Hvor lidt er nok?
En analyse af minimumsstandarder i GDPR-artikel 32

Aalborg Universitet 2026
Studerende: Simon Okholm Maymann
Vejleder: Tanja Kammersgaard Christensen
Anslag: 138.829

Abstract

This thesis sets to answer whether a set of minimum standards for "appropriate technical and organizational measures" can be found through an analysis of GDPR-article 32 and what are the pros and cons of this. The thesis explores this question by interpreting the wording of GDPR-article 32 and analyzing rulings made by the European Court of Justice and national courts in Denmark. By analyzing the wording, a set of minimum standards is not immediately portrayed, other than that of the initial wording of GDPR-article 32. The wording clarifies that a risk analysis must take place and that GDPR-article 32 is open, dynamic and must cover a wide specter of considerations. From the analysis of the rulings there are indications of a minimum standard where lack of control, lack of procedure and lack of effective utilization of measures, will result in the measures not being appropriate to the required security level. Though the indications of a minimum standard are portrayed, the analysis does not provide a more concrete take on a lower limit and what measures should be implemented. This provides an uncertainty for the controller, as the implementation of measures as found by the thesis both demanding and expensive. This uncertainty is further explored in the thesis, and it appears that its risk of uncertainty does not only affect the controller, but society as a whole. Therefore it is explored whether a set of minimum standards should be provided by the judicial system of EU, where pros include enhanced clarity and better predictability for the controller, a uniform minimum security level across EU, better opportunity for the control of controllers and better understanding of the theory for easier implementation in general practice. The cons on the other hand is the risk of losing a risk based method of analyzing necessary measures, resulting in controllers just trying to meet the minimum requirements, it will likely increase the risk of measures being outdated and not living up to the requirement for them to be state of the art and at last the risk of a minimum standard being too general or too specific and resulting in either a lower security level for all, or it not being proportionally to the required security level. This thesis therefore concludes that there are indications of a minimum standard for what is not appropriate and portrays it as lack of control, lack of procedure and lack of effective utilization of measures. But on the other hand, a more concrete set of minimum standards may not be beneficial, as they could result in the primary objective of GDPR which is the protection of fundamental rights and freedoms of natural persons in particular their right to the protection of their personal data as portrayed by GDPR-article 1, becoming second hand because of the controllers just implanting measures according to the minimum standard.

Indholdsfortegnelse

Kapitel 1. Indledning **5**

1.1 Baggrund og emne *5*

1.2 Problemformulering *6*
1.2.1 Specialets struktur 6

1.3 Metode *6*
1.3.1 Retsdogmatisk metode 6
1.3.2 Retskilder 7

1.4 Metodiske udfordringer *12*
1.4.1 Litteratur 12

1.5 Afgræsning og præcisering *12*
1.5.1 Ordlydsfortolkning 12
1.5.2 Databeskyttelsloven 13
1.5.3 Tekniske betegnelser 13

Kapitel 2 GDPR-artikel 32 anvendelsområde identificeres og sammenhæng med GDPR's principper **14**

2.1 Anvendelsesområde *14*

2.2 Grundlæggende principper i GDPR *15*

2.3 GDPR-artikel 32 ..... *16*

3 Fortolkning af GDPR-artikel 32 ..... **17**

3.1 Ordlydsfortolkning *17*
3.1.1 "Under hensyntagen til" 18
3.1.2 "Det aktuelle tekniske niveau" 18
3.1.3 "Implementeringsomkostninger" 20
3.1.4 "Behandlingens karakter, omfang, sammenhæng og formål" 22
3.1.5 "Risici for fysiske personers rettigheder og frihedsrettigheder" 24
3.1.6 "Et sikkerhedsniveau, der passer til risikoen" 25
3.1.7 Ordlyden af GDPR-artikel 32 stk. 1 26
3.1.8 Stk. 2 27
3.1.9 Stk. 3 29
3.1.10 Stk. 4 30

3.2 Fortolkning af foranstaltninger *30*
3.2.1 Foranstaltninger generelt 30
3.2.2 Tekniske foranstaltninger 31
3.2.3 Organisatoriske foranstaltninger 33
3.2.4 Tekniske og organisatoriske foranstaltninger 35

3.3 Fortolkning af passende *37*
3.3.1 "Passende" som retlig standard 37
3.3.2 Den risikobasrede tilgang 38
3.3.4 Proportionalitet og afvejning 39
3.3.5 Det aktuelle tekniske niveau 40
3.3.6 Behandlingens kontekst 42
3.3.7 Standarder, praksis og dokumentation 43
3.3.8 Dynamik, løbende vurdering og muligheden for en minimumsgrænse 51

Kapitel 4 Økonomiske betragtninger og usikkerhed om, hvad er nok? **52**

4.1 Økonomiske betragtninger *52*
4.2 Udfordringer og usikkerhed om hvad der er nok? *54*
4.3 Minimumsgrænsen *57*
4.3.1 Fordele ved minimumsgrænsen *57*
4.3.2 Ulemper ved minimumsgrænsen *59*
4.4 Konklusion *60*
5. Litteraturliste **63**
5.1 Bøger *63*
5.2 Domme og afgørelser *63*
5.3 Anden litteratur *64*

Kapitel 1. Indledning

I kapitel 1 etableres specialets overordnede fundament. Kapitlet indledes med baggrunden for emnet, efterfulgt af en fastlæggelse af emnets relevans, med henblik på at danne grundlag for problemformuleringen. Herefter følger en gennemgang af de metodiske overvejelser, samt de foretagne afgræsninger og metodiske udfordringer.

1.1 Baggrund og emne

Som ansat i en juridisk konsulentvirksomhed med, fokus på at rådgive organisationer i overholdelsen af GDPR har dette medført at i rådgivningsmæssige sammenhæng opstår der en usikkerhed ved vurderingen af, hvilke foranstaltninger der er "passende". Dette speciale ønsker derfor at fastlægge en teoretisk mulighed for en minimumsgrænse af "passende tekniske og organisatoriske foranstaltninger".
Det forekommer af EU's General Data Protection Regulation[1] Artikel 32 stk. 1 at hensyntagen til behandlingssikkerheden af personlige oplysninger skal af den dataansvarlige og databehandleren ske med passende tekniske og organisatoriske foranstaltninger. I arbejdet med GDPR forekommer foranstaltningerne som særdeles vigtige og med et stort fokus fra de dataansvarlige, derfor forekommer "passende tekniske og organisatoriske foranstaltninger" som et krav der kan være svært at efterleve i praksis, da det teoretisk kan være svært at forstå. Dette kan medføre enten overimplementering der for de dataansvarlige kan have store økonomiske konsekvenser, eller mangelfuld implementering der resulterer i at de registreredes oplysninger ikke behandles med den nødvendige sikkerhed, hvorved fortrolighed, tilgængelighed og integritet ikke opretholdes.
Denne usikkerhed understøttes ligeledes af Mona Juul, IT-ordfører fra konservative, der ønsker en tydeliggørelse af retningslinjerne, så virksomheder ved, hvornår de har gjort tilstrækkeligt for at sikre oplysninger, de behandler, samt få et klart svar på om de tiltag, virksomhederne har foretaget sig er tilstrækkelige for at overholde loven.[2] Som det står nu ved virksomhederne det reelt først ved et besøg fra datatilsynet. Behovet for GDPR er stadig voksende, dette understøttes af SAMSIK der i en analyse fra 2025 konkludere at det især er små og mellemstore virksomheder, der har problemer med at implementere tekniske og organisatoriske foranstaltninger.[3] Ligeledes ses det i en rapport fra Datatilsynet at mængden af databrud ikke er faldende over perioden 2020 – 2025, og kun stigende fra 2018.[4]

[1] General Data Protection Regulation, LOV nr. (EU) 2016/679 (2016) Herefter "GDPR"
[2] Juul, M. (2021, 26. april)
[3] *ANALYSE AF CYBER- OG INFORMATIONSSIKKERHED I DANMARK* (2025, December) S. 43
[4] *Antal anmeldte brud på persondatasikkerheden over tid*. (s.d.)

Den manglende afklaring af passende tekniske og organisatoriske foranstaltninger, sammenlagt med den stigende nødvendighed for behandlingssikkerheden af personoplysninger, leder frem til følgende problemformulering:

1.2 Problemformulering

> "Kan der ud fra ordlyden i og praksis om GDPR-artikel 32 udledes en teoretisk minimumsgrænse for passende tekniske og organisatoriske foranstaltninger og hvad er fordelene og ulemperne herved?"

1.2.1 Specialets struktur

Problemformuleringen behandles i 3 hovedafsnit

Kapitel 2	GDPR-artikel 32 anvendelsområde identificeres og sammenhæng med GDPR's principper
Kapitel 3	Fortolkning af GDPR-artikel 32
Kapitel 4	Økonomiske betragtninger og usikkerhed om, hvad er nok?

1.3 Metode

I dette afsnit præsenteres den tilgang, der anvendes i specialet for at besvare problemformuleringen, herunder metoden og de anvendte retskilder. Metodeafsnittet er inddelt i to hovedafsnit 1) Retsdogmatisk metode og 2) retskilder.

1.3.1 Retsdogmatisk metode

I dette speciale anvendes den retsdogmatiske metode til at fastlægge og beskrive den egentlige retstilstand. Formålet med den retsdogmatiske metode er at analysere, beskrive og fortolke gældende ret,[5] dette sker på baggrund af relevante retskilder, herunder lovgivning, retspraksis, administrative afgørelser og juridisk litteratur.

[5] Nielsen, R. & Tvernø, C.D. (2017) S. 29

I nærværende speciale vil den retsdogmatiske metode blive brugt til at beskrive, systematisere og fortolke EU retten,[6] her navnlig GDPR-artikel 32 omhandlende behandlingssikkerhed. Dette medfører en analyse af GDPR-artikel 32's ordlyd, med henblik på at fastlægge dens umiddelbare betydning. Herefter vil der blive inddraget andre fortolkningsbidrag, herunder GDPR-artikel 32's formål og relevante betragtninger fra GDPR's præambler. For at opnå en bredere forståelse af GDPR-artikel 32, suppleres specialet løbende af praksis fra EU-domstolen samt nationale domstole og tilsynsmyndigheder, hvor det findes relevant for at belyse, hvordan GDPR-artikel 32 fortolkes og anvendes i praksis. Praksissen analyseres med henblik på at undersøge, hvordan "passende sikkerhedsniveau" og "tekniske og organisatoriske foranstaltninger" skal forstås samt, hvilke sikkerhedsforanstaltninger der anses som værende "passende".
Ligeledes inddrages juridisk litteratur, herunder kommentarer til GDPR og videnskabelige artikler, for at nuancere specialet og afdække eventuelle usikkerheder og fortolkningsspørgsmål i teorien.

1.3.2 Retskilder

Retsdogmatisk metode anvendes til at fastlægge gældende ret, også kendt som de lege lata,[7] hvorfor det ligeledes er væsentligt at kende retskilderne.[8] Derfor er det vigtigt at få fastlagt de for specialet relevante retskilder, og hvor deres placering er i retskildehierarkiet, for at kunne fastlægge, hvilken retskildeværdi de har i specialet.[9]

1.3.2.1 EU-Retskilder

Traktaten om Den Europæiske Unions Funktionsmåde-artikel 16[10] er hjemlen bag GDPR.[11] GDPR udgør en central retskilde i dette speciale, hvori specialets fokusområde som værende kravet til behandlingssikkerhed og GDPR-artikel 32 også findes. GDPR-artikel 32 spiller en central rolle i specialet da den indeholder de grundlæggende krav til fastsættelse af sikkerhed i forbindelse med selve behandlingen af personoplysninger og dermed er central for udarbejdelsen af analysen.
Forordninger er almengyldige og bindende i alle sine enkeltheder og gælder umiddelbart i alle medlemslande jf. TEUF 288 og derfor også direkte anvendelse direkte i Danmark. På trods af at GDPR er en forordning og formålet har været en harmoniseret lovgivning for alle medlemsstaterne,[12] medbringer dette

[6] Neergaard, U. & Nielsen, R. (2020) S. 128
[7] Dalberg-Larsen, J. (2021, 19. Januar)
[8] Blume, P. (2020) S. 34
[9] Ibid S. 31
[10] Herefter "TEUF"
[11] GDPR-præambel 1
[12] Sørensen, K. E. & Danielsen, J. H. (2022) S. 104 & Blume, P. (2020) S. 61

at medlemsstaterne får mulighed for et nationalt råderum som angivet i GDPR-artikel 6 stk. 2.[13] Det forekommer dog af EU-rettens principper at medlemsstaterne har pligt til en konform fortolkning og at EU-retten har forrang, over national ret.[14]
Dette medfører at i praksis må de nationale lovgivninger, i dette tilfælde Databekyttelsesloven, fravige såfremt de ikke er i overensstemmelse med EU-retten, herunder GDPR.[15]

1.3.2.2 Forarbejder

Forarbejderne til GDPR anvendes ikke grundet deres tvivlsomme retskildeværdi, [16] der vil i højere grad blive inddraget GDPR's præambler i ordlydsfortolkningen af GDPR-artikel 32.[17] Dette skyldes at forarbejderne sjældent anvendes efter at lovgivningsprocessen er afsluttet.[18] Dog inddrages justitsministeriets betænkning da, [19] der forekommer overvejelser der er relevante for besvarelsen af specialets centrale spørgsmål, betænkningens betragtninger vil ikke blive brugt selvstændigt til konkludere på retsstillingen, men som supplement til den samlede analyse.

1.3.2.3 Præambler

GDPR's Præambler inddrages for at besvare problemformuleringen og bringe et yderligere element til analysen, [20] derfor er det vigtigt at få fastlagt hvilken retskildeværdi de har. Modsat forarbejderne, er præamblerne vedtaget og udgør dermed en del af GDPR. Præamblerne kan indeholde uddybende forklaringer, omkring formålet bag de enkelte bestemmelser i GDPR og præamblerne har derfor en høj retskildeværdi,[21] da de forekommer som et vigtigt fortolkningsbidrag til de individuelle artikler og anvendes dermed til at forstå deres ordlyd. Dette understøttes ligeledes af at EU Domstolen ofte henviser og anvender præamblerne når artiklerne skal fortolkes.[22]

---

[13] Blume, P. (2020) S. 58 f.
[14] Sørensen, K. E. & Danielsen, J. H. (2022) S.189 ff. & Neergaard, U. & Nielsen, R. (2021) S. 221 se også EU-Domstolens retspraksis. (s.d.)
[15] Blume, P. (2020) S. 61
[16] Ibid S. 61
[17] Se nærmere om præambler i afsnit 1.3.2.3
[18] Blume, P. (2020) S. 61
[19] Databeskyttelsesforordningen: og de retlige rammer for dansk lovgivning: Betænkning 1565. (2016).
[20] Herefter vil GDPR's præambler blot blive beskrevet som "præambler"
[21] Sørensen, K. E. & Danielsen, J. H. (2022) S. 119 & Blume, P. (2020) S. 62
[22] Ibid S. 120 og S. 140 f

1.3.3.4 GDPR-artikel 32

For at kunne besvare specialets centrale spørgsmål anvendes ordlyden fra GDPR-artikel 32. Ved ordlydsfortolkningen bruges der den sædvanlige og naturlige forståelse af ordlyden.[23] Ordlydsfortolkningen foretages ved brug af den danske oversættelse, da alle autentiske sproglige versioner er gyldige og kan bruges ved fortolkningsspørgsmål.[24]

For at besvare specialets centrale spørgsmål vil der imidlertid også blive anvendt formålsfortolkning til at fortolke GDPR-artikel 32 efter sit eget formål, hvor der ligeledes inddrages andre af GDPR's regler,[25] for at få en udvidet forståelse af GDPR som en helhed og dermed forbedre forståelsen af GDPR-artikel 32. Formålsfortolkningen behøver ikke tage udgangspunkt i en ordlyd fra formålsbetragtningen, hvorfor det ikke er afgørende om et formål har fundet sprogligt udtryk.[26] Hvorfor det fortolkes efter GDPR's primære formål navnlig beskyttelsen fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig retten til beskyttelse af personoplysninger efter GDPR-artikel 1 stk. 2, der ligeledes også forekommer af GDPR-artikel 32 stk. 1.

Retspraksis og juridisk litteratur anvendes ligeledes i løbet af specialet for at komme fortolkningen af GDPR-artikel 32 nærmere. Beskyttelsen af personoplysninger forstås ligeledes efter Den Europæiske Unions charter om grundlæggende rettigheder, her navnlig artikel 8.

1.3.3.5 Retsregler i øvrigt

Specialet baserer sig hovedsageligt på GDPR-artikel 32, men inddrager ligeledes andre relevante bestemmelser i GDPR for at sikre en sammenhængende og helhedsorienteret analyse da de enkelte Artikler i GDPR ikke kan forstås isoleret, men må fortolkes i lyset af GDPR's overordnede struktur og sammenhæng.[27]

I den forbindelse vil særligt GDPR-artikel 5, som fastlægger de grundlæggende principper for behandlingen af personoplysninger blive inddraget. GDPR-artikel 5 udgør et centralt fortolkningsbidrag da den fastsætter principperne for de overordnede krav og hensyn som behandlingen af personoplysninger skal leve op til. GDPR-artikel 5 vil derfor blive brugt som væsentligt udgangspunkt for analysen af GDPR-artikel 32.

[23] Evald, J. (2019) S. 36
[24] Neergaard, U. & Nielsen, R. (2020) S. 131
[25] Evald, J. (2019) S. 36
[26] Neergaard, U. & Nielsen, R. (2020) S. 135 f
[27] Korfits Nielsen, K. & Lotterup, A. (2020) S. 309

Inddragelsen af yderligere bestemmelser fra GDPR, herunder men ikke afgrænset til GDPR-artikel 5, har til formål at skabe en mere nuanceret forståelse af GDPR-artikel 32 og sikre at fortolkningen sker i lyset af den samlede systematik og forståelse af GDPR.
I Danmark er GDPR suppleret og gennemført via Databeskyttelsensloven.[28] DBL har til formål at implementere GDPR i overensstemmelse med EU-retten.[29] Dog forekommer der i DBL ikke væsentlige tilføjelser der kan bidrage til forståelsen af, hvilke krav der stilles til behandlingssikkerheden.[30]

1.3.3.6 Retspraksis

I dette speciale anvendes retspraksis fra EU-domstolen,[31] herunder navnlig domme omhandlende GDPR-artikel 32, da EU-domstolen afgørelser er en af EU-rettens centrale retskilder.[32] EUD må anses for at have høj retskildeværdi, da det er den sidste instans med kompetencen til at kunne fortolke og fastlægge gældende ret.[33] Det findes derfor relevant at anvende EUD's afgørelser til at analysere GDPR-artikel 32 og besvare problemformuleringen. EUD anses også at have høj præjudikatværdi,[34] hvilket forekommer ved at det alene er EUD og EU-Lovgiver, der kan være med til at ændre retsopfattelsen hos EUD[35]. Dette medfører ydermere at EUD's afgørelser har bindende virkning for medlemsstaterne, hvilket i praksis betyder at de nationale domstole og tilsynsmyndigheder, hvilket i dette speciale vil være de nationale datatilsyn skal anderkende EUD's afgørelser.[36]

Herudover inddrages der også nationale domme, navnlig fra Danmark, hvor retskildehierarkiet anvendes for at fastlægge den enkelte afgørelses retskildeværdi.[37] I den forbindelse tillægges Højesterets afgørelse den største retskildeværdi, da den er sidste appelinstans i det danske retssystem, og hovedsagligt bruges i sager af principiel værdi.[38] Specialet anvender imidlertid kun afgørelser fra 1. og 2. instans, dog med muligheden for yderligere anke in mente. Der vil ligeledes blive inddraget afgørelser fra det danske Datatilsyn, hvis kompetencer er reguleret af GDPR-artikel 51.[39]

[28] Databeskyttelsesloven § 1, Herefter "DBL"
[29] Korfits Nielsen, K. & Lotterup, A. (2020). S. 160 f. og S. 961 f.
[30] Se næremere herom i afsnit 1.5.2
[31] Herefter "EUD"
[32] Sørensen, K. E. & Danielsen, J. H. (2022). S. 115
[33] Blume, P. (2020) S. 68
[34] Sørensen, K. E. & Danielsen, J. H. (2022) S. 116
[35] Ibid S. 116
[36] Ibid S. 189 ff
[37] Se nærmere herom i Evald, J. (2019) S. 43 f
[38] Munk-Hansen, C. (2021) S. 61
[39] Se nærmere herom i afsnit 1.3.3.8

1.3.3.7 Databeskyttelsesrådet

Databeskyttelsesrådet[40] har blandt andet til formål at give generelle retningslinjer for at præcisere lovgivningen.[41] EDPB's vejledninger tillægges høj værdi i relation til fortolkningsspørgsmål, da en af rådets opgaver, er netop at opklare fortolkningsspørgsmål og dermed hjælpe med ensartet fortolkning på tværs af EU-lande.[42] Dette understøttes af at rådet fremstår som en vigtig retskilde,[43] blandt andet fordi de nationale tilsyn skal begrunde deres afgørelser med EDPB's opfattelse, hvilket gør at der ved fastlæggelsen af gældende ret skal deres udtalelser ligeledes tages i betragtning.[44]

1.3.3.8 Datatilsynet

Datatilsynet er tillagt funktionel uafhængighed, hvilket medfører at tilsynet udfører sine beføjelser uden instruks fra andre myndigheder, som følge heraf forekommer der en mulighed for at prøve tilsynets afgørelser ved domstolene.[45]
Det betyder ligeledes at datatilsynets afgørelser kun underkendes ved domstolene,[46] hvorfor datatilsynets afgørelser ikke tillægges den højeste retskildeværdi, hvorfor der i specialet ikke drages endelige retlige konklusioner på baggrund af disse men, bruges til at udvide fortolkningen.
Datatilsynets vejledninger og retningslinjer vil ligeledes blive inddraget i specialet, herunder særligt datatilsynets katalog over foranstaltninger og deres vejledning omkring behandlingssikkerhed.[47] Disse vil dog ikke blive tillagt særlig retskildeværdi og kun anvendes som et supplement til fortolkningen, da det netop kun er vejledninger og derfor ikke medfører nogle retslige forpligtigelser.[48]

[40] Herefter "EDPB"
[41] GDPR-artikel 70 og Det Europæiske Databeskyttelsesråd. (s.d.)
[42] GDPR præambel 13, Blume, P. (2020) S. 62
[43] Blume, P. (2020) S. 65
[44] Ibid S. 65
[45] Blume, P. (2020) S. 48 & Korfits Nielsen, K. & Lotterup, A. (2020) S. 911 ff.
[46] Blume, P. (2020) S. 48
[47] Katalog over foranstaltninger. (s.d.)
[48] Blume, P. (2020) S. 43

1.3.3.9 Retslitteratur

I specialet vil der løbende blive inddraget retslitteratur, med henblik på at understøtte og nuancere analysen. Retslitteraturen inddrages hovedsageligt for at belyse forskellige fortolkningsmuligheder, begrebsafklaringer og teoretiske perspektiver, indenfor databeskyttelsesretten. Der skal understreges at retslitteraturen ikke tillægges samme retskildeværdi som de primære retskilder som lovgivning, retspraksis og administrative afgørelser.[49]

Retslitteraturen anvendes derfor alene som supplement til de primære retskilder og anvendes til at understøtte konklusioner, eller afklare områder der ikke måtte være besvaret af de primære retskilder. Retslitteraturen anvendes derfor ikke til alene at danne grundlag for retlige konklusioner.

