



Aarhus, 27. januar 2023

Bilagssamling
til åben dagsorden til møde i bestyrelsen for Midttrafik
3. februar 2023 kl. 09.30
Midttrafik
Søren Nymarks Vej 3,
8270 Højbjerg



Transportminister
Thomas Danielsen
trm@trm.dk



20-01-2023

To forslag til en midlertidig løsning for trafikskabernes økonomi

Kære Thomas Danielsen

Trafikskabernes økonomi er fortsat presset. Der er stadigvæk et passagerefterslæb efter corona, som påvirker billetindtægterne. Men det er imidlertid især de stigende brændstofpriser, der belaster økonomien. Den tidligere regerings energiforsyningstilskud var en hjælp, men løser ikke hele udfordringen. Trafikskaberne står i en ekstraordinær økonomisk situation, og vi har to forslag til løsning, som trafikskaberne vurderer, tilsammen, vil kunne løse deres økonomiske udfordringer. Løsningerne vil ikke belaste regioners og kommuners økonomi.

KL og Danske Regioner efterspørger, at Transportministeriet assisterer den lokale og regionale kollektive trafik med disse to tilpasninger af rammevilkårene:

1. Udvidet låneadgang for de regionale trafikskaber: Af lånebekendtgørelsen fremgår, at trafikskabernes kassekredit er 125 kr pr. indbygger. Vi efterspørger en fordobling til 250 kr. pr. indbygger i 2023-25 samt Transportministeriets assistance i dialogen med Indenrigs- og Sundhedsministeriet om ændring af lånebekendtgørelsen.
2. Fremrykkelse af takststigninger: Takststigningerne for 2023 indfases aktuelt medio januar 2024. Vi efterspørger dispensation til, at takststigningerne for 2023 kan indfases hurtigst muligt og dermed afspejle prisudviklingen i det øvrige samfund.

En forudsætning for at vinde passagerne tilbage er, at bussen fortsat kører. Regioner, kommuner og trafikskaberne har gjort en omfattende indsats for

DANSKE REGIONER
DAMPFÆRGEVEJ 22
2100 KØBENHAVN Ø
+45 35 29 81 00
REGIONER@REGIONER.DK
REGIONER.DK

at finde løsninger, der kan udskyde, at vi må reducere yderligere i antal afgange og nedlægge ruter. Med de to ønsker til tilpasninger af trafikselskabernes rammevilkår, vurderer vi, at vi kan afhjælpe behovet for yderligere nedskæringer. Det er vores overbevisning, at der er tale om en midlertidig situation, da passagerne er på vej tilbage og brændstofpriserne formentlig vil stabilisere sig. Derfor er det afgørende, at vi kan komme igennem 2023 med så få tilpasninger i serviceniveauet som muligt. Vi håber derfor, at du vil tage positivt imod vores forslag.



Martin Dam
Formand, KL



Anders Kühnau
Formand, Danske Regioner

Ny takst på handicapkørsel

Søren Nymarks Vej 3
8270 Højbjerg

Tlf.: 87 40 82 00
midttrafik.dk

27. januar 2023

Journalnr.:
5.5.6-00028-2020

Sagsbehandler:
Christina Nysten Justesen

E-mail:
cnj@midttrafik.dk

Resumé

Taksten på handicapkørsel er ikke blevet ændret siden 2008, bortset fra i Aarhus Kommune som senest havde en ændring i 2012. På grund af stigende priser i samfundet, ønsker administrationen at hæve den nuværende takst. Den nuværende takst for ture under 100 km er 3 kr. pr. km, min. 30 kr. og ønskes hævet til 4,5 kr. pr. km, min. 45 kr. Fra 101 km ønskes taksten hævet fra 9 kr. pr. km til 12 kr. pr. km.

Udover en ændring af taksten ønsker administrationen også at ændre muligheden for at medtage et barn under 15 år gratis, til at disse rejser på samme vilkår som andre medrejsende til 50 %.

Slutteligt ønsker administrationen, at bestyrelsen træffer beslutning om, hvorvidt der i fremtiden skal ske en årlig indeksregulering på taksten for handicapkørsel, som følger bussidens indeksregulering.

Sagsfremstilling

Som det fremgår af bilag 1, er taksten på handicapkørsel ikke blevet ændret siden 2008, bortset fra i Aarhus Kommune som senest havde en ændring i 2012. Sammenligner man taksten for handicapkørsel med busbilletter, er fx en voksen enkeltbillet på bussiden steget med 29 % fra 2007 til 2023. Stigningen tager udgangspunkt i prisen for en voksen enkeltbillet i Midttrafik Øst (gældende fra 2007 - 2014), samt prisen gældende i hele regionen fra 2015.

Den nuværende takst på handicapkørsel er:

Minimumspris (10 km inkluderet)	30 kr.
Kilometertakst tom. 100 km	3 kr.
Kilometertakst fra 101 km	9 kr.
Medrejsende (op til to stk.)	50 % rabat
Barn under 15 år	Gratis
Visiteret ledsager	Gratis

Der kan bestilles op til fire personer på en tur, inkl. personen der bestiller. Personen, der bestiller, betaler fuld pris for turen.

Oplæg til den nye takst og fremtidig indeksregulering

Administrationen ønsker at ændre taksten til:

Minimumspris (10 km inkluderet)	45 kr.
Kilometertakst tom. 100 km	4,5 kr.
Kilometertakst fra 101 km	12 kr.

Medrejsende/barn under 15 år (op til to stk.)	50 % rabat
Visiteret ledsager	Gratis

Der kan fortsat bestilles op til fire personer på en tur, inkl. personen der bestiller. Personen, der bestiller, betaler også fortsat fuld pris for turen.

Den ændrede takst og ændringen af muligheden for at medtage et barn under 15 år gratis, til at disse rejser på samme vilkår som andre medrejsende til 50 %, foreslås implementeret fra d. 1. marts 2023.

Udover ønsket om en ændret takst, ønsker administrationen også, at bestyrelsen træffer beslutning om, hvorvidt der til fremtiden skal ske en årlig indeksregulering på taksten for handicapkørsel svarende til nærmeste 0,50 kr. Hvis bestyrelsen træffer beslutning herom, vil indeksreguleringen følge den, der foretages på bussiden. Begrundelse herfor er, at administrationen gerne vil undgå, at kunderne i fremtiden oplever en stor prisstigning på taksten. Samtidig sikres det også, at taksten afspejler forholdene i samfundet.

Taksten i de andre trafiksekskaber

Trafik-selskab	Minimumstakst	Kilometertakst	Rabatter	Medlems-abonnement
Movia	24 kr., inkl. 5 km (svarer til en 2 zoners kontantbillet i bus, tog eller metro)	Tom. 40 km: 2,4 kr. Fra 41 km og op-efter: 1,2 kr.	Ledsagere: 50 % af turens pris (op til to stk.) Børn under 12 år: Gratis (op til to stk.)	300 kr. pr. år
NT	45 kr.	4,5 kr.	Visiteret ledsager: Gratis	
Sydtrafik	40 kr.	3,5 kr.	Medrejsende: halv pris (op til tre stk.) Visiteret ledsager: Gratis	
FynBus	40 kr., inkl. 10 km	Tom. 100 km: 4 kr. Max. pris pr. tur: 150 kr.	Visiteret ledsager: Gratis Børn 0-15 år: Halv pris	

Økonomisk betydning for kunder og bestillere

Ved at ændre taksten og ændre muligheden for at medtage et barn under 15 år gratis, til at disse rejser på samme vilkår som andre medrejsende til 50 % på handicapkørsel, vil bestillerne som udgangspunkt opleve en besparelse. Det vides dog ikke, om takstændringen påvirker benyttelsesgraden af handicapkørsel (antallet af kørte ture).

Bestillernes besparelse og merudgiften for kunderne fremgår af følgende skema, hvor der er taget udgangspunkt i budget 2023:

Kommune	BUDGET 2023			NYE PRISER			Kommunens mer-/mindreudgift	Kundens mer-/mindrebetaling (EB)
	Kommunens betaling	Kundens egenbetaling	Antal ture	Kommunens betaling	Kundens egenbetaling	Antal ture		
FAVRSKOV	1.845.000	395.000	6.300	1.638.000	602.000	6.300	-207.000	207.000
HEDENSTED	2.663.000	486.000	8.400	2.405.000	744.000	8.400	-258.000	258.000
HERNING	2.866.000	518.000	8.600	2.603.000	781.000	8.600	-263.000	263.000
HOLSTEBRO	2.338.000	455.000	8.800	2.125.000	668.000	8.800	-213.000	213.000
HORSENS	3.904.000	852.000	16.600	3.498.000	1.258.000	16.600	-406.000	406.000
IKAST-BRANDE	1.453.000	305.000	4.400	1.295.000	463.000	4.400	-158.000	158.000
LEMVIG	1.170.000	200.000	3.000	1.064.000	306.000	3.000	-106.000	106.000
NORDDJURS	1.291.000	252.000	3.800	1.164.000	379.000	3.800	-127.000	127.000
ODDER	1.503.000	300.000	5.400	1.361.000	442.000	5.400	-142.000	142.000
RANDERS	5.382.000	949.000	20.900	4.952.000	1.379.000	20.900	-430.000	430.000
RINGKØBING-SKJERN	2.503.000	421.000	6.300	2.284.000	640.000	6.300	-219.000	219.000
SILKEBORG	3.994.000	774.000	14.500	3.612.000	1.156.000	14.500	-382.000	382.000
SKANDERBORG	2.644.000	482.000	9.500	2.406.000	720.000	9.500	-238.000	238.000
SKIVE	2.514.000	441.000	7.500	2.300.000	655.000	7.500	-214.000	214.000
STRUER	953.000	174.000	3.000	864.000	263.000	3.000	-89.000	89.000
SYDDJURS	1.965.000	290.000	5.300	1.822.000	433.000	5.300	-143.000	143.000
VIBORG	4.380.000	889.000	15.800	3.947.000	1.322.000	15.800	-433.000	433.000
ÅRHUS	18.605.000	3.935.000	87.700	16.716.000	5.824.000	87.700	-1.889.000	1.889.000
	61.973.000	12.118.000	235.800	56.056.000	18.035.000	235.800	-5.917.000	5.917.000

Kommunikation

Administrationen kommunikerer om ændringen til aktive kunder, som har benyttet handicapkørsel indenfor det sidste år via e-Boks eller almindelig post, hvis de ikke har e-Boks. Handicapfolderen og Midttrafiks hjemmeside opdateres også.

Der sendes også en informationsskrivelse til Midttrafiks tilgængelighedsforum og bestillere.

Med ændringen af taksten kan interesse og reaktioner fra kunder, interesseorganisationer og pressen forventes.

Direktøren indstiller,

- At taksten for handicapkørsel ændres pr. 1. marts 2023.
- At et barn under 15 år rejser på samme vilkår som andre medrejse til 50 % rabat.
- At bestyrelsen beslutter, om der til fremtiden skal ske en årlig indeksregulering af taksten på handicapkørsel svarende til bussidens.

Bilag

- Bilag 1: Takstens historie

Bilag 1

Takstens historie

2007: Bestyrelsen besluttede i 2007, at taksten på handicapkørsel i alle kommuner, bortset fra Aarhus Kommune, skulle være til 3 kr. pr. km, min. 30 kr. pr. 1. januar 2008. Dette oplæg var i høring i kommunerne.

Taksten i Aarhus Kommune fulgte buszonetaksten.

2010/2011/2012: I 2010 godkendte bestyrelsen, at administrationen i samarbejde med udvalgte repræsentanter i kommunerne, skulle arbejde på et oplæg til en fælles takst i hele regionen, inkl. Aarhus Kommune.

Oplægget til taksten blev 3 kr. pr. km, min. 30 kr. tom. 100 km. Bestyrelsen godkendt i juni 2011 dette og implementeringen skete d. 1. marts 2012. Inden bestyrelsen blev forelagt oplægget, havde det været i høring i kommunerne.

Det blev også vedtaget i juni 2011, at hvis turen er mere end 100 km er taksten 9 kr. pr. km fra 101 km. Dette blev også implementeret fra marts 2012.

2018: Bestyrelsen godkendt i 2018, at give 50 % rabat for medrejsende (op til to stk.) på handicapkørsel med implementering fra d. 1. januar 2019.



Midttrafik

Bestyrelsen for Midttrafik

26. januar 2023

Side 1 af 1

Stigning i egenbetalingen for handicapkørslen

Kære bestyrelse i Midttrafik

På jeres bestyrelsesmøde i december besluttede I at hæve egenbetalingen for handicapkørslen med 50% pr. 1. marts 2023.

Fra Aarhus Kommunes side frygter vi at den store stigning i egenbetalingen, vil påvirke borgernes brug af ordningen. Mulighederne for transport er afgørende for borgernes mulighed for at deltage i det sociale liv, for at have oplevelsen af frihed og for at begrænse ensomhed.

Vi vil derfor opfordre jer i bestyrelsen i Midttrafik til at indfase stigningen over mindst 3 år, i stedet for i ét hug.

Baggrunden for stigningen er egenbetalingen ikke er blevet reguleret siden 2012 for Aarhus Kommune og ikke siden 2008 for resten af regionens kommuner. Vi anerkender fuldt ud, at egenbetalingen skal reguleres så den kommer på niveau med egenbetalingen i de øvrige regioner, og fremover reguleres løbende. Vi ser dog ikke behovet for så hastig en implementering, men derimod netop udfordringer ved så hastig en implementering.

I en tid med stor inflation rammes målgruppen for handicapkørsel generelt hårdt. Og med en ekstraordinær større stigning i egenbetalingen for kørslen for denne gruppe, vil det forventeligt påvirke brugen af ordningen, men en række negative konsekvenser til følge.

Takstændringen har ingen økonomisk effekt for Midttrafik, da differencen mellem egenbetalingen og vognmænds betaling afholdes af kommunen.

Stigning i egenbetalingen for handicapkørslen har ikke forud for jeres beslutning været i høring hos hverken kommunerne eller relevante organisationer og råd.

Med venlig hilsen

Christian Budde, Rådmand for Sundhed og Omsorg, Aarhus Kommune
Finn Amby, Formand for Handicaprådet, Aarhus Kommune
Jan Radzewicz, Formand for Ældrerådet, Aarhus Kommune

SUNDHED OG OMSORG

Strategi og Udvikling
Aarhus Kommune

Ledelsessekretariat

Rådhuset, Rådhuspladsen 2
8000 Aarhus C

Direkte telefon: 28 55 56 80

Direkte e-mail:
klbj@aarhus.dk

Sagsbehandler:
Klaus Bach Trads

envision

Midttrafik

December 2022

KAMPAGNEEVALUERING

"FÅ MERE UD AF TUREN"

- 01 Om undersøgelsen
- 02 Executive summary
- 03 Kampagneevaluering
- 04 Generelle udsagn
- 05 Baggrund

AGENDA

OM UNDERSØGELSEN

BAGGRUND



Formålet med kampagnen har været få flere midtjyder til at bruge den kollektive trafik. Kampagnen har forsøgt at tiltrække nye kunder og give eksisterende kunder incitament til at rejse mere. Formålet med målingerne er at måle og dokumentere effekten af kampagnen "Få mere ud af turen.". Kampagnen blev afsluttet d. 6/12/22.



Målgruppen er borgere i Region Midtjylland nationalt repræsentativt på køn og alder (18+)



Metoden Undersøgelsen er foretaget á 2 omgange:

- 1) Der er blevet gennemført en præ-måling inden kampagnens start. Data er indsamlet i uge 37 og 38. Dette blev gjort for at etablere et basisniveau for udvalgte holdningsspørgsmål samt kendskabstal.
- 2) Efter kampagnen er der gennemført en post-måling i uge 50 med de samme holdningsspørgsmål, som i præ-målingen samt yderligere spørgsmål om kampagnen.



Feltarbejdet er foretaget via online spørgeskema, udviklet og administreret af Envision på vegne af Midttrafik.

Dataindsamlingen er foretaget via Norstats national repræsentative panel.

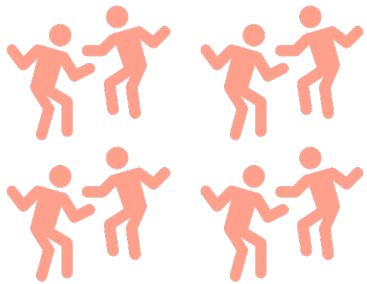
Data er vægtet på alder og Region ift. den danske population jf. Danmarks Statistik, stikprøven er således national repræsentativ i forhold til alder og Region.

Der er gennemført i alt 2.023 brugbare interviews.

Tabelrapporter er vedlagt i Excel.

EXECUTIVE SUMMARY

SAMLET EFFEKT AF KAMPAGNEN



1.062.000 midtjyder
(hele målgruppen)



20%

kan huske at have set kampagnen

212.000 midtjyder



43%

har i høj eller nogen grad fået lyst til at benytte mere kollektiv transport på baggrund af kampagnen

91.000 midtjyder

KONKLUSION

- Kampagnen har en liking over benchmark og modtages positivt i målgruppen.
- Der er en rigtig høj afsendergenkendelse i kampagnen. Det er tydeligt for modtageren, at det er Midttrafik der er afsender af kampagnen.
- Kampagnens to vigtigste budskaber, der handler om, at du kan få mere ud af din transporttid, og at du kan bruge tiden som du vil i kollektiv transport, er også de to budskaber, der afkodes bedst af målgruppen.
- Kampagnen er markant over benchmark på troværdighed, interesse og relevans. Særligt for relevans scorer kampagnen højt blandt de personer i målgruppen, der kan huske reklamen. Den høje relevans tyder på, at kampagnen rammer et aktuelt samfundsrelevant emne og i kombinationen med den høje liking, interesse og troværdighed er det en kampagne, der passer godt til en aktør som Midttrafik.
- Kampagnen formår at give modtagerne en mere positiv oplevelse af Midttrafik – dette ses ved, at der i posttesten er markant højere score for parametre som "Midttrafik er relevant for mig", "Midttrafik er et moderne trafiksselskab" og "Midttrafik giver mig gode muligheder for at komme fra a til b" – end der er i prætesten.
- Efter kampagnens afslutning er stor del af målgruppen blevet mere overbevist om, at de skal bruge kollektiv transport endnu mere. Derudover svarer flere i målgruppen efter posttesten, at de i højere grad overvejer kollektiv transport end de gjorde i prætesten. Flere svarer også, at de i højere grad bruger kollektiv transport end de gjorde i prætesten.
- Ud fra de KPI'er der blev opsat i Envisions oprindelige oplæg, som handlede om kendskab, ad liking, holdninger til Midttrafik og højere overvejelsesgrad ift. at benytte Midttrafik, så kan vi konkludere, at kampagnen performer på alle parametre – med undtagelse af kendskabet. Dette er forventeligt og svært at rykke på, da Midttrafiks kvalificeret kendskabstal i forvejen er rigtig højt. Det vil kræve en større medieinvestering over en længere periode.

KAMPAGNEOPSUMMERING

HUSKER HUSKER IKKE

KAMPAGNEOPSUMMERING	HUSKER	HUSKER IKKE	
KAMPAGNEERINDRING	20 %		☹️
AFSENDERGENKENDELSE	96 %		😊
BUDSKABSFORSTÅELSE <small>(top 3 over budskaber forstået)</small>	69 %-83 %	69 %-86 %	😊
LIKING	79 %	63 %	😊
TROVÆRDIG	70 %	51 %	😊
INTERESSANT	69 %	49 %	😊
RELEVANT	79 %	60 %	😊
LYST TIL AT BRUGE MERE KOLLEKTIV TRAFIK	43 %		😊

PRÆ/POST OPSUMMERING

HUSKER PRÆ

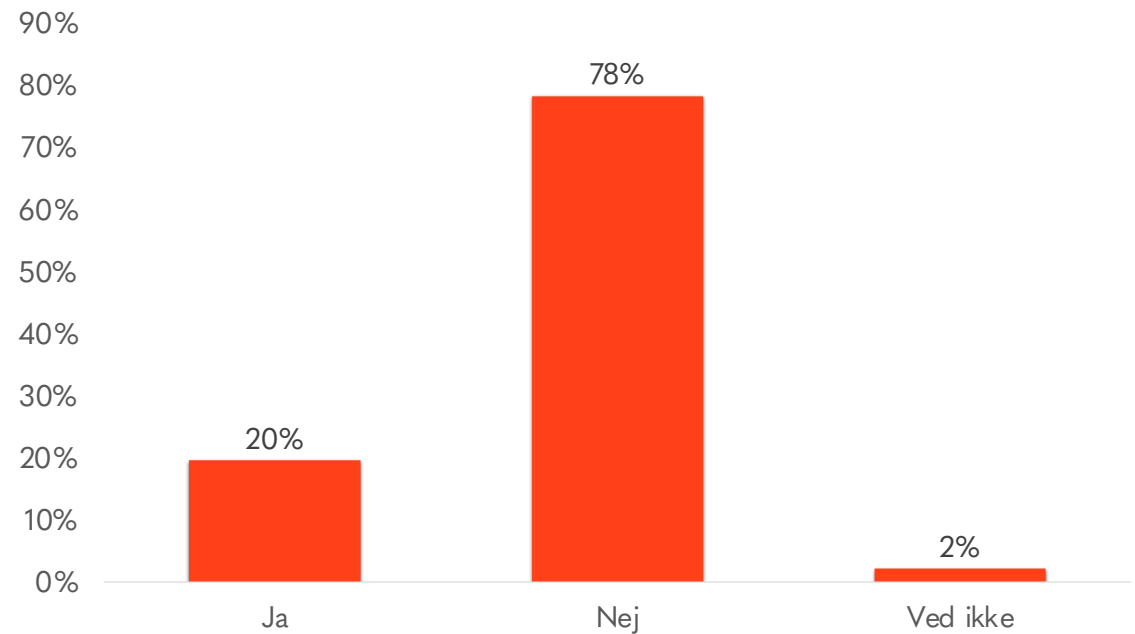
PRÆ/POST OPSUMMERING	HUSKER	PRÆ	
OVERVEJER KOLLEKTIV TRAFIK <small>(hver gang / ofte)</small>	40 %	23 %	😊
BRUGER KOLLEKTIV TRAFIK <small>(minimum ugentligt)</small>	34 %	17 %	😊
MODERNE TRAFIKSELSKAB	66 %	36 %	😊
RELEVANT FOR MIG	59 %	41 %	😊
GODE MULIGHEDER FOR AT KOMME FRA A TIL B	93 %	82 %	😊
STØRRE LYST TIL AT BRUGE OFFENTLIG TRANSPORT	39 %	17 %	😊
KENDER MIDTTRAFIK GODT	86 %	86 %	☹️
HAR HØRT OM MIDTTRAFIK	13 %	13 %	☹️

EVALUERING AF KAMPAGNEN

KAMPAGNE- ERINDRING

20 % af alle i målgruppen kan huske at have set en eller flere af reklamefilmene.

