Om dette regneark..

Formål
At skaffe et overblik over relevante kontroller, som med fordel kan gennemføres for at afgøre graden af GDPR compliance.
At dokumentet kan udvikle sig over tid og blive til en bruttoliste for kontroller.

Anvendelse
Regnearket skal ses som inspiration til forskellige GDPR kontroller.
Hvad der er relevant for netop din virksomhed eller institution bliver du nødt til at arbejde dybere i.

Bidrag
Da du frit kan anvende dokumentet, forventer initiativtageren, at du også bidrager, hvis du har tilføjelser, korrektioner, mv.
Send gerne input, kommentarer mv. til initiativtageren, se nedenfor.

Copyright
Regnearket og indholdet kan frit anvendes.
Når du bidrager til regnearket, vil dine input kunne blive delt med andre.
Du kan ikke påberåbe dig rettigheder til dokumentet eller informationer hentet fra dokumentet.

Ansvarsfraskrivelse
Initiativtageren og dennes virksomhed kan ikke holdes ansvarlig for indhold og anvendelse af indholdet i dette regneark.
Der er således fuldstændig ansvarsfraskrivelse ved download og brug af regnearket/indholdet i regnearket.

Inititativtager
Initiativtageren til dokumentet er Poul Qvist Christensen
pqc@qvistmanagement.dk
telefon 30234013

Bidragsydere
Rasmus Carstensen, Eniig

Hovedemne	Emne	Kontrol	Status/Bemærkning
Politik			
	Politik for GDPR, kunder, medarbejdere	Er der udarbejdet en politik for GDPR * Kunder * Borgere * Medarbejdere	
	DPO	Er roller og ansvar for DPO beskrevet?	
	DPO	Udfylder DPO det beskrevne?	
	Lokal GDPR ansvarlig (hvis relevant)	Er roller og ansvar for Lokal GDPR ansvarlig beskrevet?	
	Lokal GDPR ansvarlig (hvis relevant)	Udfylder Lokal GDPR ansvarlig det beskrevne?	
	Dataansvarlig	Er det fastlagt i hvilke situationer virksomheden er dataansvarlig	
	Databehandler	Er det fastlagt i hvilke situationer virksomheden er databehandler	
	Privatlivspolitik på hjemmeside	Er der offentliggjort en fyldestgørende privatlivspolitik på hjemmesiden	
Regler(retningslinjer)/Processer			
	Fortegnelse	Er der fastlagt regler for opdatering af fortengelsen, ansvar og hyppighed	
	Nye behandlingsaktiviteter	Er der regler for vurdering af nye behandlingsaktiviteter i forhold til risikovurdering, konsekvensanalyse, dataminimering, privacy by design, standardindstillinger, behandlingssikkerhed, mv.	
	Ændring af behandlingsaktiviteter	Er der regler for hvornår ændringer i behandlingsaktiviteterne medfører vurdering i forhold til risikovurdering, konsekvensanalyse, dataminimering, privacy by design, standardindstillinger, behandlingssikkerhed, mv.	
	Nye systemer/ændrede systemer	Dataminimering, Privacy by design, Standardindstillinger	
	Risikovurdering	Er der regler for hvornår der skal laves risikovurdering og forefindes model for hvordan risikovurdering gennemføres	
	Konsekvensanalyse	Er der regler for hvornår der skal laves konsekvensanalyse og forefindes der model for hvordan konsekvensanalyse gennemføres	
	Databehandleraftaler, fortrolighedserklæringer	Er der regler og proceser for hvornår og hvordan der skal laves databehandleraftaler eller fortrolighedserklæringer	
	Sletning af personoplysninger	Er der regler for hvornår personoplysninger slettes eller anonymiseres	
	Håndtering af databrud	DPO, datatilsynet, den registrerede	
	Oplysningspligten	Findes der en processer for overholdelse af oplysningespligten	
	Håndtering af henvendelser fra den registrerede	Er der processer for håndtering af henvendelser fra registrede personer (kunder, ansatte, mm.)	
	Kontroller	Er der en plan for GDPR kontroller	
	Auditplan	Er der en auditplan for GDPR compliance	
Awareness			
	Kendskab til GDPR	Er kendskabet til GDPR, herunder virksomhedens forpligtigelser og ansvar kommunikeret til ledere og medarbejdere?	
	Leveregler GDPR	Er der kommunikeret GDPR leveregler til ledere og medarbejdere?	
	Leveregler ISMS	Er der kommunikeret ISMS leveregler til ledere og medarbejdere?	
	Hvad er et databrud	Er det kommunikeret til ledere og medarbejdere hvad der betragtes som et databrud	
	Håndtering af databrud	Er det kommunikeret til ledere og medarbejdere hvordan processen for et databrud er?	
	Implementering	Er der konkrete GDPR tiltag som er nødvendige i pågældende afdeling/team implementeret så medarbejderne ved præcist hvad de skal foretages sig i forhold til GDPR?	
Dokumentation			
	Fortegnelse	Er alle behandlingsaktiviteter dokumenteret, er minimumskravene til oplysninger overholdt	
	Databehandleraftaler	Er der indgået databehandleraftaler, Indeholder de det de skal, er alt udfyldt. Er alle databehandleraftalerne arkiveret/journaliseret korrekt. Er liste over databehandleraftlerrelationer ajourført. Er der plan for tilsyn af databehandleraftaler.	
	Konsekvensanalyse (DPIA)	Er gennemførte konsekvensvurderinger dokumenteret	
	Passende sikkerhedsniveau	Dokumentation af databeskyttelse med passende tekniske og organisatoriske foranstaltninger, herunder behandlingssikkerhed	
Personoplysninger			
	Alm	Behandles der almindelige personoplysninger	
	Navne og adresse beskyttelse	Behandles personoplysninger omfattet af adressebeskyttelse. Er der tilstrækkelig behandlingssikkerhed?	
	Fortrolige personoplysninger (CPR, mm.)	Behandles fortrolige personoplysninger. Er der tilstrækkelig behandlingssikkerhed?	
	Straf	Behandles oplysninger om strafbare forhold. Er der tilstrækkelig behandlingssikkerhed?	
	Følsom	Behandles følsomme personoplysninger. Er der tilstrækkelig behandlingssikkerhed?	