1.4 Metodiske udfordringer

1.4.1 Litteratur

Der har i udarbejdelsen af specialet været en metodisk udfordring i at de nyeste versioner af enkelte relevante bøger ikke har været tilgængelige. Dette har medført at ældre versioner af litteraturen er blevet anvendt. Det vurderes imidlertid ikke at have haft betydning for analysens kvalitet eller konklusioner, idet specialet i væsentligt omfang er baseret på gældende ret, herunder lovtekst, præambler samt nyere praksis fra både EU-domstolen og nationale domstole.

1.5 Afgræsning og præcisering

1.5.1 Ordlydsfortolkning

I dette speciale afgrænses analysen til alene at inddrage den danske sprogversion af GDPR, idet alle sproglige versioner har samme gyldighed.[50]

Denne afgrænsning skyldes, at en fyldestgørende inddragelse af alle sprogversioner forudsætter sproglige kompetencer, som ligger uden for den studerenes kompetencer, ligeledes vurderes anvendelsen af automatiske oversættelsesværktøjer til ikke at være metodisk forsvarligt, idet disse værktøjer ikke kan

[49] Blume, P. (2020) S. 54 f
[50] Neergaard, U. & Nielsen, R. (2020). *EU-ret* (8. udg.) S. 131

gengive de juridiske og sproglige nuancer, som er afgørende for fortolkningen. Der forekommer imidlertid ikke væsentlige sproglige variationer mellem den danske og engelske oversættelse.
Derfor afgrænses der fra øvrige sprogversioner, idet det vurderes at en analyse på dansk forsat giver et forsvarligt og retvisende grundlag for fortolkningen af GDPR-artikel 32, på baggrund af at den danske oversættelse er en autentisk version.[51]

1.5.2 Databeskyttelsloven

I dette speciale afgrænses der fra DBL. Der forekommer umiddelbart ikke noget af DBL der supplerer fortolkningen af GDPR-artikel 32 og dermed bidrager DBL ikke til besvarelsen af specialets overordnede spørgsmål. Det begrundes yderligere af at specialets fokus er rettet mod GDPR som den direkte anvendelige regulering på databeskyttelsesområdet. Dette skyldes GDPR's forrang og ensartede anvendelse på tværs af medlemslandene, hvilket gør at GDPR er det centrale grundlag for analysen.

1.5.3 Tekniske betegnelser

Specialet afgrænser sig fra uddybende forklaringer af tekniske begreber, herunder eksempelvis IT-sikkerhedsmæssige termer. Dette skyldes at specialets fokus er den retlige analyse af GDPR-artikel 32, frem for en teknisk gennemgang af de enkelte løsninger og metoder for sikkerhedsbrud. Der vil i tilfælde af det findes nødvendigt for forståelsen af analysen blive henvist til de relevante beskrivelser og definitioner. Dette sker med henblik på at sikre klarhed, uden at udvide specialet til at skulle analysere og fortolke de individuelle tekniske begreber.

[51] Neergaard, U. & Nielsen, R. (2020). *EU-ret* (8. udg.) S. 131

Kapitel 2 GDPR-artikel 32 anvendelsområde identificeres og sammenhæng med GDPR's principper

I dette kapitel fastlægges den retlige baggrund for GDPR-artikel 32, for at forstå dens anvendelsesområde, samt at dens sammenhæng med GDPR's andre principper efter GDPR-artikel 5.

2.1 Anvendelsesområde

GDPR-artikel 2 stk. 1 regulere det materielle anvendelsesområde, hvoraf det fremgår at GDPR finder anvendelse ved behandlingen af personoplysninger der helt eller delvist foretages ved hjælp af automatisk databehandling, og på anden ikke automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.[52] Det materielle anvendelsesområde bør fortolkes bredt og omfatter enhver form for behandling af personoplysninger der ikke er begrænset af undtagelserne der findes i GDPR-artikel 2, stk. 2-4.[53]

Ligeledes reguleres det territorielle anvendelsesområde af GDPR-artikel 3, og finder anvendelse på behandlingen af personoplysninger, som foretages som led i aktiviteter der udføres af for en dataansvarlig eller en databehandler, som er etableret i Unionen uanset om behandlingen finder sted i Unionen eller ej.[54]

GDPR's undtagelser findes i GDPR-artikel 2, stk. 2, litra a-d, hvilket er en udtømmende liste, hvor det eksempelvis kan nævnes at GDPR ikke finder anvendelse, hvis behandlingen foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger jf. GDPR-artikel 2, stk. 2, litra d.[55]

[52] GDPR-artikel 2, stk. 1
[53] Korfits Nielsen, K. & Lotterup, A. (2020) S. 207 f
[54] GDPR-artikel 3, stk. 1
[55] Jf. GDPR art. 2, stk. 2, litra c. Se også: Korfits Nielsen, K. & Lotterup, A. (2020) S. 214 og 220

2.2 Grundlæggende principper i GDPR

GDPR's grundlæggende principper udfolder sig i GDPR-artikel 5, stk. 1 litra a-f, hvoraf det fremgår at enhver personoplysning der behandles skal ske i overensstemmelse med netop disse principper. Det er den dataansvarliges ansvar altid at være opmærksom på at disse overholdes, da de samlet danner fundamentet for databeskyttelsen.[56] Det fremgår ligeledes af GDPR-artikel 5, stk. 2 at det er den dataansvarliges ansvar at kunne påvise overholdensen af stk. 1. Ydermere er det vigtigt at forstå at disse principper generelt er dynamiske og skal overholdes, hver gang behandlingen justeres og at databehandlingen ikke kan gennemføres såfremt et af principperne ikke er opfyldt,[57] hvorfor det også betyder at der ikke forekommer en rangorden af principperne, hvor et er vigtigere end det andet. Såfremt et af principperne ikke er opfyldt skal behandlingen justeres eller ophøre.[58]

Principperne der følger af GDPR-artikel 5 stk. 1 litra a-f udfolder sig som krav om lovlighed, rimelighed og gennemsigtighed, formålbegrænsning, rigtighed, rigtighed, opbevaringsbegrænsning, integritet og fortrolighed. For nærværende speciale er det særligt GDPR-artikel 5, stk. 1 litra f der er relevant da det er her kravet om beskyttelse af personoplysninger, ved brug af passende og tekniske foranstaltninger fremgår.

Princippet om integritet og fortrolighed som findes i GDPR-artikel 5 stk. 1 litra f, indeholder krav om at behandlingen af personoplysninger skal ske på en måde der sikrer tilstrækkelig sikkerhed for behandlingen, herunder specificeres der yderligere at sikringen skal imødegå uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, ved anvendelse af passende tekniske og organisatoriske foranstaltninger. Dette princip udfolder sig i GDPR-artikel 32 stk. 1, hvor kravet om passende tekniske og organisatoriske foranstaltninger fastslås.

[56] Blume, P. (2020) S. 151 f
[57] Ibid S. 151 f
[58] Ibid S. 151 f

2.3 GDPR-artikel 32

"Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:"

I dette speciale findes det relevant at inddrage EU's primære ret, herunder særligt Charteret om Grundlæggende Rettigheder artikel 8,[59] der omhandler beskyttelse personoplysninger og hvilke krav der stilles til behandlingen af disse. Den sekundære ret, herunder GDPR,[60] må derfor fortolkes i lyset af de principper der følger af charteret.

Artikel 32 opdeles i dette speciale i en række analytiske elementer med henblik på at skabe struktur for analysen. En sådan opdeling findes nødvendig, da artiklen er forekommer som værende kompleks og består af flere vurderingsmomenter, som, hver især har betydning for fastlæggelsen af en eventuel minimumsgrænse.

Ved at opdele artiklen i dens enkelte elementer, tydeliggøres de forskellige retlige kriterier og deres sammenhæng. Opdelingen bidrager dermed til at tydeliggøre artiklens centrale elementer, såsom risikovurderingen, kravet om passende foranstaltninger og vurderingen af sikkerhedsniveauet på baggrund af risici, så disse kan analyseres selvstændigt, for at forstå deres sammenhæng.

GDPR-artikel 32 fastsætter at der ved vurderingen af "passende tekniske og organisatoriske foranstaltninger" skal tages hensyn til række faktorer. GDPR-artikel 32 stk. 1 angiver at der ved vurderingen skal lægges vægt på blandt andet det aktuelle tekniske niveau, samt implementeringsomkostningerne. Der skal ligeledes foretages en vurderingen af den pågældende behandlings karakter, omfang, sammenhæng og formål. GDPR-artikel 32 stk. 1 fremhæver ligeledes at fysiske personers rettigheder og frihedsrettigheder skal indgå i den samlede vurdering.[61]

[59] Trakowski, J. & Gersvang Sørensen, M. (2019) S. 47
[60] Ibid S. 48
[61] Europa-Parlamentets og Rådets forordning (EU) 2016/679 (GDPR), artikel 32, stk. 1

GDPR-artikel 32 ligger derfor op til en risikobaseret tilgang, hvor flere hensyn skal afvejes og at der i fastsættelsen af et passende sikkerhedsniveau, skal tages hensyn til tekniske, økonomiske og kontekst relaterede forhold, samt konsekvenserne for de registrerede.[62]

På baggrund af den samlede analyse og sammenholdning af kriterierne der inddrages i vurderingen ovenfor, skal den dataansvarlige og databehandleren træffe passende tekniske og organisatoriske foranstaltninger jf. GDPR-artikel 32, [63] her opstilles der dog ikke en udtømmende liste og foranstaltninger, hvilket må forstås af formuleringen "herunder b.la." og "hvad der er relevant". Disse formuleringer leder altså til at der kan være behov for supplerende foranstaltninger afhængigt af den konkrete behandlingssituation.

3 Fortolkning af GDPR-artikel 32

For at kunne besvare problemformuleringen er det nødvendigt at foretage en nærmere analyse af, hvad begrebet "passende" nærmere indeholder. "Passende" er et centralt begreb i GDPR-artikel 32 stk. 1, men efterlades samtidigt åbent og som et skøn, hvorfor det er afgørende for forståelsen at klarlægge dets indhold gennem en systematisk fortolkning. I dette kapitel vil GDPR-artikel 32 blive fortolket på baggrund af ordlyden og formålet. GDPR-artikel 32 stk. 1 deles op i dens forskellige relevante elementer for at forstå konkret hvad der forventes af beskyttelsesniveauet. GDPR-artikel 32 stk. 2,3,4 deles ikke op på samme måde da de ikke bringer lige så mange individuelle kriterier, hvoraf det ligeledes forstås at de i sig selv bidrager til den samlede forståelse af, hvordan "passende" vurderes

3.1 Ordlydsfortolkning

Som nævnt i afsnit 2.3, forekommer GDPR-artikel 32 som værende sammensat af flere komplekse begreber. GDPR-artikel 32 opstiller ikke standarder, men angiver en række momenter og hensyn der skal tages, ved vurderingen af hvad der "passende". I dette afsnit vil disse hensyn fortolkes, for at få en bedre forståelse af hvad "passende" indebærer. Begrebet "passende" og "organisatoriske og tekniske foranstaltninger" analyseres ikke i denne ordlydsfortlokning, men analyseres separat i senere afsnit af specialet. I ordlydsfortolkningen bliver GDPR-artikel 32 stk. 1 som ovennævnt delt op i hver af de kriterier der opstilles, for at forstå konteksten i relation til "passende". Ligeledes fortolkes sandsynligheden og alvor

[62] GDPR-præambel 83 & Korfits Nielsen, K. & Lotterup, A. (2020) S. 634

[63] GDPR artikel 32 stiller krav til både den dataansvarlige og databehandleren, fremadrettet vil der som udgangspunkt blot blive henvist til den dataansvarlige og ikke begge, dette gøres på baggrund af at kravene til GDPR-artikel 32 ikke adskiller sig om man er dataansvarlig eller databehandler.

ikke ses som individuelt kriterie, da de femstår som værende i tæt sammenhæng med de andre kriterier og fortolkes løbende med de andre hensyn.

3.1.1 "Under hensyntagen til"

GDPR-artikel 32 stk. 1 indledes med formuleringen "Under hensyntagen til", hvilket sætter rammen for GDPR-artikel 32's metodiske tilgang. Formuleringen indikerer, at den efterfølgende vurdering ikke er baseret på faste eller udtømmende krav, hvilket ligeledes understøttes af præambel 83, hvori det tydeliggøres at den dataansvarlige bør forholde sig til de risici behandlingen medfører og derefter forsøge at begrænse dem.[64] Dette ligger op til at fastsættelsen af foranstaltninger, ikke forekommer som en konkret eller udtømmende liste,[65] men fastsættes på baggrund af en samlet vurdering af de oplistede hensyn. Ligeledes ligger udtrykket "Under hensynstagen til", op til at de enkelte kriterier ikke bør forstås hierarkisk eller isoleret, men bør derimod fortolkes samlet, hvilket forstås af præambel 76. Præambel 76 stiller krav til at risikoens sandsynligheden og konsekvens for de registreredes, rettigheder bør fastlægges med henvisning til behandlingens karakter, omfang, sammenhæng og formål. Præambel 83 omhandler de kriterier der bør overvejes ved fastsættelsen af en sådan risiko. Dette understreger at kriterierne i GDPR-artikel 32 stk. 1 bør vurderes ud fra en konkret behandlingssituation. Det forekommer ligeledes af præambel 76 og 83 at selvom GDPR-artikel 32 stk. 1, har en fleksibel karakter, der tillader den at tilpasse sig specifikke behandlings situationer, er det centrale for vurderingen de potentielle risici for den registreres rettigheder og frihedsrettigheder. Den metodiske fremgang i GDPR-artikel 32 opstiller derfor umiddelbart en ramme der forpligter den dataansvarlige til aktivt inddrage og afveje relevante forhold, frem for blot at opfylde et sæt minimumskrav.

3.1.2 "Det aktuelle tekniske niveau"

Det forekommer af GDPR-artikel 32 stk. 1 at det aktuelle tekniske niveau inddrages som et vurderingskriterium. Det aktuelle tekniske niveau henviser til den enhver tid tekniske udvikling og er med til at gøre GDPR-artikel 32 teknologineutral,[66] begrebet indebærer at den dataansvarlige ikke skal knytte sig til statiske standarder, men må følge med den teknologiske udvikling, for hvad der er ansvarligt for behandlingensaktivitetens sikkerhed. Formuleringen medfører derfor at der skal foretages en kontinuerlig

[64] Korfits Nielsen, K. & Lotterup, A. (2020) S. 634
[65] Ibid S. 657
[66] Teknologineautral forstås efter Erhvervsministeriets formulering VEJLEDNING OM PRINCIPPER FOR AGIL ERHVERVS- RETTET REGULE- RING. (s.d.) S. 11

vurdering af den dataansvarliges sikkerhedsforanstaltninger i takt med at nye teknologier udvikles og nye trusselsbilleder opstår.[67]

Dette understøttes af præambel 76, hvoraf der som nævnt ovenfor skal tages stilling til sandsynlighed og konsekvens ved behandlingen af personoplysninger, hvoraf sandsynligheden kan ændre sig, ud fra et aktuelt trusselsbillede og den teknologiske fremgang. [68] Det aktuelle tekniske niveau må ligeledes forstås som værende i relation til netop denne sandsynlighedsvurdering, da der i fastlæggelsen niveauet bør inddrages behandlingens karakter, omfang, sammenhæng og formål, for at finde ud af hvad der med rimelighed kan forventes af en foranstaltning på baggrund af den teknologiske udvikling og det aktuelle trusselsbillede.[69]

Forståelsen understøttes yderligere af præambel 78, hvori det fremhæves at den dataansvarlige bør implementere foranstaltninger under hensyntagen til den teknologiske udvikling. Præambel 78, understreger endvidere betydningen af databeskyttelse gennem design og standardindstillinger,[70] dermed fastslår præambel 78, at det aktuelle tekniske niveau altså ikke kun er relevant ved implementeringstidspunktet, men allerede ved udviklingen af systemer der behandler personoplysninger.[71] Hvilket tydeliggøres af GDPR-artikel 25, hvor kravene til databeskyttelse gennem design og standardindstillinger fremgår, hvor af der stilles krav til at der tages stilling til beskyttelsesniveauet allerede ved fastlæggelsen af midlerne hertil.

Dette indikerer at det aktuelle tekniske niveau, har fremtidsrettet tilgang,[72] hvor databeskyttelse skal implementeres som en grundlæggende del af teknologiske løsninger der behandler personoplysninger. Denne forståelse suppleres af præambel 83, der fremhæver, at det sikkerhedsniveau der etableres, bør passe til de risici der måtte være forbundet med behandlingen. I det sammenhæng kan det aktuelle tekniske niveau, anvendes som en målestok, for hvad der med rimelighed må forventes af de foranstaltninger der etableres for at afværge de risici der måtte være identificeret, herunder hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til personoplysninger og kan forsage fysisk, materiel eller immateriel skade, hvilket overordnet betyder et brud på persondatasikkerheden jf. GDPR-artikel 4 stk. 1, nr. 12.[73] Heraf bør det overvejes hvorvidt manglen på implementering af anerkendte og tilgængelige foranstaltninger såsom kryptering og pseudonymisering,[74]

[67] Korfits Nielsen, K. & Lotterup, A. (2020) S. 639
[68] Ibid S. 639
[69] Ibid S. 638 & 639
[70] GDPR- artikel 25
[71] Databeskyttelse gennem design og standardindstillinger. (s.d.)
[72] Korfits Nielsen, K. & Lotterup, A. (2020) S. 639
[73] Ibid S. 636
[74] For beskrivelse af pseodonymisering se GDPR artikel 4 stk. 1, nr. 5

der nævnes som et konkret eksempel i GDPR artikel 32 stk. 1 litra a og præambel 83, kan indikere at kravene til beskyttelsesniveauet ikke er overholdt.

For at komme nærmere hvad risikoanalysen kan indeholde kan bet. 1565/2017 supplere forståelsen,[75] heraf fremgår det at risikovurderingen kan indeholde 4 punkter 1. Identifikation og vurdering af risici 2. Identifikation af mulige foranstaltninger 3. gennemgang af, hvilke foranstaltninger som imødegår relevante risici, så et passende sikkerhedsniveau opnås 4. implementeringen af de foranstaltninger som besluttes at gennemføre. [76] Det er derfor den dataansvarliges opgave at beslutte nærmere fremgangsmåde og systematik.[77] Dog stilles der ligeledes i vejledningen spørgsmålstegn ved om det er en opgave der kan gribes af den dataansvarlige.[78]

Sammenfattende indikerer det at det aktuelle tekniske niveau, fungere som en fleksibel og teknologineutral, standard, der forpligter den dataansvarlige til at løbende tilpasse de implementerede foranstaltninger. Det aktuelle tekniske niveau stiller altså ikke krav til at anvende den nyeste teknologi, men derimod en forpligtigelse til at gøre brug af løsninger der bruges til behandlingen af personoplysninger er tidsvarende og effektive i forhold til de konkrete risici.[79]

3.1.3 "Implementeringsomkostninger"

Implementeringsomkostninger som kriterie i GDPR-artikel 32 stk. 1, stiller krav til at når vurderingen af passende tekniske og organisatoriske foranstaltninger udarbejdes, skal der være en hensyntagen til de økonomiske implikationer der er forbundet der er forbundet med implementeringen af disse. Implementeringsomkostningerne kan ligesom de andre kriterier ikke vurderes alene.[80] Eksempler på konkrete trusler der kan medføre høj risiko ved behandlingen af persondata nævnes Phishing, spear phishing, malware, ransomware, tab af krypteringsnøgle, utilstrækkelig kryptering, manglende backups og manglende viden i organisationen om håndtering af persondata og it-systemer,[81] og da der ikke stilles krav til en minimumsgrænse må det være op til den dataansvarlige selv at vurdere, hvilke foranstaltninger der er passende, her medtaget implementeringsomkostningerne.[82] Der ligges dog op til et

[75] Databeskyttelsesforordningen: og de retlige rammer for dansk lovgivning: Betænkning 1565. (2016)
[76] Ibid S. 487
[77] Ibid S. 486 & Korfits Nielsen, K. & Lotterup, A. (2020). s. 635
[78] Databeskyttelsesforordningen: og de retlige rammer for dansk lovgivning: Betænkning 1565. (2016) S. 486
[79] Korfits Nielsen, K. & Lotterup, A. (2020) S. 638
[80] Ibid S. 638
[81] Ibid S. 638
[82] Ibid S. 639

proportionalitetshensyn, hvor det ikke kræves at den dataansvarlige implementere enhver tænkelig sikkerhedsforanstaltning, men at der sammen med de andre kriterier, må foretages en afvejning mellem de omkostninger der følger af en given sikkerhedsforanstaltning og det sikkerhedsniveau der opnås. Dette understøttes af præambel 83, hvori det fremhæves at sikkerhedsniveauet og foranstaltninger skal svare til den risici der er forbundet med behandlingsaktiviteten.
Endvidere understøttes dette af præambel 77, hvoraf det fremgår at databeskyttelsesrådet kan komme med retningslinjer, godkendte adfærdskodekser og godkendte certificeringer.[83] Ved at følge disse anvisninger fra databesykttelsesrådet kan den dataasnvarlige, gøre processen for at identificere et "passende" sikkerhedsniveau mindre ressourcekrævende og undgå at implementere potentielt mere ressourcekrævende løsninger end dem der følger af kravene. Det ses ligeledes i GDPR-artikel 32 stk. 3 at anvendelsen af et adfærdskodeks eller certificeringsmekanismer kun fungere som et element til for at påvise overholdelsen af GDPR-artikel 32 stk. 1 og 2.
Et eksempel på en anden standard der kan bruges, for at fastlægge og mitigere risici er ISO 27001, som er en del af den offentlige digitaliseringsstrategi at alle statslige myndigheder skal gøre brug af standarden.[84] mens alle offentlige myndigheder skal følge principperne heri.[85] ISO 27001 standarden er ligeledes et udtryk for den risikobaserede tilgang GDPR-artikel 32 kræver,[86] og tager udgangspunkt i en enkelt virksomhed og hjælper med at fastlægge de foranstaltninger der netop er passende for dem.[87]

Samlet set indikere det at kravet om hensynstagen til implementeringsomkostninger i GDPR-artikel 32 ikke opstiller et krav om maksimal sikkerhed. Omkostningshensynet fungerer som hensyn mod uforholdsmæssige krav til foranstaltninger, men ændrer ikke ved det faktum at den dataansvarlige skal sikre den registreredes rettigheder og frihedsrettigheder, ved at implementere et sikkerhedsniveau der reelt beskytter de registrerede mod identificerede risici. Dermed indgår implementeringsomkostningerne i den samlede afvejning af, hvilke foranstaltninger der er "passende", men ikke som et afgørende element i den samlede vurdering , hvor beskyttelsen af personoplysninger og praktisk gennemførlighed skal afvejes, da det umiddelbart må antages at beskyttelsen af de registrerede rettigheder og frihedsrettigheder må prioriteres højest.