Kan du huske at have set en eller flere af disse film inden for de seneste par uger?



MEDIE-ERINDRING

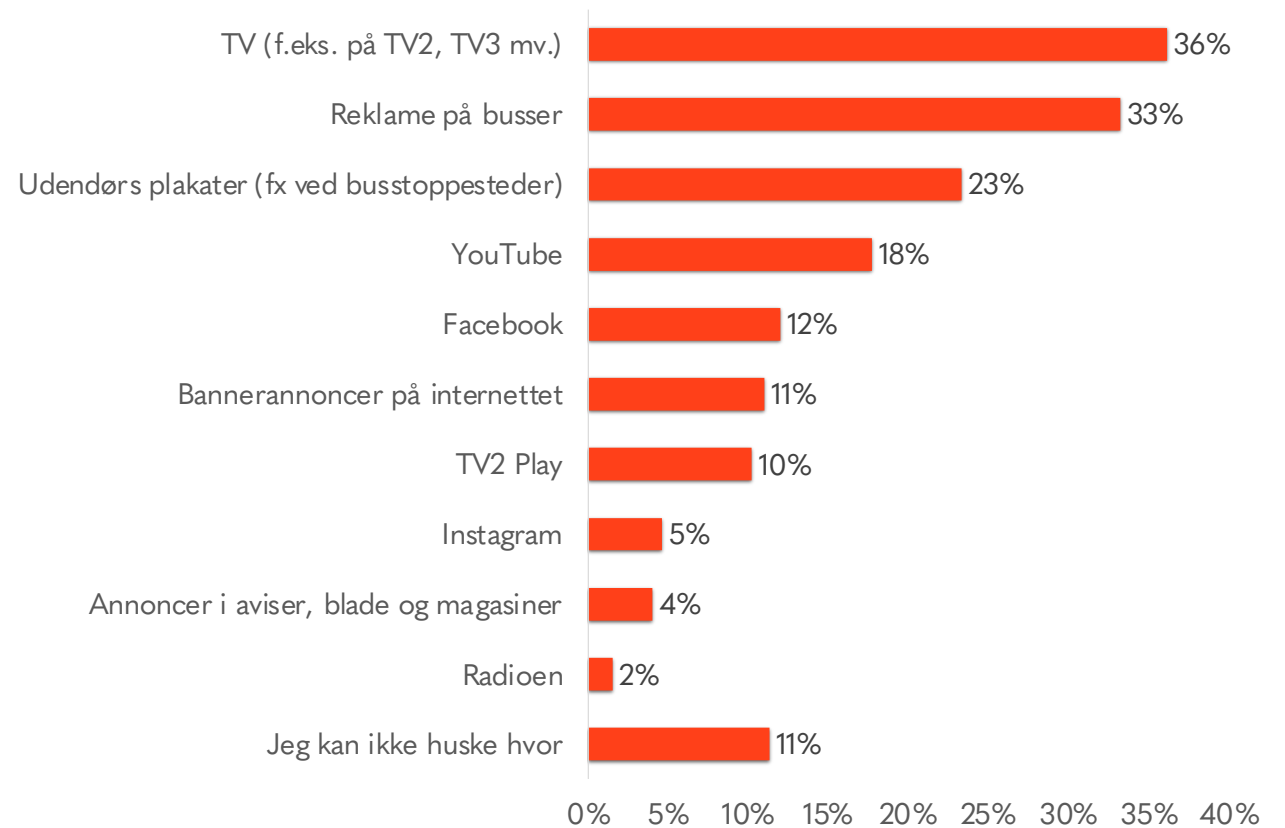
TV er det medie, hvor flest i målgruppen kan huske at have set en eller flere af reklamefilmene. Dette er på trods af, at kampagnen ikke har kørt på TV, men derimod på TV2 Play.

Det tyder dog på, at respondenterne har svært ved at skelne reklamerne på tv fra reklamerne på TV2 Play.

Dernæst kommer reklamer på busser, hvilket kan skyldes målgruppens associationer mellem busser og Midttrafik.

Hvor kan du huske at have set/hørt denne reklame?

(blandt dem der har set/hørt reklamen)

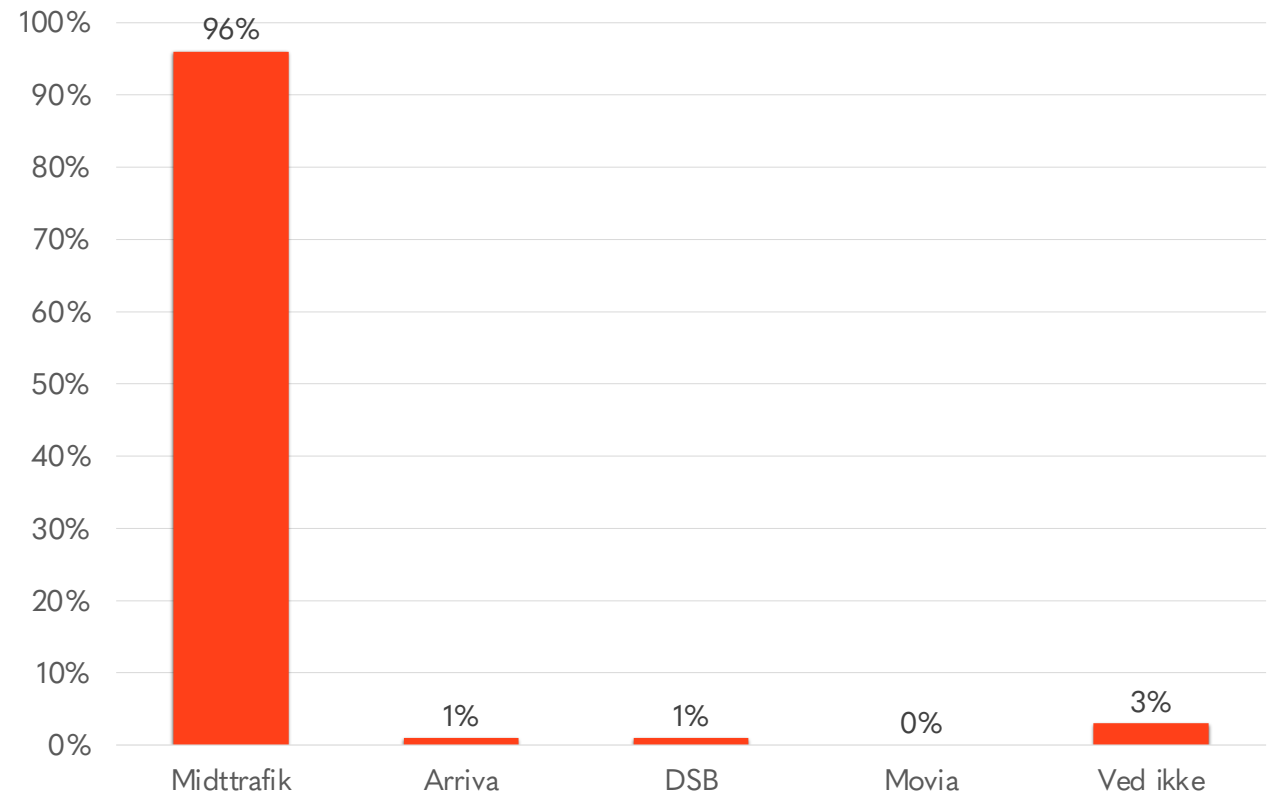


Base: Husker at have set kampagnen = 199

AFSENDER- ERINDRING

Der er en meget tydelig afsendererindring. Stort set alle i målgruppen tror, at Midttrafik er afsender af kampagnen.

Hvem tror du er afsender af kampagnen?



BUDSKABS- FORSTÅELSE

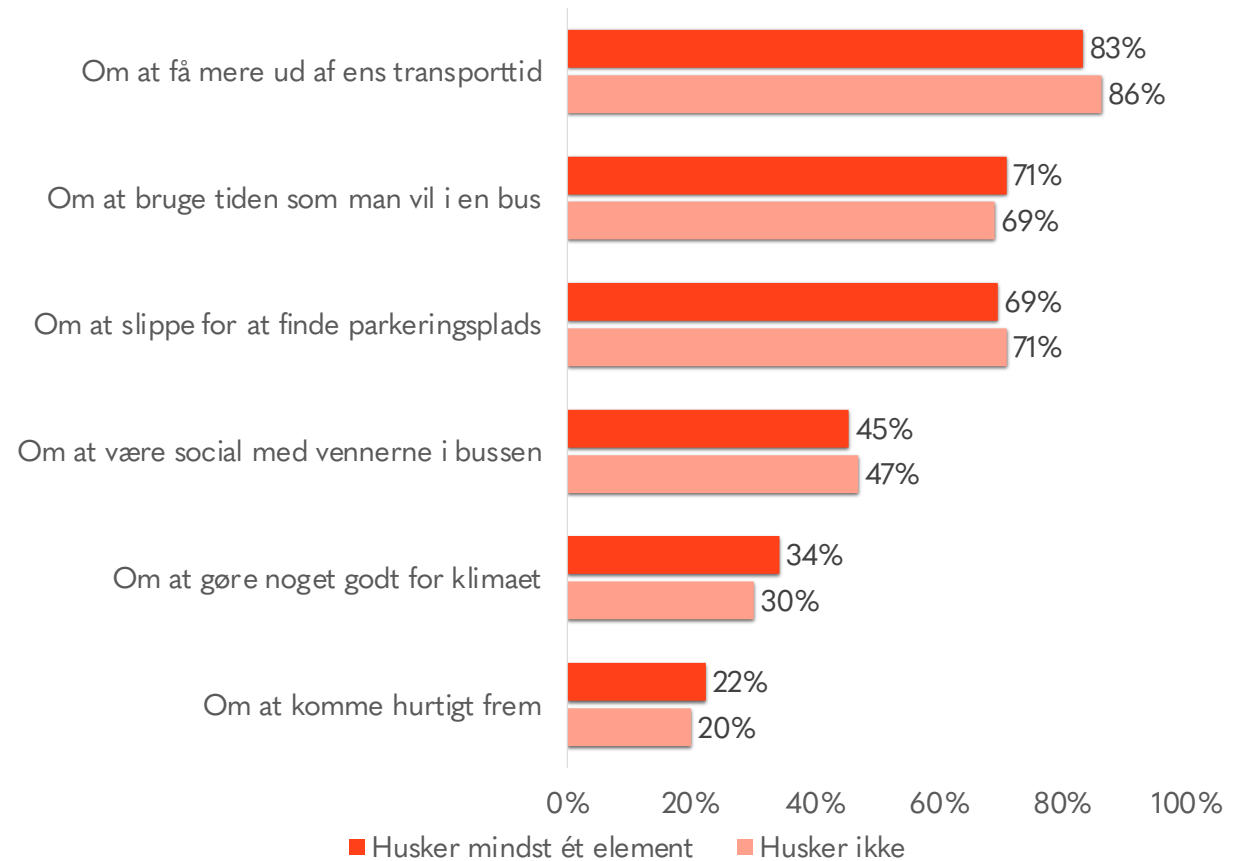
Kampagnebudskabet går særdeles godt igennem.

Over 8 ud af 10 angiver, at kampagnen handler om, at du kan få mere ud af din transporttid.

Derudover svar 7 ud af 10, at kampagnen handler om, at du kan bruge tiden som man vil i en bus.

Der er stort set ingen forskel mellem dem, der husker og dem, der ikke husker kampagnen.

Hvad handlede kampagnen om?



LIKING

Der er højere liking end benchmark for de personer, der kan huske at have set kampagnen.

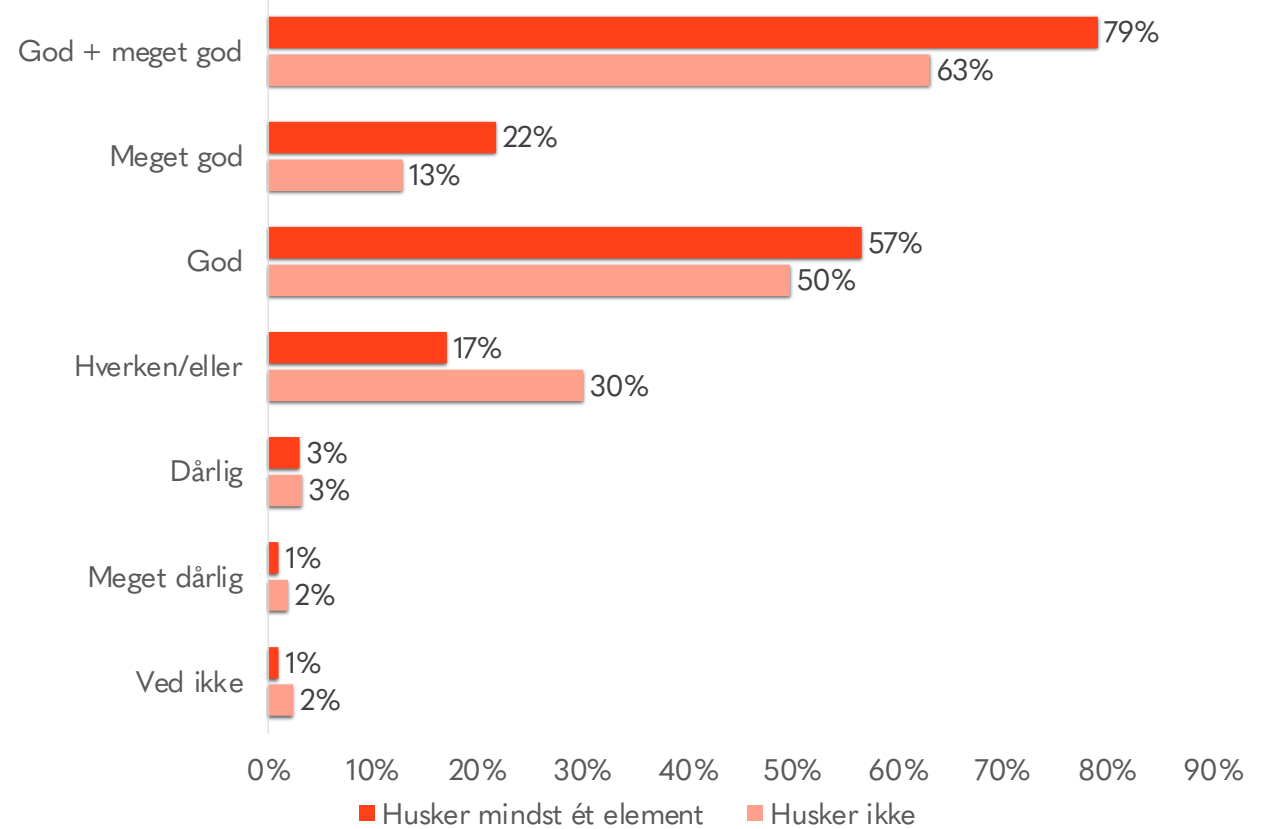
8 ud af 10 af dem, der husker den synes meget godt/godt om kampagnen.

Ingen synes dårligt om kampagnen.

Benchmark, TV (husker)

Liking = 70 % (gns)

Hvad synes du alt i alt om kampagnen?



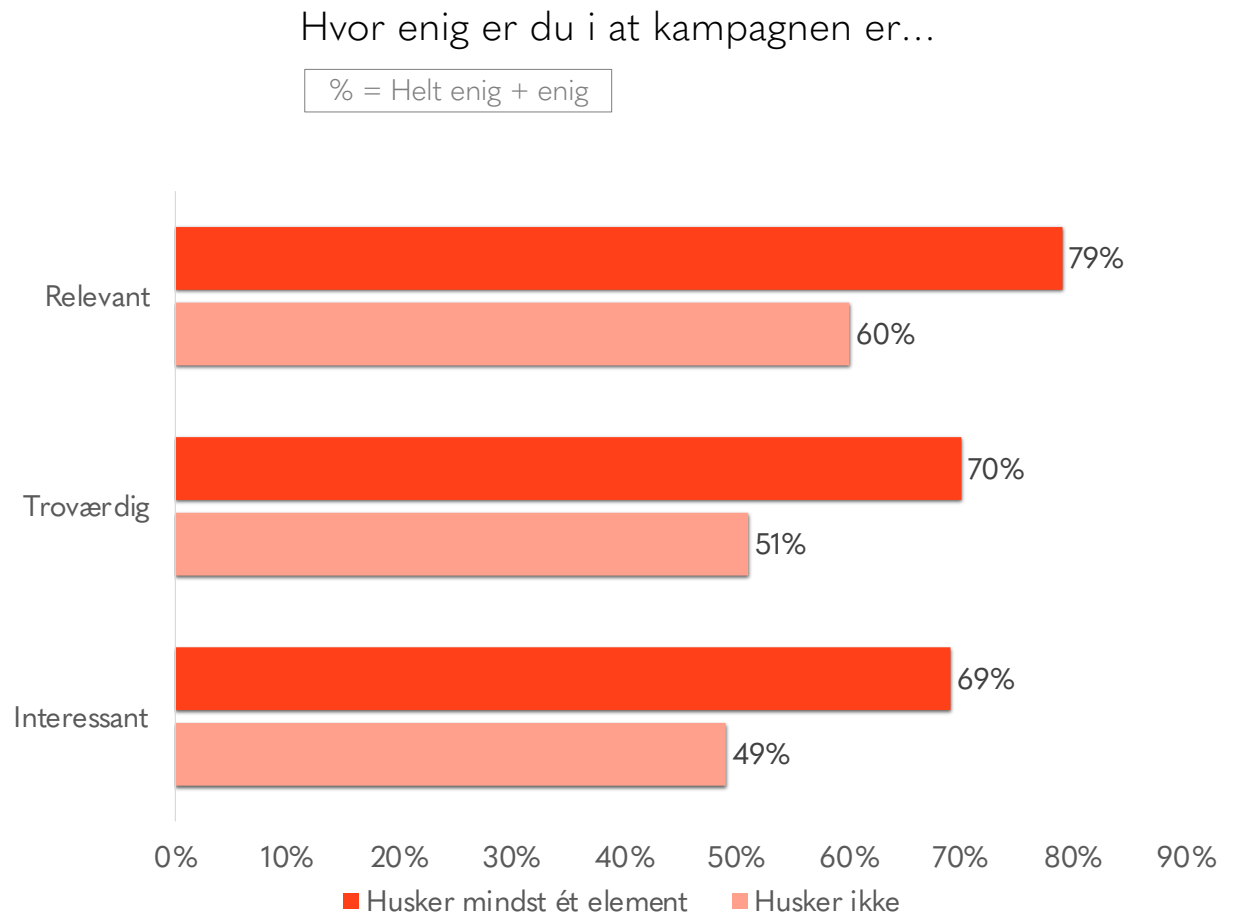
TROVÆRDIG INTERESANT RELEVANT

Kampagnen er markant over benchmark på troværdighed, interesse og relevans.

Særligt for relevans scorer den højt blandt de personer i målgruppen, der kan huske reklamen.

Benchmark, TV (husker)

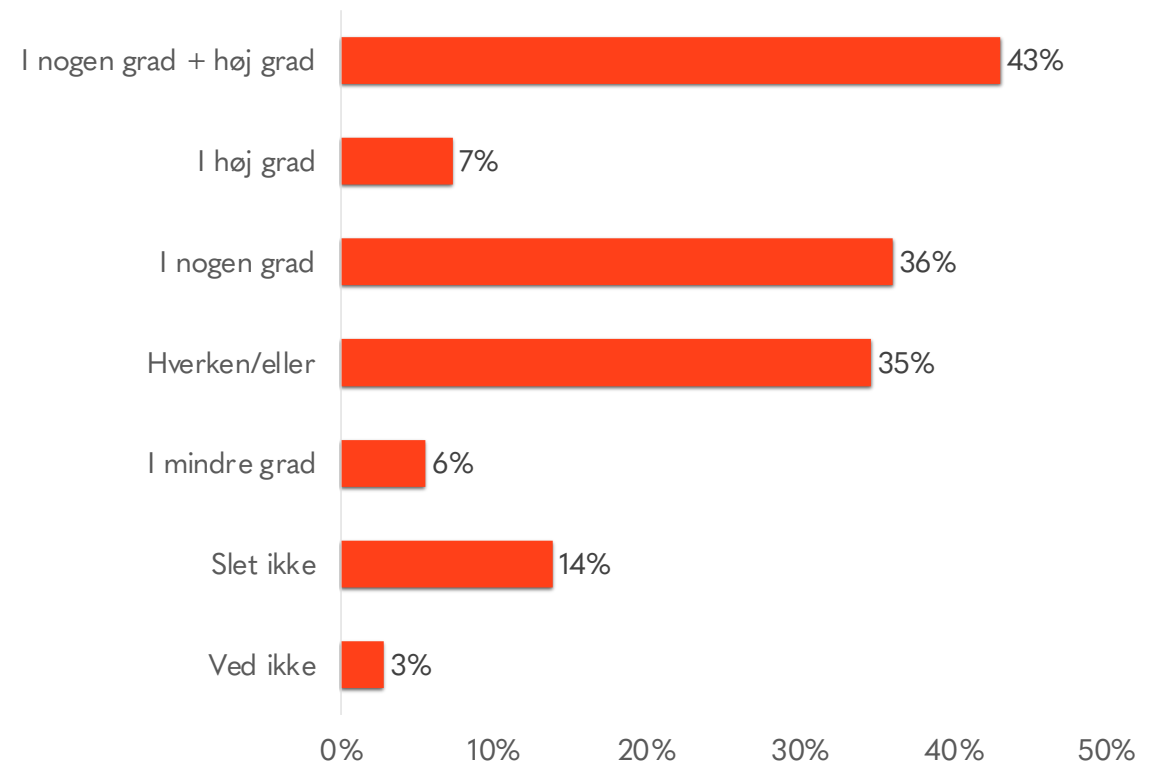
Interessant = 50 % (gns)
 Relevant = 46 % (gns)
 Troværdig = 54 % (gns)



INTENDERET ADFÆRD

43 % af de personer, der kan huske reklamen svarer, at de på baggrund af kampagnen har fået mere lyst til at benytte kollektiv trafik.

