
TILSYNSDOKUMENT

I

Maxtel.dk ApS

Tilsyn udført af	:	Peter Serop
Dato for tilsyn	:	03-08-2021
Godkendt af	:	Matt Krank
Dato for godkendelse	:	09-08-2021

TILSYNSDOKUMENT

Indholdsfortegnelse

1.	Ansvarlige	2
2.	Den Dataansvarliges forpligtigelser.....	2
3.	Systemoversigt	2
4.	Udførelse af egenkontrol	5
5.	Tilsynsspørgsmål	5

Maxtel.dk ApS gør brug af en ekstern og uafhængig tredjepart for tilsyn og egenkontrol af virksomheden.

Tilsynet afdækker de tekniske og organisatoriske sikkerhedsforanstaltninger, der måtte være heri og tilsynet udføres via skriftlig informationsindsamling.

Skemaet er udarbejdet til brug for tilsyn af virksomhedens behandling af personoplysninger og udføres årligt af ekstern og uafhængig tredjepart.

1. Ansvarlige

Understående er ansvarlig for udførelse af ekstern egenkontrol af Maxtel.dk ApS

Ekstern GDPR-ansvarlig	Ansatte. ApS
	CVR nr.: 29135789
	Nyvej 9, 4261 Dalmore
	www.ansatte.dk
	Peter Serop
	peter@ansatte.dk
	93102032

2. Den Dataansvarliges forpligtigelser

Jf. databeskyttelsesforordningens art. 32 skal Den dataansvarlige gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, som passer til de risici, der er forbundet med behandlingen af virksomhedens persondata.

3. Systemoversigt

Herunder tilføjes alle de IT-systemer hvor virksomheden behandler persondata

SYSTEM – 1	Office 365 – Outlook
IT-system	Mailprogram fra Microsoft
Risikovurdering af system	Lav
Bemærkninger	Anvendes som mailprogram i hele virksomheden.
Indehold af persondata	Navn, mail, beskeder – alt relaterede til generelle mails. Der er udarbejdet slettepolitikker alt efter hvilken afd. Der anvender mailprogrammet
Sikkerhed	Der anvendes Office 365, hvor sikkerhedsniveauet er større.

SYSTEM – 2	Danløn
IT-system	Lønssystem
Risikovurdering af system	Lav
Bemærkninger	Anvendes til lønkørsel
Indehold af persondata	Alm. Persondata jf. Art. 6 - iht. bogføringsloven
Sikkerhed	Danløn er udviklet af Danske Lønssystemer A/S, som er ejet af Lessor Group, der løbende får udarbejdet en IT-revisorerklæring ISAE 3402 Type II samt IT-revisorerklæring ISAE 3000 Type II

SYSTEM – 3	e-conomic
IT-system	Bogføring, fakturering og regnskab
Risikovurdering af system	Lav
Bemærkninger	Anvendes i økonomiafdelingen
Indehold af persondata	Alm. Persondata jf. Art. 6 - iht. bogføringsloven
Sikkerhed	e-conomic, som ejes af Visma får løbende udarbejdet en ISAE 3402 Type 2 rapport. Yderlig gør de brug af isae 3000

SYSTEM – 4	Slack.com (Projektstyring & intern kommunikation)
IT-system	Persondata vil kunne forekomme.
Risikovurdering af system	Middel
Bemærkninger	Anvendes dels i supporten
Indehold af persondata	Alm. Persondata jf. Art. 6
Sikkerhed	Slack har flere sikkerhedscertificeringer fra <i>American Institute of Certified Public Accountants</i> heraf SOC 2 og SOC 3. Slack anvender internationale anerkendte sikkerhedscertificeringer såsom ISO 27001 (informationssikkerhedsstyringssystem), ISO 27017

	(sikkerhedskontrol til levering og brug af cloud -tjenester) og ISO 27018 (til beskyttelse af personlige data i skyen).
--	-------------------------------------------------------------------------------------------------------------------------