[83] Se nærmer om i efterfølgende afsnit
[84] Korfits Nielsen, K. & Lotterup, A. (2020). s. 639 se også Opdatering af sikkerhedsstandarden ISO 27001:: Statslige myndigheder skal implementere den nye version. (2023, 20. September)
[85] Korfits Nielsen, K. & Lotterup, A. (2020) S. 639
[86] Ibid S. 640
[87] Ibid S. 640

3.1.4 "Behandlingens karakter, omfang, sammenhæng og formål"

Kriteriet der omhandler behandlingens karakter, omfang, sammenhæng og formål i GDPR-artikel 32 stk. 1 indebærer at det er den enkelte behandlingsaktivitet der afgør,[88] hvad der er passende for den enkelte foranstaltning, uafhængigt om den er teknisk eller organisatorisk, hvilket udledes af GDPR-artikel 32 stk. 1 der specificerer at det er den "pågældende" behandling der skal afvejes for at fastlægge et "passende" sikkerhedsniveau. Ved at sætte kravene til sikkerhedsniveauet i kontekst til selve behandlingen, fastsætter GDPR-artikel 32 stk. 1 at det ikke er tilstrækkeligt at anvende standardiserede foranstaltninger, uden hensyn til karakteren, omfanget, sammenhængen og formålet ved den konkrete behandling af personoplysninger. De førnævnte elementer for sikkerhedsniveauet, skal derfor anvendes af den dataansvarlige som analytiske elementer for at forstå, hvilket sikkerhedsniveau den enkelte behandling bør have.

Karakter omhandler navnlig typen af personoplysninger og den måde de behandles, hvilket følger af præambel 51, her præciseres det at personoplysninger kan af deres karakter være særligt følsomme, i forhold til grundlæggende rettigheder og frihedsrettigheder, hvorfor de dermed også bør have et højere sikkerhedsniveau. De særligt følsomme oplysninger kan nærmere beskrives som eksempelvis værende helbredsoplysninger eller seksuel orientering, m.m. efter GDPR-artikel 9 stk. 1 eller personoplysninger om straffedomme eller lovovertrædelser efter GDPR-artikel 10 stk. 1. Dermed antages at det modsat må betyde at behandlingen af mindre følsomme personoplysninger, også kendt som almindelige personoplysninger, må medføre kravet til sikkerhedsniveauet er lavere. Ligeledes kan det omhandle behandlingens tekniske karakter, eksempelvis hvis der er tale om automatiseret behandling, hvoraf følsomme personoplysninger kan bringes til uvedkommendes kendskab.[89] Dette hænger sammen med præambel 75, hvoraf det fremgår at visse typer af behandling kan medføre særlige risici for de registrerede rettigheder og frihedsrettigheder, herunder både behandlingen af førnævnte GDPR-artikel 9 og 10 oplysninger.

Omfang relaterer sig til mængden af oplysninger og antal af registrerede behandlingen af personoplysninger. Det fremgår flere steder af GDPR at behandling af personoplysninger i stort omfang kan medføre særlige krav.[90] Behandlingen af personoplysninger i stort omfang, selvom dette ikke er videre defineret i GDPR, kan medføre et øget risikobillede og dermed også øge kravene til

[88] Korfits Nielsen, K. & Lotterup, A. (2020) S. 634
[89] Ibid S. 634
[90] Se GDPR-artikel 35 stk. 3, litra c og GDPR-artikel 37 stk. 1, litra c

sikkerhedsforanstaltningerne. Dette perspektiv kan udledes af præambel 75, hvoraf det fremgår at risici for fysiske personers rettigheder og frihedsrettigheder af varierende sandsynlighed og alvor kan påvirkes af at behandlingen vedrører en stor mængde af personoplysninger eller berører et stort antal registrerede. Selvom der forekommer mangel på identificering af en konkret betegnelse for "stort omfang" i GDPR, har EU Kommissionen konstateret at behandling af personoplysninger i stort omfang kan omhandle, antallet af registrerede, volumen af data, varigheden ved behandlingen og det geografiske omfang.[91] EU Kommissionen vurdere ligeledes at behandlingen af personoplysninger i stort omfang kan medføre en høj risiko.[92] Dette kan skyldes at flere registrerede potentielt kan medføre en større mængde af fysiske personer skaden påføres eller at større datamængder kan øge risikoeksponereingen, hvilket hænger sammen med betragtningerne i præambel 76, hvoraf det fremgår at alvoren og sandsynligheden for de registreredes rettigheder og frihedsrettigheder bør bestemmes med henvisning til de samlede krav, herunder omfanget.

Sammenhæng relaterer sig til de omstændigheder behandlingen finder sted under, dette kan eksempelvis være forholdet mellem den dataansvarlige og de registrerede eller de forventninger de registrerede kan have til den dataansvarlige. Dette perspektiv understøttes af præambel 75, hvoraf det kan udledes at i visse sammenhæng kan behandlingen have en højere alvor eller sandsynlighed for den registreredes rettigheder og frihedsrettigheder. Ligeledes ses det at en ubalance i magtforholdet kan opstå mellem den dataansvarlige og den registrerede, hvis de registrerede er børn, er i særligt udsatte positioner eller ansatte hos den dataansvarlige.[93] Ud fra denne vejledning og præambel 76, må det forstås at skulle der opstå en magtubalance og der påvirker sammenhængen ved behandlingen kan det medføre forøget risici for de registreredes rettigheder og frihedsrettigheder og kan derfor stille højere krav til sikkerhedsniveauet.[94]

Formål udgør det sidste af disse fire kriterier der skal overvejes i forhold til den konkrete behandlingsaktivitet. Behandlingens formål, må ses i relation til GDPR-artikel 5, stk. 1, litra b, hvoraf princippet om formålsbegrænsning fremgår. Deraf forstås det at det ikke blot er en beskrivelse af formålet, men kravet om hensyntagen til formålet danner de retlige rammer for selve behandlingen. Dette understøttes af præambel 39, hvoraf det fremgår at personoplysninger skal indsamles og behandles, til kun relevante formål og begrænset til, hvad der er nødvendigt til formålet med behandlingen. Det følger

[91] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. (2017, 4 . Oktober) S. 10
[92] Ibid S. 8
[93] Ibid S. 10
[94] Ibid) S. 10

ligeledes af flere af GDPR's artikler at behandlingen af personoplysninger kun er lovlige ved specifikke formål,[95] som også danner kriteriet for at der skal være et lovligt behandlingsgrundlag, som også relatere sig til GDPR overordnede princip om lovlighed jf. GDPR-artikel 5 stk. 1 litra. a.
Formålene må derfor ses som et element der skal være med til at begrænse indsamlingen af unødvendige personoplysninger, og dermed sænke de overordnede risici for de registreredes rettigheder og frihedsrettigheder ved ikke at have personoplysninger der ikke er relevante. En formålsbegrænsning vil derfor ikke blot sikre den registrerede mod at få behandlet sine personoplysninger imod GDPR's regler, men også hjælpe den dataansvarlige, da det potentielt vil kunne sænke det overordnede sikkerhedsniveau, på baggrund af at den dataansvarlige behandler færre personoplysninger.

3.1.5 "Risici for fysiske personers rettigheder og frihedsrettigheder"

De fysiske personers rettigheder og frihedsrettigheder, udgør et af de helt centrale vurderingskriterier ved GDPR-artikel 32 stk. 1 og fungere som et styrende element for, hvad der kræves af sikkerhedsniveauet, hvilket understøttes af GDPR-artikel 1 stk. 2, hvoraf det fremgår som et centralt formål af GDPR at beskytte fysiske personers rettigheder og frihedsrettigheder, herunder navnlig beskyttelsen af deres personoplysninger, samt GDPR afdeling 3 og 4, hvori de registreredes rettigheder udfoldes yderligere.
Dette gør at fokus flyttes fra at det udelukkende er et organisatorisk eller teknisk perspektiv, men at det må være de fysiske personer der behandles oplysninger om der er det centrale for beskyttelsesniveauet.[96]
Det centrale er derfor ikke om der foreligger en risiko for brud på datasikkerheden, men om denne risiko kan medføre skade for de registrerede.[97]

Denne risici må forstås bredt, og kan omhandle fysisk, materiel og immateriel skade.[98] Dette understøttes yderligere af præambel 75, hvoraf det fremgår at behandlingen af personoplysninger kan medføre risici, disse kan være fysiske, materielle eller immaterielle, herunder eksempelvis identitetstyveri, finansielle tab, skade på omdømme, tab af fortrolighed og forskelsbehandling.[99] Hvoraf det ligeledes fremgår af præambel 88 at særlige risici, såsom muligheden for identitetstyveri kan medføre skærpede krav til sikkerhedsforanstaltninger.[100] Præambel 75 illustrere dermed at risikovurderingen ikke begrænser sig til

[95] Navnlig GDPR-artikel 6, 9, 10 & 87
[96] Korfits Nielsen, K. & Lotterup, A. (2020) S. 634
[97] Ibid S. 634
[98] Ibid S. 636
[99] Ibid S. 636
[100] Ibid S. 636

mere traditionelle sikkerhedshændelser, men omfatter ligeledes mere indirekte konsekvenser for den registrerede.

Det fremgår af præambel 76, at der ved risikovurderingen skal foretages en objektiv vurdering om behandlingsaktiviteten indebærer en risiko eller høj risiko.[101] Dette medfører at kravene til behandlingssikkerheden skærpes desto større risici der er forbundet med den konkrete behandling .[102] Dette hænger sammen med EU's proportionalitetsprincip, hvoraf det fremgår at handlinger der er underlagt princippet, ikke bør overgå, hvad der er nødvendigt for at nå Charteret om Grundlæggende Rettigheder og dermed også GDPR's formål,[103] og deraf følger det at højere risici nødvendiggør et højere sikkerhedsniveau for behandlingen af personoplysninger.

Kriteriet indebærer derfor at den samlede risikovurderingen er GDPR-artikel 32 tager udgangspunkt i den registreredes rettigheder og frihedsrettigheder. Hvoraf det forekommer at det ikke er nok at fokusere på de økonomiske eller organisatoriske konsekvenser for den dataansvarlige og det er derfor afgørende, hvordan behandlingen af personoplysninger kan påvirke de registreredes rettigheder, herunder blandt andet retten beskyttelse af deres personoplysninger jf. Den Europæiske Unions charter om grundlæggende rettigheder artikel 8.

3.1.6 "Et sikkerhedsniveau, der passer til risikoen"

Kriteriet om et sikkerhedsniveau der passer til risikoen i GDPR-artikel 32 stk. 1, fastslår at GDPR-artikel 32 ikke umiddelbart indeholder en særlig minimumsgrænse og må afvejes i lyset af en objektiv risikovurdering af de forskelige risici behandlingersaktiviteterne medfører.[104] Der er derfor tale om standard, hvor sikkerhedsniveauet ændres afhængigt af, hvordan behandlingen foregår og i relation til de andre kriterier i GDPR-artikel 32 stk. 1. Endvidere understreges dette af præambel 76, hvoraf det fremgår at sikkerhedsniveauet skal hænge sammen med alvoren af risiciene.[105] Derfor følger det at det ikke er nok blot at identificere risici, de skal ligeledes afvejes for at finde et sikkerhedsniveau der imødegår risiciene forbundet hermed. Derfor indeholder kriteriet i GDPR-artikel 32 stk. 1, ikke en maksimal standard men et

[101] Korfits Nielsen, K. & Lotterup, A. (2020) S. 636
[102] Ibid S. 636 f
[103] Nærhedsprincippet og nationale parlamenters rolle. (2025, 17. Februar). se også Neergaard, U. & Nielsen, R. (2020). side 194
[104] Korfits Nielsen, K. & Lotterup, A. (2020) S. 637 f
[105] Ibid S. 637 f

krav om et ”passende” sikkerhedsniveau og til løbende at ajourføre, afveje og tilpasse sikkerhedsforanstaltninger i lyset af det konkrete risikobillede der måtte være for den dataansvarlige. [106]

3.1.7 Ordlyden af GDPR-artikel 32 stk. 1

GDPR-artikel 32 er central for behandlingssikkerheden og stiller kravene til behandlingssikkerheden.[107] Samlet set viser fortolkningen af kriterierne i GDPR-artikel 32 stk. 1 at artiklen er et udtryk for en risikobaseret og fleksibel tilgang til fastsættelse af sikkerhedsniveauet, der ikke opstiller faste og udtømmende krav, men derimod ligger til grund at der skal foretages en konkret vurdering af risiciene. Indledning til artiklen ”under hensyn tagen til” fastslår denne tilgang, hvor artiklens efterfølgende kriterier ikke skal anvendes isoleret men derimod indgå i den samlede afvejning. GDPR-artikel 32 stk. 1 etablerer derfor en ramme, hvor den dataansvarlige pålægges en pligt til at løbende identificere, vurdere og håndtere risici der måtte forekomme ved behandlingen af personoplysninger.
Kriteriet om ”det aktuelle tekniske niveau” bidrager ligeledes til den dynamiske tilgang GDPR-artikel 32 stk. 1 har for, hvilke sikkerhedsforanstaltninger der bør implementeres. Det indebærer således at risikovurderingen og dermed sikkerhedsniveauet ikke kan fastslås på ét bestemt tidspunkt, men må følge den teknologiske udvikling og aktuelle ændringer i trusselsbilledet. Samtidig anvendes hensynet til ”implementeringsomkostninger” som et kriterie der ligger sig op af proportionalitetshensynet der sikrer at der ikke stilles krav til den dataansvarlige der er uforholdsmæssige i forhold til behandlings karakter, omfang, sammenhæng og formål. Implementeringsomkostningerne bør dog ikke stå alene, men derimod afvejes i forhold til den aktuelle behandling og de risici den medfører, således at der ikke forekommer økonomiske betragtninger, der kan medføre et sikkerhedsniveau der ikke er tilstrækkeligt.
GDRP-artikel 32 stk. 1’s kriterier bliver videre konkretiseret i formuleringen ”behandlingens karakter, omfang, sammenhæng og formål”, hvoraf det fremgår at der skal tages stilling til den konkrete behandlingsaktiviet. Dette indebærer at der skal tages stilling til typen af oplysninger, behandlingens udbredelse, de omkringliggende forhold og formålet med behandlingen. Her kan der nævnes at særligt begrebet ”sammenhæng” understreger at vurderingen ikke kun beror sig på den tekniske del af, hvor behandlingen finder sted, men at der må tages højde for de omstændigheder, hvor behandlingen finder sted, herunder de registreredes forventninger og eventuelle magtubalancer. GDPR- artikel 32 stk. 1 afspejler derfor en bred forståelse af datasikkerhed, hvor tekniske, organisatoriske og sociale forhold spiller ind i den samlede vurdering af, hvilket sikkerhedsniveau der er ”passende”.

[106] ”Passende” analyseres selvstændigt senere i specialet
[107] Korfits Nielsen, K. & Lotterup, A. (2020) S. 636

Det centrale omdrejningspunkt for GDPR-artikel 32 stk. 1 er imidlertid risiciene for fysiske personers rettigheder og frihedsrettigheder. Dette kriterium udfoldes ved den rettighedsbaseret tilgang, hvor fokusset som før nævnt ikke blot omhandler data, men beskyttelsen af de fysiske personer oplysningerne omhandler. Risikobegrebet må fortolkes bredt, hvor både materiale, immaterielle og fysiske skader er omfattet, hvilket leder til at også mere indirekte konsekvenser må inddrages, i vurderingen, her kan nævnes tab af omdømme eller diskrimination.[108] I forlængelse heraf fastslår kravet om et sikkerhedsniveau der passer til risikoen, at der skal forekomme proportionalitet mellem foranstaltningerne der bliver truffet og risikoens alvor, heraf desto større risiko, desto større krav til sikkerhedsniveauet, hvilket varier efter den enkelte behandlings karakter.

Af GDPR-artikel 32, stk. 1 litra a – d fremgår der ligeledes eksempler på hvilke foranstaltninger der kan være relevante, disse vil blive gennemgået i senere afsnit af specialet, med henblik på at fastsætte og fortolke hvad foranstaltninger er og kan være.

3.1.8 Stk. 2

GDPR-artikel 32, stk. 2 fremstår som et væsentligt supplement til risikovurderingen der forekommer i GDPR-artikel 32 stk. 1, ved at være mere konkret omkring hvordan risiko vurderingen skal foretages.[109] GDPR-artikel 32 stk. 2 fastslår ligeledes hvilke risici der er væsentlige at inddrage i vurderingen, heraf fremgår det at behandlingen skal tage højde for de risici som behandlingen indebærer, herunder navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger der er transmitteret, opbevaret eller på anden måde behandlet.[110] Hermed gøres det overordnede risikobegreb der følger af stk. 1 mere praktisk anvendeligt i det stk. 2 angiver konkrete kategorier af risici som den dataansvarlige bør forebygge, dog er dette ikke en udtømmende liste, hvilket forstås af ordet ”navnlig”.[111]

Risiciene nævnt ovenfor, afspejler informationssikkerhedsprincipperne omkring ”fortrolighed, integritet, tilgængelighed og robusthed”,[112] der forekommer af GDPR-artikel 32 stk. 1 litra b.

[108] GDPR-præambel 75 og 85
[109] Korfits Nielsen, K. & Lotterup, A. (2020) S. 656 f
[110] GDPR-artikel 32 stk. 2 og Korfits Nielsen, K. & Lotterup, A. (2020) S. 656 f
[111] Korfits Nielsen, K. & Lotterup, A. (2020) S. 656 f
[112] En styrket, fælles indsats for cyber- og informationssikkerhed. (s.d.) S. 9

Uautoriseret videregivelse eller adgang til personoplysninger relateres sig til fortroligheden, da systemet og de data der er tilknyttet systemet, kun skal kunne tilgås af de personer og andre systemer det er meningen skal have adgang.[113]
Ændring af oplysninger vedrører integriteten der forsøger at sikre at oplysninger er korrekte, pålidelige, nøjagtige og fuldstændige.[114]
Hændelig eller ulovlig tilintetgørelse relaterer sig til tilgængeligheden, der sigter efter at behandlingssystemer og -tjenester er tilgængelige ved anmodning fra autoriseret bruger.[115]
Udtrykket robusthed antages at sigte efter at sikre behandlingssteder og -tjenester tekniske og organisatoriske modstandsdygtighed.[116]
Det fremgår ligeledes af GDPR-artikel 32 stk. 1, litra b at det at sikringen af principperne skal være vedvarende, hvorfor det bliver til en løbende teknisk og organisatorisk forpligtigelse for den dataansvarlige, der ikke blot skal opfyldes en gang.[117] Derfor må det forstås at datasikkerhed i GDPR ikke kun relatere sig til beskyttelse mod databrud i snæver fortand, men en bredere fortolkning af sikring af oplysninger mod forskellige former for databrud.
Dette understøttes ligeledes af præambel 83, 75 og 76, hvoraf det samlet fremgår at sikkerheden løbende skal sikre fortrolighed, integritet, tilgængelighed og robusthed i behandlingsaktivieten,[118] samt at risikoens sandsynlighed skal iagttages for at sikre et "passende" sikkerhedsniveau,[119] for at sikre de registreredes rettigheder og frihedsrettigheder.[120]

Samlet set indebærer GDPR-artikel 32 stk. 2 at risikovurderingen skal være konkret og rettet mod at identificerbare trusler mod sikkerheden af personoplysninger. Deraf forstås det at GDPR-artikel 32 stk. 2 er med til at klarificere, hvad der er særligt vigtigt at have fokus på ved fastlæggelsen af risici og implementeringen af foranstaltninger.