I hvilken grad har kampagnen givet dig lyst til at benytte kollektiv trafik?



Base: Husker at have set kampagnen = 199

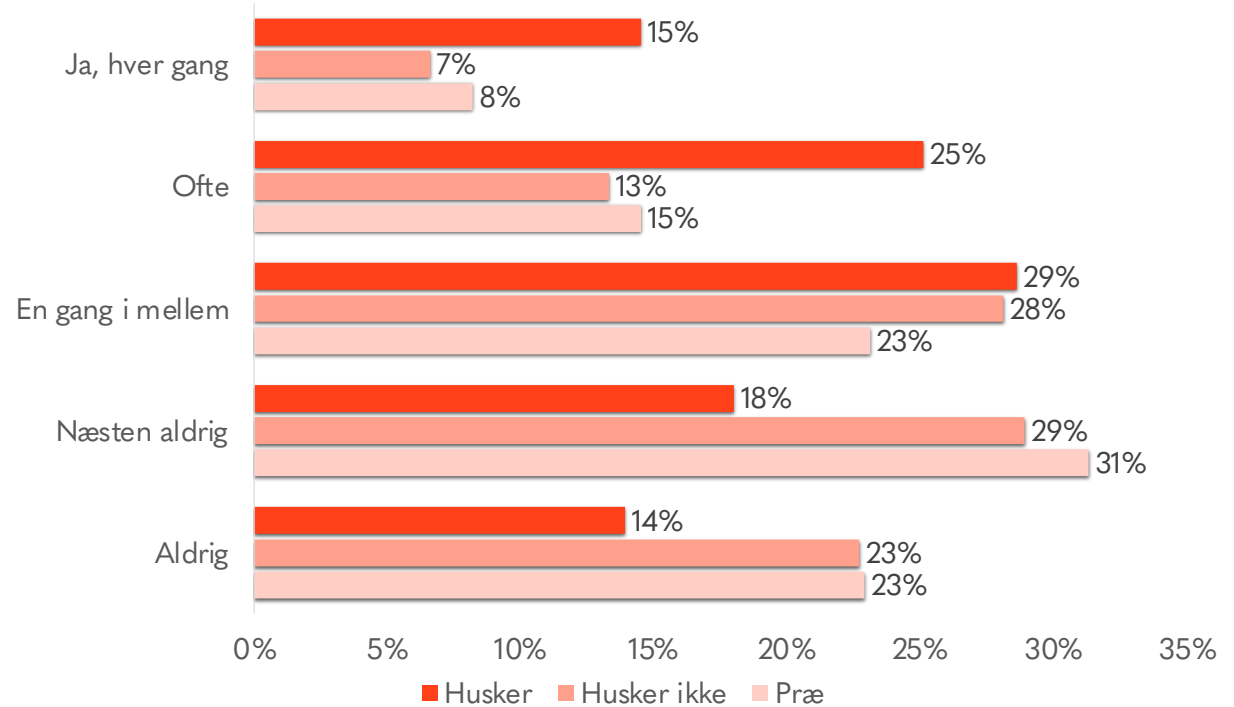
MERE OVERVEJELSE

Kampagnen har fået flere personer i målgruppen til at overveje kollektiv trafik, når de skal transportere sig fra a til b.

40 % af de personer, der kan huske kampagnen svarer, at de hver gang eller ofte overvejer at benytte kollektiv trafik.

Dette er væsentligt højere end de personer, der ikke husker kampagnen – og de personer, som vi stillede spørgsmålet til i præ-testen.

Overvejer du at bruge kollektiv trafik (fx tog og/eller bus), når du skal transportere dig fra a til b?



Base:
Præmåling = 1010
Postmåling = 1013

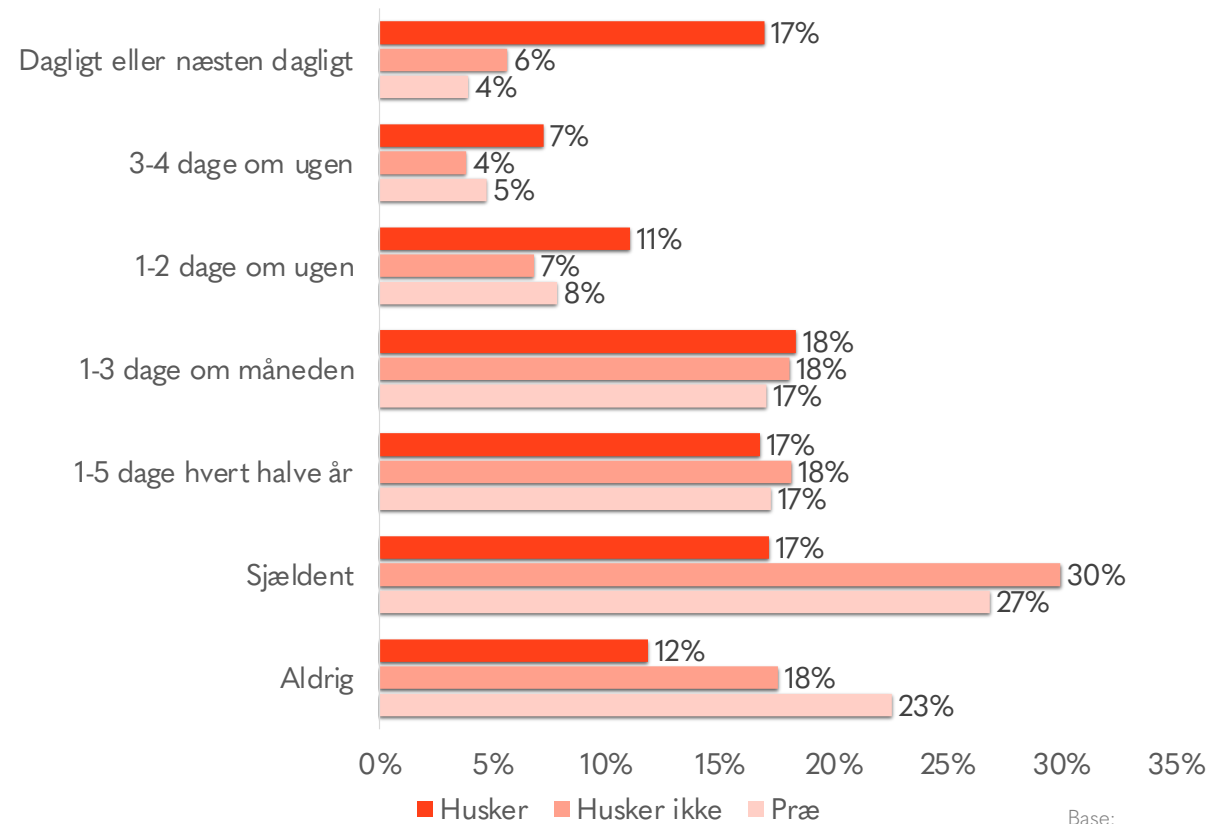
MERE BRUG

I vores posttest er der flere personer i målgruppen, der svarer, at de bruger kollektiv trafik minimum ugentligt sammenlignet med præ-testen.

Dette er en rigtig stærk indikator på, at kampagnen har været effektivt ift. at få målgruppen til at bruge kollektiv trafik oftere.

Der kan også være andre eksterne påvirkninger i spil, som fx tidspunkterne for målinger (efterår vs. vinter).

Hvor ofte bruger du kollektiv trafik i dag?



Base:
Præmåling = 1010
Postmåling = 1013

GENERELLE UDSAGN

IMAGE- UDSAGN

Kampagnen har givet Midttrafik et markant løft på de udvalgte imageparametre.

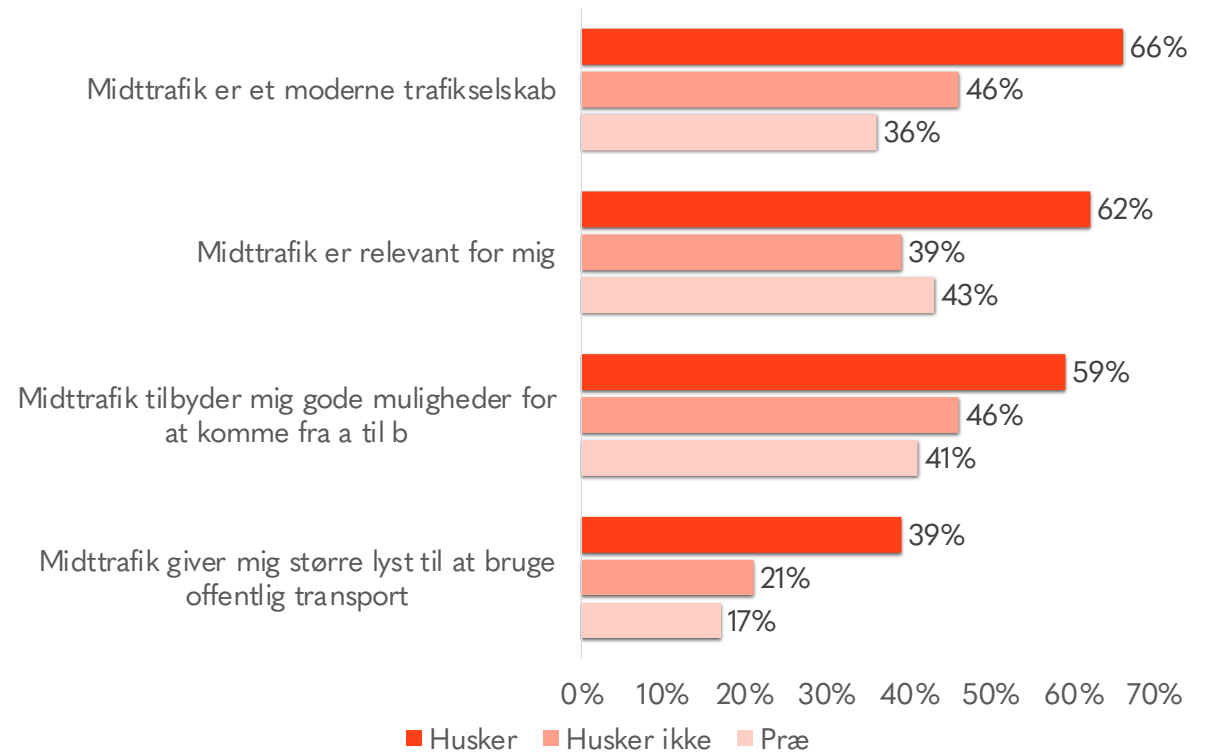
På baggrund af kampagnen er der dobbelt så mange i målgruppen, der svarer, at Midttrafik er et moderne trafiksselskab.

Samtidig opleves Midttrafik mere relevant blandt de personer, der kan huske kampagnen.

Derudover har kampagnen fået flere personer i målgruppen til at opleve, at Midttrafik tilbyder gode transportmuligheder samtidig med, at kampagnen har givet større lyst til at bruge kollektiv trafik.

Hvor enig er du i følgende udsagn?

% = Helt enig + enig



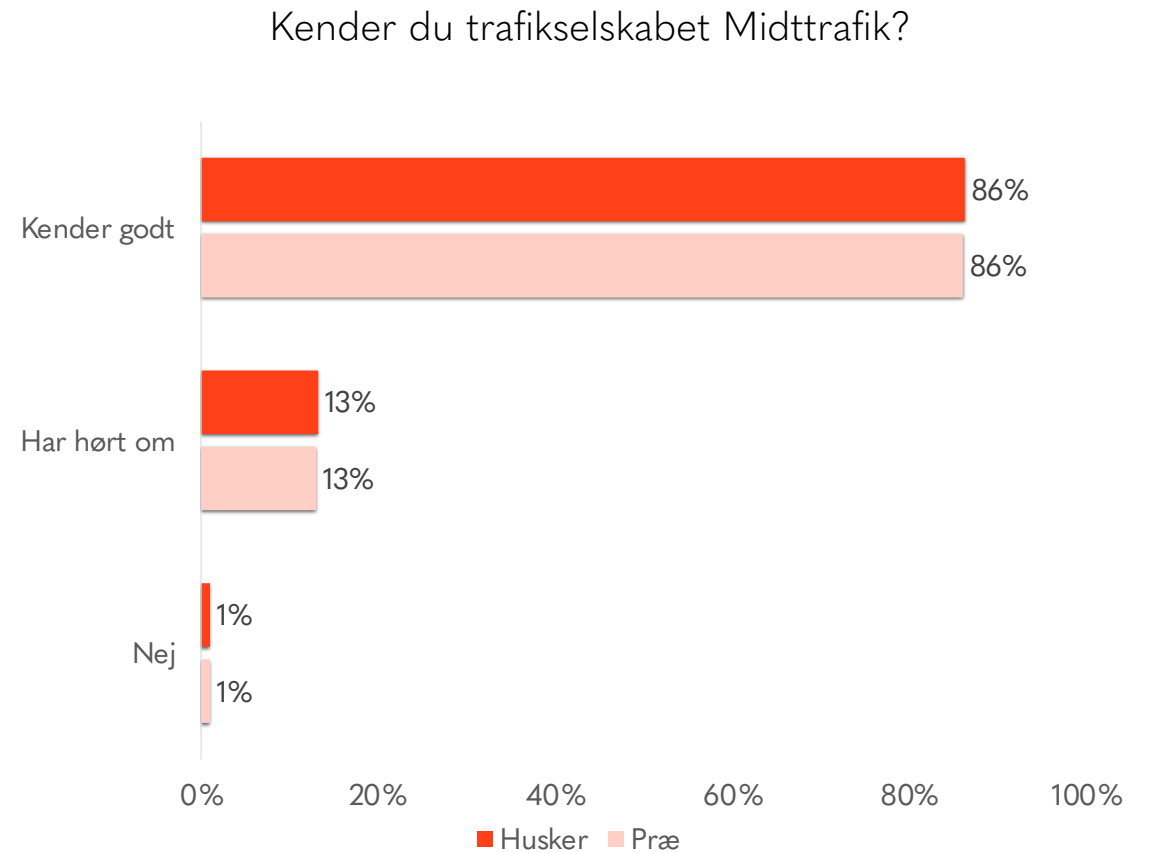
Base:
Præmåling = 1010
Postmåling = 1013

KENDSKAB MIDTTRAFIK

Kendskabsgraden er ikke formået at blive løftet. Det er status quo.

Det hænger sammen med, at det er markant sværere og dyrere at løfte kendskabsniveauet, når udgangspunktet er så højt som det er for Midttrafik.

Det kræver en længerevarende og mere kontinuerlig kampagneindsats - særligt, når man allerede står så stærkt.



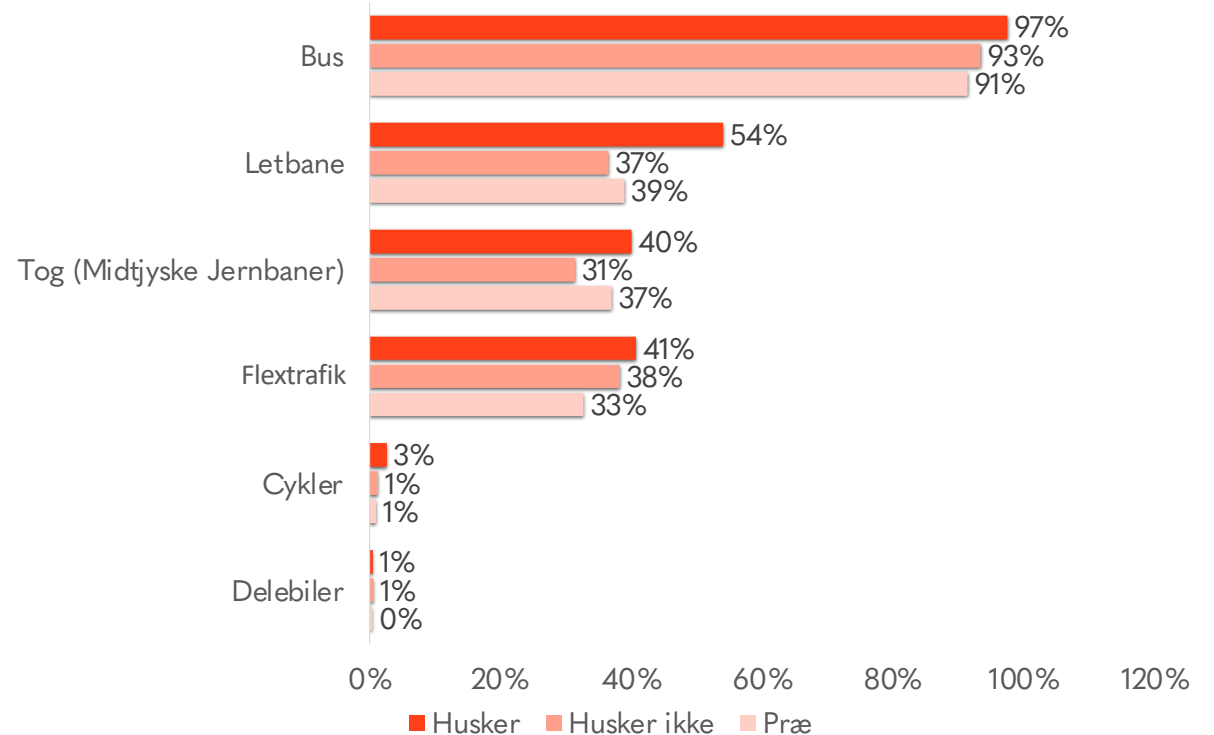
KENDSKAB MIDTTRAFIK YDELSER

Postmålingen viser, at der for Midttrafiks fire kerne-transportformer er opnået et højere kendskab.

Der er stadig flest, der kender Midttrafik for busser, dernæst letbane, tog og taxa (flextrafik).

Kendskabet til transportformen letbane har opnået den største procentuelle stigning fra præ- til postmåling.

Hvilke af følgende transportformer tilbyder trafikkselskabet Midttrafik?



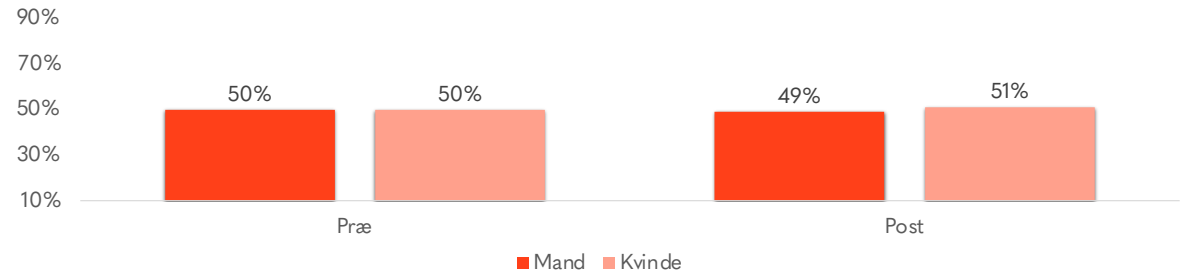
Base:
Præmåling = 1010
Postmåling = 1013

BAGGRUND

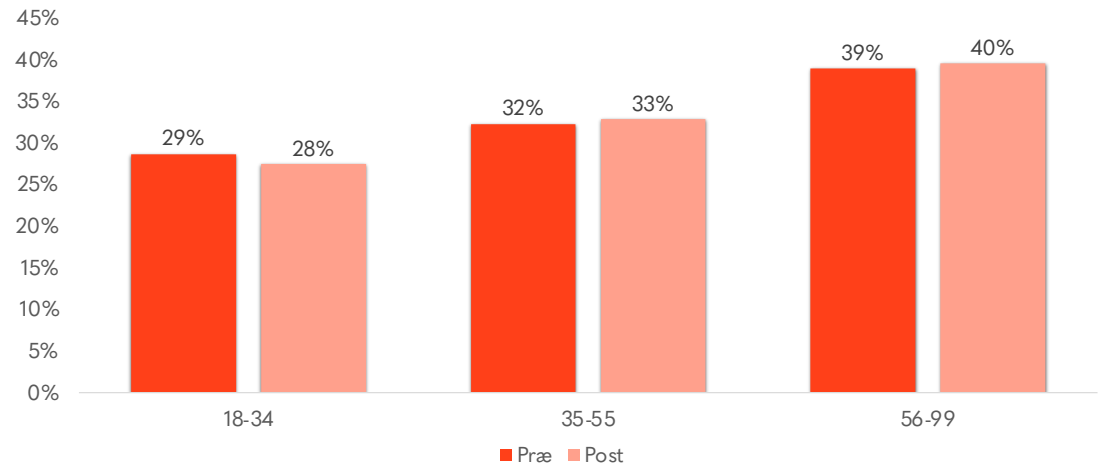
KØN ALDER



Køn



Hvad er din alder?