SYSTEM – 5	Teleudbydere (Telenor, TDC, inMobile)
IT-system	Hoveddata/system leveres af leverandør, hvorefter Maxtel selv koder backend og frontend.
Risikovurdering af system	Middel
Bemærkninger	Der er tale om Wholesale aftaler
Indehold af persondata	Alm. Persondata jf. Art. 6, CPR-nummer. Jf. §11, Følsomme oplysninger jf. Art 9, Strafbare forhold jf. §8
Sikkerhed	Telenor efterlever ISO 27001 (Yderlig leverer de årligt en Authority Requests Disclosure report TDC har en ISAE 3402 Type 2 revisionserklæring inMobile får årligt udarbejdet en ISAE 3000 erklæring af Deloitte

SYSTEM – 6	DLX
IT-system	Hosting & Backup
Risikovurdering af system	Middel
Bemærkninger	Anvendes til hosting og backup i virksomheden
Indehold af persondata	Alm. Persondata jf. Art. 6, CPR-nummer. Jf. §11, Følsomme oplysninger jf. Art 9, Strafbare forhold jf. §8 <i>Da der tages backup, kan vi ikke frasige os, at der foretages behandling af ovenstående persondata</i>
Sikkerhed	DLX årligt udarbejdet en ISAE3402 erklæring af Deloitte

SYSTEM – 7	Dropbox
IT-system	Fildeling
Risikovurdering af system	Middel
Bemærkninger	Anvendes til fildeling i virksomheden

Indehold af persondata	Alm. Persondata jf. Art. 6, CPR-nummer. Jf. §11, Følsomme oplysninger jf. Art 9, Strafbare forhold jf. §8 <i>Da der er tale om fildeling, kan vi ikke frasige os, at der foretages behandling af ovenstående persondata.</i>
Sikkerhed	Dropbox anvender ISO 27001 (informationssikkerhedsstyringsystem), ISO 27018 (til beskyttelse af personlige data i skyen), HIPPA / HITECH, Germany BSI C5, and SOC 1, 2, and 3.

4. Udførelse af egenkontrol

Den dataansvarlige oplyser at have gennemført egenkontrol ved udfyldelse af understående oplyste tilsynsspørgsmål, samt at denne har fået foretaget tilsyn iht. tredjepart.

5. Tilsynsspørgsmål

Tilsynet føres via skriftlig informationsindsamling hos Den dataansvarlige.

GRUNDLÆGGENDE PRINCIPPER – DATABESKYTTELSESFORORDNINGENS ART. 5				
Den dataansvarlige har implementeret procedurer og kontroller som sikre - <i>indsamling, behandling og opbevaring</i> af personoplysninger i overensstemmelse med principperne for behandling heraf.				
Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
		<i>Efterleves behandlingen af kontrolmål?</i>		
1	Der anvendes praktiske procedurer, der sikrer de grundlæggende principper for behandling: <ul style="list-style-type: none"> - Lovlighed, rimelighed og gennemsigtighed af behandlingen - Formålsbegrænsning - Dataminimering - Personoplysningernes rigtighed - Opbevaringsbegrænsning - Integritet og fortrolighed 	X		<i>Ingen anmærkninger</i>
2	Der foretages løbende kontrol af, at principperne for behandling af personoplysninger overholdes.	X		<i>Ingen anmærkninger</i>
3	Procedurerne opdateres løbende og efter behov iht. nedskrevne retningslinjer herfor.	X		<i>Ingen anmærkninger</i>

FORTEGNELSER OVER BEHANDLINGSAKTIVITETER – DATABESKYTTELSESFORORDNINGENS ART. 30				
Den dataansvarlige har lavet fortegnelse over dennes behandling af dennes behandling af persondata				
Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
		<i>Efterleves</i>		

		behandlingen af kontrolmål?		
1	Den dataansvarlige har et klart overblik over alle it-systemer, fysiske it-faciliteter, outsourcing, cloud-løsninger, Apps, SAAS-løsninger mv., hvor personoplysninger opbevares	X		<i>Ingen anmærkninger</i>
2	Er der udarbejdet en fortegnelse for behandling af den dataansvarliges personoplysninger?	X		<i>Ingen anmærkninger</i>
3	Foreligger der en klar ansvarsfordeling for opdatering og kvalitetskontrol af fortegnelsen?	X		<i>Ingen anmærkninger</i>
4	Opdateres fortegnelsen minimum én gang årligt og altid i forbindelse med større ændringer?	X		<i>Ingen anmærkninger</i>
5	Kan der ved anmodning herom fremvises en fortegnelse, som er opdateret inden for de sidste 12 måneder?	X		<i>Ingen anmærkninger</i>
6	Hvornår har Den dataansvarlige sidst gennemgået fortegnelserne?			Besvar: 02. juni 2021