[113] Korfits Nielsen, K. & Lotterup, A. (2020) S. 649
[114] Ibid S. 649
[115] Ibid S. 649
[116] Robusthed. (2023, 9. Maj).
[117]Databeskyttelsesforordningen: og de retlige rammer for dansk lovgivning: Betænkning 1565. (2016). side 482 & Korfits Nielsen, K. & Lotterup, A. (2020). S. 649
[118] GDPR-præambel 83
[119] GDPR-præambel 76
[120] GDPR-præambel 75

3.1.9 Stk. 3

GDPR-artikel 32 stk. 3 vedrører anvendelsen af godkendte adfærdskodekser og certificeringsmekanismer som omhandlet i GDPR-artikel 40 og 42 og hvordan de kan anvendes som et element i den samlede vurdering, om at påvise sin overholdelse af de af stk. 1 fastsatte krav. GDPR-artikel 32 stk. 3 fremsætter det som værende element i overholdelsen af kravene, fastligger at anvendelsen af adfærdskodekser og certificeringsmekanismer alene ikke vil medføre overholdelse, hvorfor de kun fungerer som dokumentationsredskab for at påvise overholdelse. Anvendelsen af godkendte adfærdskodekser og certificeringsmekanismer kan fungere som en måde at dokumentere, at relevante sikkerhedsforanstaltninger er blevet implementeret. Som eksempel på et godkendt adfærdskodeks, kan kirkeministeriets adfærdskodeks nævnes [121] da det er godkendt til brug af Datatilsynet. Dog forudsætter adfærdskodekset at de dataansvarlige skal være veldefineret og det bør klart angives, hvilken branche eller sektor de som adfærdskodekset ønsker at finde anvendelse for arbejder under.[122] Derfor afgrænses adfærdskodekset også til de dataansvarlige der udføre de behandlingsaktiviteter og tilhører den branche adfærdskodekset er tilsigtet at finde anvendelse for.[123] Der forekommer i øjeblikket ikke nogen danske certificeringsorganer, men der findes organer på tværs af EU der er godkendte.[124] Certificering kan udstedes til dataanvsarlige af et akkrediteret certificeringsorgan og kan være med til at øge gennemsigtigheden i niveauet for databeskyttelse i forbindelse med specifikke produkter, processer eller tjenester, certificeringen udstedes i sidste ende på baggrund af specifikke behandlingsaktiviteter.[125] Samlet set indebærer GDPR-artikel 32 stk. 3 at anvendelsen af ovennævnte adfærdskodekser og certificeringsmekaniske kan hjælpe med dokumentationskravet, men ikke stå alene for at påvise overholdelsen, da det stadigvæk er pålagt den dataansvarlige at udføre risikovurderinger efter stk. 1. GDPR-artikel 32 stk. 3 understøtter dermed GDPR's bredere fokus på ansvarlighed,[126] da ansvaret for overholdensen af kravene ikke fuldstændigt kan fralægges den dataansvarlige ved at anvende de ovennævnte adfærdskodekser og certificeringsmekanismer.

[121] Kirkeministeriets adfærdskodeks er godkendt. (s.d.)
[122] Vejledning om adfærdskodekser. (2023, Juni) S. 16
[123] Ibid S. 22
[124] Register of certification mechanisms, seals and marks. (s.d.).
[125] Adfærdskodekser og certificeringsordninger. (s.d.)
[126] GDPR-artikel 5 stk. 2

3.1.10 Stk. 4

GDPR-artikel 32 stk. 4 fastslår at den dataansvarlige tager skridt for at sikre sig at enhver fysisk person der udfører arbejde for den dataansvarlige og som har adgang til personoplysninger kun behandler disse oplysninger efter instruks fra den dataansvarlige, medmindre at behandlingen kræves i henhold til EU-retten eller medlemsstaternes nationale ret, hvilket ligeledes fremgår af GDPR-artikel 29.[127] Dette giver altså datasikkerheden et menneskeligt aspekt, hvor der konkretiseres at det altså ikke er nok med tekniske foranstaltninger, men at det er vigtigt for den dataansvarlige at give instrukser for behandlingen til sine ansatte og forekommer derfor som et mere organisatorisk hensyn at tage.
Ligeledes gør GDPR-artikel 32. stk. 4 det helt klart at det er den dataansvarlige, der bærer ansvaret for behandlingen, hvorfor det er dem der bærer ansvaret for behandlingen, da det skal sikre at behandlingen kun sker efter instruks fra netop den dataansvarlige.

3.2 Fortolkning af foranstaltninger

I dette afsnit vil kravet om organisatoriske og tekniske foranstaltninger i GDPR-artikel 32 stk. 1 blive fortolket. Her findes det hensigtsmæssigt at opdele foranstaltninger i henholdsvis tekniske og organisatoriske for at få en mere systematisk forståelse af, hvad disse foranstaltninger indebærer og hvilke typer foranstaltninger der forventes implementeret. Opdelingen sker på trods af at GDPR-artikel 32 stk. 1 nævner dem i sammenhæng.
På baggrund af dette vil følgende afsnit gennemgå tekniske og organisatoriske foranstaltninger for at klarlægge dets funktion og betydning i relation til den samlede vurdering der forekommer af GDPR-artikel 32 stk. 1.

3.2.1 Foranstaltninger generelt

Foranstaltninger efter GDPR forekommer som de tiltag, der bevarer og/eller ændrer risikoen.[128] Af GDPR-artikel 32 stk. 1 litra a - d fremgår der en række eksempler på foranstaltninger, dog må denne liste forstås som værende ikke udtømmende, da der inden opremsningen forekommer ”blandt andet”.[129] Men det konkretiseres ligeledes at de skal være relevante for at imødegå den pågældende risici. Heraf fremgår det af præambel 83 at foranstaltninger særligt skal sikre mod hændelig eller ulovlig tilintetgørelse, tab, ændring

[127] Korfits Nielsen, K. & Lotterup, A. (2020). S. 657
[128] Katalog over foranstaltninger. (s.d.)
[129] Disse vil blive gennemgået næremere nedenfor under henholdsvis afsnittet om ”tekniske” og ”organisatoriske” foranstaltninger

eller uautoriseret videregivelse af eller adgang til personoplysninger. Foranstaltninger skal tilsammen udgøre tekniske løsninger og organisatoriske tiltag der skal sikre integritet, fortrolighed, tilgængelighed og robusthed som nævnt i kapitel 3 og forekommer af GDPR-artikel 32 stk. 1 litra b, hvoraf det fremgør at sikringen skal vedvarende.

3.2.2 Tekniske foranstaltninger

Tekniske foranstaltninger forstås som værende IT-løsninger fx brugeradministrering, automatisk adgangskontrol, kryptering og sletning, men kan også være fysiske døre eller løse.[130]
Tekniske foranstaltninger forekommer som en central del af vurderingen som følger af GDPR-artikel 32 stk. 1, og som beskrevet ovenfor omfatter de blandt andet IT-løsninger. De tekniske foranstaltninger retter sig mod de it-systemer der bruges til at behandle og opbevare personoplysninger, dette udledes blandt andet af GDPR-artikel 32 stk. 1 litra a, hvoraf det fremgår at en foranstaltning kunne være kryptering og pseudonomisering, hvoraf disse forekommer som en integreret del af IT-systemet i sig selv. Datatilsynets katalog over foranstaltninger henviser til en række foranstaltninger, hvoraf IT-sikkerhedsforanstaltninger fremgår som eksempelvis backup, multifaktorautentifikation, netværkssegmentering m.m.[131] dog som det også fremgår ovenfor, afgrænser tekniske foranstaltninger sig ikke til IT-systemer, EDPB fremhæver her at det er anbefalelsesværdigt at tekniske foranstaltninger forsøger at sikre hardware, software, kommunikationskanaler, papir dokumenter, og fysiske lokationer.[132] Dette understreges ligeledes af datatilsynet der indstiller Region Midtjylland til bøde for manglende fysisk adgangskontrol til faciliteter, hvor der blev opbevaret op mod 100.000 patientjournaler, den utilsigtede adgang til disse journaler, forekom både ved manglen af adgangskontrol på adgangskort, der gjorde at alle med et adgangskort, herunder både patienter og personale havde adgang til lokalet, samt at forbipasserende fra vinduerne på ydersiden af bygningen kunne se omslaget på journaler, hvoraf der både kunne aflæses navne og CPR-nummer.[133]
Dette udvider altså den direkte forståelse af tekniske foranstaltninger, til ikke kun at omhandle IT-systemer. EDPB bringer ligeledes eksempler på, hvad der kan være relevant ved sikringen af en arbejdsstation, her fremhæves session lockout, brug af firewall, regulær opdatering af antivirusprogrammer og software, automatisk system opdatering, opsætning af backup og ikke forbinde til eksterne medier.[134] Ligeledes fremhæves eksempler på, hvad der bør undgås ved sikringen af en arbejdsstation, heraf fremgår at der ikke

[130] Katalog over foranstaltninger. (s.d.)
[131] Ibid
[132] Secure Personal Data. (s.d.)
[133] Region Midtjylland indstillet til bøde. (2021, 08. September)
[134] Secure Personal Data. (s.d.)

skal gives administratorrettigheder til personer uden den nødvendige IT-træning, samt at der ikke bruges forældede styresystemer.[135] Dette må forstås som være en form for minimum, som EDPB mener burde forekomme ved sikringen af en arbejdsstation, da der ligeledes fremgår en liste over tekniske foranstaltninger, den dataansvarlige kan implementere hvis de vil "go further".[136]

Når forståelsen af tekniske foranstaltninger udvides til at inkludere beskyttelsen af fysiske lokationer følger der ligeledes en liste fra EDPB, med foranstaltninger der anbefales at den dataansvarlige implementerer, her fremgår tyverialarm, røgalarm og fysisk brandsikkerhed, beskyttelse af nøgler, definering af bygninger og deres risici, lister med autoriseret personer og kontrol over gæsteadgang. Ligeledes fremgår det at vedligehold og beskyttelse af især serverrum ikke bør neglegeres da dette kan have betydning for dataene såvel som de andre sikkerhedsforanstaltninger.[137] Disse foranstaltninger forekommer ligeledes som værende en minimumsgrænse for hvad der kan være relevant, da der igen forekommer en "go further" liste, med yderligere foranstaltninger der kan træffes. Der forekommer tilsvarende eksempler for håndteringen af autorisation og pseudonymisering.

EDPB kommer ligeledes med praktiske eksempler på, hvordan disse foranstaltninger kan implementeres og hvilken påvirkningen de har. Her kan eksemplet om fysisk beskyttelse af serverrum fremhæves, her fremgår det at serverrummet bør have adgangskontrol, for at sikre at uvedkommende ikke får adgang og røgalarm, for hurtigt at identificere brand og aktivere de nødvendige ressourcer, eksempelvis brandvæsnet for at minimere skaden.[138] Da det i sidste ende er den dataansvarlige der er ansvarlig for behandlingen og opbevaringen af personoplysninger er det derfor ligeledes vigtigt at de behandlingen og opbevaringen kun sker i systemer godkendt af den dataansvarlige.[139]

En yderligere dimension til disse foranstaltninger forekommer ved at der skal forekomme regelmæssig afprøvning, vurdering og evaluering af foranstaltninger, der sikrer behandlingssikkerheden jf. GDPR-artikel 32 stk. 1 litra d, hvilket understøttes af præambel 83, hvoraf det fremgår at sikringen skal opretholdes. Derfor fremgår det at disse foranstaltninger ikke må være statiske og skal skræddersyes til den individuelle dataansvarliges behov.[140] Hvilket ligeledes understreges af præambel 83, hvoraf det fremgår at foranstaltninger skal være svarende til det aktuelle tekniske niveau, og opdateres i forlængelse af udviklingen af ny teknologi og skift i samfundets brug af teknologi.[141] Derfor er det vigtigt den dataansvarlige holder sig opdateret og implementere løsninger der er anerkendte på området, ved at

[135] Secure Personal Data. (s.d.)
[136] Forstås som "Gå videre", altså gøre mere
[137] Secure Personal Data. (s.d.)
[138] Ibid
[139] Trakowski, J. & Gersvang Sørensen, M. (2019) S. 220
[140] Ibid S. 221 f
[141] Ibid S. 221 f

eksempelvis bruge Datatilsynets katalog over foranstaltninger, for at sikre at netop deres risici håndteres korrekt og med de rigtige foranstaltninger. Derfor vil vurderingen af , hvilke foranstaltninger der er korrekte ligeledes være varierende, afhængigt af den konkrete behandlingssituation.

Samlet set udgør tekniske foranstaltninger en vigtig del af behandlingssikkerheden. De fungerer som konkrete værktøjer og systemer til at beskytte personoplysninger. Deres effekt er samtidig afhængig af at det er de korrekte foranstaltninger der implementeres, samt at vedligeholdes løbende og opdateres i forhold til det aktuelle tekniske niveau. Hermed fremgår tekniske foranstaltninger som en praktisk dimension til de juridiske krav der stilles af GDPR-artikel 32, hvor kravene kan omsættes til konkrete løsninger.

3.2.3 Organisatoriske foranstaltninger

De organisatoriske foranstaltninger udgør den anden væsentlige foranstaltning nævnt i GDPR-artikel 32 stk. 1 og omfatter blandt andet sikkerhedspolitikker, interne procedurer og uddannelse i korrekt anvendelse af IT-systemer.[142] De tekniske foranstaltninger retter sig mod tekniske IT-systemer og fysisk beskyttelse af lokationer, retter de organisatoriske foranstaltninger sig mod den menneskelige del af datasikkerhed. Her ligger kravet om organisatoriske foranstaltninger sig op af GDPR-artikel 32 stk. 1 litra c, hvoraf det fremgår at den dataansvarlige skal sikre sig evnen til at rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse der fører til brud på persondatasikkerheden[143]. Her harmonere de tekniske foranstaltninger sig med de organisatoriske, ved at manglen på procedurer der diktere hvem der gør hvad i tilfælde af en hændelse, kan lede til manglende udnyttelse af tekniske foranstaltninger og kan i sidste ende føre til at hændelsen forværres.[144] Organisatoriske foranstaltninger omhandler især, hvordan personale bedst muligt bliver klædt på til at kunne imødegå en hændelse Organisatoriske foranstaltninger der kan implementeres inkludere awereness træning, regulær opdatering af procedurer og intern kommunikation der påminder peronsale om datasikkerhed.[145] Ligeledes forekommer det relevant at have opdaterede driftsprocedurer, der kan være med til at beskrive præcis, hvordan en behandlingsaktivitet skal udføres, hvilket ikke blot er en organisatorisk foranstaltning, men ligeledes et krav efter GDPR-artikel 32 stk. 4.[146] Awareness træning

[142] Katalog over foranstaltninger. (s.d.)
[143] Se GDPR-artikel 4 stk. 1 nr. 12
[144] Secure Personal Data. (s.d.)
[145] Ibid
[146] Ibid

forekommer særligt relevant som en organisatorisk foranstaltning, da det er den dataansvarliges ansvar at dens ansatte forstår, hvordan de skal behandle personoplysninger i deres rolle.[147] Datatilsynet understreger ligeledes vigtigheden om at nogle foranstaltninger ikke kan stå alene, hvilket konkretiseres af Datatilsynets kritik af tre politikredse. Her blev der i første omgang uddelt kritik på baggrund af manglende logning, hvor der efter implementering af logningen og awerenesstræning, blev foretaget en vurdering af at logning og awarenesstræning sammenlagt var en "passende" foranstaltning.[148]

Der forekommer imidlertid flere måder den dataansvarlige kan instruere sine ansatte i, hvordan de skal håndtere deres behandlingsaktiviteter, men særligt relevant findes her, awereness træningssessioner, regulær opdatering af procedurer, beskrivelser af forpligtelser og forklare de sanktioner der medfølger overtrædelse af GDPR.[149] I praksis anvendes awerness som en opsamlingsbetegnelse der dækker over alle opmærksomheds skabende tiltag.[150] Her kan det både være, hvad medarbejdere under den dataansvarlige må og ikke må, samt hvad de bør og ikke bør gøre, derfor ses awereness som en måde at motivere medarbejder til at ændre eller korrigere adfærd når det omhandler håndteringen af personoplysninger.[151] Awereness træning kan både bruges som en forebyggende men også en opdagende foranstaltning, her prøver den forebyggende del altså at imødegå sikkerhedsbrud, ved eksempelvis at træne medarbejdere i at spotte phisingmails, så sikkerhedsbruddet ikke forekommer.[152] Den opdagende foranstaltning derimod fokusere mere på hvad de skal gøre, hvis de eksempelvis opdager at et adgangskort er væk, her vil hurtig og effektiv spærring af kortet kunne imødegå en hændelse, inden adgangskortet misbruges.[153] Derfor ses i praksis at compilerne træning i støerer organisationer består af e-learning og gamification,[154] dog er det nødvendigt at sådanne initiativer bliver støttet af stærk IT-sikkerhed,[155] altså de tekniske foranstaltninger.

De ovennævnte foranstaltninger, bør dog ikke kun rettes de personer der udføre behandlingsaktiviteterne, men ligeledes mod den dataansvarliges ledelseslag, for at sikre forståelsen af GDPR's forpligtelser, samt at sikre at de nødvendige ressourcer bliver allokeret til at kunne løse opgaven.[156] Der bør derfor også opsættes procedurer for, hvordan den dataansvarlige sikre sig at en databehandler behandler personoplysninger på vejene af den dataansvarlige.[157] Præambel 81 stiller ligeledes krav til at der skal indgås en aftale for, hvordan databehandleren behandler oplysninger på vejene den dataansvarlige, der bør

[147] Trakowski, J. & Gersvang Sørensen, M. (2019) S. 217
[148] Tre politikredse får kritik for manglende behandlingssikkerhed. (2024, 17. Maj)
[149] Trakowski, J. & Gersvang Sørensen, M. (2019) S. 217 f
[150] Foranstaltning: Awareness. (s.d.)
[151] Ibid
[152] Ibid
[153] Ibid
[154] For beskrivelse af Gamification og spilbaseret læring. (2025, 11. Juli)
[155] Trakowski, J. & Gersvang Sørensen, M. (2019) S. 218
[156] Ibid S. 218
[157] GDPR præambel 81

derfor opsættes procedurer for at kontrollere indholdet i en sådan databehandleraftale, for at sikre at indholdet lever op til det sikkerhedsniveau der forventes. Dette har medført GDPR-artikel 28 og 29 der stiller krav til at databehandleren kun må behandle oplysninger på instruks fra den dataansvarlige, hvor i GDPR-artikel 28 stk. 3 bliver det præciseret at der skal være indgået en kontrakt mellem databehandleren og den dataansvarlige. Manglende kontrol af databehandlere her i praksis medført at, Datatilsynet har udtalt kritik af en databehandler, der har videregivet dele af opgaver fra gymnasieelver til forskere, hvilket er imod databeskyttelsesretlige regler, da dette er blevet gjort uden instruks fra den dataansvarlige.[158] GDPR-artikel 28 stk. 3, litra c henviser til en mere konkret mængde af foranstaltninger ved at henvise til at der skal iværksættes alle foranstaltninger der fremgår af GDPR-artikel 32, hvilket kan medføre en fejlfortolkning i forhold til den liste der forekommer i GDPR-artikel 32 stk. 1 litra a-d, da det som nævnt ikke er en fuldstændig liste og ikke er deciderede krav, men i højere grad eksempler på foranstaltninger der kan vurderes til at være "passende".
Som nævnt ovenfor i afsnittet om tekniske foranstaltninger fremgår det at foranstaltningerne skal være vedvarende og opretholdes, dette gælder ligeledes for de organisatoriske foranstaltninger, hvorfor det er vigtigt at justere til når arbejdsgange ændres eller andre former for forandring der vil medføre at en justering er påkrævet.

3.2.4 Tekniske og organisatoriske foranstaltninger

Det forekommer ikke afgørende om en foranstaltning placeres i en af de to kategorier, det er derimod afgørende om der er truffet foranstaltningerne og at de tilsammen yder tilstrækkelig sikkerhed for beskyttelsen af personoplysninger.[159] Et eksempel på dette fremgår af datatilsynets vejledning, hvor "firewall" fremhæves, her beskrives det at selve indkøbet af foranstaltningen ikke er nok, den skal derimod også implementeres, administreres og holdes opdateret.[160] Derfor vil en sådan foranstaltning både have elementer af organisatoriske og tekniske foranstaltninger, da selve "firewallen", vil være et IT-produkt der forebygger mod hændelser, men for at denne yder den tilstrækkelige sikkerhed, kræver det at den holdes opdateret og at personalet er instrueret i hvordan den bruges, hvorfor den også har karaktere af en organisatorisk foranstaltning.[161] Derfor vil en foranstaltning formodentligt sjældent være kun teknisk eller organisatorisk, og understreger derfor vigtigheden i at de understøtter hindanden, da det ikke vil være tilstrækkeligt kun at have den ene frem for den anden. Ligeledes bør det understreges at der ikke

[158] Videregivelse af opgavebesvarelser. (2020, 18. Juni)
[159] Katalog over foranstaltninger. (s.d.)
[160] Ibid
[161] Ibid

forekommer en fuldkommen liste over foranstaltninger og ud fra ovenstående må det forstås at alle tiltag der træffes for at styrke sikkerhedsniveauet for behandling af personoplysninger, kan ses som en foranstaltning.