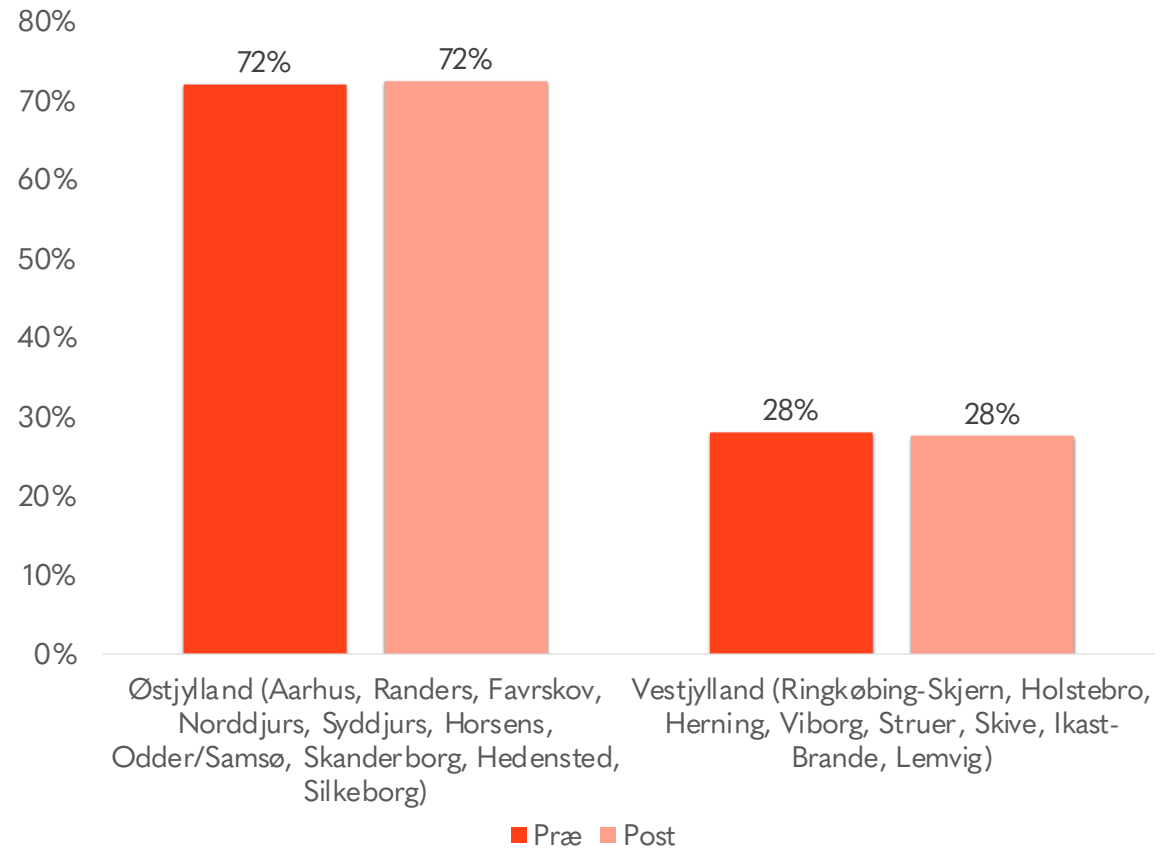


Base:
Præmåling = 1010
Postmåling = 1013

GEOGRAFI



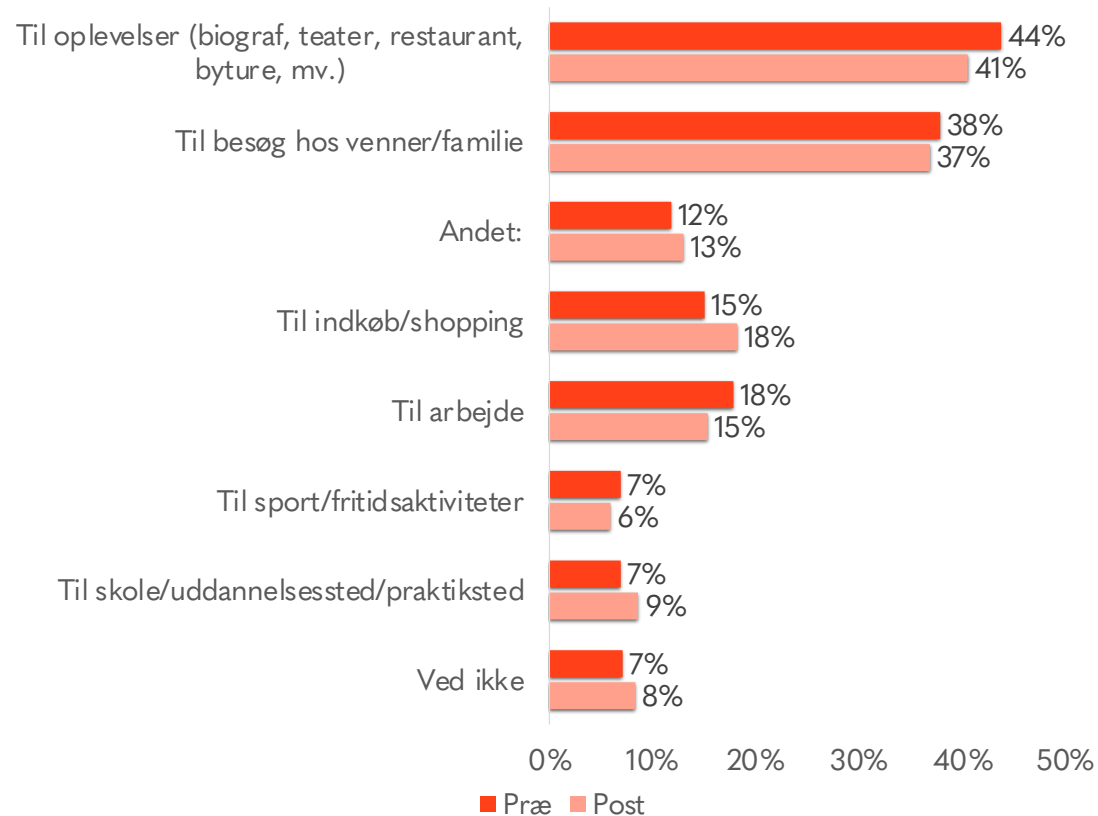
Hvilken region bor du i?



Base:
Præmåling = 1010
Postmåling = 1013

BRUG AF KOLLEKTIV TRAFIK

I hvilke sammenhænge bruger du oftest den kollektive trafik?



Base:
Præmåling = 781
Postmåling = 842

enVISION

Modtager Bestyrelsen for Midttrafik
 Udarbejdet af Thomas Dalgaard Mikkelsen
 Cc
 Emne Bilag - Opfølgning på medieomtale om skærpede reklamebestemmelser

Søren Nymarks Vej 3
 8270 Højbjerg

Tlf.: 87 40 82 00
 midttrafik.dk

19. januar 2023

Journalnr.:
 2.2.10-05515-2022

Kontaktperson:
 Thomas Dalgaard Mikkelsen

E-mail:
 tdm@midttrafik.dk

Eksempler på fortsat gyldige reklamer:



<i>Reklamen er for strip- eller sexklubber, pornografi og lignende samt varer eller tjenester relateret til disse.</i>	Nej
<i>Reklamer indeholder billeder eller tekst af pornografisk karakter.</i>	Nej
<i>Reklamer indeholder billeder, hvor der gøres brug af udpræget nøgenhed eller nøgenhed i en kontekst, som er egnet til at vække anstød.</i>	Nej



<p><i>Reklamen er for strip- eller sexklubber, pornografi og lignende samt varer eller tjenester relateret til disse.</i></p>	<p>Nej</p>
<p><i>Reklamer indeholder billeder eller tekst af pornografisk karakter.</i></p>	<p>Nej</p>
<p><i>Reklamer indeholder billeder, hvor der gøres brug af udpræget nøgenhed eller nøgenhed i en kontekst, som er egnet til at vække anstød.</i></p>	<p>På fotoet til venstre er manden nøgen. Dog vurderes det, at han ikke er nøgen i udpræget grad. Derfor vil reklamen ikke blive afvist på denne baggrund.</p>



<i>Reklamen er for strip- eller sexklubber, pornografi og lignende samt varer eller tjenester relateret til disse.</i>	Nej
<i>Reklamer indeholder billeder eller tekst af pornografisk karakter.</i>	Nej
<i>Reklamer indeholder billeder, hvor der gøres brug af udpræget nøgenhed eller nøgenhed i en kontekst, som er egnet til at vække anstød.</i>	Nej



Reklamen er for strip- eller sexklubber, pornografi og lignende samt varer eller tjenester relateret til disse.	Nej
Reklamer indeholder billeder eller tekst af pornografisk karakter.	Nej
Reklamer indeholder billeder, hvor der gøres brug af udpræget nøgenhed eller nøgenhed i en kontekst, som er egnet til at vække anstød.	Begge fotos kan vurderes til at vise nøgenhed nogen grad, dog ikke udpræget. Derfor vil reklamerne ikke blive afvist på denne baggrund.



Reklamen er for strip- eller sexklubber, pornografi og lignende samt varer eller tjenester relateret til disse.	Nej
Reklamer indeholder billeder eller tekst af pornografisk karakter.	Nej
Reklamer indeholder billeder, hvor der gøres brug af udpræget nøgenhed eller nøgenhed i en kontekst, som er egnet til at vække anstød.	Nej

Eksempler på reklamer, der fremover afvises:


<i>Reklamen er for strip- eller sexklubber, pornografi og lignende samt varer eller tjenester relateret til disse.</i>	Ja, og vil blive afvist på denne baggrund
<i>Reklamer indeholder billeder eller tekst af pornografisk karakter.</i>	Nej
<i>Reklamer indeholder billeder, hvor der gøres brug af udpræget nøgenhed eller nøgenhed i en kontekst, som er egnet til at vække anstød.</i>	Fotoet kan vække anstød, dog er kvinden på fotoet ikke udpræget nøgen.



<i>Reklamen er for strip- eller sexklubber, pornografi og lignende samt varer eller tjenester relateret til disse.</i>	Ja, og vil blive afvist på denne baggrund
<i>Reklamer indeholder billeder eller tekst af pornografisk karakter.</i>	Nej
<i>Reklamer indeholder billeder, hvor der gøres brug af udpræget nøgenhed eller nøgenhed i en kontekst, som er egnet til at vække anstød.</i>	Fotoet kan vække anstød, dog er kvinderne på fotoet ikke udpræget nøgne.



<p>Reklamen er for strip- eller sexklubber, pornografi og lignende samt varer eller tjenester relateret til disse.</p>	<p>Ja, og vil blive afvist på denne baggrund</p>
<p>Reklamer indeholder billeder eller tekst af pornografisk karakter.</p>	<p>Nej</p>
<p>Reklamer indeholder billeder, hvor der gøres brug af udpræget nøgenhed eller nøgenhed i en kontekst, som er egnet til at vække anstød.</p>	<p>Fotoet kan vække anstød, dog er kvinden på fotoet ikke udpræget nøgen.</p>



<p>Reklamen er for strip- eller sexklubber, pornografi og lignende samt varer eller tjenester relateret til disse.</p>	<p>Ja, og vil blive afvist på denne baggrund</p>
<p>Reklamer indeholder billeder eller tekst af pornografisk karakter.</p>	<p>Nej</p>
<p>Reklamer indeholder billeder, hvor der gøres brug af udpræget nøgenhed eller nøgenhed i en kontekst, som er egnet til at vække anstød.</p>	<p>Begge fotos kan vække anstød, og kvinden til venstre kan vurderes til at være nøgen i nogen grad, dog ikke udpræget.</p>



Holst, Advokater Advokatpartnerselskab
Hans Broges Gade 2
8000 Aarhus C
Att.: Advokat Kristian Torp

Dato: 9. december 2022

Sag: FO-19/14501-22

Sagsbehandler: /ajk

Direkte tlf.: +45 41 71 50 15

Sendt via digital post til CVR-nummer 35680470

Midttrafiks praksis vedr. byttepenge i flextrafikken (jeres j.nr.: 120097/150 KTO/RUH)

Forbrugerombudsmanden har modtaget klager over, at trafikskaber ikke giver byttepenge tilbage ved kontant betaling, herunder en klage fra Favrskov Kommune som sekretariat for Ældrerådet og Handicaprådet i kommunen vedrørende kundernes betalingsmuligheder for kørsel med flextrafik hos Midttrafik, herunder flextur og handicapkørsel, som Forbrugerombudsmanden modtog den 5. november 2019.

Det fremgår af klagen, at flextur og handicapkørsel bestilt via telefon alene kunne betales med kontanter med lige penge, da chaufførerne ikke havde byttepenge med. Midttrafik indførte dog en praksis ultimo 2019, hvorefter chaufførerne kan give byttepenge tilbage op til nærmeste hundrede kroner.

Flextrafikken, herunder flextur og handicapkørsel, er en del af den offentlige servicetrafik. Kunder kan bestille flextur og handicapkørsel via Midttrafiks hjemmeside, mobil app eller telefon.

På baggrund af klagen rettede Forbrugerombudsmanden henvendelse til Midttrafik den 29. maj 2020 og bad om selskabets bemærkninger til klagen.

På vegne af Midttrafik har Holst Advokater anført i høringssvaret af 12. juni 2020, at selskabet frit kan oprette en eller flere salgskanaler, som hver skal drives i overensstemmelse med lovgivningen, herunder betalingsloven. Salg af flextur og handicapkørsel via trafikskabets hjemmeside samt mobil app foregår som fjernsalg eller som ubemandet selvbetjening, og trafikskabets tilbud om telefonisk bestilling og kontant betaling er en selvstændig ydelse, som skal vurderes selvstændigt, hvorfor kontantreglen ikke finder anvendelse for denne salgskanal.

I høringssvaret henvises til vurderingen i et notat af 8. juli 2019, udarbejdet af Holst Advokater for Midttrafik, om vurdering af trafikskabets udbud af bestillings- og betalingsløsninger i forhold til kontant betaling:

FORBRUGEROMBUDSMANDEN

Carl Jacobsens Vej 35
2500 Valby

Tlf. 41 71 51 51

CVR-nr. 10 29 48 19

EAN-nr. 5798000018006

forbrugerombudsmanden@
forbrugerombudsmanden.dk

www.forbrugerombudsmanden.dk

ERHVERVSMINISTERIET

Medlem af International Consumer
Protection & Enforcement Network
(ICPEN)

www.icpen.org

- ”Bestilling og betaling via Midttrafiks netløsning sker i et selvstændigt system, der i relation til betalingsloven må opfattes som én salgskanal. Både bestilling og betaling sker online og dermed uden kontakt med fysiske medarbejdere. Salg via denne salgskanal er derfor omfattet af undtagelsen til kontantreglen i § 81, stk. 2, om fjernsalg.
- Bestilling via telefonsalg og betaling kontant til chaufføren sker i et andet selvstændigt system, der ligeledes i relation til betalingsloven må opfattes som én salgskanal. Her sker betaling til chaufføren, som modtager denne på vegne af Midttrafik. Da betaling imidlertid aktuelt alene kan ske med kontanter, omfattes transaktionen ikke af betalingsloven, jf. § 1, jf. § 7, nr. 11, jf. nr. 18. Det følger af de citerede bestemmelser grundlæggende, at betalingsloven kun finder anvendelse på betalinger, når modtageren tilbyder betaling med eksempelvis Dankort, MasterCard eller MobilePay”.

Med høringsvaret er endvidere vedlagt et bilag med oversigt over bestillings-/betalingsflow ved online-/app-bestilling af flexture og handicapkørsel. Det fremgår af bilaget, at chaufføren bl.a. har til opgave at modtage betaling fra kunden i de situationer, hvor bestillingen af flextur eller handicapkørsel er sket telefonisk og ved online-/app-bestilling af handicapkørsel uden et tilknyttet betalingskort. Bestillingen skal senest ske en time før afgang og kan afbestilles indtil samme tidspunkt. Chaufføren kan ikke indgå aftaler om køb af flextur eller handicapkørsel.

Forbrugerombudsmanden modtog den 23. juni 2020 supplerende høringsvar i sagen fra Holst Advokater. Heri er anført, at Forbrugerombudsmanden skulle have anerkendt, at et eventuelt billetsalg fra en chaufføren må bedømmes særskilt fra et salg fra en app eller en internetløsning samt fra betaling med rejsekort.

Forbrugerombudsmanden erindrer ikke at have givet udtryk herfor og har heller ikke praksis for, at billetsalg i busser skal bedømmes særskilt fra betaling med rejsekort.

Forbrugerombudsmanden har netop forespurgt Favrskov Kommune som sekretariat for Ældrerådet og Handicaprådet i kommunen, om betaling med kontanter for flexture og handicapkørsler fortsat giver anledning til vanskeligheder, efter at Midttrafik indførte en praksis ultimo 2019, hvorefter chaufførerne kan give byttepenge tilbage op til nærmeste hundrede kroner. Ældrerådet har oplyst til kommunen, at

”Det er meget besværligt, næsten umuligt at få vekselpenge retur. Vi skal på forhånd helst have samlet aftalt beløb sammen. Når vi kører en tur, vi har kørt før, kender vi beløbet og så forsøger vi at have det med. Men vi bruger jo ikke kontanter ellers, så det er virkelig besværligt. Vi får oplyst, at det skal være aftalt beløb.”

På baggrund af Ældrerådets oplysninger antager Forbrugerombudsmanden, at det fortsat forekommer, at Midttrafiks chauffører kræver lige penge for flexture og handicapkørsler.

Retsgrundlaget

Kontantreglen i betalingslovens § 81 har følgende ordlyd:

”§ 81. En betalingsmodtager er forpligtet til at modtage betaling med kontanter i tidsrummet fra kl. 06.00 til kl. 22.00, hvis denne modtager betalingsinstrumenter omfattet af denne lov, jf. dog § 5 i hvidvaskloven og stk. 2-6.

Stk. 2. Stk. 1 finder ikke anvendelse ved fjernsalg eller ved betalingstransaktioner i ubemandede selvbetjeningsmiljøer.

Stk. 3. Betalingsmodtagere, som er beliggende i områder, hvor der kan være en forhøjet risiko for røveri forbundet med modtagelse af kontanter, er uanset stk. 1 alene forpligtet til at modtage kontanter fra kl. 06.00 til kl. 20.00. Betalingsmodtagere, der ikke modtager kontanter i tidsrummet kl. 20.00-22.00, skal opsætte skilte herom. Erhvervsministeren fastsætter, i hvilke områder i Danmark der kan være en forhøjet risiko for røveri forbundet med modtagelse af kontanter. Erhvervsministeren offentliggør en meddelelse herom på Erhvervsministeriets hjemmeside.

Stk. 4. Betalingsmodtagere kan fravige stk. 1, for så vidt angår betalinger fra betalere, der ikke er forbrugere.

[...]

Stk. 6. Erhvervsministeren kan fastsætte regler om, at bestemte typer af betalingsmodtagere er forpligtet til altid at modtage betaling med kontanter uanset stk. 1-3.”

Overtrædelse af betalingslovens § 81, stk. 1, kan straffes med bøde, jf. § 152, stk. 2.

Formålet med indførelsen af kontantreglen fremgår bl.a. af forarbejderne¹ til den dagældende betalingskortlovs § 18, svarende til den nugældende § 81 i betalingsloven, hvor følgende står anført:

”Reglen indeholder et forbud mod diskrimination af kontantkunder til fordel for kortindehavere, således at en betalingsmodtager ikke blot på grund af betalingsmåden (kort/kontant) kan nægte at indgå en forpligtelse til at (ud)levere varer/tjenesteydelser. Betalingsmodtager må således ikke ved skiltning, i sine forretningsbetingelser eller ved faktiske foranstaltninger tilkendegive, at kontant betaling ikke kan finde sted.
[...]

Kontantreglen skal således hindre diskrimination af kontantkunder.

Ifølge betalingslovens § 81, stk. 2, gælder forpligtelsen til at modtage betaling med kontanter ikke i fjernsalgssituationer som fx køb over inter-

¹ Betænkning af 15. maj 1984, FT 1983/84, 2. samling, tillæg B, sp. 896, ”Til nr. 20”

nettet, eller hvis salget sker i et ubemandet selvbetjeningsmiljø. Det fremgår af forarbejderne² til lov om betalinger, at

”Forslaget viderefører § 56, stk. 1, 2. pkt., i den nugældende lov om betalingstjenester og elektroniske penge. Med bestemmelsen fastsættes det, at den generelle forpligtelse til at modtage betaling med kontanter i stk. 1, ikke finder anvendelse ved fjernsalg, eksempelvis salg via internet, salg via en app på en smartphone, salg via ubemandede selvbetjeningsmiljøer, som eksempelvis ubemandede benzinstationer eller offentlige busser. Hvornår et betjeningsmiljø kan anses for at være ubemandet afhænger af, om der er personale fysisk til stede, og hvad personalets funktion er. Det er således et krav, at der skal være personale til stede, og at personalet er ansat til at modtage betaling i forbindelse med salg. Er en buschauffør eksempelvis alene ansat til at føre bussen og ikke til at forestå salg af billetter, vil der være tale om et ubemandet selvbetjeningsmiljø, idet det fysiske tilstedeværende personales funktion ikke er at modtage betaling for en vare eller tjenesteydelse.”

Undtagelsen om fjernsalg og ubemandede selvbetjeningsmiljøer blev indført ved lovændringen i år 2000.³ Baggrunden for indførelsen af undtagelsen er ifølge betænkningen følgende⁴:

”Bestemmelsen har imidlertid vist sig at være uhensigtsmæssig i situationer, hvor der ikke er personlig kontakt mellem forbrugeren og betalingsmodtageren. Dette gælder fjernsalg og ubemandede selvbetjeningsmiljøer.

Begge salgsmetoder er lagt an på at kunne fungere uden personlig kontakt mellem forbrugeren og betalingsmodtageren og harmonerer derfor dårligt med modtagelsen af kontant betaling. Forbrugeren har desuden ikke den samme forventning om at kunne betale kontant som f.eks. ved det traditionelle butikssalg.”

Fjernsalg er ikke nærmere defineret i betalingsloven eller dennes forarbejder, men begrebet fjernsalg anvendes i forbrugeraftaleloven⁵:

”§ 3. I denne lov forstås ved:

- 1) Fjernsalgsaftale: Enhver aftale om varer, tjenesteydelser eller løbende levering af varer eller tjenesteydelser, når aftalen
 - a) indgås ved brug af kommunikation, der foregår, uden at forbrugeren og den erhvervsdrivende mødes fysisk (fjernkommunikation), og
 - b) indgås som led i et system for fjernsalg, som drives af den erhvervsdrivende.

² Forslag til lov om betalinger L 157, fremsat den 15. marts 2017, specielle bemærkninger, s. 213

³ Lov nr. 414 af 31. maj 2000 om visse betalingsmidler.

⁴ Tillægsbetænkning over Forslag til lov om visse betalingsmidler (L 63) afgivet af Erhvervsudvalget den 24. maj 2000.

⁵ Lov nr. 1457 af 17. december 2013 om forbrugeraftaler.

[...].”