LOVLIG BEHANDLING – DATABESKYTTELSSEFORORDNINGENS ART. 6

Sikre den dataansvarlige det retlige grundlag (hjemmel) for behandlingen af dennes behandling af personoplysninger ved dokumentation i f.eks. hjemmellister, som løbende opdateres.

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
		<i>Efterleves behandlingen af kontrolmål?</i>		
1	Der er udarbejdet dokumentation, hvor de enkelte retlige grundlag (hjemmel) fremgår	X		Størstedelen er udarbejdet for HR – da det er den funktion, som behandler flest persondata
2	Dokumentationen for det retlige grundlag (hjemmel) opdateres løbende og i det omfang, der indføres nye behandlingssystemer eller lignende.	X		<i>Ingen anmærkninger</i>
3	Der foretages ikke behandling af persondata uden et retligt grundlag (hjemmel).	X		<i>Ingen anmærkninger</i>
4	Der er lavet kontrolforanstaltning, som sikrer at der ikke sker behandling af personoplysninger uden retligt grundlag (hjemmel).	X		<i>Ingen anmærkninger</i>

PERSONFØLSOMME OPLYSNINGER – DATABESKYTTELSESFORORDNINGENS ART. 9 og 10

Behandling af personoplysninger vedrørende straffedomme, lovovertrædelse og særlige kategorier, behandles kun efter klar instruks fra den dataansvarlige og med de fornødne garantier for behandlingens sikkerhed.

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
1	Er der udarbejdet skriftlige retningslinje, politik, vejledning, procedure, som sikrer, at behandling af personfølsomme oplysninger?	X		
2	Den dataansvarlige foretager løbende kontrol af, om der er sket behandling af personfølsomme oplysninger uden forudgående instruks	X		Dette sker årligt via audit

OPLYSNINGSPLIKT – DATABESKYTTELSESFORORDNINGENS ART. 13 og 14

Der er lavet og fremsendt skriftlige procedure mv. som sikrer, at den registrerede modtager tilstrækkelig information ved indsamlingen af dennes personoplysninger, dennes rettigheder, klagemuligheder mv.

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
1	Der er udarbejdet en skriftlig politik som sikrer, at den registrerede modtager oplysning såsom: <ul style="list-style-type: none"> - Kontaktoplysninger på Den dataansvarlige og den GDPR-ansvarlige - Formål, og hjemmelsgrundlaget for behandlingen - Evt. modtagere eller kategorier af modtagere - Evt. overførsel til tredjelande eller internationale organisationer 	X		Ingen anmærkninger
2	Der er udarbejdet og implementeret politikker som sikrer, at den registrerede modtager yderlige oplysninger om: <ul style="list-style-type: none"> - Perioden for opbevaring af personoplysningerne 	X		Ingen anmærkninger

	<ul style="list-style-type: none"> - Dennes rettigheder, heraf; Retten til indsigt, berigtigelse, sletning og begrænsning i behandlingen - Tilbagekaldelse af evt. samtykke - Klagemuligheder - Evt. profilering 			
3	De omtalte politikker efterleves og opdateres løbende efter behov.	X		<i>Ingen anmærkninger</i>
4	Der foretages løbende kontrol af, at de registrerede har modtaget de oplysninger, som de har krav på, herunder deres rettigheder.	X		Dette sker årligt via audit

INDSIGTSANMODNINGER – DATABESKYTTELSESFORORDNINGENS ART. 12 og 15

Den dataansvarlige kan udlevere oplysninger iht. behandlingen af den registreredes personoplysninger i skriftligt format på en gennemsigtig og letforståelig måde.