Ligeledes ses det i GDPR-artikel 25 at databeskyttelsen forekommer som et udtryk for nyskabelse og i høj grad relatere sig til GDPR-artikel 32.[162] Det fremgår ligeledes af præambel 46 at der træffes de fornødne tekniske og organisatoriske foranstaltninger allerede ved udformningen og iværksættelsen af behandlingen, med det primære fokus at varetage sikkerheden og dermed imødegå utilsigtede behandlinger.[163]
GDPR-artikel 25 udformer sig dermed som værende databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.[164] Databeskyttelsen gennem design udformer sig i GDPR-artikel 25 stk. 1 stiller krav til at den dataansvarlige træffer passende tekniske og organisatoriske foranstaltninger, som er designenet til både at medbringe effektiv implementering og integrere de fornødne garantier i behandlingen.[165] Her nævnes i GDPR-artikel 25 stk. 1 dataminimeringensprincippet jf artikel 5 stk. 1, litra c, hvoraf det udledes at et IT-system skal være sådan designet at det ikke behandler flere oplysninger end nødvendigt.[166] Dog betyder dette imidlertid ikke at de andre principper der følger af GDPR-artikel 5 ikke skal overholdes.[167] Det følger ligeledes af vejledningen fra Datatilsynet, Justitsministeriet og Digitaliseringstyrelsen fra juni 2018 omhandlende behandlingssikkerhed en liste med ydereligere eksempler på hvad databeskyttelse gennem design kan være.[168] Heraf fremgår eksempelvis minimering af persondatabehandling, pseudonymisering af personoplysninger, kryptering af data i transit eller hvile, sikring af infrastrukturen mod uautoriseret indtrængning og effektive organisatoriske kontroller til autorisation og styring af adgangsrettigheder.[169] Heraf udledes det at effektive foranstaltninger ikke kun relatere sig til selve behandlingen af personoplysninger, men altså også en aktiv stillingstagen til hvilke personoplysninger der ikke kræves af en konkret behandling, for at minimere risiciene forbundet hermed. Dette understøttes ligeledes af GDPR-artikel 25 stk. 2, hvoraf det fremgår at foranstaltninger der skal træffes sker gennem standardindstillinger, hvor det skal begrænses til alene det der er nødvendigt for at opfylde formålet.[170] Standardindstillinger skal forstås bredt, da det både kan omfatte organisatoriske, såvel

[162] Korfits Nielsen, K. & Lotterup, A. (2020) S. 591
[163] Ibid S. 592
[164] Ibid S. 594 & 597
[165] Ibid S. 594
[166] Ibid S. 594
[167] Ibid S. 594
[168] Ibid S. 595
[169] Ibid S. 595
[170] Ibid S. 597

som tekniske foranstaltninger.[171] En standardindstilling kan eksempelvis være IT-tekniske indstillinger der begrænser de oplysninger der som standard behandles.[172] Dette understøtter ligeledes formodningen om at der for at overholde kravene til hvilke foranstaltninger der skal implementeres, skal forekomme en aktiv stilling tagen til, hvilke personoplysninger der er nødvendige at behandle for at løse opgaven. Det antages derfor at for at overholde kravene til foranstaltninger af GDPR-artikel 32 stk. 1, skal kravene i GDPR-artikel 25 stk. 1 og 2 ligeledes overholdes. Derfor afspejler kravet om foranstaltninger, at det ikke er de konkrete tiltag, der er fokus på, men effekten af tiltagene i relation til de identificerede risici.

3.3 Fortolkning af passende

Fortolkningen af begrebet ”passende” i GDPR-artikel 32 stk. 1 udgør et centralt emne i GDPR-artikel 32, den medbringer en, hvis kompleksitet, hvor der som anført i kapitel 3’s forgående afsnit forekommer en række kriterier der skal tages stilling til ved fastlæggelsen af, hvorvidt en teknisk eller organisatorisk foranstaltning er ”passende”. Heraf forekommer det ligeledes at GDPR-artikel 32 er en åben standard, hvor der ikke gives konkrete foranstaltninger der skal træffes, men overlader det til en risikovurdering af de konkrete behandlingsaktiviteter.[173] For at forstå ”passende” må der derfor fortetages en samlet afvejning af de kriterier der fremstår af GDPR-artikel 32 stk. 1 og praksis afgivet omkring emnet. Dette rejser det overordnede spørgsmål nærværende speciale tager udgangspunkt i, nemlig om der på trods af GDPR-artikel 32’s ellers fleksible karakter, hvor der ikke er fastsat nogle helt konkrete krav til, hvilke foranstaltninger der skal træffes, kan fastsættes en teoretisk minimumsgrænse, for hvornår en foranstaltning kan anses for værende ”passende” og i sidste ende hjælpe den dataansvarlige eller databehandlere med at konkretisere kravene der skal overholdes, eller eventuelt, hvornår en foranstaltning ihvertfald ikke er passende.

3.3.1 ”Passende” som retlig standard

Begrebet ”passende” forekommer som en retsstandard,[174] hvilket indebærer at der efter formuleringen i GDPR-artikel 32 stk. 1 gives mulighed for at dens anvendelse kan tilpasses efter aktuelle og skiftende forhold. Dette udledes blandt andet af at der skal tages stilling til det aktuelle tekniske niveau, hvorfor GDPR-artikel 32 altså må kunne ændres i takt med samfundets adgang til og brug af eksempelvis IT-

[171] Korfits Nielsen, K. & Lotterup, A. (2020) S. 597
[172] Ibid S. 597
[173] Ibid S.634 f
[174] Dalberg-Larsen, J. (2024, 2. April). Retsstandard.

systemer. Derfor adskiller GDPR-artikel 32 sig altså fra detaljerede regler, hvoraf specifikke krav fremgår. Dog er det værd at nævne at kryptering og pseudonymisering fremgår som konkrete eksempler på foranstaltninger der kan være relevante at træffe,[175] hvilket formodentligt gør at GDPR-artikel 32 stk. 1 ikke er fuldstændigt teknologineutral, da det ikke endnu vides om denne form for sikkerhed vil være forældet i fremtiden. Dog forekommer selve GDPR-artikel 32 stk. 1 at være teknologineutral indtil eksemplet der fremgår af GDPR-artikel 32 stk. 1, litra a, hvilket er et kendetegn for retsstandarder.[176] Her kan det teknologiske niveau der fremgår af GDPR-artikel 32 stk. 1 formeligt sammenlignes med aftalelovens § 36 hvoraf det fremgår at en aftale kan tilsidesættes hvis den er i strid med "redelig handlemåde", der forekommer som et klassisk eksempel på en retlig standard.[177] I denne sammenhæng fungere "passende" som et kriterium for at den dataansvarlige eller databehandleren foretager vurdering frem for blot at implementere forudbestemte krav.

Dette kriterie overlades i høj grad til den dataansvarlige, hvilket ses ved at det er pålagt at implementere foranstaltninger, ved hensyntagen til opremsningen der følger af GDPR-artikel 32 stk. 1, dette undstreger ansvarlighedsprinippet jf. GDPR-artikel 5 stk. 2, hvor det netop er den dataansvarlige der har ansvaret for at GDPR's principper overholdes. [178] Samtidigt åbnes der for at tilsynsmyndigheder efter GDPR-artikel 51, kan sikre overholdelse af GDPR og dermed gøre det mere konkret hvad der ligges vægt på ved afvejningen af, hvad der "passende".

3.3.2 Den risikobasrede tilgang

Som beskrevet i ordlydsfortolkningen skal vurderingen af "passende" foretages ud fra en risikobaseret tilgang. Hvorvidt en foranstaltning er passende må som udgangspunkt forstås i direkte relation til de identificerede risici der måtte være for den registreredes rettigheder og frihedsrettigheder i forbindelse med behandlingen.[179] Dette indebærer som beskrevet i ordlydsfortolkningen, at risiciene skal vurderes ud fra både sandsynlig og konsekvens for den registreredes rettigheder og frihedsrettigheder, altså at desto højere risikoen for at en hændelse forekommer, desto højere krav vil der blive stillet til foranstaltningerne. Her findes det ligeledes relevant at såfremt der forekommer en tilpas høj risiko, kan behandlingen blive omfattet af GDPR-artikel 35 og have yderligere krav for dokumentation og test. Dette kan formodentligt ses som en organisatorisk foranstaltning der kan medregnes i den samlede vurdering af "passende" da den

[175] GDPR-artikel 1 stk. 1 litra a
[176] Bryde Andersen, M. (2002) S. 183
[177] Ibid S. 183
[178] GDPR-artikel 5 stk. 1 litra a - f
[179] Korfits Nielsen, K. & Lotterup, A. (2020) S. 636

dataansvarlige i højere grad får klarlagt evt. risici og konsekvenser.[180] Hvilket understreges af Datatilsynet, der har uddelt kritik af Kertemindes kommune, hvoraf det fremgår at foranstaltninger skal vurderes i forhold til behandlings risici og at desto højere risiciene er, desto oftere skal testen og evalueringen af foranstaltningen forekomme.[181]

Denne tilgang med de identificerede risici som omdrejningspunkt, medfører at for nuværende medfølger der ikke et mere konkret sikkerhedsniveau der skal overholdes. Dog skal det nævnes at GDPR-artikel 32 stk. 3 tillader at anvende adfærdskodekser, hvor kirkeministeriets adfærdskodeks kan anvendes af de menighedsråd der tilslutter sig. Af adfærdskodekset fremgår der konkrete tiltag til databeskyttelse, der må vurderes som værende passende da kodekset er godkendt af datatilsynet og på baggrund af dette foranstaltninger heri må forstås som værende "passende"[182]. Foranstaltningerne fastsat af adfærdskodekset må altså vurderes at være "passende" og dataansvarlige der har mulighed for at tilslutte sig en sådan adfærdskodeks, kan med fordel tilslutte sig, for nemmere at kunne overskue, hvad "passende" betyder i relation til netop deres behandling af personoplysninger og hvilke risici der er taget stilling til.[183] Så selvom der ikke umiddelbart forekommer et generelt minimumsgrænse af GDPR-artikel 32, kan brugen af adfærdskodekser, være med til at identificere hvilke foranstaltninger, der bør træffes, hvis den dataansvarlige behandler personoplysninger inden for specifikke brancher eller sektorer der er udarbejdet adfærdskodekser for. Dog hvis der ikke er foretaget adfærdskodekser for netop den dataansvarliges branche forekommer "passende" stadigvæk som et relativt begreb og det er dermed stadigvæk den risikobaserede tilgang der bør tages. Dette eliminerer dog stadigvæk ikke kravet om den risikobaserede tilgang, da det ligeledes forekommer af GDPR-artikel 32 stk. 3 at det kun kan bidrage til den samlede overholdelse af kravene og dermed ikke kan stå alene.

3.3.4 Proportionalitet og afvejning

Begrebet "passende" må ligeledes forstås at medbringe en proportionalitetsvurdering,[184] hvor de forskellige hensyn der følger af GDPR-artikel 32 stk. 1 må afvejes samlet for at forstå, hvad der er "passende". Her må det forstås at på den ene side fremgår behovet for beskyttelse af fysiske personers rettigheder og frihedsrettigheder, som værende navnlig deres personoplysninger, som det overordnede hensyn der følger af GDPR og på den anden side hensyn om blandt andet teknisk mulighed og økonomiske

[180] For yderligere se side 687 – 710 i Korfits Nielsen, K. & Lotterup, A. (2020). GDPR-artikel 35 vil ikke blive analyseret yderligere i nærværende speciale da der i højere grad fokuseres på GDPR-artikel 32 som helhed for at klarlægge "passende"
[181] Kerteminde Kommune får kritik for deres sikkerhedsprocedurer. (2024, 23. Februar)
[182] Adfærdskodeks for menighedsråds behandling af personoplysninger som led i sognepleje. (2021, 22. Juni). *Datatilsynet*.
[183] Adfærdskodekser og certificeringsordninger. (s.d.).
[184] Se afsnit 3.1.5

omkostninger.[185] Implementeringsomkostninger giver ikke den dataansvarlige ret til ikke at implementere foranstaltninger, blot fordi de kommer med en stor omkostning, da foranstaltningerne skal implementeres, hvis den samlede risikovurdering fastsætter det, da det må forstås at det er GDPR's overordnede hensyn der vægtes højest. Hensynene indgår derfor alle i den samlede vurdering, men kan ikke i sig selv medføre et lavt beskyttelsesnivau, såfremt risikoen er høj.

Dette medfører ligeledes at der gives et spændefelt at arbejde i for den dataansvarlige, hvor der ikke fastsættes konkrete krav til foranstaltninger, der i teorien kan være dyrere alternativer, til eventuelt billigere og mindre teknologiske løsninger. Så på den ene side medfølger det af proportionalitetshensynet at den dataansvarlige ikke tvinges til at foretage foranstaltninger, der ikke er proportionelle i forhold til de identificerede risici og på den anden side at den dataansvarlige selv bærer ansvaret, for at identificere risici og fastslå, hvilke foranstaltninger der er "passende", hvoraf der kan forekomme en hvis tvivl hos den dataansvarlige omkring, hvad netop dette er.[186]
Proportionaliteten, må ligeledes anses som værende et dynamisk element, det forekommer som anført ovenfor at GDPR-artikel 32 er en retlig standard, hvorfor proportionaliteten ligeledes kan ændre sig i takt med at foranstaltninger, arbejdsgange eller lignende bliver forældet. Derfor kan et af de vigtigste elementer den dataansvarlige skal fokusere på ved fastlæggelsen af passende foranstaltninger være at definere klare roller for deres ansatte,[187] samt procedure for regelmæssig afprøvning, vurdering og evaluering der følger af GDPR-artikel 32 stk. 1, litra d. Dette kan have karaktere af både tekniske og organisatoriske foranstaltninger, hvor det igennem disse tiltag kan sikres at foranstaltningerne forholder sig "passende" og dermed proportionelle i relation til det nuværende tekniske niveau og samfundet generelt.

3.3.5 Det aktuelle tekniske niveau

For at vurdere, hvorvidt en foranstaltning er "passende" i relation til det tekniske niveau er det ligeledes vigtigt at vurdere teknologiens udvikling. Af datatilsynets rapport for sikkerhedsbrud fremgår det at den hændelsestype der oftest forekommer er rigtige oplysninger der utilsigtet bliver sendt til forkert modtager,[188] dette kræver formodentligvis i højere grad organisatoriske foranstaltninger at imødegå, her kan eksempelvis awereness træning være nødvendigt for at øge fokusset på disse hændelser og muligvis kombinere det med mere lavpraktiske tiltag såsom at fjerne autoudfyld når der skal sendes mails for at sikre at der bliver tænkt over, hvem mailen sendes til. Ligeledes er det her værd at diskutere

[185] Implementeringsokostninger og det aktuelle tekniske niveau
[186] Smirnova, Y. & Travieso-Morales, V. (2025, 1. August).
[187] Trakowski, J. & Gersvang Sørensen, M. (2019) S. 218
[188] *Detaljeret statistik på anmeldelser om brud på persondatasikkerheden*. (2026, April). Datatilsynet.

proportionaliteten, da disse to foranstaltninger nævnt ovenfor formentligt vil kunne imødegås med en rimelig overskuelighed for den dataansvarlige. Problemet vil dog også kunne løses med tilkøb af ekstra IT-sikkerhed hvor mails bliver end-to-end krypteret eller at modtageren skal bruge en selvstændig nøgle for at åbne dokumentet. Dette vil i nogen henseender kunne forekomme som værende en "passende" foranstaltning, men i daglig virksomhedskommunikation kan dette ses som en hindring eller unødig besværliggørelse af arbejdsgange, så selvom at kravet om "passende foranstaltninger" bliver opfyldt er dette ikke nødvendigvis proportionalt i relation til de andre krav der stilles af GDPR-artikel 32 stk. 1.
Der opstår ligeledes spørgsmål til, hvad der skal tænkes ind i det aktuelle tekniske niveau, her findes det relevant at det aktuelle trusselsbillede indgår i vurderingen for hvad der er "passende", det ses i samfundet at flere virksomheder rammes af cyberangreb,[189] derfor er de mest gængse metoder der anvendes som cyberangreb ligeledes relevant for vurderingen. Det fremgår at en af de mest almindelige typer for cyberangreb forekommer som værende phising,[190] og at de i de fleste tilfælde er det offentlige virksomheder der bliver ramt, hvilket stemmer overens med at det fleste rapporterede hændelser kommer fra offentlige virksomheder.[191] Derfor stilles der spørgsmål til om typen af virksomhed ligeledes skal inddrages i vurderingen af om en foranstaltning er passende. Det forekommer at den samlede risiko for cyberkriminalitet i Danmark er meget høj, [192] dette omfatter blandt andet ransomware angreb,[193] derfor vurderes det, at det ikke er branchen i sig selv der skal fokuseres på, men i højere grad at de dataansvarlige implementerer foranstaltninger der stemmer overens med GDPR-artikel 32 stk. 1, litra c, hvor det i lyset af trusselsniveauet og Samsisk trusselanalyse, er vigtigt at kunne genoprette tilgængeligheden og adgangen til personoplysninger rettidigt for at kunne begrænse konsekvenserne af sikkerhedsbruddet. Ligeledes er det vigtigt for den dataansvarlige at have procedurer der kan identificere disse risici. Dette understreger at vurderingen af, hvilke foranstaltninger der er "passende" ikke alene er fremadskuende, men også skal være løbende, da trusselsbilledet kan ændre sig. Der stilles derfor krav til at den dataansvarlige kontinuerligt kontrollere deres sikkerhedsniveau, for at vurdere om det er "passende". Dette understøttes af datatilsynet kontrolbesøg hos Kerteminde kommune, her udtaler Datatilsynet at kravet, såfremt der logges anvendelse af personoplysninger i IT-systemer, vil Kertemindes kommunes stikprøvekontrol kun lige leve op til minumumsstandarden og anbefaler derfor yderligere foranstaltninger for at sikre behandlingens

[189] Cyberangreb mod danske virksomheder fordoblet på ét år. (2026, 4. Marts). *Via Ritzau*.
[190] *Cybersikkerhed: De vigtigste og største trusler*. (2022, 26. Januar). Europa-parlamentet.
[191] *Detaljeret statistik på anmeldelser om brud på persondatasikkerheden*. (2026, April). Datatilsynet.
[192] For definition se *Cyberkriminalitet i virtuelle verdener*. (2025, 31. Marts). Europa Kommissionen. & *Cybertruslen mod Danmark*. (2025, November) S. 6
[193] For definition se *Ransomware*. (s.d.)

sikkerheden.[194] Her ligger Datatilsynet altså vægt på at det forekommer som et krav at implementere faste procedurer løbende at vurdere foranstaltningerne.[195]

3.3.6 Behandlingens kontekst

Som beskrevet i afsnit 3.1.4 fremgår det at fortolkningen af ”passende” i høj grad afhænger af behandlingens karakter og sammenhænh. Det medfører at fastlæggesen af risikoen, skal foretages på baggrund af karakteren af personoplysningerne der behandles og de konkrete omstændigheder omkring behandlingen. Her er behandlingens karakter som beskrevet i afsnit 3.1.4, navnlig typen af personoplysninger, mens sammenhæng omfatter de organisatoriske rammer hvori behandlingen udføres. Sammen udgør de centrale kriterier for fastlæggelsen af ”passende”
Når det omhandler behandlingens karakter er det dermed vigtigt at fastlægge om de personoplysninger der behandles medfører en særlig risiko for den registreredes rettigheder og frihedsrettigheder. Som beskrevet i afsnit 3.1.4 vil behandlingen af følsomme oplysninger såsom helbredsoplysninger, typisk indebærer en højere risiko end behandlingen af mindre indgribende personoplysninger, som eksempelvis kontaktoplysninger, da konsekvenserne ved et sikkerhedsbrud, hvor der behandles personoplysninger af særligere karakter, kan være mere alvorlige. Ligeledes skal vurderingen af ”passende” ikke blot tage stilling til, hvilke personoplysninger der behandles, men samtidigt hvordan de anvendes da det kan medføre en nødvendig justering af risikovurderingen som set ved, behandlinger der inkluderer automatiseret behandling, der typisk vil øge risikoeksponeringen og dermed skærpe kravene til hvad der er ”passende”.[196]

Samtidig må *sammenhæng* forstås som de konkrete omstændigheder omkring behandlingen herunder, hvordan systemer anvendes i praksis og hvem der har adgang til oplysningerne. Ligeledes må det forstå af præambel 75 at personoplysninger kan skifte karakter på baggrund af behandlingens sammenhæng. Her kunne et eksempel være behandlingen af navn, som beskrevet ovenfor normalt ville medføre en lav risiko. Behandlingen kan skifte karakter i forbindelse med sammenhængen, hvis den fysiske person bag dette navn er under navnebeskyttelse, hvorfor dette kan medføre eksempelvis store sociale eller økonomiske konsekvenser for den registrerede, dette understreger ligeledes at behandlingens karakter, forekommer som være flydende set i relation til behandlingens sammenhæng.
Behandlingens karakter og sammhæng, illustreres yderligere i afgørelsen fra Datatilsynet omhandlende Kerteminde Kommune.[197] Datatilsynet lagde i denne forbindelse vægt på at, Kerteminde Kommune ikke

[194] Kerteminde Kommune får kritik for deres sikkerhedsprocedurer. (2024, 23. Februar)
[195] Ibid
[196] Afsnit 3.1.4
[197] Kerteminde Kommune får kritik for deres sikkerhedsprocedurer. (2024, 23. Februar)

havde etableret tilstrækkelige procedurer for logkontrol, men foretog kun kontrol ved konkret mistanke om misbrug. Her blev der lagt vægt på behandlingens karakter og omfang, hvilket resulterede i at Datatilsynet så sig nødsaget til at uddele kritik. Dette hænger sammen med GDPR-artikel 32 stk. 1 litra d, hvoraf det fremgår at en foranstaltning der kan være relevant at implementere er procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af implementerede foranstaltninger. Dette understreger ligeledes at sikkerhedsforanstaltninger ikke kan stå alene og dermed blot implementeres, men de skal ligeledes anvendes korrekt, hvorfor logkontrol ikke blev anset som værende ”passende” uden den regelmæssige kontrol. Det afgørende var ikke alene at der fandtes muligheder for kontrol, men at disse ikke blev anvendt, i et omfang der effektivt adresserer risikoen. Det understreges yderligere at sammenhængen også omfatter den måde en organisation strukturer og kontrollere adgangen til personoplysninger. Når der som i denne kritik fra Datatilsynet, forekommer mange medarbejdere der har adgang til personoplysninger, opstår der en risiko, som bør imødegås med løbende kontrolmekanismer, herunder løbende kontrol med logfiler. Fraværet af kontrolmekanismer kan i denne afgørelse, ikke anses som værende ”passende”, på baggrund af at behandlingen foregår i et miljø, hvor risikoen er forhøjet. Samlet viser afgørelsen at behandlingens karakter og sammenhæng bør vurderes i tæt sammenhæng. Behandlinger der indebærer en vis risiko, kan kræve yderligere foranstaltninger, hvis den foregår i et miljø, hvor risikoen øges, eksempelvis gennem brede adgangsrettigheder. Ligeledes kan en mindre risikofyldt behandling i en stramt kontrolleret miljø stille lavere krav til hvad der er ”passende”. Ud fra denne afgørelse må det altså forstås at ”passende” skal fastlægges efter en samlet vurdering, hvor både hvilke personoplysninger der behandles samt, hvordan behandlingen finder sted er afgørende for den samlede vurdering og dermed fastlæggelsen af ”passende” foranstaltninger. Datatilsynet illustrerer dermed i denne afgørelse at manglende forståelse af konteksten kan føre til at kravene ikke er opfyldt.