I lovbemærkningerne⁶ til § 3 i forslag til lov om forbrugeraftaler er anført, at hverken aftaler, der forhandles på den erhvervsdrivendes forretningssted, men indgås endeligt ved hjælp af fjernkommunikation, eller reservationer foretaget af en forbruger ved hjælp af en fjernkommunikationsteknik med henblik på levering af en tjenesteydelse fra en erhvervsdrivende, fx bestilling af tid hos frisør eller tandlæge, er omfattet af fjernsalgsbegrebet.

Forbrugeraftaleloven gennemfører forbrugerrettighedsdirektivet⁷, herunder definitionen på en fjernsalgsaftale. I 20. præambelbetragtning er bl.a. anført, at en aftale, der indledes ved hjælp af fjernkommunikation, men indgås endeligt på den erhvervsdrivendes faste forretningssted, ikke bør betragtes som en fjernsalgsaftale. I direktivets artikel 2, nr. 7, er fjernsalgsaftaler defineret som:

”Enhver aftale, der indgås mellem den erhvervsdrivende og forbrugeren i henhold til et organiseret system for fjernsalg eller levering af fjernydelse uden den erhvervsdrivendes og forbrugersens samtidige fysiske tilstedeværelse, og hvor der til og med tidspunktet for aftalens indgåelse udelukkende anvendes en eller flere former for fjernkommunikationsteknikker”.

Med undtagelse af forbrugeraftalelovens §§ 4, 12, 30 og 31 gælder loven dog ikke for aftaler om personbefordring, jf. § 1, stk. 1, nr. 4.

Nationalbanken har i Kvartaloversigt, 3. kvartal 2006, s. 40, anført følgende vedrørende spørgsmålet om, hvorvidt afvisning af flere seddelstørrelser er i konflikt med den dagældende § 10 i lov om visse betalingsmidler, svarende til den nugældende § 81 i betalingsloven:

”Spørgsmålet er, om afvisning af flere seddelstørrelser eller møntenheder er i konflikt med § 10 i lov om visse betalingsmidler, der vedrører forbud mod diskrimination af kontant betaling i forhold til betalingskort, jf. nedenfor om denne bestemmelse.

Dette må antages at gælde, hvis fx en erhvervsdrivende generelt nægter at modtage sedler af en vis størrelse, idet dette indirekte kan tvinge køber til at anvende betalingskort. Derimod vil et afslag på at modtage særlige seddel- eller møntstørrelser efter omstændighederne være acceptabelt, hvis afslaget er konkret begrundet, fx i aktuelle oplysninger om, at falske mønter eller sedler i visse denominationer er i omløb.”

⁶ Forslag nr. 39 til lov om forbrugeraftaler, fremsat den 9. oktober 2013, de specielle bemærkninger til § 3

⁷ Europa-Parlamentets og Rådets direktiv 2011/83/EU af 25. oktober 2011 om forbrugerrettigheder, om ændring af Rådets direktiv 93/13/EØF og Europa-Parlamentets og Rådets direktiv 1999/44/EF samt om ophævelse af Rådets direktiv 85/577/EØF og Europa-Parlamentets og Rådets direktiv 97/7/EF.

Forbrugerombudsmandens vurdering

Efter betalingslovens § 81, stk. 1, er betalingsmodtagere forpligtet til at modtage betaling med kontanter, hvis de også modtager elektroniske betalingsinstrumenter. Midttrafik modtager elektroniske betalingsinstrumenter, da der betales med betalingskort for bestilling af flextur og handicapkørsel online og via app. Derfor er Midttrafik også forpligtet til at modtage betaling med kontanter, medmindre betaling sker i et ubemandet selvbetjeningsmiljø, eller der er tale om fjernsalg, jf. betalingslovens § 81, stk. 2.

Der er tale om undtagelser til kontantreglen, som ifølge forarbejderne er tiltænkt situationer, hvor der ikke er personlig kontakt mellem forbrugeren og betalingsmodtageren.⁸ Ved personbefordring er der personlig kontakt mellem forbrugeren og betalingsmodtageren.

Hertil kommer, at aftaler om personbefordring er undtaget fra *forbruger-aftalelovens* bestemmelser om fjernsalg. Hvis personbefordring ikke var undtaget, ville det efter Forbrugerombudsmandens opfattelse kunne give anledning til tvivl, om og i så fald under hvilke omstændigheder aftaler om personbefordring ville være omfattet af forbrugerrettighedsdirektivets definition på fjernsalgsaftaler, således som gengivet ovenfor, da den erhvervsdrivende og forbrugeren er tilstede på trafikskabets ”forretningssted” – i form af den bestilte vogn – ved levering af transportydelsen.

Forbrugeren kan således også betale kontant ved indstigning i vognen efter en telefonisk bestilling af flexture og handicapkørsel samt ved online-/app-bestilling af handicapkørsel, uden at dette indebærer anden forskel i leveringen af ydelsen end selve betalingsmåden.

På den baggrund er Forbrugerombudsmanden mest tilbøjelig til at mene, at undtagelsen om fjernsalg i § 81, stk. 2, i betalingsloven ikke finder anvendelse på Midttrafiks salg af flextur og handicapkørsel, som kan bestilles telefonisk, online eller via en app og betales med elektroniske betalingsinstrumenter via en hjemmeside eller en app eller kontant til vognens chauffør.

Under hensyn til, at spørgsmålet om, hvorvidt kontantreglen finder anvendelse, kan give anledning til tvivl, og da Midttrafik har indført en praksis ultimo 2019, hvorefter chaufførerne kan give byttepenge tilbage op til nærmeste hundrede kroner, foretager Forbrugerombudsmanden sig ikke mere i sagen, idet Forbrugerombudsmanden antager, at Midttrafik drager omsorg for, at Midttrafiks chauffører *fremover* altid giver byttepenge tilbage op til i hvert fald nærmeste hundrede kroner.

⁸ Jf. også Forbrugerombudsmandens sag nr. 16/10011.

Forbrugerombudsmanden skal i den forbindelse gøre opmærksom på, at det efter Forbrugerombudsmandens opfattelse under alle omstændigheder vil være i strid med markedsføringslovens regler om god skik, hvis chauffør afslår en anmodning om at give byttepenge tilbage til mere end nærmeste hundrede kroner, selv om chaufføren har tilstrækkelig kontantbeholdning til faktisk at kunne efterkomme en sådan anmodning.

Forbrugerombudsmanden skal endvidere oplyse, at Forbrugerombudsmanden har inviteret Trafikselskaberne i Danmark til et møde med henblik på en drøftelse af spørgsmålet om overholdelse af kontantreglen ved rejser med bus.

Forbrugerombudsmanden skal beklage den lange sagsbehandlingstid.

Afslutningsvist skal Forbrugerombudsmanden gøre opmærksom på, at vi forventer at offentliggøre en pressemeddelelse om sagerne, efter afholdelse af møde med Trafikselskaberne i Danmark. Midttrafik vil modtage pressemeddelelsen til orientering inden offentliggørelsen.

Midttrafik er velkommen til at kontakte Forbrugerombudsmanden, hvis ovenstående giver anledning til spørgsmål.

Med venlig hilsen
På Forbrugerombudsmandens vegne

Anette Jin Kristensen
Specialkonsulent

The logo for DPO Danmark, featuring the letters 'DPO' in a bold, red, sans-serif font. The letter 'O' is stylized as a red circle with a blue dot in the center.

danmark

- et trygt samfund med it og data

A photograph showing the silhouettes of four business professionals in a meeting. They are seated around a table in a room with large windows overlooking a sunset. The scene is backlit by the warm light of the setting sun, creating a professional and collaborative atmosphere.

Tilsynsrapport Midttrafik - December 2022

DPO-Danmark ApS | www.DPO-Danmark.dk

Højbro Plads 10, 1200 København K

CVR: 30 98 85 31 | Tlf. 33 11 81 00

Indholdsfortegnelse

Introduktion.....	2
Vurderingsskala.....	3
Tilsynstemaer og kontroller.....	4
Ledelsesresume.....	5
Afsluttende bemærkninger og næste tilsyn.....	12
Bilag 1: Læsevejledning.....	13
Bilag 1A-1D: kontroller, vurderinger, anbefalinger og prioriteringsforslag.....	
Bilag 2: Organisationens bemærkninger til rapportens udkast.....	
Bilag 3: Årets handlinger.....	

Introduktion

DPO-Danmark har i 4. kvartal 2022 gennemført et årligt tilsyn vedrørende GDPR-compliance hos Midttrafik.

Resultaterne fra tilsynet afrapporteres i denne rapport til ledelsen. Rapporten giver en status på niveauet for GDPR-compliance hos Midttrafik.

Rapporten kan samtidig bruges af Midttrafik som et benchmarkings-værktøj til over tid at øge niveauet for GDPR-compliance, som et redskab til arbejdet med implementering af GDPR i bund og/eller som et grundlag til at iværksætte prioriteret afhjælpning.

Tilsynet udføres som en del af DPO-Danmarks lovpligtige opgave som DPO for Midttrafik med at føre tilsyn med GDPR-compliance hos Midttrafik.

Rapporten indeholder følgende afsnit: Vurderingsskala, tilsynstemaer og kontroller, ledelsesresumé og afsluttende bemærkninger. Rapportens bilag 1 indeholder læsevejledning til skema med kontroller, bilag 1A-1D indeholder skema med kontroller og DPO'ens vurderinger, anbefalinger og prioriteringsforslag. Bilag 2 fremlægger organisationens bemærkninger til udkastet og bilag 3 viser årets handlinger.





Vurderingsskala

DPO Danmarks tilsyn vedrørende databeskyttelse hos Midttrafik er baseret på en 4-trins skala, hvor 1 er lavest og 4 er højest complianceniiveau.

Niveau 1-3 indikerer manglende GDPR-compliance, hvor niveau 1 er kritisk mangel, niveau 2 er væsentlig mangel og niveau 3 er mindre væsentlig mangel. Niveau 4 indikerer GDPR-compliance.

Midttrafik bør stræbe efter at være på niveau 3 eller højere.

På niveau 1-2 er der risiko for alvorlig kritik og bøder fra Datatilsynet i tilfælde af tilsyn. På niveau 3 er der risiko for kritik fra Datatilsynet i tilfælde af tilsyn.

Complianceniiveau		Beskrivelse	Prioritet
1		Kritisk mangel Anvendes ved forhold eller risici, der anses for kritiske. Et <i>forhold</i> anses som kritisk, når der er tale om en alvorlig mangel i strid med databeskyttelsesretlige krav. En <i>risiko</i> anses for kritisk, hvis der er en høj grad af sandsynlig risiko for de registreredes rettigheder og frihedsrettigheder. Prioritet 1 markeringer (P1) rapporteres til ledelsen med anbefaling om at afhjælpe forholdet straks.	P1
2		Væsentlig mangel Anvendes ved forhold eller risici, der anses for væsentlige. Et <i>forhold</i> anses for væsentligt, når der er tale om en mangel i strid med databeskyttelsesretlige regler. En <i>risiko</i> anses for væsentlig, hvis der er middel grad af sandsynlig risiko for de registreredes rettigheder og frihedsrettigheder. Prioritet 2 markeringer (P2) rapporteres til ledelsen med anbefaling om, at ledelsen afhjælper forholdet.	P2
3		Mindre væsentlig mangel Anvendes ved forhold eller risici, der anses for mindre væsentlige. Et forhold anses for mindre væsentligt, når det er tale om en uvæsentlig mangel i strid med databeskyttelsesretlige regler. En risiko anses for mindre væsentlig, hvis der er en lille grad af sandsynlig risiko for de registreredes rettigheder og frihedsrettigheder. Prioritet 3 markeringer (P3) rapporteres kun til ledelsen som opmærksomhedspunkter, men med en anbefaling til ledelsen om at tage stilling til, om forholdet giver anledning til yderligere opfølgning.	P3
4		Overholdelse Databeskyttelsesretlige krav overholdes, med mulighed for forbedring i konkrete tilfælde.	N/A

Tilsynstemaer og kontroller

DPO Danmarks tilsyn dækker fire tilsynstemaer med tilhørende kontroller, som afspejler krav efter GDPR eller på anden måde har betydning for beskyttelse af persondata.

A. Gennemsigtighed og kontrol med personoplysninger

- | | |
|--|---------------------------------------|
| A1. Hjemmel til behandling af persondata | A5. Registreredes rettigheder |
| A2. Samtykke | A6. Fortegnelse |
| A3. Sletning af persondata | A7. Overførsel til usikre tredjelande |
| A4. Oplysningspligt | |

B. Sikring af databeskyttelse

- | | |
|----------------------------------|---|
| B1. Privacy by design og default | B5. Håndtering af brud på persondatasikkerhed |
| B2. Databehandleraftaler | B6. Konsekvensanalyse (DPIA) |
| B3. Tilsyn af databehandlere | |
| B4. Risikovurderinger | |

C. Tekniske foranstaltninger

- | | |
|-----------------------------|---|
| C1. Antivirus | C7. Kryptering af harddisk og filsystem |
| C2. Firewall | C8. Kryptering via internettet |
| C3. Segmentering af netværk | C9. Sårbarheder og penetrationstests |
| C4. Adgangsstyring | C10. Opdateringer og patches |
| C5. Logning | C11. Multi faktor autentifikation (MFA) |
| C6. Systemovervågning | C12. Backup |

D. Organisatoriske foranstaltninger (governance)

- | | |
|-----------------------------------|-----------------------------|
| D1. Informationssikkerhedspolitik | D5. Uddannelse og awareness |
| D2. Roller og ansvar | D6. Business Recovery Plan |
| D3. Ledelsesforankring | D7. Disaster Recovery Plan |
| D4. Årshjul | D8. Fysisk sikkerhed |

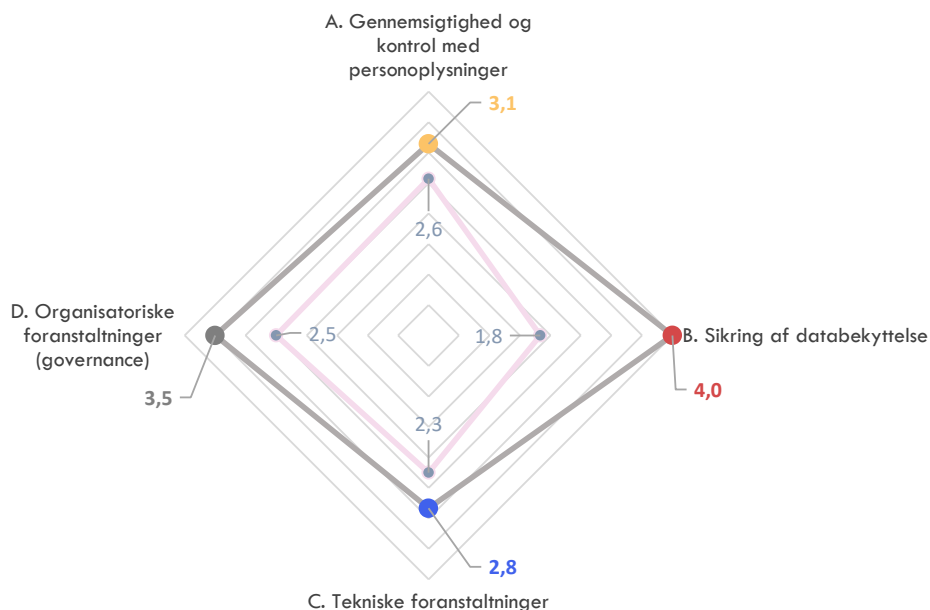
Ledelsesresumé

Samlet set viser resultaterne fra tilsynet, at organisationen har et højt GDPR-complianceniiveau på 4 for så vidt angår 46% af kontrollerne og 3 for så vidt angår 23% af kontrollerne. Det betyder, at organisationen generelt overholder mange GDPR-krav på tidspunktet for tilsynet. Det er positivt, at organisationens arbejde med GDPR og informationssikkerhed har båret frugt, og at dette afspejles positivt i resultaterne fra tilsynet. Der er dog flere kontroller, hvor organisationens GDPR-complianceniiveau ligger på 1 (6%) eller 2 (25%). Det betyder, at organisationen i forhold til de pågældende kontroller ikke overholder GDPR-krav. Det medfører en risiko for manglende beskyttelse af de registreredes rettigheder og frihedsrettigheder, herunder risiko for kritik eller bøder fra Datatilsynet, hvis tilsynet skulle undersøge organisationens overholdelse af de pågældende GDPR-krav.

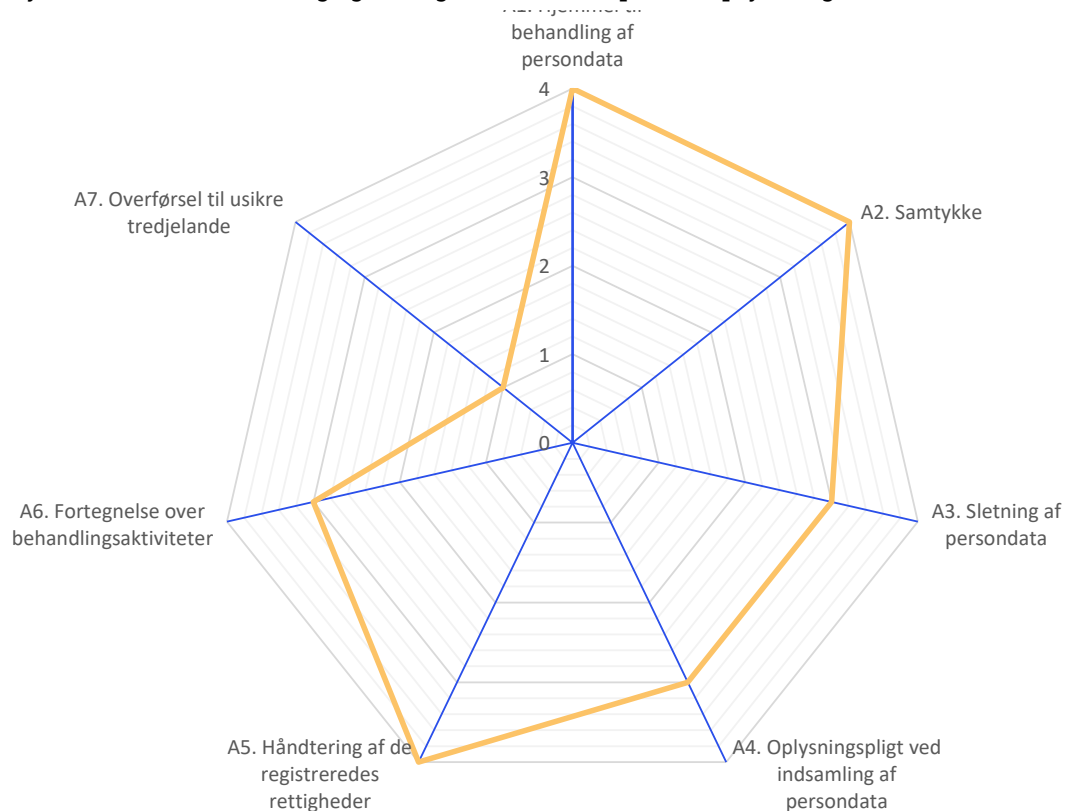
Organisationens gennemsnitlige GDPR-complianceniiveau var på tidspunktet for tilsynet i 2022 på 3,3. Dette er et flot resultat i sammenligning med complianceniiveauet, som sidste år var på 2,3. Gennemsnitstallet afspejler dog, at selvom organisationens complianceniiveau var på 4 eller 3 i forhold til mange kontroller, ligger organisationens complianceniiveau på 1-2 i forhold til flere kontroller, som har betydning for beskyttelse af persondata og informationssikkerhed i organisationen (se nedenfor).

Gennemsnit på baggrund af kontroltemaer

I den følgende model præsenteres gennemsnitsresultaterne for tilsynet, fordelt på kontroltemaerne. De fire scorer udgør gennemsnittet af organisationens samlede score indenfor det pågældende kontroltema.