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
		<i>Efterleves behandlingen af kontrolmål?</i>		
1	Forefindes der allerede skriftlige vejledninger for besvarelse og håndtering af anmodninger fra registrerede om indsigt.	X		Der er udarbejdet vejledning iht. Håndtering af indsigtsbegæring samt en skabelon for indsigtsbegæring
2	Vejledningen sikrer, at anmodninger besvares skriftligt, fyldestgørende og indenfor gældende frister, samt at eventuelle afslag begrundes	X		<i>Ingen anmærkninger</i>
3	Den dataansvarlige har en politik for at videregive oplysninger i en letforståelig og gennemsigtig form.	X		<i>Ingen anmærkninger</i>
4	Er der modtaget indsigtsanmodninger siden sidste tilsyn		X	Hvis, ja - Angiv antal: <i>Hvis udfyldt vedlægges minimum et anonymiseret eksemplar på en indsigtsbegæring. (Dato bedes fremgå)</i>
5	Hvor mange indsigtsanmodninger er besvaret indenfor 1 måned efter modtagelsen heraf			Angiv antal: 0 <i>Hvis udfyldt vedlægges minimum et anonymiseret eksemplar på en indsigtsbegæring. (Dato bedes fremgå)</i>
6	Er der indsigtsanmodninger som jf. Databeskyttelsesforordningens retningslinjer ikke er besvaret rettidigt?		X	Hvis, ja - Angiv antal: <i>Hvis udfyldt vedlægges minimum et anonymiseret eksemplar på en indsigtsbegæring. (Dato bedes fremgå)</i>
7	Har Den dataansvarlige underrettet den registrerede om, at der sker forlængelse af			Hvis, nej (Uddyb hvorfor): <i>Der er ikke modtaget nogen</i>

	svarfristen senest 1 måned efter modtagelsen af henvendelsen sammen med begrundelse herfor?			
8	Den dataansvarlige kontrollerer løbende, at indsigtanmodninger fra registrerede besvares korrekt og rettidigt indenfor 30 dage fra modtagelse.	X		Den GDPR-ansvarlige vil ved en indsigtanmodning håndtere denne

BERIGTIGELSE, SLETNING OG BEGRÆNSNING AF OPLYSNINGER – DATABESKYTTELSESFORORDNINGENS ART. 16, 17, 18 og 19

Den dataansvarlige har nedskrevet retningslinjer for *berigtigelse*, *sletning* og *begrænsning* ved behandlingen af personoplysninger, herunder at det sker uden unødigt ophold. Der er endvidere nedskrevet retningslinjer for besvarelse og videregivelse ved anmodninger herom til eventuelle modtagere af oplysningerne.

Nr.	Spørgsmål	Ja Nej		Evt. Kommentar
		Efterleves behandlingen af kontrolmål?		
1	Forefindes der allerede skriftlige vejledninger der fastlægger en procedure for at berigtige ukorrekte eller ufuldstændige oplysninger uden unødigt ophold?	X		<i>Ingen anmærkninger</i>
2	Der er lavet vejledninger der sikrer sletning af personoplysninger uden unødigt ophold, såfremt: - Behandlingen ikke længere er nødvendig for opfyldelse af behandlingens formål - Et samtykke tilbagetrækkes - Der sket ulovlig behandling	X		<i>Ingen anmærkninger</i>
3	Der er lavet en vejledning som sikrer, at behandlingen af personoplysninger begrænses, hvis den registrerede har en berettiget indsigelse.	X		<i>Ingen anmærkninger</i>
4	Forefindes der allerede tekniske foranstaltninger i f.eks. IT-systemerne, som muliggør <i>berigtigelse</i> , <i>sletning</i> og <i>begrænsning</i> af persondata hos Den dataansvarlige?		X	Hvis, ja (Uddyb hvilke): Hvis, nej (Uddyb hvorfor): IT-system er tredjepart, hvorved virksomheden ikke har indflydelse herpå

DATAPORTABILITET OG INDSIGELSE – DATABESKYTTELSESFORORDNINGENS ART. 20 og 21

Den dataansvarlige har nedskrevet retningslinjer for *Dataportabilitet* og *indsigelse* ved behandlingen af personoplysninger.