3.3.7 Standarder, praksis og dokumentation

”Passende” forekommer som klarlagt i afsnit 3.3.1 som en retlig standard, der både er fleksibel og åben. Der forekommer ikke umiddelbart en minimumsgrænse af ordlyden, ud over at en foranstaltning ikke umiddelbart vil være ”passende”, hvis hensynene i GDPR-artikel 32 er blevet overholdt. På baggrund af dette anvendes der i specialet retspraksis for at konkretisere GDPR-artikel 32’s indhold. Der anvendes afgørelser fra EU-Domstolen, samt nationale domstole, der spiller en central rolle i fastlæggelsen af standarden. Her fokuseres der på, hvilke krav der i praksis stilles til vurderingen og hvor grænserne for, hvad der er ”passende” går. Dette er med henblik på at forsøge at fastlægge en teoretisk minimumsgrænse på baggrund af retspraksis. Retspraksis anvendes for at tydeliggøre, hvordan hensynene i GDPR-artikel 32 stk. 1 vægtes i konkrete situationer. Ved domstolene vægtes behandlingens karakter, de organisatoriske

rammer og de konkrete hændelsesforløb, for at vurdere om foranstaltningerne har været "passende" til de identificerede risici.[198] Dette medfører ligeledes at forståelsen begrebet "passende" udfyldes gennem en række konkrete vurderinger, hvor der skabes præcedens for hvilke mangler eller tiltag der anses som værende "passende" eller ikke "passende.

Retspraksis forventes at kunne bidrage til at identificere nedre grænser for, hvad der ikke anses for værende "passende" foranstaltninger. Gennem domstolenes afgørelser kan det klarificeres, hvilke mangler der generelt fører til at en foranstaltning ikke anses for at være "passende", eksempelvis generel mangel af kontrolmekanismer eller utilstrækkelig håndtering af åbenlyse risici, og om disse selvstændigt kan fører til at kravene ikke er opfyldt. Dermed følger det at afgørelserne ikke kun bruges som en konkretisering af GDPR-artikel 32 stk. 1, men også som en afgræsning af, hvad der findes "passende".

På denne baggrund findes det nødvendigt at foretage en analyse af relevante domme, for at afdække hvordan passende organisatoriske og tekniske foranstaltninger anvendes og fortolkes i praksis. I de følgende underafsnit vil en række afgørelser fra EU-domstolen og nationale domstole blive analyseret, med det formål at afdække de kriterier og vurderinger der ligger til grund for afgørelsen og dermed belyse hvorvidt der kan fastsættes en teoretisk minimumsgrænse for hvornår organisatoriske og tekniske foranstaltninger er "passende".

3.3.7.1 Russmedia (C-492/23)

Russmedia dommen bringer et bidrag til fortolkningen af GDPR-artikel 32 og spørgsmålet om hvorvidt der kan fastlægges en teoretisk minimumsgrænse for "passende tekniske og organisatoriske foranstaltninger". Dommen udspringer sig af en situation, hvor der på en online platform drevet af Russmedia, af en ukendt tredjemand blev offentliggjort en annonce der indeholdte personoplysninger om en kvinde, herunder billeder og kontaktoplysninger der fejlagtigt fremstillede hende som udbyder af seksuelle ydelser. Offentliggørelsen skete uden den kvindelige parts samtykke og selvom annoncen blev fjernet mindre end en time efter forespørgslen om sletning fra kvinden, havde materialet hurtigt spredt sig til andre hjemmesider. Sagen rejste dermed spørgsmål til behandlingssikkerheden og de krav der følger hertil af GDPR-artikel 32. EU-domstolen fastslår at Russmedia forekommer som dataansvarlig, hvorfor de også bærer ansvaret for behandlingen efter GDPR-artikel 5 stk. 2, dette forekommer selvom at personoplysningerne er offentliggjort af brugerne selv. Heraf følger det således også at Russmedia er ansvarlig for datasikkerheden og må overholde de krav der stilles af GDPR-artikel 32 til behandlingssikkerheden. Domstolen fremhævede ligeledes at vurderingen af, hvilket sikkerhedsniveau der

[198] Dette uddybes ved følgende domsanalyser

er ”passende” skal ske under hensyntagen til behandlingens karakter, risiciene for den registrerede og alvoren af disse.[199] I den konkrete dom fastslog EUD at der var tale om oplysninger af særlig følsom karakter jf. GDPR-artikel 9 stk. 1.[200] Dette medføre ligeledes at der stilles et højere krav til sikkerhedsniveauet grundet risiciene forbundet med behandlingen af netop denne form for oplysninger.[201] Herefter foretog EUD en konkret vurdering af, hvilke foranstaltninger der kunne anses som ”passende”. EUD konkluderede at det ikke anses som værende ”passende” at Russmedia reagerede hurtigt på forsørgelsen om sletning.[202] Tværtimod imod fastlagde EUD at Russmedia er forpligtiget til at indføre foranstaltninger der sikre at den ulovlige offentliggørelse og for så vidt muligt at kopiering til andre hjemmesider slet ikke finder sted.[203] Dette indebærer at blandt andet at Russmedia skal sikre overholdesen af kravene der fremgår af GDPR-artikel 32 og dermed nedbringe risikoen ved at indføre passende kontrolmekanismer.[204] Samt at der skal træffes foranstaltninger der begrænser eller forhindre videre spredning af ulovlig offentliggjorte personoplysninger.[205]

Dommen illustrerer at vurderingen af ”passende tekniske og organisatoriske foranstaltninger”, ikke basere sig på om der formelt er implementeret visse tiltag, men om disse tiltag reelt imødegår risiciene. EUD fastlægger dermed en tilgang, hvor fokusset må anses for at være den effektive risikohåndtering, og manglen af denne i sig selv, vil lede til manglende overholdelse af kravene i GDPR-artikel 32. Heraf følger det at en foranstaltning ikke kan anses som værende ”passende”, hvis den ikke i praksis reducere risikoen for den registrerede rettigheder og frihedsrettigheder i forhold til den konkrete behandling.

Samtidig gør dommen det klart at det ikke er nok med en reaktiv tilgang til behandlingssikkerheden, hermed forstås at det ikke er nok hurtigt at kunne reagere på sikkerhedsbrud, men at der må tages en mere proaktiv tilgang til kravene, hvor at der skal der skal implementeres foranstaltninger der arbejder på at imødegå sådanne risici inden hændelsen indtræffer.

I relation til spørgsmålet om, hvorvidt der kan fastlægges en nedre grænse for ”passende tekniske og organisatoriske foranstaltninger”, kan der af dommen udledes nogle indikationer herom. EUD fastholder at vurderingen skal være konkret og vurderes ud fra den individuelle behandling. Ligeledes forekommer der indikationer omkring at fraværet af helt grundlæggende sikkerhedsforanstaltninger, vil medføre at kravet ikke er opfyldt. I den konkrete sag blev manglen på kontrol af brugere og indhold af oplysninger, inden offentliggørelsen anset for ikke at leve op til kravene for sikkerhedsniveauet.

[199] Russmedia: C-492/23. (2025, 2. December) Præmis 96
[200] Ibid Præmis 53
[201] Ibid Præmis 125
[202] Ibid Præmis 125
[203] Ibid Præmis 125 og 126
[204] Ibid Præmis 102 og 106
[205] Ibid Præmis 114

Dommen illustrerer at begrebet ”passende” er dynamisk og skal ses som en risikobaseret standard. På baggrund af denne dom kan det udledes en minimumsgrænse som består af, at de foranstaltninger der implementeres som minimum skal imødegå de risici der er identificeret og der dermed som minimum skal forekomme en form for risikostyring. Ved risici hvor foranstaltninger mangler eller ikke anvendes effektivt vil kravet om ”passende tekniske og organisatoriske foranstaltninger” ikke være opfyldt. Russmedia dommen bidrager således til at konkretisere kravene af GDPR-artikel 32 gennem praksis og understøtter altså forståelsen af at vurderingen skal foretages ved en risikobaseret tilgang og kravene stiger i relation til risikoen.

3.3.7.2 Másdi (C-169/23)

Másdi dommen bidrager yderligere til fortolkningen af GDPR-artikel 32’s krav og spørgsmålet om, hvorvidt der kan fastsættes en teoretisk minimumsgrænse for ”passende og organisatoriske foranstaltninger”. Dommen omhandler behandlingen af personoplysninger forbindelse med udstedelse af Covid-19 certifikater i Ungarn, hvor personoplysninger ikke blev indsamlet direkte fra den registrerede, men fra andre end den registrerede. Den centrale problemstilling var her, hvorvidt den dataansvarlige kan undtages for oplysningspligten efter GDPR-artikel 14 stk. 5, litra c, samt hvilke krav der stilles der stilles til ”passende foranstaltninger” der skal beskytte den registreredes rettigheder.[206]
EUD fastslår at undtagelsen i GDPR-artikel 14 stk. 5 litra c, kun finder anvendelse såfremt den nationale lovgivning der ligger hjemmel til behandling indeholder passende foranstaltninger der imødegår den registreredes legitime interesser.[207] Vurderingen af ”passende” er derfor i dette eksempel er derfor ikke alene knyttet til den dataansvarliges egne tiltag, men også det retlige grundlag for behandlingen. EUD understreger derfor, at de foranstaltninger der skal træffes skal sikre et beskyttelsesniveau, der følger de af GDPR-artikel 14 stk. 1-4 fastsatte krav.[208]
Dommen kobler ligeledes vurderingen af ”passende” foranstaltninger til kravene der følger af GDPR-artikel 32. Den fastslår at tilsynsmyndigheden i en klagesag ikke kun kan efterprøve spørgsmålet om, hvorvidt der foreligger lovhjemmel, men også om de foranstaltninger den dataansvarlige er pålagt at implementere herunder kravene der følger af GDPR-artikel 32 er passende for at imødegå beskyttelsen af de registreredes rettigheder.[209] Dermed integreres GDPR-artikel 32 som en del af vurderingen for samlede sikkerhedsniveau, selvom det i det konkrete spørgsmål omhandler undtagelsen til oplysningspligten. EUD fastlægger en

[206] Másdi: C-169/23. (2024, 28. November) Præmis 21-35
[207] Ibid Præmis 53
[208] Ibid Præmis 54 og 64
[209] Ibid Præmis 56 og 70

funktionel tilgang til begrebet ”passende” og uddyber hermed at ”passende” ikke er ydereligere konkretiseret i GDPR, men fastholder at vurderingen skal sikre effektiv beskyttelse af den registrerede.[210] Másdi dommen illustrerer dermed at vurderingen af ”passende” ikke foretages isoleret i forhold til GDPR-artikel 32, men må ses i et bredere sammenhæng, hvor også andre artikler og GDPR's overordnede formål tages med i vurderingen.[211] Særligt forekommer det at kravene til beskyttelsesniveauet der følger af GDPR-artikel 32, ikke kan fraviges gennem national ret. Selv hvor der forekommer en national undtagelse, skal selve behandlingen stadigvæk leve op til GDPR's krav om et ”passende” beskyttelsesniveau.
EUD fastlægger ikke konkrete foranstaltninger der skal implementeres, men understreger at beskyttelsesniveauet skal være ”mindst tilsvarende” det der følger af GDPR-artikel 14 stk. 1-4, herunder at sikre at den registrerede kan udøve kontrol med sine personoplysninger og udøve sine rettigheder i henhold til GDPR.[212] Deraf forekommer der tegn på en minimumsgrænse, hvor det ikke er nok blot at implementere foranstaltninger, men også at sikre at de registrerede kan udøve deres rettigheder.
Másdi dommen adskiller sig derfor fra Russmedia dommen ved ikke at give hvordan eksempler på hvordan fastsættelsen af skal finde sted ved foranstaltninger der skal implementeres ved behandlingsaktiviteter med høj risiko, men bidrager i stedet til forståelsen af at de registreredes rettigheder og frihedsrettigheder, også skal tænkes ind i vurderingen omkring, hvornår en foranstaltning er ”passende” og dermed i overensstemmelse med GDPR's overordnede formål.
Samlet viser Másdi dommen at ”passende” må forstås som en fleksibel standard, der viser tegn på at kunne have en nedre grænse. Denne grænse består af at foranstaltninger samlet skal sikre alle rettigheder de registrerede har, og at beskyttelsesniveauet ikke må være lavere end det der følger af GDPR som helhed.

3.3.7.3 Juris (C-741/21)

Juris dommen bringer et yderligere bidrag til fortolkningen af GDPR-artikel 32's krav til datasikkerhed og ansvar. Dette er på trods af at dommen overordnet vedrører GDPR-artikel 82 omhandlende erstatningsansvar for henholdsvis materiel og immateriel skade. Dommen udspringer af en situation, hvor en registreret part, søgte erstatning for behandlingen af hans personoplysninger, der angiveligt var i strid med GDPR.[213] Den centrale problemstilling forekommer som værende, hvorvidt en dataansvarlig kan undgå ansvar ved at henvise til, at overtrædelsen af GDPR's regler skyldes en medarbejders fejl og hvilke krav der i den forbindelse stilles til den dataansvarliges sikkerhedsniveau. EUD fastslog overtrædelsen af GDPR ikke i

[210] Másdi: C-169/23. (2024, 28. November) Præmis 64
[211] Ibid) Præmis 54
[212] Ibid Præmis 64
[213] Juris: C-741/21. (2024, 11. April) Præmis 17-27

sig selv ville være ansvarspådragende, men at der skal være sket en skade og at der skal forekomme kausalitet.[214] Dette forekommer som værende i overensstemmelse med tidligere retspraksis,[215] men det centrale for vurderingen af "passende" forekommer her ved den dataansvarliges ansvar, EUD fastslår at den dataansvarlige som udgangspunkt vurderes at være ansvarlige for behandlingen.[216] Det forekommer særligt vigtigt at EUD afviser at den dataansvarlige kun undgå ansvar, blot fordi det er en medarbejder der har handlet forkert,[217] dette understreger vigtigheden i awereness træning og kontrol af medarbejder, for at sikre at arbejdet bliver udført korrekt, men også for at kunne løfte bevisbyrden efterfølgende, såfremt der skulle forekomme ansvarspådragende adfærd. Dermed knyttes vurdering også direkte til GDPR-artikel 32, idet spørgsmålet om ansvar, ikke adskiller sig fra spørgsmålet om, hvorvidt der er implementeret foranstaltninger der imødegår sikkerhedsniveaut og de risici der ligger til grund herfor.
EUD tager i denne dom, nogle af de samme punkter op som ses i Russmedia, her ligges der vægt på at der kræves proaktive mekanismer der forebygger sikkerhedsbrud, samt at det understreges at interne instrukser ikke er tilstrækkelige, hvis de ikke håndhæves og kontrolleres, dette følger ligeledes af GDPR-artikel 32 stk. 4. Begge disse domme understreger at der i vurderingen af "passende" skal være fokus på om de implementerede foranstaltninger, rent faktisk imødegår de identificerede risici. Samtidig adskiller Juris dommen sig fra Másdi dommen, der fokuserer mere på at beskyttelsesniveauet skal vurderes på baggrund af GDPR som helhed. Her konkretisere Juris dommen dette ved at tydeliggøre at manglende intern kontrol, vil medføre mangel på overholdelse af reglerne. I relation til de centrale spørgsmål, bidrager Juris dommen yderligere til forståelsen af "passende" og dermed, hvorvidt der kan fastsættes en teoretisk minimumsgrænse. EUD opstiller ikke specifikke foranstaltninger der skal imødegå specifikke behandlingers risici, men det kan udledes at mangel på kontrolmekanismer i sig selv vil medføre at kravet om "passende" foranstaltninger ikke er opfyldt. Det er dermed ikke nok at have formelle instrukser, men der skal forekomme konkrete kontrolmekanismer der sikrer at instrukserne efterleves i praksis. Juris dommen understøtter dermed at kravene der følger af GDPR-artikel 32 ikke kan opfyldes blot ved dokumentation eller procedurer, men foranstaltningernes effekt skal ligeledes forekomme som en del af vurderingen. Dermed peger Juris dommen på at minimumsgrænsen kan forekomme ved at der som minimum kræves at den dataansvarlige implementerer effektive kontrolmekanismer til kontrol og identificering af risici ved behandlingen af personoplysninger. Samlet viser Juris dommen at "passende" skal fastlægges på baggrund af en vurdering i en organisations egentlige evne til imødegå risici effektivt, herunder både forebyggelsen og håndteringen. Juris dommen supplerer dermed også Russmedia og Másdi ved at fastslå at sikkerhed og

[214] Juris: C-741/21. (2024, 11. April) Præmis 34
[215] Ibid Præmis 34
[216] Ibid Præmis 46
[217] Ibid Præmis 24

ansvar skal vurderes sammen, og at manglende kontrolmekanismer kan føre til at foranstaltninger ikke er ”passende”. Derfor kan en minimumsgrænse muligvis identificeres ved at der som minimum skal forekomme kontrol og risikostyring, men samtidigt at der ikke fastsættes generelle krav til hvilke foranstaltninger der imødegår specifikke risici ved konkrete behandlingsaktiviteter.

3.3.7.4 Byrets dom, stadfæstet af Vestre Landsret 3-5399/2023

Den foreliggende dom fra byretten, analyseres for at bringe et nationalt bidrag til fortolkningen af GDPR-artikel 32 og dets krav til vurderingen af ”passende”. Dommen er efterfølgende blevet stadfæstet ved landsretten, dog med en bødenedsættelse.[218] Stadfæstelsen medfører ligeledes at dommen tillægges større retlig værdi. Dette er særligt relevant for fortolkningen af ”passende” og GDPR-artikel 32 da der forekommer en vurdering af, hvornår sikkerhedsniveauet ikke er ”passende” fra to instanser. Sagen vedrører behandlingen af personoplysninger i en offentlig myndighed, hvor der uberettiget blev videregivet personoplysninger om patienter.[219] Der var truffet sikkerhedsforanstaltninger i form af loginsystem, samt kontroller med sletning af brugeres tilgang til systemet. Dog kunne der ved at ændre i URL-adressen tilgås andres oplysninger. Det bliver forklaret af IT-direktøren i den offentlige myndighed, at dette havde været muligt at imødegå.[220] Personoplysninger der kunne tilgås indebar både følsomme oplysninger efter GDPR-artikel 9, herunder helbredsoplysninger, og i nogle tilfælde personnumre efter GDPR-artikel 87.[221]
Karakteren af disse oplysninger forøger risikoen og er dermed med til at stille større krav til sikkerhedsniveauet. Ligeledes må der på baggrund af behandlingens karakter forstås at selvom der forekommer relativt begrænset mængde fejl, og at der findes andre foranstaltninger, kan det medføre konsekvenser for den registrerede og må dermed indgå i vurderingen af hvad der er ”passende”.
Det centrale i sagen forekommer derfor som værende at den offentlige myndighed havde truffet foranstaltninger for at beskytte personoplysningerne, men at disse ikke blev anvendt korrekt. Fejlene udsprang derfor af manglen på procedurer, utilstrækkelig kontrol og manglende sikring af korrekt anvendelse. Dette understreger at vurderingen af, hvornår foranstaltninger er ”passende” ikke beror sig på selve den tekniske eller organisatoriske løsning i sig selv, men hvorvidt den fungerer i praksis og lever op til dets formål.
Stadfæstelsen fra landsretten ændrer ikke denne vurdering fra byretten og bekræfter den derimod. Derved ligges der ved to instanser vægt på at det er effektiviteten der skal lægges vægt på frem for egentlig

[218] Stadfæstelsen: 192/26. (2026, 23. Marts)
[219] Byrets dom : 5399/2023. (2024, 23. December) S. 2
[220] Ibid S. 2
[221] Ibid S. 13

implementering.[222] Det skal dog nævnes at den offentlige myndighed frifindes i landsretten for forhold to, her vurderes deres tekniske samt, deres organisatoriske foranstaltninger i form af webaktører og generel orientering af medarbejdere, som værende værende ”passende”, dette skete efter en konkret afvejning af risici,[223] dette kan bidrage til forståelsen af hvilke konkrete foranstaltninger der bør træffes i forhold til denne behandling og muligvis lignende.
Derfor antydes det på baggrund af denne dom samt, de tre ovenstående EU-domme at det ikke er nok at have systemer og tekniske muligheder, men at der skal forekomme organisatoriske procedurer og kontroller der sikrer den korrekte anvendelse. Det understreges ligeledes at manglen på procedurer og kontrol i sig selv kan medføre at kravet til ”passende” ikke er opfyldt.

Af denne dom kan der derfor udledes følgende minimum, om at der skal forekomme effektiv kontrol med behandlingen, der skal være procedurer der sikrer korrekt håndtering og der skal forekomme sammenhæng mellem tekniske muligheder og den faktiske anvendelse. Dette minimum udledes af den samlede baggrund for vurderingen der ikke beror sig på konkrete foranstaltninger og at fraværet af dette minimum ikke blev anset som værende tilstrækkeligt og resulterede i at den samlede mængde af foranstaltninger ikke blev vurderet til at være ”passende”.

Sammenholdt med Russmedia-dommen kan der antydes den samme grundstruktur, her kravet om forebyggelse. Altså en mere proaktiv tilgang fremfor en reaktiv. Her adskiller dommene sig ved at Russmedia tager udgangspunkt i en digitalplatform, hvorimod denne dom er for en offentlig myndighed. Dog peger begge domme på at manglende kontrol i sig selv kan være afgørende for vurderingen af om foranstaltninger er ”passende”.

Sammenholdt med Másdi-dommen, fungere denne dom til at vise, hvordan formålene bag beskyttelsen skal implementeres i praksis. Másdi-dommen opstiller dermed formålene med beskyttelsen, hvor denne dom konkretiserer, hvad beskyttelsen bør indeholde.