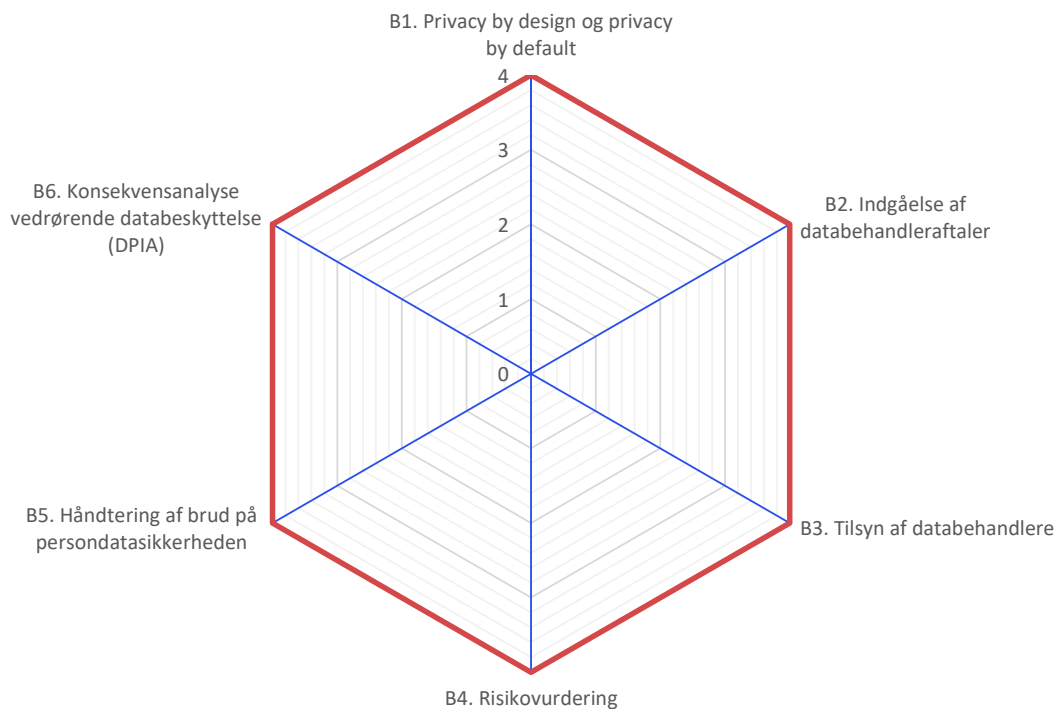


Tilsystema A - Gennemsigtighed og kontrol med personoplysninger



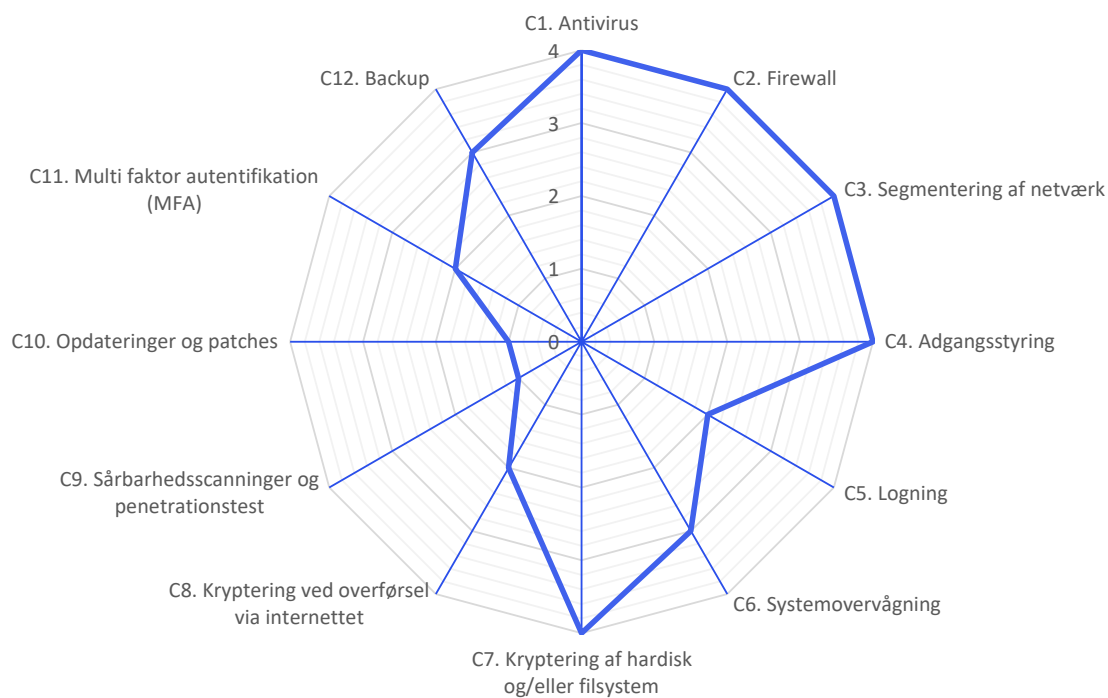
På dette området udgør gennemsnitsniveauet for compliance 3,1. Sidste års niveau var 2,6. Det er positivt, at organisationen har arbejdet mod et højere niveau af compliance. Det trækker navnlig ned, at organisationen i nogle tilfælde overfører persondata ulovligt til usikre tredjelande. Overførsel af persondata til usikre tredjelande er et fokusområde for Datatilsynet i de kommende år, da EU-Domstolens afgørelse i Schrems II-sagen bl.a. fastslår, at nationale tilsyn skal håndhæve reglerne om overførsel til tredjelande.

Tilsystema B - Sikring af databeskyttelse



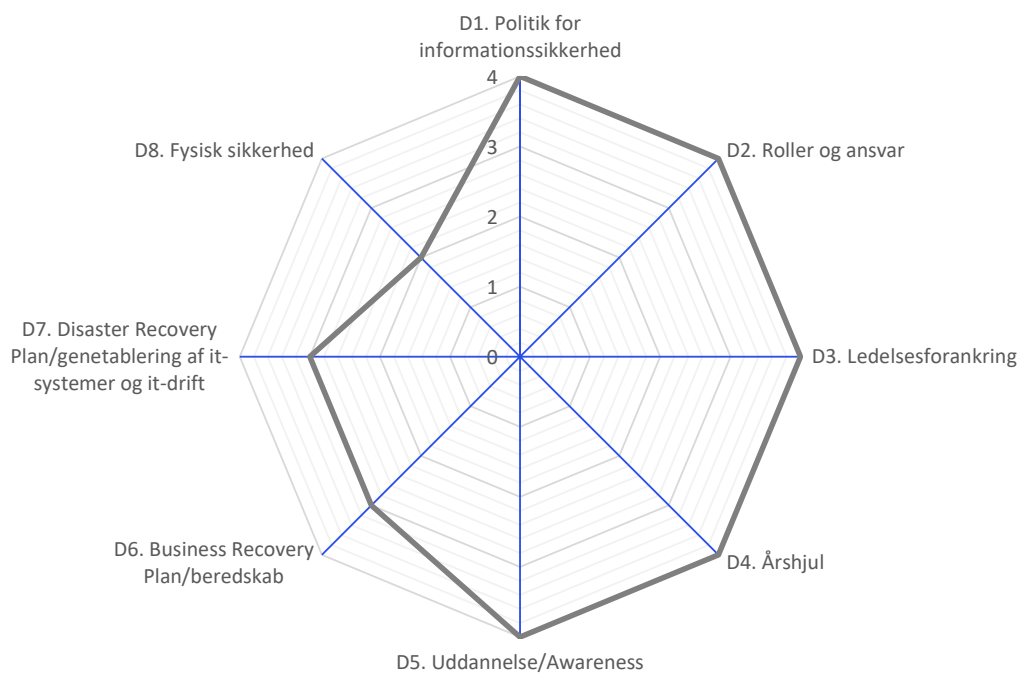
På området her udgør gennemsnitsniveauet for compliance 4,0. Sidste års niveau var 1,8. Organisationen har gjort et rigtig godt stykke arbejde med at højne persondatasikkerheden på området. styr på indgåelse af databehandleraftaler og håndtering af brud på persondatasikkerheden. Selvom der kan være mulighed for forbedring i de konkrete tilfælde, skal organisationen have ros for sin indsats.

Tilsynsystema C - Tekniske foranstaltninger



På dette område er gennemsnitsniveauet for compliance 2,8. Sidste års niveau var 2,4. Organisationen har implementeret mange relevante tekniske foranstaltninger, som beskytter informationssikkerhed og persondata. Men det trækker navnlig ned, at der mangler politikker, styring og/eller planlægning med logning, kryptering via internettet, sårbarhedsscanninger og penetrationstests, opdateringer og patches, multi faktor autentifikation og backup.

Tilsynsystema D - Organisatoriske foranstaltninger/governance



På området her udgør gennemsnitsniveauet for compliance 3,5. Sidste års niveau var 2,5. Det er positivt, at organisationen har arbejdet mod et højere niveau af compliance. Organisationen har implementeret mange relevante organisatoriske foranstaltninger, som beskytter informationssikkerhed og persondata. Det trækker dog navnlig ned, at organisationen ikke er helt i mål med proceduren for fysisk adgangssikkerhed for lokaliteter, hvori der opbevares og behandles persondata.

Anbefalinger

DPO-Danmark anbefaler organisationen som første prioritet at øge complianceniiveauet i forhold til følgende kontroller:

Prioritet P1

- P1 A7. Overførsel til usikre tredjelande
- P1 C9. Sårbarhedsscanninger og penetrationstest
- P1 C10. Opdateringer og patches

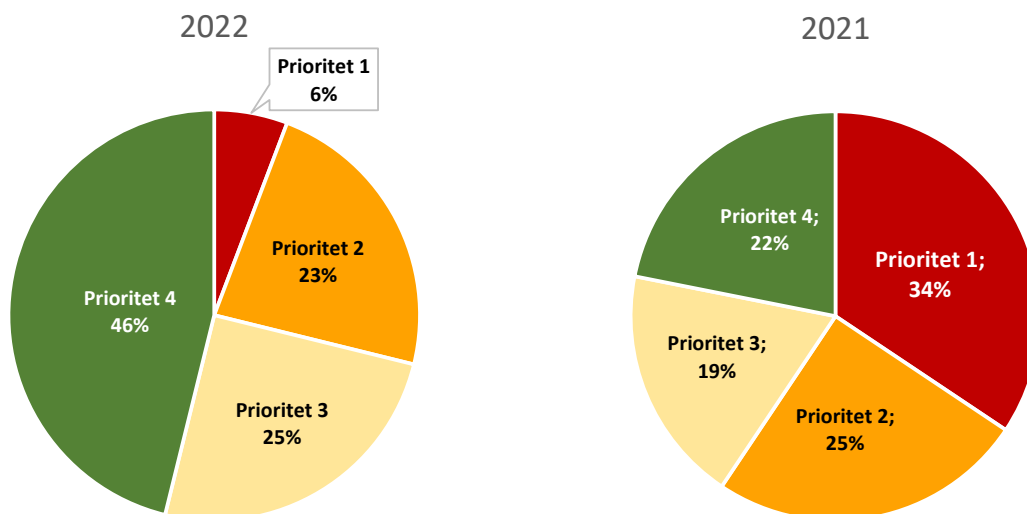
Prioritet P2

- P2 C5. Logning
- P2 C8. Kryptering ved overførsel via internettet
- P2 C11. Multi faktor autentifikation (MFA)
- P2 D8. Fysisk sikkerhed

Der henvises i øvrigt til DPO-Danmarks konkrete vurderinger og anbefalinger i forhold til de enkelte kontroller i bilag 1A-1D.

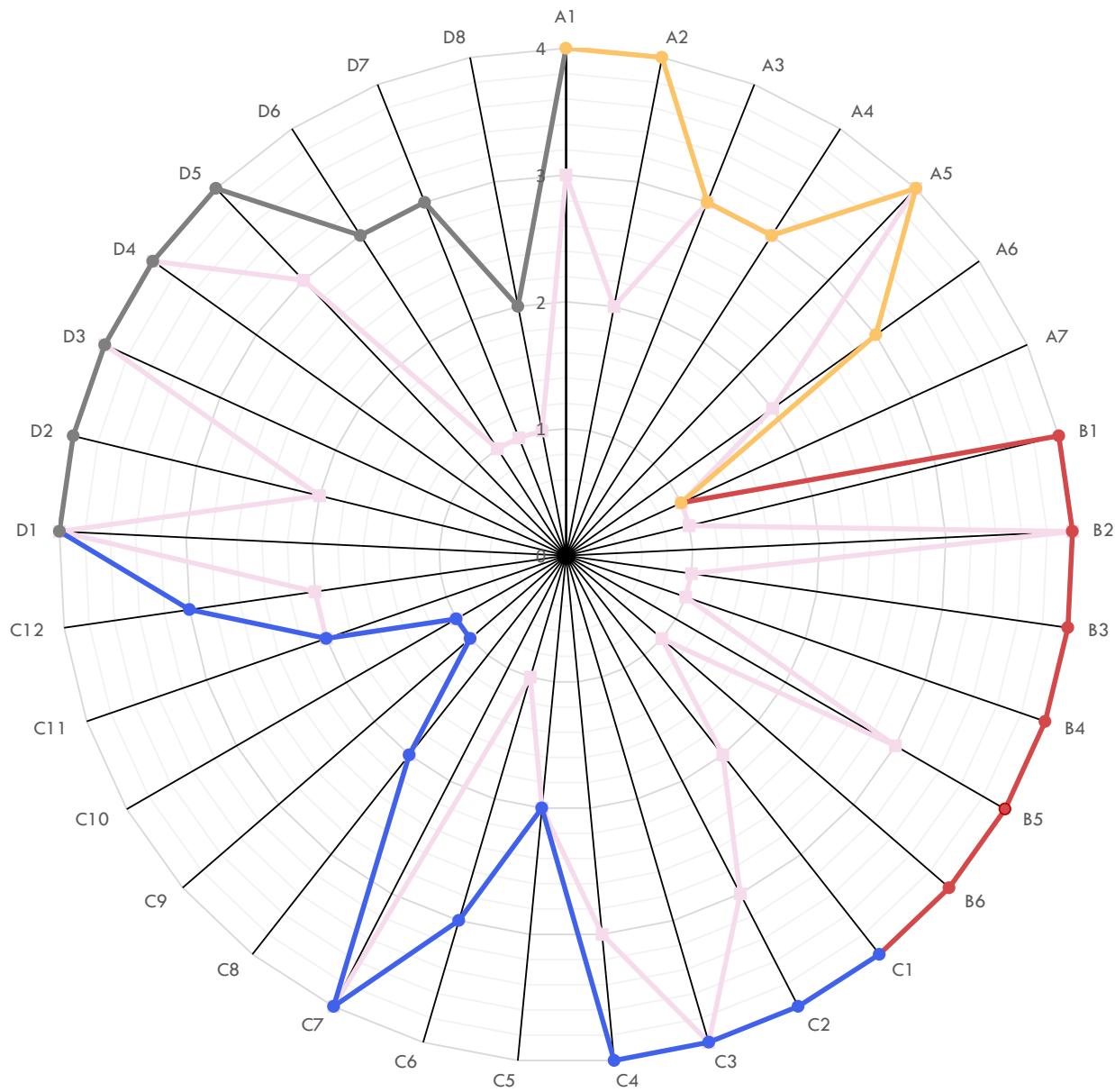
Oversigt over fordeling af prioriteter

Nedenstående model repræsenterer fordelingen af de forskellige prioteter på tværs af kontrollerne.



Oversigt over alle kontroller

I nedenstående model præsenteres de samlede resultater fra tilsynet med kontrollerne. Samtlige af organisationens scorer for de udvalgte kontroller uddybes i vurderingsskalaen på side 3. Den indre, blågrå linje er organisationens scorer fra sidste år. En uddybning af kontrollernes score findes i bilag 1A-1D.



Afsluttende bemærkninger og næste tilsyn

Indeværende rapport er d. 14. december 2022 udarbejdet af

Michael Nielsen

Partner, Direktør

DPO Danmark ApS

og

Isabella Westh

Compliancekonsulent, cand.jur.

DPO Danmark ApS

Det næste DPO tilsyn bliver udført i 4. kvartal 2023.

Bilag 1: Kontroller og læsevejledning til disse

Skema med kontroller i bilag 1A-1D indeholder felter, som betyder følgende:


Felt	Beskrivelse
Compliancemål	Kontrollens mål. Det, som organisationen skal opfylde for at efterleve kontrollen.
Complianceniveau	Markering af organisationens aktuelle complianceniveau (score) baseret på en konkret vurdering af niveauet for efterlevelse af kontrollen.
Prioritet	Markering af prioritet for afhjælpning afhængig af organisationens aktuelle complianceniveau.
Undersøgelse	Handlinger, som DPO'en har foretaget for at undersøge complianceniveauet for kontrollen. "Undersøgelse" betyder, at DPO'en har stillet spørgsmål til relevant personale i organisationen om, hvordan kontrollen efterleves. "Inspicering" betyder, at DPO'en har gennemgået materiale fra organisationen, som indeholder information om efterlevelse af kontrollen. "Observation" betyder, at DPO'en har observeret, hvordan kontrollen efterleves hos organisationen.
Vurdering	DPO'ens konkrete vurdering af niveauet for efterlevelse af kontrollen hos organisationen.
Anbefaling	DPO'ens konkrete anbefaling til organisationen.

Bilag 1A: Vurderingsgrundlag og anbefalinger for gennemsigtighed og kontrol med personoplysninger

A. Gennemsigtighed og kontrol med persondata


A1. Hjemmel til behandling af persondata

Der må kun behandles persondata, hvis der er hjemmel til behandling af persondata (GDPR artikel 6 og 9)

Compliancemål	Complianceniveau	Prioritet
Der er identificeret hjemmel til behandling af persondata.	4 	n/a
Undersøgelse		
Undersøgt, om der er en opdateret oversigt over behandlingshjemmel for enhver behandling af persondata. Inspiceret, om dokumenteret oversigt over behandlingshjemmel er opdateret, og at behandlingshjemmel forekommer korrekt.		
Vurdering		
Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.		
Anbefaling		
Ingen.		

A2. Samtykke

Behandling af persondata på grundlag af samtykke skal altid være baseret på gyldigt samtykke fra de personer, som er genstand for behandlingen (de registrerede) (GDPR artikel 4, nr. 11 og artikel 7).

Compliancemål	Complianceniveau	Prioritet
Der behandles kun persondata på baggrund af gyldigt samtykke fra de registrerede.	4 	n/a

Undersøgelse

Undersøgt, om der foreligger skriftlig procedure, som sikrer, at der indhentes gyldigt samtykke fra de registrerede forinden behandling af persondata på grundlag af samtykke.

Inspiceret for en udvalgt behandlingsaktivitet, at indhentet samtykke fra de registrerede forekommer gyldigt.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

A3. Sletning af persondata

Persondata må ikke opbevares i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende persondata behandles. Det vil med andre ord sige, at man ikke må behandle persondata længere end nødvendigt. Herefter skal oplysninger slettes eller anonymiseres (GDPR artikel 5)

Compliancemål	Complianceniveau	Prioritet
Persondata opbevares ikke længere end nødvendigt.	3	P3

Undersøgelse

Undersøgt, om der foreligger opdateret skriftlig procedure, som sikrer, at persondata slettes.

Inspiceret, at skriftlig procedure er opdateret og forekommer tilstrækkelig for sletning af persondata.

Vurdering

Det vurderes, at organisationen har oprettet en slettepolitik, som årligt kontrolleres gennem kontrol for sletning samt udfyldelse af skema for sletning hos den sletteansvarlige på det givne område, hvilket er positivt. Det vurderes desuden, at organisationen ikke på nuværende tidspunkt udfører stikprøvekontrol af, om sletning faktisk er tilstrækkeligt udført, ifølge slettepolitikken.

Anbefaling

Det anbefales, at organisationen udfører stikprøver på om sletning er foretaget efter den i politikken beskevne metode mindst én gang årligt.

Det anbefales yderligere, at organisationen opsætter en halvårlig slettekontrol på HR-området.

A4. Oplysningspligt ved indsamling af persondata

Når der indsamles persondata om personer, som er genstand for behandling (de registrerede), skal der udleveres skriftlig information om behandlingen til de registrerede. Der skal udleveres information om: Navn på og kontaktoplysninger for den dataansvarlige og databeskyttelsesrådgiveren, formål og retsgrundlag for behandling, typer af persondata (kun artikel 14), kilder hvorfra persondata hidrører (kun artikel 14), kategorier af modtagere som oplysningerne videregives til, herunder GDPR-rettighederne for de registrerede. (GDPR artikel 13-14)

Compliancemål	Complianceniveau	Prioritet
Der udleveres tilstrækkelig skriftlig information om behandlingen til de registrerede ved indsamling af persondata.	3	P3

Undersøgelse

Undersøgt, om der foreligger opdateret skriftlig procedure, som sikrer, at der udleveres information om behandlingen til de registrerede ved indsamling af persondata.

Inspiceret for en udvalgt behandlingsaktivitet, at udleveret information til de registrerede forekommer i overensstemmelse med minimumskravene efter GDPR artikel 13-14.

Vurdering

Organisationen har gjort et godt stykke arbejde med udarbejdelse af privatlivspolitik til jobansøgere og til nye medarbejdere.

Anbefaling

Det anbefales at organisationen linker til privatlivspolitikken under selve jobannoncen.

A5. Håndtering af de registreredes rettigheder

De personer, som er genstand for behandling af persondata (de registrerede), har en række rettigheder efter GDPR fx ret til indsigt i persondata, ret til berigtigelse af forkert persondata, ret til at anmode om sletning af persondata, og ret til at gøre indsigelse mod behandling af persondata. Henvendelser fra de registrerede, som gør brug af deres GDPR-rettigheder, skal håndteres hurtigst muligt og senest inden for en 30-dages frist. (GDPR artikel 12 og artikel 15-22).

Compliancemål	Complianceniveau	Prioritet
De registreredes rettigheder kan håndteres	4 	n/a

Undersøgelse

Undersøgt, om der foreligger skriftlig procedure, som sikrer, at henvendelser fra de registrerede kan håndteres.

Inspiceret, at skriftlig procedure er opdateret og forekommer tilstrækkelig for håndtering af de registreredes rettigheder.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

A6. Fortegnelse over behandlingsaktiviteter

Der skal føres en skriftlig og elektronisk fortegnelse (oversigt) over alle behandlinger af persondata (behandlingsaktiviteter).

Fortegnelsen skal bl.a. indeholde følgende oplysninger: Navn på og kontaktoplysninger for den dataansvarlige og databeskyttelsesrådgiveren, formålene med behandlingerne af persondata, beskrivelse af kategorierne af registrerede og typer af persondata, herunder kategorier af modtagere, som persondata videregives til. (GDPR artikel 30).

Compliancemål	Complianceniveau	Prioritet
Der føres en fortegnelse over alle behandlingsaktiviteter	3	P3

Undersøgelse

Undersøgt, om der føres en opdateret fortegnelse over alle behandlingsaktiviteter.

Inspiceret, om fortegnelsen er opdateret og forekommer i overensstemmelse med minimumskravene efter GDPR artikel 30.

Vurdering

Det vurderes, at organisationen har gjort et godt stykke arbejde med opdatering af sin fortegnelse siden sidste år. Det vurderes dog, at visse slettefrister for opbevaring af persondata i henhold til behandlingsaktivitetens formål ikke er opdateret i forhold til slettepolitikens indhold.

Anbefaling

Det anbefales slutteligt, at organisationen opdaterer fortegnelsen med de i slettepolitikken angivne frister for sletning.

A7. Overførsel til usikre tredjelande

Der må kun må overføres persondata til usikre tredjelande, hvis der der foreligger et gyldigt overførselsgrundlag efter GDPR artikel 46-49. Overførsel til usikre tredjelande ved brug af standard contractual clauses (SCCs) kræver herudover, at der forinden overførsel er foretaget en undersøgelse af, om det pågældende modtagerlands beskyttelsesniveau i det væsentligste svarer til niveauet i henhold til EU-retten. Hvis beskyttelsesniveauet i modtagerlandet er utilstrækkeligt, skal der forinden overførsel implementeres effektive supplerende foranstaltninger, som garanterer et tilstrækkeligt niveau svarende til i henhold til EU-retten (transfer impact assessment). (GDPR artikel 45-49)

Compliancemål	Complianceniveau	Prioritet
Der sker alene overførsel af persondata til usikre tredjelande på baggrund af gyldigt overførselsgrundlag.	1	P1

Undersøgelse

Undersøgt, om der er identificeret overførsel af persondata til usikre tredjelande, og om der foreligger skriftlig procedure, som sikrer, at der alene overføres persondata på baggrund af gyldigt overførselsgrundlag.