Nr.	Spørgsmål	Ja Nej		Evt. Kommentar
		Efterleves		

		<i>behandlingen af kontrolmål?</i>		
1	Den dataansvarlige har udarbejdet retningslinjer, politikker, vejledninger eller procedure for Indsigelse	X		
2	Forefindes der allerede tekniske foranstaltninger i f.eks. IT-systemerne, som muliggør <i>Dataportabilitet</i> af persondata hos Den dataansvarlige?		X	Hvis, ja (Uddyb hvilke): Hvis, nej (Uddyb hvordan en anmodning herom så vil foregå): Dette vil ske via en manuel proces foretages af den GDPR-ansvarlige
3	Den dataansvarlige opdaterer løbende alle retningslinjer, politikker, vejledninger eller procedure iht. <i>Dataportabilitet</i> og <i>indsigelse</i>	X		
4	Den dataansvarlige fører løbende egenkontrol med, at <i>Dataportabilitet</i> og <i>indsigelse</i> sker i overensstemmelse med de gældende politikker.	X		<i>Den GDPR-ansvarlige foretager i samarbejde med ledelsen løbende egenkontrol heraf</i>

DATABESKYTTELSE – DATABESKYTTELSESFORORDNINGENS ART. 24 og 25

Der er sikret tilstrækkelige tekniske og organisatoriske sikkerhedsforanstaltninger, såvel fysisk omkring IT som i interne systemer gennem design og gennem standardindstillinger (*by default*).

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
		<i>Efterleves behandlingen af kontrolmål?</i>		
1	Der er udarbejdet skriftlige retningslinjer, politikker, vejledninger eller procedure der sikrer databeskyttelse gennem design og default.		X	Dette er ikke muligt på de tredjepart IT-systemer der anvendes. Dog er det udarbejdet i egenudviklede IT-systemer
2	Der er udarbejdet skriftlige vejledninger og procedure der sikrer databeskyttelse i hverdagen, som omfatter alle medarbejdere, der kommer i kontakt med persondata.	X		
3	Der er udarbejdet skriftlige retningslinjer, vejledninger og procedure for Den dataansvarliges IT-sikkerhed og IT generelt.	X		
4	Den dataansvarlige forsikrer at der ved udvikling af programmer eller indførsel af nye	X		Hvis, nej (Uddyb hvorfor):

	behandlingsystemer (efter den 25. maj 2018), sikres databeskyttelse gennem designet af programmet/behandlingssystemet.			
5	Standardindstillingerne i de fysiske og elektroniske systemer er sat op på en sådan måde, at personoplysninger ikke stilles til rådighed for et ubegrænset antal personer.	X		Virksomheden kan se at der er organisatorisk opdeling i de anvendte IT-systemer som indeholder persondata hos tredjepart og i egenudviklede IT-systemer
6	Den dataansvarlige har etableret tekniske og organisatoriske sikringsforanstaltninger, som svarer til standardkrav for tekniske og organisatoriske sikringsforanstaltninger, som f.eks. pseudonymisering, dataminimering, sikkerhed af fysiske lokaliteter, strøm, osv.	X		
7	De tekniske og organisatoriske tiltag opdateres løbende i de skriftlige politikker.	X		Denne del foreligger hos tredjepart, men den GDPR-ansvarlige vil ved hvert årlige audit – heraf via tilsyn med Databehandlere sikre dette
8	Det kontrolleres løbende, at politikkerne efterleves, og at standardindstillingerne er sat op som påkrævet.	X		Ja, dette sker via den årlige audit

DATABEHANDLERE – DATABESKYTTELSESFORORDNINGENS ART. 28 og 29

Parterne har indgået en databehandleraftaler, der opfylder kravene i Databeskyttelsesforordningen og databeskyttelsesloven. Yderligere er der implementeret procedurer mv. for at sikre overholdelse af aftalevilkårene, og at der udelukkende handles efter instruks fra den dataansvarlige.

