhed. Indsatserne er endnu ikke planlagt, men vil blive inkluderet i det omfang, det er muligt at allokere ressourcer til dem. Chefgruppen vil blive orienteret om igangsættelse af disse indsatser, når det bliver aktuelt.

Indsats	**Nye retningslinjer for sikkerhed på mobile enheder**
Beskrivelse	Flere og flere af kommunens ansatte bruger mobile enheder som mobiltelefoner og tablets til at behandle personoplysninger i forbindelse med deres arbejde. Mobile enheder er generelt omfattet af en lavere sikkerhed end pc, og mange apps får vidtrækkende adgang til data på enhederne, hvis de downloades. Derfor vil det være formålstjenligt at udarbejde retningslinjer for sikkerhedsindstillinger, opsætning og brug af applikationer.

Indsats	**Oplysningspligten og de registreredes rettigheder**
Beskrivelse	I databeskyttelsesforordningen gælder der særlige rettigheder for personer (de registrerede), når der indsamles og behandles personoplysninger om dem (GDPR, artikel 15-22). For at den registrerede kan benytte sig af sine rettigheder, skal de kende dem. Af denne grund skal kommunen som dataansvarlig oplyse de registrerede om, at deres personoplysninger indsamles. Dette kaldes oplysningspligten (jf. GDPR artikel 13 og 14). Opgaven går ud på at sikre, at kommunen oplyser den registrerede tilstrækkeligt i alle situationer, hvor kommunen indsamler personoplysninger. I 2021 blev oplysningspligten gennemgået på tværs af alle online formularer, hvor borgere giver personoplysninger. Der bør foretages en lignende gennemgang af andre situationer, hvor borgere giver oplysninger til kommunen og af eksisterende tekster på hjemmesiden og i brevskabeloner.