Inspiceret, at skriftlig procedure er opdateret og forekommer tilstrækkelig i forhold til sikring af transfer impact assessment forinden overførsel.

Vurdering

Det vurderes, at organisationen har nu ophørt samarbejdet med Publico og Kraftvaerk er ophørt med at anvende en russisk underleverandør. Dog anvender organisationen Microsoft Azure som hostingleverandør, uden at der ses at være udført fornøden transfer impact assessment og implementeret tilstrækkelige supplerende foranstaltninger, som sikrer et passende beskyttelsesniveau for persondata.

Anbefaling


Det anbefales at organisationen, som dataeksportør, implementerer passende sikkerhedsforanstaltninger, som følger det Europæiske Databeskyttelsesråds Henstilling af 2020 og Datatilsynets Cloudvejledning af 2022.

Bilag 1B: Vurderingsgrundlag og anbefalinger for sikring af databeskyttelse

B. Sikring af databeskyttelse

B1. Privacy by design og privacy by default

Privacy by design og privacy by default skal indgå i overvejelserne i forbindelse med design og implementering af nye systemer, herunder ved ændringer i eksisterende systemer. Privacy by design betyder, at alle systemer til persondatabehandling skal designes, så de tager højde for beskyttelse af persondata. Privacy by default betyder, at konfigurerbare muligheder i systemer og alle standardindstillinger skal indstilles til det minimalt nødvendige for persondatabehandlingen. (GDPR artikel 25)

Compliancemål	Complianceniveau	Prioritet
Kravene om privacy by design i nye systemer og privacy by default (standardindstillinger) efterleves	4 	n/a

Undersøgelse

Undersøgt, om der er etableret skriftlige procedurer eller anden dokumentation, hvori sikring af databeskyttelse gennem design og standardindstillinger er beskrevet.

Vurdering


Organisationen har gjort et godt stykke arbejde med udarbejdelse af politik for privacy by design og default. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Organisationen kan overveje at indsætte en beskrivelse af, hvordan behandlingsprincipperne efter GDPR artikel 5 efterleves i den nye politik for privacy by design og default.

B2. Indgåelse af databehandleraftaler

Den dataansvarlige skal indgå databehandleraftaler med leverandører (databehandlere), som den dataansvarlige har valgt til at behandle persondata på sine vegne. (GDPR artikel 4, litra 7, og artikel 28).

Compliancemål	Complianceniveau	Prioritet
Der er indgået databehandleraftaler med alle databehandlere	4 	n/a

Undersøgelse

Undersøgt, om der er etableret en formaliseret proces, som sikrer, at der indgås databehandleraftaler med alle databehandlere.

Inspiceret, at der foreligger et opdateret register (oversigt) over databehandlere, som giver et samlet overblik over anvendte databehandlere.

Vurdering


Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

B3. Tilsyn af databehandlere

Den dataansvarlige skal føre kontrol med, at databehandleren overholder sine forpligtelser som beskrevet i databehandleraftalen. Der skal føres kontrol med, at databehandleren opretholder et passende beskyttelsesniveau for de personer, som er genstand for behandling (de registrerede). Kontrol kan gennemføres ved at stille spørgsmål til databehandleren eller ved at ved at gennemgå revisorerklæringer (fx ISAE 3000 GDPR erklæring) for databehandleren. (GDPR artikel 28).

Compliancemål	Complianceniveau	Prioritet
Der føres regelmæssigt tilsyn med databehandlers opfyldelse af betingelserne i databehandleraftalen.	4 	n/a

Undersøgelse

Undersøgt, om der er etableret en formaliseret proces, som sikrer, at der føres tilsyn af databehandlere.

Inspiceret, om der foreligger en opdateret tilsynsplan, som afspejler risici for de registrerede forbundet med behandlingen.

Inspiceret dokumentation for, at der er gennemført tilsyn af databehandlere.

Vurdering


Organisationen har gjort et godt stykke arbejde med at etablere en plan for tilsyn med samtlige databehandlere, som er udarbejdet ud fra Datatilsynets vejledning om tilsyn med databehandlere. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

B4. Risikovurdering

Risici for de personer, som er genstand for behandling (de registrerede) skal evalueres på baggrund af en metode, som sikrer identificering af sandsynlighed for, at en eller flere trusler indtræder, samt identificering af konsekvenser for registrerede, hvis der sker tab af fortrolighed, integritet og tilgængelighed for persondata (risici for de registrerede). På baggrund af evaluering af risici skal det vurderes, om der skal implementeres sikkerhedsforanstaltninger for at sikre et passende beskyttelsesniveau for de registrerede (GDPR artikel 32).

Compliancemål	Complianceniveau	Prioritet
Der gennemføres risikovurdering, som identificerer risici for de registreredes rettigheder og frihedsrettigheder forbundet med behandling med henblik på at sikre et passende sikkerhedsniveau.	4 	n/a

Undersøgelse

Undersøgt, om der er etableret en formaliseret proces for risikovurdering, som sikrer identificering af risici for de registrerede. Inspiceret dokumentation for, at der er gennemført risikovurdering. Inspiceret, at seneste gennemførte risikovurdering forekommer at identificere risici for de registrerede rettigheder og frihedsrettigheder. Inspiceret, at seneste risikovurdering er forelagt til godkendelse på ledelsesniveau.

Vurdering


Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

B5. Håndtering af brud på persondatasikkerheden

Et "brud på persondatasikkerheden" er typisk en hændelse (et uheld eller ved en bevidst handling), hvor persondata kommer til uvedkommendes kendskab, hvor persondata ikke er tilgængelige eller hvor personoplysninger ikke længere er retvisende. Et sådant brud vil efter omstændighederne kunne medføre en risiko for de personer, som oplysningerne vedrører (de registrerede), og i visse tilfælde skal brud anmeldes til Datatilsynet samt meddeles til de registrerede. (GDPR art. 33 og 34).

Compliancemål	Complianceniveau	Prioritet
Brud på persondatasikkerheden håndteres	4 	n/a

Undersøgelse

Undersøgt, om der foreligger en skriftlig procedure, som sikrer, at brud på persondatasikkerheden kan håndteres.

Undersøgt, om der er etableret en proces, som sikrer, at der foretages regelmæssig gennemgang af tidligere brud for at vurdere, om særlige typer af brud kan undgås i fremtiden.

Inspiceret, at der er etableret et register, som giver en systematisk oversigt over alle tidligere brud.

Vurdering


Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

B6. Konsekvensanalyse vedrørende databeskyttelse (DPIA)

Der skal gennemføres konsekvensanalyse vedrørende databeskyttelse (DPIA) forud for behandlinger, som sandsynligvis vil indebære en høj risiko for rettigheder og frihedsrettigheder for de personer, som der skal behandles persondata om (de registrerede). Med "høj risiko for de registreredes rettigheder og frihedsrettigheder" menes de registreredes GDPR-rettigheder, herunder retten til databeskyttelse samt retten til privatliv for de registrerede i henhold til EU's charter om grundlæggende rettigheder (GDPR artikel 35).

Compliancemål	Complianceniveau	Prioritet
Der foretages ikke højrisiko behandlinger uden, at der forinden er gennemført konsekvensanalyse vedrørende databeskyttelse.	4 	n/a

Undersøgelse

Undersøgt, om der foreligger en formaliseret proces, som sikrer identificering af højrisiko behandlinger og gennemførelse af en DPIA forud for udførelse af højrisiko behandlinger.

Inspiceret, at skriftlig procedure eller anden dokumentation forekommer tilstrækkelig til at identificere højrisiko behandlinger og gennemføre en DPIA.

Inspiceret dokumentation for, at seneste gennemførte DPIA forekommer i overensstemmelse med minimumskravene i artikel 35, stk. 7.

Vurdering

Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

Bilag 1C: Vurderingsgrundlag og anbefalinger for tekniske foranstaltninger

Generelt om tekniske foranstaltninger

Tekniske foranstaltninger er tiltag, der primært er implementeret via tekniske mekanismer fx hardware, software og firmware i informationssystemer, og som bidrager til at beskytte fortrolighed, integritet og tilgængelighed af organisationens informationer, herunder persondata. Der skal implementeres passende tekniske foranstaltninger, som sikrer et passende sikkerhedsniveau for de personer, som er genstand for behandling (de registrerede). Kontrollerne, som hører under temaet tekniske foranstaltninger, er inspireret af sikkerhedsstandarderne ISO27001 og ISO27002.

C1. Antivirus

I et højt digitaliseret samfund, hvor truslen fra fx cyberkriminelle er meget høj, er det vigtigt, at organisationen har forholdt sig til risikoen for cyberangreb som fx ransomware. Dette vil ofte betyde, at der skal installeres antivirus på servere, databaser og medarbejdernes computere og servere. Alt efter organisationens aktiviteter kan det være nødvendigt at overveje, om andre enheder skal beskyttes mod cybertrusler. Det kan være fx være computere, som er delt mellem flere medarbejdere. Hertil kommer, at smartphones og tablets i stadig højere grad anvendes af organisationer til kommunikation og udveksling af oplysninger på lige fod med computere, og derfor kan behovet for beskyttelse med antivirus også være relevant i denne sammenhæng.

Compliancemål

Der er for systemer og databaser, der anvendes til behandling af persondata, installeret antivirus, som opdateres løbende

Complianceniveau

4



Prioritet

n/a

Undersøgelse

Undersøgt, om der for systemer og databaser, der anvendes til behandling af persondata, er installeret antivirus, som løbende opdateres.

Vurdering


Det vurderes at organisationens IT-afdeling på nuværende tidspunkt har overblik over incidents og opdateringscyklus, eftersom de har fået adgang til dashboardet via GlobalConnect.

Anbefaling

Ingen.


C2. Firewall

En firewall er en digital barriere mellem organisationens eget netværk og andre netværk. En sådan firewall overvåger indgående og udgående netværkstrafik og blokerer for uønsket data baseret på allerede opsatte sikkerhedsregler. En firewall kan både være software- og hardwarebaseret.

Compliancemål	Complianceniveau	Prioritet
Der er etableret firewalls for at beskytte it-udstyr, systemer og databaser, der anvendes til behandling af persondata.	4 	n/a
Undersøgelse		
Undersøgt om der er etableret firewalls for at beskytte it-udstyr, systemer og databaser, der anvendes til behandling af persondata.		
Vurdering		
Det vurderes, at organisationens løsning på er outsourcet til Global Connect, Globeteam og Lector (ESDH). Det vurderes, at organisationen har afdækket ansvars- og rollefordeling med leverandørerne på kontraktniveau og at der føres årlig kontrol med leverandørernes overholdelse heraf gennem indsamling af ISAE 3000-erklæring årligt. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.		
Anbefaling		
Ingen.		

C3. Segmentering af netværk

Ved at segmentere/adskille netværk kan organisationen begrænse skaden ved f.eks. hackerangreb eller malware. Alt efter organisationens størrelse, kompleksitet og typer af behandlingsaktiviteter kan det være nødvendigt at overveje om opdeling af netværk skal ske på baggrund af tillidsniveauer (f.eks. offentligt domæne, pc-domæne, serverdomæne), på baggrund af organisatoriske enheder (f.eks. HR, økonomi, marketing) eller en kombination af begge (f.eks. serverdomæne koblet til flere organisatoriske enheder). Med "segmentering (adskillelse) af egne netværk" menes, at organisationen har opdelt sin netværksinfrastruktur i to eller flere separate netværk typisk adskilt af en firewall.

Compliancemål	Complianceniveau	Prioritet
Egne netværk er segmenteret for at begrænse adgang til systemer og databaser, der anvendes til behandling af persondata.	4 	n/a

Undersøgelse

Undersøgt, om interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af persondata.

Inspiceret netværksdiagrammer og anden netværksdokumentation for vurdering af, om segmentering er behørig.

Vurdering


Det vurderes, at segmentering af netværk er udliciteret til Atea. Organisationens IT har selv adgang til Cisco ISE dashboard, og der følges op på, om netværk er segmenteret. Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

C4. Adgangsstyring

Alt efter organisationens størrelse og kompleksitet kan det være nødvendigt at udarbejde en procedure for at administrere brugeres (fx ansattes) systemadgange – fx deres adgang til persondata. En sådan administration af brugeradgange til persondata skal være begrundet i brugernes arbejdsbetingede behov og skal forebygge, at brugerne ikke kan tilgå oplysninger, som de ikke har behov for at anvende.

Compliancemål	Complianceniveau	Prioritet
Adgang til persondata er isoleret til brugere med arbejdsbetinget behov herfor.	4 	n/a

Undersøgelse

Undersøgt, om der er udarbejdet en skriftlig procedure for tildeling og nedlæggelse af brugeradgange og rettigheder til it-systemer, som afspejler need-to-know princippet, når nye medarbejdere ansættes eller eksisterende medarbejdere fratræder. Undersøgt, om der regelmæssigt foretages dokumenteret kontrol af medarbejdernes adgangsrettigheder for at sikre, at tildelte brugeradgang og rettigheder fortsat er korrekte (i overensstemmelse med need-to-know princippet).

Inspiceret, at der foreligger dokumentation ("Procedure for brugeradgange- og rettigheder) for regelmæssig vurdering og godkendelse af tildelte brugeradgange.

Vurdering


Det vurderes, at organisationen har etableret en procedure for tildeling og nedlæggelse af brugeradgange og rettigheder til it-systemer. Løbende kontroller på brugerstyring kører i ControlGDPR, hvor systemejere skal kontrollere, at adgange alene tildeles til personer med et arbejdsbetinget behov. Awareness omkring dette emne er høj både hos IT og HR. Organisationens HR-afdeling udsender månedligt en liste over medarbejdere, som er fratrådt til de respektive systemejere. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

C5. Logning

Logning er et vigtigt redskab til at kortlægge, f.eks. hvordan brugere af et it-system har ageret. Logningen/registreringerne af brugernes adfærd gengives i en såkaldt logoversigt eller logfil, som efterfølgende kan anvendes til bl.a. at analysere og dokumentere eventuelt misbrug af oplysninger. Logning kan i øvrigt også være et vigtigt værktøj til at opdage eventuelle hackere eller andre uvedkommendes adgang til organisationens systemer.

Compliancemål	Complianceniveau	Prioritet
Der er etableret logning og denne er beskyttet mod manipulation og uautoriseret adgang.	2	 P2

Undersøgelse

Undersøgt om der automatisk sker logning af bruger aktiviteter i it-systemer, som anvendes til behandling af personoplysninger (logoversigt). Undersøgt, om opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.

Inspiceret ud fra en tilfældigt udvalgt dags logning, at logfiler har det forventede indhold i forhold til opsætning, herunder inspiceret dokumentation, logopfølgning og håndtering af evt. sikkerhedshændelser, aktiviteter udført af systemadministratorer og andre med særlige rettigheder.

Vurdering

Der vurderes, at findes logs på en flerhed af forskellige systemer hos organisationen. IT tager sig af netværk igennem ISE Cisco. Azure foretager logning igenem design guide igennem Globeteam. Det vurderes også, at der mangler et fuldstændigt overblik over samtlige systemer og logning af persondata heri.

Anbefaling

Det anbefales at sikre beskyttelse af logning af brugeraktiviteter i it-systemer mod manipulation og sletning samt at sikre opsætning af logfiler på en måde, som giver et systematiseret overblik og sikre opfølgning og håndtering af sikkerhedshændelser.

Det anbefales desuden, at organisationen skaber overblik over alle systemer, som anvendes til behandling af persondata med fokus på, hvilke systemer, som endnu ikke logges.

C6. Systemovervågning

Systemovervågning (monitorering) hjælper med at forebygge, opdage og korrigere potentielle sikkerhedshændelser i systemer og databaser.

Compliancemål	Complianceniveau	Prioritet
Der er for de systemer og databaser, der anvendes til behandling af persondata, etableret systemovervågning med alarmering	3	P3

Undersøgelse

Undersøgt, om der for de systemer og databaser, der anvendes til behandling af persondata, er etableret systemovervågning med alarmering (monitorering).

Vurdering


Det vurderes, at GlobalConnect håndterer systemovervågning via managed service på serverne. På eksterne systemer ligger opgaven hos produktejerne. DDOS beskyttelse er håndteret hos GlobalConnect, som sender incidents til organisationens IT. Det vurderes yderligere, at organisationen har bedt GlobeTeam om at implementere SIEM efter best practice.

Anbefaling

Det anbefales, at alle servere løbende bliver indrullet i SIEM systemet.

C7. Kryptering af hardisk og/eller filsystem

Kryptering er en sikkerhedsforanstaltning, som bl.a. beskytter oplysninger mod uvedkommende adgang. Med "kryptering af harddisk og/eller filsystem" menes en software- eller hardwarebaseret krypteringsløsning, der sikrer, at indholdet er krypteret før indtastning af brugerens password. Ved harddisk kryptering (full disk encryption) er harddiskens indhold altid krypteret, og kun dele dekrypteres og placeres i hukommelsen (RAM) ved brug. Ved kryptering af filsystemet sikres indholdet af hele/dele af filsystemet, men ikke selve operativsystemet/systemfiler, mv. Eksempler på kendte software løsninger er BitLocker(Microsoft), FileVault (Apple), LUKS (Linux) eller VeraCrypt (IDRIX).

Compliancemål	Complianceniveau	Prioritet
Der er implementeret kryptering af harddisk og/eller filsystemer på medarbejdernes computere for at beskytte persondata.	4 	n/a

Undersøgelse

Undersøgt, om der er implementeret kryptering af hardisk og/eller filsystemer på medarbejdernes computere.

Inspiceret for tilfældigt udvalgt harddisk eller filsystem, at kryptering er effektiv.

Vurdering

Det vurderes, at alle enheder bliver krypteret med Bitlocker og at enhederne er låst på BIOS. Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.


Anbefaling

Ingen.

C8. Kryptering ved overførsel via internettet

Når oplysninger sendes over åbne netværk som f.eks. internettet, har man som afsender eller modtager som udgangspunkt ingen kontrol over, hvilke maskiner (servere m.v.) de konkrete oplysninger passerer igennem undervejs, herunder hvor i verden disse maskiner er lokaliseret. For at sikre sig mod, at de overførte oplysninger tilgås af uvedkommende, kan man anvende kryptering.

Med "overførsel" menes ikke kun transmission af oplysninger med e-mails, men også anden form for transmission af personoplysninger over netværk, som organisationen ikke har fuld kontrol over.

Compliancemål	Complianceniveau	Prioritet
Der anvendes effektiv kryptering ved overførsel af fortrolige og følsomme personoplysninger via internettet og med e-mail	2	 P2

Undersøgelse

Undersøgt om fortrolige og følsomme personoplysninger krypteres ved overførsel via internettet fx via HTTPS eller FTPS, og/eller med e-mail.

Vurdering


Det vurderes, at persondata krypteres ved overførsel via internettet gennem HTTPS. Det vurderes, at organisationen ikke på nuværende tidspunkt har en politik for kryptering.

Anbefaling

Det anbefales, at organisationen først udarbejder en politik for kryptering af transmission over netværk. Dernæst anbefales det, at organisationen udarbejder en krydsreference mellem den af organisationen etablerede systemoversigt og organisationens risikovurdering, for at sikre, om krypteringen tjener som passende teknisk foranstaltning.

C9. Sårbarhedsscanninger og penetrationstest

Sårbarhedsscannere kan tjekke systemer for at verificere, at operativsystemet er opdateret, har opdateret antivirussoftware og har en aktiveret firewall, herunder verificere at systemer ikke kører visse tjenester og protokoller, som kan blive udnyttet af trusler. Penetrationstest går videre end sårbarhedsscanninger og forsøger at udnytte de opdagde sårbarheder for at vise, i hvilket omfang det er muligt at opnå uautoriseret adgang til netværk, systemer, databaser, servere og persondata.

Compliancemål	Complianceniveau	Prioritet
De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og/eller penetrationstests.	1	 P1

Undersøgelse

Undersøgt, om de etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og/eller penetrationstests.
Undersøgt, om eventuelle afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret
Inspiceret om der foreligger dokumentation for den seneste test af de etablerede tekniske foranstaltninger.

Vurdering


Det vurderes ikke at være påvist, at der udført sårbarhedsscanninger eller penetrationstest. Organisationen oplyser dog, at de er i processen med at få styr på dette og har indhentet tilbud.

Anbefaling

Det anbefales, at der kommer sårbarhedsscanninger og/eller penetrationstests i stand for at klarlægge eventuelle afvigelser og svagheder ved de implementerede sikkerhedsforanstaltninger.

C10. Opdateringer og patches

Leverandører udgiver regelmæssigt patches, rettelser og opdateringer. Grundlæggende hærdningspraksis sikrer, at systemerne har alle relevante patches installeret, inklusive patches til operativsystemer og applikationer, herunder sikkerhedspatches, som har til formål at lukke sikkerhedshuller i programmer.

Compliancemål	Complianceniveau	Prioritet
Der er etableret en proces for regelmæssigt at opdatere og patche i programmer, styresystemer og andre softwareløsninger.	1	 P1

Undersøgelse

Undersøgt om der er etableret en proces for regelmæssigt at opdatere og patche i programmer, styresystemer og andre softwareløsninger.

Inspiceret for et tilfældigt udvalgt program, styresystem eller anden softwareløsning, at dette forekommer opdateret med relevante opdateringer, patches og sikkerhedspatches.

Vurdering

Det vurderes, at der er proces for opdatering og patching på OS niveau på klienter. Dette gøres igennem Ivanti, hvor der er styr på alle klienter. Det vurderes dog ikke, at organisationen har det fulde overblik over andre software programmer på klienterne. Der er ikke regelmæssig procedure for at opdatere Android og iOS på mobile enheder mv. IOT-devices i billetautomater og hardware-enheder med OS på er ukendt.

Anbefaling


Det anbefales, at der laves en procedure og årlige stikprøvekontroller for patching og opdatering af:

- IOT devices
- Software på klienter

Det anbefales at der følges op med databehandlere, som har instruks om at opdatere fagsystemer.