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
1	Der er indgået en databehandleraftale, der som minimum regulerer: <ul style="list-style-type: none"> - Udpegning af roller - Forpligtelser og rettigheder - Sikkerhedsforanstaltninger (tekniske og organisatoriske) - Ansvarsfordeling - Overførsel af data til tredjelande 	X		

	- Evt. brug af underdatabehandlere			
2	Der foreligger en evt. senere opdatering af databehandleraftalen, som er skriftligt dokumenteret	X		Hvis, nej (Uddyb hvorfor):
3	Databehandleren forsikrer at der ikke sker behandling uden for den Dataansvarliges instruks herom.	X		
4	Den dataansvarlige får årligt via tredjepart sikret udførelse og overholdelse af det lovpligtige tilsyn med dennes Databehandlere, samt disses evt. underdatabehandlere	X		Hvis, nej (Uddyb hvorfor):

RISIKOVURDERING – DATABESKYTTELSESFORORDNINGENS ART. 32

Den dataansvarlige har nedskrevet og implementeret vejledninger og procedure, der sikrer, at denne foretager risikovurderinger og konsekvensanalyser ved behandling af personoplysninger, som lever op til gældende lovkrav herom.

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
		<i>Efterleves behandlingen af kontrolmål?</i>		
1	Den dataansvarlige etablerer på baggrund af sine risikovurderinger passende tekniske og organisatoriske foranstaltninger, der imødekommer det højeste sikkerhedsniveau i overensstemmelse med gældende lovgivning.	X		<i>Ingen anmærkninger</i>

DATABRUD – DATABESKYTTELSESFORORDNINGENS ART. 33 og 34

Den dataansvarlige har nedskrevne vejledninger for at sikre rettidig og fyldestgørende anmeldelse til Datatilsynet ved eventuelle brud på persondatasikkerheden, herunder underretning af de registrerede.

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
		<i>Efterleves behandlingen af kontrolmål?</i>		
1	Foreligger der en procesbeskrivelse af, hvordan brud på persondatasikkerheden håndteres heraf stillingtagen til ansvarsfordeling, vurdering, håndtering, evaluering og efterfølgende forbedring?	X		Hvis, nej (Uddyb hvorfor):
2	Den dataansvarlige har sikrer, at dokumentation om evt. databrud som minimum indeholder gældende retningslinjer herfor	X		<i>Dette sikres af den GDPR-ansvarlige</i>

3	Den dataansvarlige har nedskrevne vejledninger og procedure i det omfang, at denne pålægges underretning af de berørte registrerede om databrudet.	X		
4	Foreligger der en nedskrevne vejledning af hvordan der foretages anmeldelse af brud til Datatilsynet?	X		Hvis, nej (Uddyb hvorfor):
5	Registreres alle brud på persondatasikkerheden?	X		Hvis, nej (Uddyb hvorfor):
6	Hvor mange brud på persondatasikkerheden har Den dataansvarliges databehandlere og /eller dennes underdatabehandler haft fra 25. maj 2018 til dags dato?			Angiv antal: Der henvises til Excel dokumentet - Sikkerhedsbrud-log
7	Er der brud på persondatasikkerheden hos Den dataansvarliges databehandlere og /eller dennes underdatabehandler, som er anmeldt til Datatilsynet?		X	Angiv antal: 0 <i>Vedlæg liste og risikovurderingsniveau herpå</i>
8	Er der brud på persondatasikkerheden hos Den dataansvarliges databehandlere og /eller dennes underdatabehandler, som <u>ikke</u> er anmeldt til Datatilsynet?		X	Angiv antal: 0 <i>Vedlæg liste og risikovurderingsniveau herpå</i>
9	Er der brud på persondatasikkerheden hos Den dataansvarliges databehandlere og /eller dennes underdatabehandler, som er anmeldt til Datatilsynet efter de 72 timer?		X	Hvis, ja: <i>Uddyb begrundelse heraf og vedlæg liste samt risikovurderingsniveau herpå</i>
10	Er der brud, som mangler at blive underrettet til de registrerede?		X	Hvis, ja: <i>Uddyb hvilke samt risikovurderingsniveau herpå</i>
11	Er der brud, som mangler at blive underrettet til eventuelle implicerede Databehandlere?		X	Hvis, ja: <i>Uddyb hvilke samt risikovurderingsniveau herpå</i>
12	Hvem foretager vurderingen af, om der er sket et brud på persondatasikkerheden?			Angiv navn: Ledelsen og den GDPR-ansvarlige
13	Hvem vurderer, om et brud på persondatasikkerheden skal anmeldes til Datatilsynet?			Angiv navn: Ledelsen og den GDPR-ansvarlige
14	Hvordan, hvornår og hvor ofte er Den dataansvarliges medarbejdere orienteret om og instrueret i at opdage og håndtere et brud på persondatasikkerheden?			Uddyb hvordan: Dato for hvornår: <i>Løbende via informationsmails</i>