Hovedemne	Emne	Kontrol	Status/Bemærkning
Indsamling			
	Formålsbestemthed	Indsamles der kun det der er nødvendigt for formålet	
	Dataminimering	Bliver der indsamlet flere data end der bruges	
	Sletning efter formål	Bliver data slettet når formålet ikke er til stede længere, formularer, mail, drev, systemer	
	Datakilde, den rigistrerede - indhentning af data	Overholdes oplysningspligten i forbindelse med indsamling af data	
	Formål	Bruges data kun til det oplyste formål	
Behandling			
	Hjemmel	Er der korrekt hjemmel til alle behandlinger	
	Lov, retslig forpligtigelse	Behandles personoplysninger efter lov eller retslig forpligtigelse, dokumentation for dette	
	Kontrakt, aftale	Behandles personoplysninger som led i en kontrakt eller aftale	
	Interesseafvejning	Er anvendelse af interesseafvejningsprincippet anvendt korrekt	
	Begrænsning af formål	Er alle behandlinger af personoplysninger begrænset til det formål de er indsamlet til	
	Andre formål	Behandles personoplysninger til andre formål end de er indsamlet til	
	Samtykke	Er alle samtikker frivilligige, specifikke, informeret, skriftelige, med mulighed for tilbagekaldelse, er de dokumenteret	
	Tilbagetrækning af samtykke	Kan tilbagetrækning af samtykke håndteres	
	Offentliggørelse	Offentliggørelse af oplysninger, billeder	
Den registreredes rettigheder			
	Oplysningspligt	I hvilken grad overholdes oplysningspligten. Ved afgivelse, indsamling fra andre, frister for afgivelse, indhold af oplysningspligt	
	indsigtsret	Fungerer processen, og er der sikring af identiteten på personen	
	Berigtigelse, korrekte og ajourførte	Fungerer processen	
	Ret til begrænsning i behandling	Fungerer processen	
	Sletning - blive glemt	Hvad kan den registrede bede om at få slettet, uden for den automatiserede sletterutine	
	Indsigelsesret	Fungerer processen	
	Automatiske afgørelser, herunder profilering	Laves der automatiske afgørelser, laves der profileringer	
	Dataportabilitet	Er dataportabilitet muligt, hvis ja, hvad kan porteres	
Opbevaring af personoplysninger			
	Oplysningspligt	Oplyses den registrerede om hvor persondata opbevares, fx ved opbevaring i 3. lande	
	Placering af persondata	Er der overblik over hvor data opbevares (Intern, eksternt, 3. lande)	
	Sletning af data	Er der kontrol over den automatiserede sletterutine. Er der en proces for manuelle sletninger, de steder hvor der ikke er automatisering	
Videregivelse eksternt			
	Videregivelse	Videregives personoplysningerne til andre parter, hvilken hjemmel	
	Videregivelse, fortrolighed	De steder hvor modtager er selvstændig dataansvarlig, Er der indgået fortrolighedserklæringer	
	Overdragelse	Overdrages data til en databehandler, er den registrerede orienteret om dette	
	Databehandleraftaler	Er der indgået databehandleraftaler med alle identificerede parter, er der plan for tilsyn af databehandleraftaler	
	Data uden for EU	Sendes data uden for EU? Hvis ja, er det på lovligt grundlag?	
Behandlingssikkerhed			
	Sikkerhedspolitik	Finder der en sikkerhedspolitik i koncernen?	
	Risikovurdering	Er der laves risikovurderinger for alle behandlingsformål?	
	Organisatoriske foranstaltninger	Er der iværksat passende organisatoriske foranstaltninger med udgangspunkt i en risikovurdering	
	Tekniske foranstaltninger	Er der iværksat passende teknsike foranstaltninger med udgangspunkt i en risikovurdering	
	Kryptering	Krypteres data, opmærksomhed på mailafsendelse	
	Backup/Restore	Laves der backup af data, så det kan genskabes hvis data mistes	
	Fysisk beskyttelse	Hvilke tiltag er der i forhold til fysisk beskyttelse af data. Sikring af arkivskabe, arkivrum eller lignende	
	+ mange flere se ISO 27001/02	Se evt. SoA(Statement of Applicability) for ISO27001	

Poul Qvist Christensen, pqc@qvistmanagement.dk, 30 23 40 13