C11. Multi faktor autentifikation (MFA)

Med "to-faktor-autentifikation" menes en login-proces, som indebærer to godkendelselementer. Man taler typisk om, at et sådant godkendelselement er: "Noget man ved" (brugernavn i kombination en adgangskode), "Noget man har" (et nøglekort eller en pc, som – via et på forhånd installeret certifikat – kan genkendes af den it-løsning, som forsøges tilgået) og "Noget man er" (et fingeraftryk eller en iris-skanning). Det er kombinationen af to af disse elementer, der udgør de to faktorer.

Compliancemål	Complianceniveau	Prioritet
Der implementeret multi-faktor-autentifikation (MFA) ved adgang til systemer og databaser, hvori der sker behandling af persondata, der medfører høj risiko for de registrerede.	2 	P2

Undersøgelse

Vi har undersøgt, om adgang til systemer og databaser, hvori der sker behandling af persondata, der medfører høj risiko for de registrerede, som minimum sker ved anvendelse af to eller flere faktorer som autentifikation.

Vi har inspiceret, om brugernes adgang til at udføre behandling af persondata, der medfører høj risiko for de registrerede, alene kan ske ved anvendelse af to eller flere faktorer som autentifikation.

Vurdering

Det vurderes, at der foreligger multi faktor autentifikation på alle vigtige systemer. Der er etableret MFA på VPN. MFA er aktiveret på Office365 (MS Premium-licenser som bl.a. tilbyder conditional access) og på Azure. Der er etableret IP-restriktioner på admin. modul på CIS (Ungdomskort). Dette gøres lige nu pr. bruger i Office365.

Anbefaling

Det anbefales, at organisationen udarbejder en procedure med kriterier for, hvilke systemer det er relevant at etablere MFA. Det anbefales også at denne proces automatiseres og kontrolleres.

C12. Backup

Backup er en kopi af organisationens data således, at organisationen til enhver tid har en (forholdsvis opdateret) kopi af sine data til rådighed – de aktuelt anvendte data, der opdateres løbende, samt backup-kopien, der er et historisk øjebliksbillede. Jo længere tid, der går mellem, at organisationen opretter og gemmer en backup-kopi af sine data, desto større forskel vil der normalt være mellem de aktuelt anvendte data og den seneste backup-kopi. Backup-kopien bør opbevares adskilt fra de aktuelt anvendte data og skal sikre, at organisationen kan genetablere it-driften, hvis de aktuelt anvendte data går tabt eller bliver beskadiget. Dette kunne f.eks. være relevant, hvis hackere har udnyttet en sårbarhed hos organisationen og krypteret oplysninger.

Compliancemål	Complianceniveau	Prioritet
Der foretages backup af data og persondata med regelmæssige mellemrum.	3	P3

Undersøgelse

Vi har undersøgt om der foretages backup af data og persondata med regelmæssige mellemrum.
Vi har undersøgt, om det inden for det seneste år er testet, hvorvidt backup data kan genindlæses (reetableres) for at forebygge datatab fx i tilfælde af ransomware angreb eller nedbrud i it-systemerne.

Vi har inspiceret dokumentation for seneste test af genindlæsning (reetablering) af data.

Vurdering

Det vurderes, at organisationen foretager backup via GlobalConnect. På fagsystemerne har systemejerne ansvaret, og der ligger krav om, at der skal tages backup.

Der bliver taget backup via Veeam og Spectrum Protect via GlobalConnect (omfatter de fagsystemer der er hostet hos Global Connect).

Anbefaling

Organisationen anbefales at etablere en politik for backup med henvisning til et overblik over alle systemer, hvilken retention og restoretest der påtænkes gennemført og hvornår.


Bilag 1D: Vurderingsgrundlag og anbefalinger for organisatoriske foranstaltninger (governance)

Generelt om organisatoriske foranstaltninger (governance)

Organisatoriske foranstaltninger fokuserer på styringen af beskyttelse af organisationens informationer, herunder persondata. Organisatoriske foranstaltninger kan fx omfatte administrative handlinger, politikker, procedurer, retningslinjer mv. til at styre, implementere, vedligeholde og forankre håndtering og beskyttelse af organisationens informationer, herunder persondata. Kontrollerne under temaet "organisatoriske foranstaltninger" er inspireret af kontroller fra sikkerhedsstandarderne ISO27001 og ISO27002.

D1. Politik for informationssikkerhed

En politik for informationssikkerhed fastsætter, på et overordnet niveau, principper for hvad organisationen, herunder medarbejderne, skal gøre i forhold til beskyttelsen af bl.a. it-systemer, computere, mobile enheder og informationer, herunder persondata. En politik for informationssikkerhed ved behandling af persondata bør afspejle, hvordan persondata skal håndteres og beskyttes i organisationen under hensyntagen til risici for de personer, som der behandles persondata om (de registrerede).

Compliancemål	Complianceniveau	Prioritet
Der er en opdateret politik for informationssikkerhed ved behandling af persondata, som er godkendt på ledelsesniveau.	4 	n/a

Undersøgelse

Undersøgt, om der er en opdateret politik for informationssikkerhed ved behandling af persondata, som godkendt på ledelsesniveau.
Undersøgt, om politikken kommunikeres til medarbejderne i organisationen.

Vurdering


Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

D2. Roller og ansvar

Der skal være en fordeling af ansvar med hensyn til, hvem der skal varetage de enkelte GDPR-opgaver for sikring af databeskyttelse (fx risikovurderinger, tilsyn af databehandlere og håndtering af brud på persondatasikkerheden). På området for informationssikkerhed vil der normalt være udpeget en person, som er ansvarlig for informationssikkerhed (læs: beskyttelse af organisationens informationer) i organisationen fx it-chef, digitaliseringschef, CISO eller CTO. Alt efter organisationens størrelse og kompleksitet vil det styrke arbejdet med informationssikkerheden, hvis der er en klar ansvarsfordeling i forhold til, hvem der skal varetage de enkelte sikkerhedsopgaver.

Compliancemål	Complianceniveau	Prioritet
Der foreligger beskrevet rolle og ansvarsfordeling med hensyn til varetagelse af GDPR- og informationssikkerhedsopgaver i organisationen	4 	n/a

Undersøgelse

Undersøgt, om der er foreligger en beskrevet rolle- og ansvarsfordeling med hensyn til varetagelse af GDPR- og informationssikkerhedsopgaver i organisationen.

Vurdering


For så vidt angår rolle og ansvarsfordeling med hensyn til varetagelse af GDPR opgaver har organisationen gjort et godt stykke arbejde. Det vurderes, at organisationen har oprettet "Retningslinjer for informationssikkerhed", hvori roller og ansvarsfordeling er beskrevet. Sammen med deres etablerede oversigt over systemer er der derfor skabt overblik og ejerskab over systemerne. Det vurderes desuden, at medarbejderne er gjort bekendt med disse retningslinjer og at medarbejderne har været involveret i at skabe oversigten over systemer. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.

D3. Ledelsesforankring

Ledelsen sætter retningen for arbejdet med informationssikkerhed og databeskyttelse i organisationen. Implementering, vedligeholdelse og forankring af informationssikkerhed, herunder databeskyttelse, afhænger af ledelsens og topledelsens involvering og engagement.

Compliancemål	Complianceniveau	Prioritet
Arbejdet med informationssikkerhed og databeskyttelse efter GDPR er forankret på ledelsesniveau.	4 	n/a

Undersøgelse

Undersøgt, om der er etableret et sikkerhedsudvalg eller anden "styregruppe" med deltagelse på ledelsesniveau, som regelmæssigt håndterer spørgsmål om informationssikkerhed og databeskyttelse.

Vurdering


Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.

Anbefaling

Ingen.


D4. Årshjul

Alt efter organisationens størrelse og kompleksitet kan det være nødvendigt systematisk at kontrollere, at væsentlige politikker og retningslinjer vedrørende informationssikkerhed og databeskyttelse er ajourførte og opdaterede med faste intervaller. I et årshjul kan organisationen på overskuelig vis samle information om de aktiviteter, der skal gennemføres og fastlægge datoer og ansvar for, at aktiviteterne bliver gennemført.

Compliancemål	Complianceniveau	Prioritet
Der er etableret et årshjul, som understøtter, at alle væsentlige politikker, retningslinjer mv. vedrørende informationssikkerhed og databeskyttelse følges.	4 	n/a
Undersøgelse		
Undersøgt, om der er etableret et årshjul, som understøtter at alle væsentlige politikker, retningslinjer mv. vedrørende informationssikkerhed og databeskyttelse følges.		
Vurdering		
Organisationen har gjort et godt stykke arbejde. Compliancemålet vurderes på det foreliggende grundlag at være opfyldt, men der kan være mulighed for forbedring i konkrete tilfælde.		
Anbefaling		
Ingen.		

D5. Uddannelse/Awareness

Der skal gennemføres uddannelse af medarbejdere med henblik på at sikre ønsket adfærd og opmærksomhed omkring beskyttelse af organisationens informationer, herunder håndtering og beskyttelse af persondata. Uddannelse kan være interne eller eksterne kurser om sikkerhed på arbejdspladsen og om behandling af persondata, som er relevante for medarbejdernes løsning af arbejdsopgaver og deres generelle adfærd. Sådant en uddannelse, ofte kaldt awareness-træning, kan også bestå af interne oplæg, møder og workshops, hvor forsvarlig adfærd og relevante scenarier drøftes. Det kan typisk være relevant at gennemføre awareness-træning for nye medarbejdere som en del af deres introduktion (onboarding). Alt efter organisationens størrelse og kompleksitet - og ved større organisatoriske ændringer - kan det være nødvendigt at gennemføre regelmæssig awareness-træning, så medarbejderne kan holde sig ajour med organisationens politikker og retningslinjer i det omfang, det er relevant for deres jobfunktion.

Compliancemål	Complianceniveau	Prioritet
Medarbejderne uddannes løbende i it-sikkerhed og databeskyttelse.	4 	n/a

Undersøgelse

Undersøgt, om medarbejdere løbende uddannes i it-sikkerhed og databeskyttelse. Undersøgt, om der følges op på, om medarbejderne gennemfører uddannelse. Undersøgt, om eventuel politik for informationsikkerhed indgår i uddannelsen af medarbejderne.

Inspiceret dokumentation for, at medarbejderne løbende uddannes. Inspiceret dokumentation for, at der løbende følges op på, at medarbejderne gennemfører uddannelse.

Vurdering

Det vurderes, at medarbejderne løbende uddannes i it-sikkerhed og databeskyttelse dels med onboarding introduktion for nye medarbejdere og dels med awareness kurser for alle medarbejdere via e-learning. Organisationen oplyser, at der nu sker halvårlig opfølgning på, om medarbejdere har gennemført de påkrævede kurser. Organisationen har desuden indgået samarbejde med en ny leverandør af software til awareness.

Anbefaling

Ingen.

D6. Business Recovery Plan/beredskab

Det er relevant at stille til i en beredsskabsplan, hvordan driften af kritiske forretningsopgaver opretholdes, hvis organisationen ikke længere har adgang til vigtige it-systemer. Kritiske forretningsopgaver er typisk arbejdsrelaterede opgaver, der er vigtige at udføre for at undgå eller begrænse (større) negative konsekvenser for organisationen og de registrerede.

Compliancemål	Complianceniveau	Prioritet
Der er etableret en beredsskabsplan for opretholdelse af kritiske forretningsopgaver.	3	P3

Undersøgelse

Undersøgt om der er etableret beredsskabsplan.

Undersøgt om der foretages regelmæssige test af beredsskabsplan.

Vurdering

Det vurderes, at organisationens beredsskabsplan nu er opdateret til at omfatte alle systemer med kritisk status. Beredsskabsplanens oversigt indeholder links til beredskab, aftalte SLA-klasser, actioncards på de enkelte systemer og handlingsplaner, som løbende revideres.

Anbefaling

Det anbefales, at organisationen igangsætter regelmæssige tests af beredsskabsplanen og fastsætter en frekvens for opdatering af denne med en hyppighed, som passer med organisationens struktur, herunder fx hvor ofte der sker udskiftning i ansvarsområder.

D7. Disaster Recovery Plan/genetablering af it-systemer og it-drift

Det er også relevant at tage stilling til, hvordan organisationen får genetableret it-systemer og den normale it-drift i tilfælde af nedbrud fx i tilfælde af hackerangreb, brand, oversvømmelser, tyveri og strømsvigt. Dette indebærer først og fremmest en stillingtagen til ansvars- og rollefordelingen i organisationen, hvis uheldet er ude. Alt efter organisationens karakter kan det også indebære en forudgående kortlægning af bl.a. centrale opgaver og processer, prioritering af ressourcer og systemer samt fastlæggelse af kommunikationskanaler.

Compliancemål	Complianceniveau	Prioritet
Der er etableret en plan for genetablering af it-systemer og it-drift.	3	P3

Undersøgelse

Undersøgt, om der er etableret plan for genetablering af it-systemer og it-drift i tilfælde af nedbrud.

Vurdering


Det vurderes, at organisationens plan for genoprettelse af it-systemer og it-drift er opdateret til at omfatte alle kritiske systemer. Organisationen oplyser, at tests af planerne er sat i årshjulet.

Anbefaling

Det anbefales, at organisationen efter første test af genetableringsplanen vurderer, med hvilket frekvens planen skal henholdsvis testes og opdateres for at sikre bedst mulig genetablering.

D8. Fysisk sikkerhed

Det er relevant at sikre, at der ikke kan opnås adgang for uautoriserede personer til lokaliteter, hvori der opbevares og behandles persondata (fx arkiver, serverrum og kontorer). Fysisk adgangssikkerhed kan bl.a. opnås ved at aflåse lokaler, herunder at afskærme vinduer, hvis sådanne kan udnyttes af uautoriserede personer til at få kiggeadgang til persondata.

Compliancemål	Complianceniveau	Prioritet
Der er etableret fysisk adgangssikkerhed for lokaliteter, hvori der opbevares og behandles persondata.	2	 P2

Undersøgelse

Undersøgt, om der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaliteter, hvori der opbevares og behandles persondata.

Observeret for tilfældigt udvalgt lokalitet, hvori der opbevares og behandles persondata, at det er sandsynligt, at kun autoriserede personer har adgang hertil.

Vurdering

Det vurderes, at organisationen på nuværende tidspunkt har etableret fysisk adgangssikkerhed på hovedkontoret ved at aflåse døre i de perioder, hvor receptionen er ubemandet.

Anbefaling

Det anbefales, at organisationen efter vurdering af, hvilke foranstaltninger, der er tilstrækkelige, etablerer en procedure for fysisk sikkerhed, som indeholder en oversigt over etablerede fysiske tiltag, en frekvens for kontrol med den fysiske adgang samt overvejelser om alarmering og monitorering.

Bilag 2: Organisationens kommentarer til rapportens udkast

Kommentarer til tilsynsrapportens udkast
A7. Tredjelandsoverførsler
Kan første sætning ikke slettes? Hvilken underdatabehandler menes der?
C12. Backup
Organisationens IT-afdeling har fremsendt log over backup.
D6. Beredskabsplan
Er det tilstrækkeligt med skrivebordstests?
D7. Genetableringsplan
Er det tilstrækkeligt med skrivebordstests?
D8. Fysisk sikkerhed
Kan DPO DK være mere specifik ift. hvad Midttrafik bør være opmærksom på?

Bilag 3: Årets handlinger

Udførte handlinger gennem 2022

Afsluttet	Frist for bemærkninger til tilsynsrapporten fra MT er torsdag d. 7. februar 2022
Afsluttet	Kontroller af refusioner i billetapp
Afsluttet	Sikkerhedsbrud? Kontrolafgift til forkert modtager
Afsluttet	Tilføjelse til privatlivspolitik vedr. aktindsigt
Afsluttet	Opbevaring af pseudonymiserede Rejsekort-data (Janne deltager)
Afsluttet	Databehandleraftale med faglige organisationer
Afsluttet	Workshop om handleplan
Afsluttet	TIA fra Kraftvaerk
Afsluttet	Hjemmelsgrundlag ved medarbejdersurveys?
Afsluttet	Sikkerhedsbrud? Kontrolafgift til forkert modtager
Afsluttet	Tilføjelse til privatlivspolitik vedr. aktindsigt
Afsluttet	Privatlivspolitik - buschauffører
Afsluttet	Databehandleraftale med faglige organisationer
Afsluttet	Workshop om handleplan
Afsluttet	TIA fra Kraftvaerk
Afsluttet	BAT ønsker at benytte Midttrafiks billetapp
Afsluttet	BAT ønsker at benytte Midttrafiks billetapp
Afsluttet	Samtykke til påmindelser, Flextrafik
Afsluttet	Midttrafiks brug af Cisions SoMe mgmt-løsning (underdatabehandlere i usikre tredjelande)
Afsluttet	Privatlivspolitik til Flextrafik-chauffører (Frank og Merete deltager 13.35-14)
Afsluttet	Privatlivspolitik - buschauffører (copy)
Afsluttet	Privatlivspolitik - Midttrafiks gæste-wifi
Afsluttet	Samtykketekst til nyhedsbrev
Afsluttet	Push-beskeder i Midttrafik Live - Jesper og udvikler fra Adibus deltager kl. 10.20 10.40
Afsluttet	Tidsplan for tilsynsdag d. 28. nov. - indkaldelser
Afsluttet	Adgangskontroller - hvordan dokumenterer vi bedst?
Afsluttet	Brug af Google Analytics på midttrafik.dk
Afsluttet	NIS2 - Midttrafik?
Afsluttet	REVI / GT
Afsluttet	ControlGDPR
Afsluttet	Brug af Google Analytics til Live appen
Afsluttet	Opbevaring af lukkede dagsordener i hhv. First Agenda og ESDH - hjemmel?
Afsluttet	Nets Danmark + øvrige - Midttrafiks ansvar? (copy)
Afsluttet	Navnekrus med HK-logo som julegaver til medarbejdere
Afsluttet	Mitigerende/supplerende sikkerhedsforanstaltninger - Law Enforcement Requests
Afsluttet	Databehandleraftale-oplæg til udbud af økonomi-system
Afsluttet	Tilsyn - dokumentation



Transportminister Thomas Danielsen
Transportministeriet
Frederiksholms Kanal 27 F
1220 København K

Brev

22. december 2022

Lone Rasmussen
Telefon: 23401639
lor@moviatrafik.dk

Kære Thomas Danielsen,

Tillykke med udnævnelsen til transportminister. Hos Trafikselskaberne i Danmark glæder vi os til samarbejdet. Vi håber, at du vil fortsætte den gode tradition vi har haft med dine forgængere og Transportministeriet om møder og tæt kontakt om samarbejde og udvikling af den kollektive trafik og mobilitet i hele landet.

Vi er glade for, at den nye regering har prioriteret en stærk infrastruktur på tværs af Danmark og en mere attraktiv offentlig transport i regeringsgrundlaget. Vi ser frem til at bidrage. I Trafikselskaberne arbejder vi hele tiden på at udvikle den offentlige transport, så den kan leve op til borgernes og virksomhedernes behov – også i fremtiden. Vi har fokus på nye fleksible løsninger, der får forskellige transportformer til at spille bedre sammen og sikre offentlig transport i udkantsområderne. Vi arbejder med grøn omstilling og i de senere år har udrulningen af grønne busser fået fart på, godt hjulpet af statslige puljemidler og moderniseringen af afgiften for el til busser.

Trafikselskaberne spiller en nøglerolle både for den grønne omstilling og for at få Danmark til at hænge bedre sammen. Men som du ved, lægger de stigende energipriser pres på trafikvirksomhedernes økonomi, både i år og i 2023. Dette belaster kommuner og regioner, og der er alvorlig risiko for, at det kan føre til behov for væsentlige reduktioner i busservicen, ikke mindst i de tyndt befolkede områder.

Vi skal fra trafikselskaberne derfor opfordre til, at der gives mulighed for at afbøde de umiddelbare og forhåbentlig midlertidige effekter af det økonomiske pres ved eksempelvis at fremrykke takststigningen for 2024, så omkostningen til det sidste års energiprisstigninger ikke skal betales af kommuner og regioner alene. DSB, Arriva er enige i dette, og trafikselskabernes direktører har sendt et fælles brev til Transportministeriet herom.

Regeringen har bebudet nedsættelsen af et ekspertudvalg, der skal komme med anbefalinger til en ny struktur for busbetjening i Danmark, se på dækningen i byer og yderområder og se på den nuværende organisering af Trafikselskaberne. I Trafikselskaberne ser vi frem til at bidrage til dette arbejde. Vi har i dag et tæt samarbejde om fælles emner, samtidig med at vores geografiske forankring gør os i stand til at imødekomme behovene hos de lokale brugere. Et af vores fælles projekter som også omfatter DSB, Arriva Tog og Metroselskabet er et forslag til en modernisering og forenkling af rabatordningerne for unge, der vil gøre det enklere og billigere for unge at bruge offentlig transport. Det vil vi gerne drøfte med dig, så det kan spille sammen med regeringens planlagte initiativ om at understøtte, at flere unge med langt til uddannelse kan få billigere adgang til offentlig transport.

I trafikselskaberne håber vi, at den gode tradition med et hilse-på-møde mellem transportministeren og TiDs bestyrelse kan fastholdes, og vi vil foreslå, at vi snart får et møde, hvor vi kan drøfte forhold af fælles interesse. Endnu en gang tillykke med udnævnelsen.

Med venlig hilsen

Steen Vindum

Formand for Trafikselskaberne i Danmark

Formand Steen Vindum
Trafikselskaberne i Danmark

18. januar 2023
2023-2

Frederiksholms Kanal 27 F
1220 København K

Telefon 41 71 27 00

Kære Steen Vindum

Tak for velkomstbrevet til mig den 22. december 2022, og for trafikelskabernes brev til Transportministeriet af 19. december 2022 om håndtering af energiprisstigninger.

Som I har kunnet læse i regeringsgrundlaget, vil regeringen gerne understøtte busdækningen både i og uden for byerne. Jeg ser frem til et godt og konstruktivt samarbejde med trafikelskaberne i forbindelse med dette arbejde, og jeg hører naturligvis også gerne nærmere om de forslag I har til håndtering af de udfordringer, som bl.a. energikrisen giver på den korte bane.

Jeg vil derfor også gerne takke ja til jeres forslag om et hilse-påmøde. Ministersekretariatet vil kontakte Trafikselskaberne i Danmark og arrangere et mødetidspunkt.

Jeg ser frem til at møde jer.

Med venlig hilsen



Thomas Danielsen