KONSEKVENSANALYSE OG HØRING – DATABESKYTTELSESFORORDNINGENS ART. 35 og 36

Den dataansvarlige har nedskrevet og implementeret vejledninger der sikrer, at denne foretager risikovurderinger og konsekvensanalyser af sin behandling af personoplysninger, som lever op til gældende lovgivning herom.

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
1	Den dataansvarlige har nedskrevne vejledninger, som sikrer, at der ved indførelse af nye typer behandlinger og /eller systemer hos denne - som medfører en høj risiko for de registreredes rettigheder – foretages en konsekvensanalyse.	X		Ingen anmærkninger

AWARENESS

Den dataansvarlige har oprettet vejledninger, procedure mv. for at sikre dennes medarbejders opmærksomhed (awareness) omkring behandling af persondata i virksomheden.

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
1	Har Den dataansvarlige implementeret retningslinjer, politikker, vejledninger, procedure/andet, for at sikre awareness?	X		Hvis, nej: Uddyb hvorfor
2	Hvilke tiltag har Den dataansvarlige lavet for at sikre awareness?			Uddyb tiltag: Der er udarbejdet plakater. Yderligere afsendes der løbende e-mails indeholdende forskellig information omkring GDPR
3	Hvad har Den dataansvarlige gjort for at uddanne medarbejderne i korrekt behandling af persondata?			Uddyb uddannelse: Der er udarbejdet en PowerPoint efterfulgt af en quiz.
4	Har Den dataansvarlige udsendt e-læring evt. med quiz og opfølgning/måling af medarbejdere			Uddyb: Igennem hele året sendes der løbende e-mails indeholdende forskellig information omkring GDPR ud til de enkelte medarbejdere
5	Har Den dataansvarlige holdt et oplæg om databeskyttelsesforordningen for medarbejdere f.eks. fra databeskyttelsesrådgiveren eller internt i virksomheden?	X		Uddyb: Ja, dette blev gjort i starten – hvor de enkelte medarbejdere kunne stille spørgsmål.
6	Hvor ofte er der awareness aktiviteter vedrørende			Dette sker løbende

	databeskyttelsesforordningen i virksomheden?			
7	Er der udarbejdet pixibøger, plakater og undervisningsmateriale i organisationen?	X		Disse mangler at blive opsat
8	Oplyst hvordan Den dataansvarlige har indtænkt awareness i forbindelse med ansættelse af nye medarbejdere			Uddyb: Ved nyansættelse skal den enkelte medarbejder gennemgå PowerPoint med tilhørende quiz. Yderlig fremsendes alt relevant GDPR materiale til den enkelte medarbejder for gennemlæsning heraf.
9	Orienter Den dataansvarlige nye medarbejdere om ansvar og opgaver vedr. behandling af persondata og om konsekvenser ved overtrædelse af reglerne?	X		
10	Har Den dataansvarlige en procedure/vejledning for brug af sikker mail?	X		
11	Har Den dataansvarlige iværksat oprydninger i Outlook og af fildrev og hvis ja, hvordan iværksætte og overholdes denne?	X		Uddyb: Sker løbende igennem hele året

TELELOVEN – Jf. ERHVERVSSTYRELSEN

Den dataansvarlige efterlever ligesom alle andre teleselskaber teleloven, som erhvervsstyrelsen fører tilsyn med.

Nr.	Spørgsmål	Ja	Nej	Evt. Kommentar
		Efterleves behandlingen af kontrolmål?		
1	Efterleves reglerne om databeskyttelse i den elektroniske kommunikationssektor, de omfattede tjenester, tilsyn, klageadgang og sanktioner jf. udstedte retningslinjer fra erhvervsstyrelsen	X		<i>Ingen anmærkninger</i>