Sammenholdt med Juris-dommen, viser de begge at medarbejder fejl, både på et mere organisatorisk plan og i selve behandlingen, ikke fritager den dataansvarlige for ansvar, dette udledes af at fejl i praksis, kan være et tegn på at der ikke forekommer ”passende organisatoriske og tekniske foranstaltninger”.

[222] Stadfæstelsen: 192/26. (2026, 23. Marts) S. 17
[223] Ibid S. 18

Stadfæstelsen af dommen styrker dens retlige værdi, dommen bekræfter at ”passende” fungerer som en retlig standard, hvor det afgørende er, hvorvidt organisationen hermed den dataansvarlige er i stand til at forebygge og kontrollere behandlingen af personoplysninger og identificere risici forbundet hermed.

3.3.8 Dynamik, løbende vurdering og muligheden for en minimumsgrænse

”Passende” må ud fra ovenstående fortolkning og analyse forstås som værende et dynamisk begreb, der må forstås i sammenhæng med de øvrige hensyn der fremgår af GDPR artikel 32. Vurderingen af, hvad der er ”passende” er ikke en engangsøvelse men indebærer et løbende krav om at sikre at behandlingen af personoplysninger forsat lever op til det krævede beskyttelsesniveau. Dette indebærer at sikkerheden skal tilpasses i takt med det aktuelle tekniske niveau, udviklingen i trusselsbilledet, implementeringsmuligheder og behandlingens karakter, sammenhæng og omfang og formål. Samtidigt fremgår det af både teori og praksis, at vurderingen af ”passende” ikke alene knytter sig til eksterne ændringer som implementeringsomkostninger eller det aktuelle tekniske niveau, men i høj grad også den interne funktion af de valgte løsninger. Det afgørende er derfor ikke om den dataansvarlige løbende opdatere deres systemer, men om der fortageres løbende kontrol af, hvorvidt foranstaltningerne fungerer i praksis og effektivt reducere de identificerede risici. Manglende løbende kontrol, evaluering og opfølgning vil dermed kunne indebære at et sikkerhedsniveau der på implementeringstidspunktet var ”passende”, i fremtiden ikke vil leve op til kravene.

”passende” må samlet forstås som en dynamisk og risikobaseret standard der tager udgangspunkt i en konkret vurdering, hvor der er flere kriterier der skal overvejes. Begrebet kan ikke reduceres til faste krav eller standardiserede løsninger. Vurderingen skal derimod tage udgangspunkt i, hvorvidt de valgte foranstaltninger er ”passende” i forhold til det sikkerhedsniveau, der medfølger af de identificerede risici.

Spørgsmålet om hvorvidt der kan fastlægges en teoretisk minimumsgrænse for ”passende tekniske og organisatoriske foranstaltninger”, må derfor vurderes af den samlede tilgang. På den ene side taler GDPR artikel 32’s fleksible og risikobaserede tilgang imod at en sådan minimumsgrænse kan fastlægges. På den anden side viser både de opstillede kriterier der fremgår af GDPR artikel 32 og den gennemgåede praksis at vurderingen ikke er ubegrænset. Dette forstås ved at det ses i praksis at visse elementer skal være tilstede for overhovedet at kunne opfylde kravet. Disse elementer er ikke defineret som særlige teknologier eller løsninger, men til et grundlæggende krav om at sikkerheden skal være effektiv mod de identificerede risici. Deraf udledes der at en minimumsgrænse hvor manglen på grundlæggende kontrol, procedurer og effektiv

anvendelse af eksisterende foranstaltninger i sig selv vil indebære at sikkerhedsniveauet ikke anses som værende "passende". Minimumsgrænsen må derfor forstås at kunne være krav om at den dataansvarlige som minimum skal kunne styre, kontrollere og tilpasse behandlingen af personoplysninger i sammenhæng med de identificerede risici.

Kapitel 4 Økonomiske betragtninger og usikkerhed om, hvad er nok?

Kapitel 4 har til formål at konkretisere de økonomiske betragtningerne og fastlægge, hvor de konkrete usikkerheder forekommer. Dette er med henblik på at vurdere om en mere konkret minimumsgrænse end den af kapitel 3 identificerede minimumsgrænse, kan være et effektivt redskab til at hjælpe de dataansvarlige med deres usikkerheder, uden at gå på kompromis med de registreredes rettigheder. Kapitel 4 slutter ligeledes af med en samlet konklusion på specialets overordnede spørgsmål.

4.1 Økonomiske betragtninger

Økonomiske hensyn spiller en central rolle i vurderingen af, hvilke foranstaltninger der skal implementeres og om de forekommer som værende "passende", dette udfolder sig i GDPR-artikel 32 stk. 1, hvor implementeringsomkostningerne, som analyseret og fortolket i afsnit 3.1.3 er et af de konkrete kriterier der skal tages hensyn til. Dette indebærer at den dataansvarlige må foretage en konkret afvejning mellem omkostningerne ved implementeringen af foranstaltninger og de risici behandlingen indebærer for den registrerede. En sådan afvejning forekommer dog i praksis som en udfordring for den dataansvarlige, da det vurderes nemmere at fastlægge omkostninger, end det er at afveje risici.[224] Dette kan i praksis medføre en underimplementering af nødvendige foranstaltninger og en undervurdering behovet for sikkerhedstiltag fra den dataansvarliges side.[225] Deraf kan der forekomme en skævridning i den samlede vurdering af hvad der er "passende", såfremt implementeringsomkostningerne tillægges en uforholdsmæssig stor værdi.

Problematikken omkring vurderingen af "passende" i relation til implementeringsomkostningerne, forstærkes af at omkostninger ikke kun afgrænser sig til at være omkostningen for selve implementeringen, men også den løbende omkostningen ved vedligeholdelse og oplæring af personale hertil.[226] De dataansvarlige organisationer, skal derfor ikke kun investere i teknologier og systemer, men ligeledes struktur, kontroller, oplæring og dokumentation, hvilket gør overholdesen af beskyttelsesniveauet der

[224] Selzer, A., Woods, D. & Böhme, R. (2021) S. 463
[225] Ibid S. 463
[226] Ibid S. 456

fremgår af GDPR til et ressourcekrævende og vedvarende forløb. De ikke udtømmende krav der forekommer som komplekse og vanskelige at implementere i praksis hos den dataansvarlige,[227] hvilket understreges af at dataansvarlige har en række bekymringer, herunder omkostninger, kompleksitet og manglende klarhed om kravene.[228] Danske Industri understreger ligeledes at GDPR medfører betydelige administrative byrder og ressourceforbrug, som i nogle tilfælde ikke vurderes som værende proportionelle med de konkrete risici forbundet med behandlingen af personoplysninger.[229]

Det fremgår samtidig af økonomiske analyser at GDPR's kompleksitet kan have bredere økonomiske konsekvenser end blot dem den dataansvarlige organisation møder[230]. Konsekvenserne kan også påvirke den bredere samfundsøkonomi, hvor kompleksiteten kan have negative konsekvenser for innovationen, konkurrenceevnen og effektivt ressourceforbrug. [231] Dermed understreges det at de økonomiske konsekvenser der følger af GDPR er væsentlige og må indgå i den samlede forståelse, om en konkret minimumsgrænse vil være fordelagtig.

Når der ikke forekommer konkrete minimumsstandarder overlades vurderingen til den dataansvarlige, der skal afveje mellem økonomiske hensyn og risikovurderinger. Dette øger behovet hos den enkelte dataansvarlige for både juridisk og teknisk hjælp, og kan føre til underimplementering eller overimplementering.[232] Begge dele medfører derfor ineffektiv brug af ressourcer og kan svække efterlevelsen af GDPR som helhed.

Der kan derfor argumenteres for at det fra lovgivers side kan identificeres minimumskrav, [233] hvilket kan hjælpe den dataansvarlige med bedre ressourceallokering. Minimumskrav vil ligeledes skabe et udgangspunkt for hvad der forventes og dermed reducere usikkerheden i vurderingen af "passende". Samtidigt kan minimumskrav modvirke at økonomiske hensyn får en uforholdsmæssig vægt i vurderingen og dermed understøtte et mere ensartet og effektivt beskyttelsesniveau. Her er det dog værd at nævne at sådan en minimumsgrænse skal tage forbehold for blandt andet brancher og størrelse af organisation, da det ellers kan have den modsatte effekt hvis uforholdsmæssige krav bliver fastlagt, for organisationer der ikke har ressourcerne til at kunne imødekomme dem.

[227] Smirnova, Y. & Travieso-Morales, V. (2025, 1. August)
[228] *Top five concerns with GDPR compliance*. (s.d.)
[229] Hansen, U. (2025, 02. Juli)
[230] Hobson, A. & Calder, A. (2018, 25. Maj)
[231] Ibid
[232] Hansen, U. (2025, 02. Juli)
[233] Her menes der lovgiver på EU plan, for at sikre ensformig anvendelse på tværs af medlemslandene

Det er dog stadigvæk væsentligt at sådanne minimumskrav ikke erstatter den risikobaserede tilgang, men fungere som et supplement den dataansvarlige kan læne sig op af. GDPR-artikel 32 forudsætter at der forekommer en konkret vurdering, hvor flere hensyn skal tages, herunder implementeringsomkostningerne, men også behandlings karakter og det aktuelle tekniske niveau m.m. Minimumskravet bør derfor blot fastlægge et grundniveau, som i alle tilfælde skal være opfyld, hvor den konkrete vurdering forsat skal sikre at sikkerheden er tilpasset den konkrete behandlingsaktivitet og de identificerede risici der følger med. Dog vil en sådan løsning heller ikke komme uden problemer og der vil følge et spørgsmål heraf om, hvorvidt den dataansvarlige blot vil læne sig op af minimumskravet, hvilket potentielt kan medføre en nedgradering i det samlede beskyttelsesniveau.

Samlet viser de økonomiske betragtninger at implementeringsomkostningerne både forekommer som en væsentlig men også problematisk del af vurderingen af "passende" efter GDPR-artikel 32 stk. 1. Implementeringsomkostninger kan i praksis besværliggøre efterlevelsen af kravene, særligt i lyset af de komplekse krav og de betydelige ressourcer det er fastlagt at overholdelse af kravene kræver. Samtidig antydes der at identificeringen af en minimumsgrænse, som der ses tegn af i praksis kan bidrage til at reducere kompleksiteten, øge forudsigeligheden og understøtte en mere effektiv implementering af sikkerhedsforanstaltninger, samtidig med at, der ikke over- eller underimplementeres grundet hensyn der ikke følger kravene opstillet af GDPR artikel 32.

4.2 Udfordringer og usikkerhed om hvad der er nok?

Usikkereden i fastsættelsen af "passende tekniske og organisatoriske foranstaltninger" beror sig ikke alene på implementeringsomkostningerne. Men udfolder sig generelt gennem GDPR-artikel 32's åbne formulering, hvor særligt hensynene der følger af stk. 1 gør fastsættelsen kompleks, men også de supplerende elementer der følger af GDPR artikel 32 stk. 2-4. GDPR-artikel 32 opstiller en række hensyn, herunder behandlingens karakter, omfang, sammenhæng og formål, det aktuelle tekniske niveau og risici for den registreredes rettigheder, der følger ikke af artiklen en klar prioritering af disse, hvorfor vurderingen overlades til den dataansvarlige, som står tilbage med et betydeligt fortolkningsspørgsmål.

Risikokriteriet der fremgår af GDPR-artikel 32 stk. 2 bidrager til usikkerheden, heraf fremgår det som beskrevet i kapitel 3 at der både skal tages hensyn til risikoens sandsynlighed og konsekvensen, dog forekommer der ikke en nærmere beskrivelse af, hvordan disse to elementer skal vurderes. Det fremgår af litteratur, samt praksis at vurderingen af behandlingsaktivitetens risiko er præget af usikkerhed, da det

forekommer som den dataansvarliges ansvar at foretage et skøn, hvilket gør det vanskeligt for organisationer at identificere, hvornår de reelt lever op til kravene.[234] Dermed bliver risikovurderingen ikke blot et teknisk skøn om, hvilke foranstaltninger der er "passende" men en samlet vurdering og analyse af samtlige hensyn, som kan variere betydeligt mellem forskellige dataansvarlige.

Usikkerheden ved den samlede vurdering forstærkes ligeledes af kriteriet om "behandlingens karakter, omfang, sammenhæng og formål". Disse elementer er i sig selv komplekse, som beskrevet i afsnit 3.1.4. Usikkerheden opstår i manglende afklaringen af afvejningen af disse hensyn, eksempelvis kan en behandlingsaktivitet have indgribende formål, men ske i et relativt begrænset omfang eller være meget omfattende men ske ved brug af relativt harmløse personoplysninger.[235] GDPR-artikel 32 stk. 1 præcisere ikke nærmere, hvordan disse hensyn skal vægtes. Det fremgår dog af Russmedia dommen, at vurderingen skal ske som helhed, så selvom at navn og billede i sig selv fremgår som relativt "harmløse" personoplysninger, kan de i nogle sammenhæng kræve strengere krav til sikkerheden. Dette medfører dog at den dataansvarlige skal vurdere om der ved alle behandlinger af personoplysninger forekommer situationer, der ændrer konteksten og dermed stillere højere krav til beskyttelsesniveauet. Dermed præciseres kravene til vurderingen en smule, men antages ikke for at løfte den egentlige byrde hos den dataansvarlige, da det stadigvæk er op til deres organisation at identificere dette og være klar over at sådanne nogle forskelle kan forekomme.

Kravet om at tage stilling til "det aktuelle tekniske niveau" kan bidrage til usikkerheden. Dette krav er som anført i afsnit 3.1.2 dynamisk og afhænger af den generelle teknologiske udvikling. Der stilles krav til at der løbende foretages vurderingerne af effekten, for at sikre at en foranstaltning der på et tidspunkt, ikke bliver utilstrækkeligt, grundet den teknologiske udvikling. Dette kan medføre tvivl hos den dataansvarlige og kan medføre at dataansvarlige skal have rådgivning for blot at implementere simple løsninger.[236]

GDPR-artikel 32 stk. 3 og 4 bidrager yderligere til den kompleksitet den dataansvarlige oplever ved fastsættelsen af "passende tekniske og organisatoriske foranstaltninger". De certificeringsordninger der følger af GDPR-artikel 32 stk. 3, kan fungere som en vejledning om, hvorvidt kravene er opfyldt. Dog som det også beskrives nærmere i kapitel 3, fungere disse blot som en vejledning om, hvorvidt kravene er opfyldt og kan altså ikke stå alene for at påvise overholdelse af kravene. Det samme kan nævnes for adfærdskodekser der ligeledes blot er et element i overholdelsen, af de samlede krav i GDPR-artikel 32. Det

[234] *Top five concerns with GDPR compliance*. (s.d.)
[235] Ibid
[236] Hansen, U. (2025, 02. Juli)

fremgår ligeledes af GDPR-artikel 32 stk. 4 og som yderligere beskrevet i afsnit 3.4 at der stilles krav om at den dataansvarlige skal sikre at personer i organisationen der håndterer personoplysninger kun behandler disse på instruks fra den dataansvarlige. Dette understreger dermed den betydning de organisatoriske forhold har og dermed også de organisatoriske foranstaltninger, men stiller ikke ydereligere krav til, hvordan dette skal implementeres i praksis.

De samlede elementer i GDPR-artikel 32 opstiller krav til vurderingen der både fremstår som fleksible og komplekse. Fleksibiliteten forekommer som værende tilsigtet, men medfører dermed også praktiske udfordringer.[237] De dataansvarlige organisationer oplever udfordringer med at omsætte kravene til konkrete handlinger,[238] blandt andet fordi at reglerne er komplekse og vejledninger ofte opleves som utilstrækkelige eller at være for generel.[239] Usikkerheden stammer ligeledes fra de vage formuleringer og sammenhængen med andre lovgivninger gør det uklart for den dataansvarlige hvordan det konkret skal implementeres og håndteres.[240] Det antydes samtidig at implementeringen ikke længere følger det overordnet formål og dermed skader den overordnede konkurrenceevne.[241] Yderligere ses det at mange dataansvarlige har svært ved at konkretisere kravene der fremgår af GDPR herunder, hvornår beskyttelsesniveauet er ”passende”.[242] Dette indikere at en grundlæggende udfordring ved GDPR-artikel 32 ikke er blot er, hvilke hensyn der skal tages men også, hvordan det skal implementeres i praksis. Her forekommer problemstillingen at den dataansvarlige selv må definere, hvad der er nok, men samtidig efterfølgende udsættes for kontrol af de nationale tilsynsmyndigheder.

Samlet viser det sig at usikkerheden omkring GDPR-artikel 32 ikke alene skyldes uklare begreber, men samspillet mellem flere åbne og dynamiske hensyn. Vurderingen af, hvornår en foranstaltning forekommer som ”passende”, udfolder sig derfor som en helhedsvurdering, hvor det ikke er de enkelte faktorer der er afgørende, men at faktorerne må afvejes i sammenhæng. Usikkerheden forekommer ikke som en tilfældighed, men et ønske fra lovgiver om at få de dataansvarlige til at tage stilling til behandlingen af personoplysninger, og ikke blot på grund af uklar regulering. Netop denne usikkerhed danner baggrund for specialets centrale spørgsmål om det på trods af fleksibiliteten i GDPR-artikel 32, er muligt at definere en nedre grænse for, hvornår beskyttelsesniveauet er ”passende”.

[237] Hansen, U. (2025, 02. Juli)
[238] Ibid
[239] Smirnova, Y. & Travieso-Morales, V. (2025, 1. August)
[240] Brinnen, M. & Westman, D. (2019, December) S. 1
[241] Hansen, U. (2025, 02. Juli)
[242] Smirnova, Y. & Travieso-Morales, V. (2025, 1. August)

4.3 Minimumsgrænsen

GDPR-artikel 32's opbygning viser at visse forudsætninger indikerer at der kan fastsættes en nedre grænse. Ordlyden i GDPR-artikel 32 stk. 1 indikere tilstedeværelsen af visse obligatoriske vurderingselementer, hvoraf det forstås af ordlydsfortolkningen at sikkerhedsniveauet ikke kan vurderes som "passende" hvis der ikke er blevet taget hensyn til de af GDPR-artikel 32 stk. 1, 2 & 4 nævnte kriterier. Deraf udfoldes den teoretiske minimumsgrænse som fastlagt i kapitel 3 som være baseret på *grundlæggende kontrol, procedurer og effektiv anvendelse af foranstaltninger*, hvor fraværet af disse, i sig selv medføre at kravene til "passende tekniske og organisatoriske foranstaltninger" ikke er opfyldt.
Dette er dog kun et tegn på at der kan findes en minimumstandard, da uden foranstaltninger til at mitigere disse risici vil sikkerhedsniveauet, ikke kunne vurderes som værende "passende". Derfor løser den som udgangspunkt, ikke usikkerheden for de dataansvarlige om, hvornår en foranstaltning er "passende" i teorien.
Derfor må behovet for en tydeligere defineret minimumsgrænse fra lovgivers side afdækkes, denne vurdering tager udgangspunkt i, hvorvidt en klart defineret minimumsgrænse kan hjælpe både den enkelte dataansvarliges og samfundets gennerelle interesser, uden at gå på kompromis med GDPR's overordnede formål om at beskytte fysiske personers rettigheder og frihedsrettigheder, herunder navnlig deres personoplysninger.

Deraf kommer der en afvejning af fordelene og ulemperne ved en minimumsgrænse, disse baseres på de usikkerheder der er identificeret i specialets forgående afsnit. Effekten af fordelene og ulemper baseres på, hvordan de kan have indflydelse på netop de identificerede usikkerheder.

4.3.1 Fordele ved minimumsgrænsen

Der forekommer et ønske om at de administrative byrder der følger af GDPR nedjusteres,[243] deraf kommer spørgsmålet om dette kan løses ved at indføre et sæt minimumskrav til beskyttelsesniveauet der konkret fastsætter rammerne for behandlingen.

En konkret fordel ved en tydligt defineret minimumsgrænse, er at den kan skabe øget klarhed og bedre forudselighed for den dataansvarlige. Som det fremgår indebærer GDPR-artikel 32 flere åbne kriterier, herunder behandlingens karakter, det aktuelle tekniske niveau og risikohåndteringen. Denne fleksibilitet

[243] Hansen, U. (2025, 02. Juli).

skaber for den dataansvarlige usikkerhed om, hvornår kravene er opfyldt. En minimumsstandard, vil kunne reducere usikkerheden, da den dataansvarlige i højere grad konkret vil kunne fastlægge bundniveauet for sikkerhedsniveauet, inden der foretages yderligere risikobaseret tilpasninger.

En anden fordel der forekommer ved fastlæggelsen af en minimumsgrænse, kan være en mere ensartet anvendelse af GDPR. Uden en minimumsgrænse forekommer der en risiko for at "passende" fortolkes anderledes på tværs af organisationer og brancher, hvilket kan medføre forskellighed i beskyttelsen af den registreredes personoplysninger og dermed deres rettigheder og frihedsrettigheder. En fastlæggelse af en mere konkret minimumsgrænse vil dermed medføre at sikkerhedsniveauet på tværs af organisationer og brancher som minimum vil have det samme beskyttelsesnivau, uden at de skal investere uproportionelt meget i at fastlægge kravene. Det vil ligeledes fører til nemmere kontrol grundet de af minimumskravets tiltag der skal implementeres.

Dommene tydeliggør ligeledes at der i forvejen arbejdes med en form for minimumsgrænse, heraf fremgår det som nævnt ovenfor at manglen på *grundlæggende kontrol, procedurer og effektiv anvendelse af foranstaltninger* i sig selv vil medføre at kravene i GDPR-artikel 32 ikke er overholdt. Den er ikke eksplicit defineret af ordlyden, dog vil en mere konkret definering af dette være med til at skabe større gennemsigtighed og styrke sammenhængen mellem teori og praksis.

Det forekommer af analysen at der fra domstolene også forekommer uklarhed omkring, hvad et "passende" sikkerhedsniveau er, hvilket ses i bødenedsættelsen i landsretten, selvom at sikkerhedsniveaut var blevet vurderet ikke "passende" ved byretten. Dermed vil en konkretisering af kravene, kunne medføre en mere effektiv kontrol, hvor der klarer vil kunne defineres, hvornår der har været en overtrædelse af loven. Dermed kan minimumsgrænsen ligeledes være med til at styrke håndhævelsen af kravene, uden at kravene om en konkret vurdering elimineres.

Samlet set indikere det at mere konkret defineret minimumsgrænse kan have en række fordele. Hvor klarhed, forudsigelighed og anvendelsen i praksis forekommer som centrale punkter. Det bliver dermed nemmere at overholde kravene for de dataansvarlige, samt det bliver nemmere at håndhæve loven for myndighederne og domstolene. Der forekommer allerede tegn på en minimumsgrænse, hvorfor det ikke nødvendigvis ses som en afgrænsning af kravene, men et middel til at styrke dens funktion og anvendelse i praksis.

4.3.2 Ulemper ved minimumsgrænsen

På trods af at der er indikationer af en minimumsgrænse og at fastlæggelsen af en mere konkret defineret minimumsgrænse kommer med sine fordele, forekommer der også en række betænkeligheder. Disse knytter sig hovedsageligt til GDPR-artikel 32's struktur, hvor fleksibilitet, risikovurderingen og teknologineutralitet forekommer som nogle hovedelementerne, hvor fraværet af faste krav vurderes til at være et bevist valg ved udarbejdelsen af loven.

En ulempe ved fastlæggelsen af minimumsgrænsen, er risikoen for at den fleksibilitet der er ønsket fra lovgivers side minimeres. GDPR-artikel 32 er udformet således at sikkerhedsniveaut skal tilpasses konkrete behandlingsaktiviteter herunder, dens karakter, omfang, sammenhæng og formål. Hvis der opstilles konkrete minimumskrav, er der risiko for at kravene standardiseres i højere grad end ønsket, hvilket kan medføre at fokus flyttes, mod blot at opfylde de fastlagte minimumskrav og at risikovurderingen får mindre vægt tillagt sig, hvilket overordnet kan medføre et potentielt lavere sikkerhedsniveau.

En anden ulempe konkrete minimumskrav kan medføre, er vanskeligheden i opretholdelse af sikkerheden i forhold til det akutelle tekniske niveau. Det følger af kriteriet om at tage hensyn til det aktuelle tekniske niveau at sikkerheden skal opretholdes i forhold til den tekniske udvikling. Faste minimumskrav risikerer derfor at blive forældet og dermed være utilstrækkelige for at opretholde det ønskede beskyttelsesniveau, [244]hvis de ikke opdateres jævnligt. Dette kan derfor medføre at minimumskravene mister sin relevans og beskyttelsesniveauet undermineres og det gennerelle formål med GDPR derfor forsvinder.

Det forekommer ligeledes som en ulempe at en sådan minimumsgrænse kan være vanskelig at fastlægge, hvor den både er generel og meningsfuld. GDPR-artikel 32 skal anvendes bredt, på både risikofyldte og mindre risikofyldte behandlingsaktiviteter. Et minimumskrav der er tilstrækkeligt i et tilfælde, er det ikke nødvendigvis i en anden kontekst. Dermed risikeres det at der fastsættes minimumskrav der enten ikke er fyldestgørende for dets formål eller for højt, hvilket kan fører til uforholdsmæssige byrder for de dataansvarlige. Heraf formodes det at den grundlæggende udfordring ved fastlæggelsen af en minimumsgrænse er at ved forsøget på at fastsætte en nedre grænse, i ellers kontekstafhængig regulering, vil medføre det modsatte af, hvad der er ønsket og dermed sænke det generelle beskyttelsesniveau.

[244] The trends reshaping cybersecurity. (2026, 12. Januar)

Samlet indikerer det at selvom en minimumsgrænse kommer med væsentlige fordele, medfølger der ligeledes ulemper. Minimumsgrænsen kan i værste fald underminere fleksibiliteten og være vanskelig at tilpasse udviklingen på området. Der kan ligeledes opstå nye fortolkningsproblemer og stille uforholdsmæssige krav til de dataansvarlige. Dermed understreges det at spørgsmålet om en minimumsgrænse ikke alene beror sig på ønsket om klarhed, men også balancen mellem forudsigelighed og den ønskede fleksibilitet der er på området og at en mere konkret minimumsgrænse overordnet ikke vil være fordelagtig, da hensynet ikke bør være at det er nemt for den dataansvarlige, men bør være GDPR overordnede formål om beskyttelse af rettigheder og frihedsrettigheder, her navnlig personoplysninger som det følger af GDPR artikel 1 stk. 2.

4.4 Konklusion

Konklusionen på specialets centrale spørgsmål om, ”hvorvidt der kan fastsættes en teoretisk minimumsgrænse for passende tekniske og organisatoriske foranstaltninger efter GDPR-artikel 32?”, tager udgangspunkt i GDPR-artikel 32’s karakter, hvor det af ordlyden og praksis forstås som værende en både fleksibel og risikobaseret standard. Analysen har vist, at GDPR-artikel 32 ikke opstiller faste krav eller bidrager med en udtømmende liste af tiltag for det samlede beskyttelsesniveau. Forudsætning er derimod at en konkret helhedsvurdering, hvor flere hensyn må medtages, disse omfatter navnlig behandlingens karakter, omfang, sammenhæng og formål, det aktuelle tekniske niveau og risici for de registreredes rettigheder og frihedsrettigheder. Denne struktur understøttes yderligere af præamblerne, der ligeledes understreger nødvendigheden af en risikobaseret tilgang og løbende vurdering af beskyttelsesniveauet.

Ordlydsfortolkningen indikerer at denne fleksibilitet ikke er ubegrænset. GDPR-artikel 32 stk. 1 opstiller først og fremmest en række kriterier der skal tages hensyn til. Ligeledes fremgår det GDPR-artikel 32 stk. 2 at der forekommer et krav om at der tages hensyn til de risici behandlingen måtte involvere. Til sidst fremgår det af GDPR-artikel 32 stk. 4 at der skal forekomme organisatorisk kontrol, hvor det skal sikres at enhver fysisk person der udfører arbejde for den dataansvarlige gør sådan efter instruks. Sammenholdt med formuleringen om ”passende tekniske og organisatoriske foranstaltninger”, forekommer der indikationer om at der forekommer en nedre grænse for, hvad der er ”passende”. Af ordlyden må denne minimumsgrænse, forstås som værende manglen på hensyntagen til de af ordlyden fremlagte krav.

Denne fortolkning konkretiseres af den praksis der er analyseret igennem specialet. Af praksis fremgår det at vurderingen af ”passende” ikke afgøres af, hvorvidt der er implementeret formelle foranstaltninger, men om disse reelt er egnede til at imødegå de identificerede risici. Minimumsgrænsen der følger af ordlyden,

kan dermed konkretiseres på baggrund af den praksis der analyseres i specialet, og fastslås som værende fokuseret på manglen på kontrol, procedurer og effektiv anvendelse af eksisterende foranstaltninger. Som minimumsgrænse gælder dette uanset om der er implementeret foranstaltninger. Praksis indikerer dermed at en tilgang, hvor det afgørende er effekten af de valgte foranstaltninger og ikke den formelle implementering. Af praksis forstås det derfor at der opereres med en teoretisk minimumsstandard, hvor manglen på kontrol, procedurer og effektiv anvendelse af eksisterende løsninger ikke accepteres.

Analysen har imidlertid også belyst at vurderingen af de enkelte kriterier i GDPR-artikel 32 er kompleks og præget af usikkerhed. Begreber som risiko, behandlingens karakter, implementeringsomkostninger og det aktuelle tekniske niveau er åbne og dynamiske og ikke konkretisere, hvordan afvejningen af de enkelte kriterier skal foretages. Samtidigt forekommer der elementer i afvejningen der kan pege i forskellige retninger, her forekommer hensynet til implementeringsomkostningerne, som værende rettet væk fra det overordene hensyn til de registreredes rettigheder og frihedsrettigheder, hvilket forstærker behovet for en mere konkret afvejning. Kompleksiteten medfører at det i praksis er besværligt for den dataansvarlige at fastlægge, hvornår beskyttelsesniveauet er ”passende” og altså dermed, hvornår der er gjort ”nok”. Usikkerheden forekommer dog ikke som en tilfældighed, men en konsekvens af GDPR-artikel 32’s opbygning og formålet om at kunne anvendes på tværs af behandlingsaktiviteter.

I denne sammenhæng har analysen vist at der vil være visse fordele ved at fastlægge en konkret minimumsgrænse. En sådan grænse vil bidrage med forøget klarhed og forudsigelighed for den dataansvarlige, i det den vil fastlægge et minimum for, hvad der kræves. Den dataansvarlige vil derfor nemmere kunne navigere i kravene og dermed reducere risikoen for henholdsvis over- og underimplementering. En minimumsgrænse, vil ligeledes kunne medføre en mere ensartet anvendelse af kravene til beskyttelsesniveauet der fremgår af GDPR, samt styrke håndhævelsen af disse krav, idet der bliver nemmere at identificere tilfælde der ikke opfylder minimumskravene. Analysen har ligeledes indikeret at en minimumsgrænse ikke er i strid med den fleksible karakter der følger af GDPR-artikel 32, men derimod fungere som et supplement dertil.

Implementering af en konkret minimumsgrænse bringer imidlertid også sine betænkeligheder. Særligt fremgår det at en minimumsgrænse kan føre til en standardiseret tilgang der ikke er i overensstemmelse med de formål GDPR-artikel 32 har og hermed resultere i at fokus flyttes fra risikobaseret tilgang, til blot at opfylde minimumskravene. Dertil fremgår det at vil være vanskeligt at fastlægge en konkret minimumsgrænse, der kan anvendes på tværs af behandlingsaktiviteter. Endeligt risikeres der ved en

konkret minimumsgrænse at den ikke er svarende til det aktuelle tekniske niveau, og dermed ikke fyldestgørende med henblik på at beskytte fysiske personers rettigheder og frihedsrettigheder.

Samlet viser analysen at der ikke kan fastlægges en konkret minimumsgrænse for, hvad ”passende tekniske og organisatoriske foranstaltninger” skal indeholde efter GDPR-artikel 32. Det vurderes derfor efter GDPR-artikel 32 ordlyd og afvejningen af fordele og ulemper at vurderingen af hvilke og hvornår en foranstaltning er ”passende” må forblive baseret på den enkelte behandling, hvilket begrundes af GDPR-artikel 32’s formål og karakter. Dog fremgår det ligeledes at der fra praksis at der forekommer en teoretisk minimumsgrænse, hvor visse grundlæggende elementer skal være tilstede, herunder kontrol, procedure og effektiv anvendelse af foranstaltninger, for at en foranstaltning og sikkerhedsniveaut kan vurderes som værende ”passende”. Fraværet af disse vil i sig selv kunne medføre at foranstaltningen ikke er ”passende”.

Konklusionen er således at GDPR-artikel 32 indeholder to sider, hvor på den ene side fremstår den som værende en fleksibel og risikobaseret standard og på den anden side at indeholde en mere implicit nedre grænse. Dermed kan der ikke fastsættes en konkret og præcis minimumsgrænse, men det er muligt at identificere et minimumsniveau, der i praksis definere en grænse for, hvornår beskyttelsesniveauet ikke kan vurderes til at være ”passende”.

5. Litteraturliste

5.1 Bøger

Blume, P. (2020). *Persondatarettens kilder og metode*. Djøf forlag.

Bryde Andersen, M. (2002). *Ret og Metode*. G.E.C. Gads Forlag.

Evald, J. (2019). *At tænke juridsk* (5. udg.). Djøf Forlag.

Korfits Nielsen, K. & Lotterup, A. (2020). *Databeskyttelsesforordningen og databeskyttelsesloven: Med kommentarer*. Jurist- og Økonomiforbundets Forlag.

Munk-Hansen, C. (2021). *Den juridiske løsning* (2. udg.). Djøf.

Neergaard, U. & Nielsen, R. (2020). *EU-ret* (8. udg.). Karnov Group.

Neergaard, U. & Nielsen, R. (2021). *EU-Ret: Fri Bevægelighed* (4. udg.). Karnov Group.

Nielsen , R. & Tvernø, C.D. (2017). *Retskilder og retsteorier* (5. udg.). Jurist- og Økonomforbundet.

Sørensen, K. E. & Danielsen, J. H. (2022). *EU-retten* (8. udg.). Juris- og Økonomiforbundets Forlag.

Trakowski, J. & Gersvang Sørensen, M. (2019). *GDPR Complience: Understanding the General Data Protection Regulation*. Ex Tuto Publishing.

5.2 Domme og afgørelser

Byrets dom : 5399/2023. (2024, 23. December). *Domsdatabasen*. https://domsdatabasen.dk/#sag/6995/8392

Juris: C-741/21. (2024, 11. April). *EUR-Lex*. https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:62021CJ0741

Kerteminde Kommune får kritik for deres sikkerhedsprocedurer. (2024, 23. Februar). *Datatilsynet*. https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/feb/kerteminde-kommune-faar-kritik-for-deres-sikkerhedsprocedurer

Másdi: C-169/23. (2024, 28. November). *EUR-Lex*. https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:62023CJ0169

Region Midtjylland indstillet til bøde. (2021, 08. September). *Datatilsynet*. https://www.datatilsynet.dk/afgoerelser/afgoerelser/2021/sep/region-midtjylland-indstillet-til-boede

Russmedia: C-492/23. (2025, 2. December). *EUR-Lex*. https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:62023CJ0492

Stadfæstelsen: 113/2025. (2026, 23. Marts). *Domsdatabasen*. https://domsdatabasen.dk/#/sag/10573/12480

Tre politikredse får kritik for manglende behandlingssikkerhed. (2024, 17. Maj). *Datatilsynet*. https://www.datatilsynet.dk/afgoerelser/afgoerelser/2024/maj/tre-politikredse-faar-kritik-for-manglende-behandlingssikkerhed-nordjyllands-politi

Videregivelse af opgavebesvarelser. (2020, 18. Juni). *Datatilsynet*. https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/jun/videregivelse-af-opgavebesvarelser

5.3 Anden litteratur

Adfærdskodeks for menighedsråds behandling af personoplysninger som led i sognepleje. (2021, 22. Juni). *Datatilsynet*. https://www.datatilsynet.dk/Media/637635046101057179/Adfærdskodeks%20for%20menighedsråds%20behandling%20af%20personoplysninger%20som%20led%20i%20sognepleje.pdf

Adfærdskodekser og certificeringsordninger. (s.d.). *Datatilsynet*. https://www.datatilsynet.dk/regler-og-vejledning/adfaerdskodekser-og-certificeringsordninger

ANALYSE AF CYBER- OG INFORMATIONSSIKKERHED I DANMARK [Analyse]. (2025, December). Samsik. https://samsik.dk/wp-content/uploads/2026/01/Analyse-af-Cyber-og-Informationssikkerhed.pdf

Antal anmeldte brud på persondatasikkerheden over tid. (s.d.). Datatilsynet. Lokaliseret den Februar 2026 på https://www.datatilsynet.dk/sikkerhedsbrud/statistik-over-brud-paa-persondatasikkerheden/antal-anmeldte-brud

Behandlingssikkerhed. (s.d.). *Datatilsynet*. https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed

Brinnen, M. & Westman, D. (2019, December). Description of the challenges for business and some proposals for improvement. *Svenskt Näringsliv*. https://www.svensktnaringsliv.se/material/skrivelser/xf8sub_whats-wrong-with-the-gdpr-webbpdf_1005076.html/What%27s+wrong+with+the+GDPR+Webb.pdf

Cyberangreb mod danske virksomheder fordoblet på ét år. (2026, 4. Marts). *Via Ritzau*. https://via.ritzau.dk/pressemeddelelse/14817899/ny-rapport-cyberangreb-mod-danske-virksomheder-fordoblet-pa-et-ar-kan-koste-120-mio-kr-pr-angreb?publisherId=12195769&lang=da

Cyberkriminalitet i virtuelle verdener. (2025, 31. Marts). Europa Kommisionen. https://digital-strategy.ec.europa.eu/da/policies/virtual-worlds-cybercrime

Cybersikkerhed: De vigtigste og største trusler. (2022, 26. Januar). Europa-parlementet . Lokaliseret den April 2026 på https://www.europarl.europa.eu/topics/da/article/20220120STO21428/cybersikkerhed-de-vigtigste-og-storste-trusler

Cybertruslen mod Danmark. (2025, November). Samsik. https://samsik.dk/wp-content/uploads/2025/11/Cybertruslen-mod-Danmark-2025.pdf

Dalberg-Larsen, J. (2021, 19. Januar). de lege lata. *LEX*. https://lex.dk/de_lege_lata

Dalberg-Larsen, J. (2024, 2. April). Retsstandard. *Lex*. https://lex.dk/retsstandard

Databeskyttelse gennem design og standardindstillinger. (s.d.). *Datatilsynet*. https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed/databeskyttelse-gennem-design-og-standardindstillinger

Databeskyttelsesforordningen: og de retlige rammer for dansk lovgivning: Betænkning 1565. (2016). *Justitsministeriet* . https://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/betaenkning_1565_dib1.pdf

Det Europæiske Databeskyttelsesråd. (s.d.). *Datatilsynet*. https://www.datatilsynet.dk/internationalt/det-europaeiske-databeskyttelsesraad-edpb

Detaljeret statistik på anmeldelser om brud på persondatasikkerheden. (2026, April). Datatilsynet. https://www.datatilsynet.dk/sikkerhedsbrud/statistik-over-brud-paa-persondatasikkerheden/detaljeret-statistik

En styrket, fælles indsats for cyber- og informationssikkerhed. (s.d.). *ISM*. https://www.ism.dk/Media/6/A/En-styrket-faelles-indsats-for-cyber-og-informationssikkerhed-tilgaengelig-pdf.pdf

EU-Domstolens retspraksis. (s.d.). Forbrugerombudsmanden. Lokaliseret den Marts 2026 på https://forbrugerombudsmanden.dk/eu-retspraksis

Foranstaltning: Awareness. (s.d.). *Datatilsynet*. https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed/katalog-over-foranstaltninger/awareness

Gamification og spilbaseret læring. (2025, 11. Juli). *Region Hovedstaden*. https://www.regionh.dk/e-learning/innovation-og-udvikling/sider/gamification.aspx

General Data Protection Regulation, LOV nr. (EU) 2016/679 (2016). https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. (2017, 4 . Oktober). *European Commission*. https://ec.europa.eu/newsroom/article29/items/611236

Hansen, U. (2025, 02. Juli). *GDPR er løbet løbsk: ”Det koster tid og penge, som kunne være brugt bedre på andre ting”*. Dansk Industri. https://www.danskindustri.dk/di-business/arkiv/nyheder/2025/7/gdpr-er-lobet-lobsk-det-koster-tid-og-penge-som-kunne-vare-brugt-bedre-pa-andre-ting/

Hobson, A. & Calder, A. (2018, 25. Maj). Data Privacy at a Price: The GDPR Just Isn't Worth It. *Mercatus Center*. https://www.mercatus.org/students/economic-insights/expert-commentary/data-privacy-price-gdpr-just-isnt-worth-it

Juul, M. (2021, 26. april). *Konservative: GDPR er endnu en byrde for erhvervslivet* [Debatindlæg]. Altinget. https://www.altinget.dk/digital/artikel/konservative-gdpr-er-endnu-en-byrde-for-erhvervslivet-men-en-af-

de-mere-forstaaelige

Katalog over foranstaltninger. (s.d.). *Datatilsynet*. https://www.datatilsynet.dk/regler-og-vejledning/behandlingssikkerhed/katalog-over-foranstaltninger

Kirkeministeriets adfærdskodeks er godkendt. (s.d.). *Datatilsynet*. https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/aug/kirkeministeriets-adfaerdskodeks-er-godkendt

Nærhedsprincippet og nationale parlamenters rolle. (2025, 17. Februar). *Folketinget*. https://www.eu.dk/da/fakta-og-tal/sådan-lovgiver-eu/naerhedsprincippet

Opdatering af sikkerhedsstandarden ISO 27001:: Statslige myndigheder skal implementere den nye version. (2023, 20. September). *Digitaliseringsstyrelsen*. https://digst.dk/nyheder/nyhedsarkiv/2023/september/opdatering-af-sikkerhedsstandarden-iso-27001-og-overgangsperiode-for-statslige-myndigheder/

Ransomware. (s.d.). Microsoft. https://www.microsoft.com/da-dk/security/business/security-101/what-is-ransomware

Register of certification mechanisms, seals and marks. (s.d.). *EDPB*. https://www.edpb.europa.eu/our-work-tools/accountability-tools/certification-mechanisms-seals-and-marks_en

Robusthed. (2023, 9. Maj). *brother*. https://www.brother.dk/business-solutions/resource-hub/blog/security/2023/what-to-include-in-your-it-resilience-plan

Secure Personal Data. (s.d.). *EDPB*. https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en#toc-2

Selzer, A., Woods, D. & Böhme, R. (2021). An Economic Analysisof Appropriateness under Article 32 GDPR. *EDPL*. https://edpl.lexxion.eu/data/article/17705/pdf/edpl_2021_03-016.pdf

Smirnova, Y. & Travieso-Morales, V. (2025, 1. August). *Why is GDPR complience still so difficult?*. LSE Blogs. https://blogs.lse.ac.uk/businessreview/2025/08/01/why-is-gdpr-compliance-still-so-difficult/

The trends reshaping cybersecurity. (2026, 12. Januar). *The world economic forum*. https://www.weforum.org/publications/global-cybersecurity-outlook-2026/in-full/3-the-trends-reshaping-cybersecurity/

Top five concerns with GDPR compliance. (s.d.). Thomson Reuters. Lokaliseret den 28. April 2026 på https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance

Vejledning om adfærdskodekser. (2023, Juni). *Datatilsynet*. https://www.datatilsynet.dk/Media/638233755631220855/Vejledning%20om%20adfærdskodekser.pdf

VEJLEDNING OM PRINCIPPER FOR AGIL ERHVERVS- RETTET REGULE- RING. (s.d.). *Erhvervsministeriet* . https://www.em.dk/media/14564/vejledning-om-principper-for-agil-erhvervsrettet-regulering_juni-2018.pdf