CONSUMERPRO

BOOSTING PROFESSIONALS
IN CONSUMER PROTECTION

Digitale rettigheder

Teoretisk baggrundsdokument

2022- 2023

Digital Rights - Denmark
October 2022 - version 1

European Commission

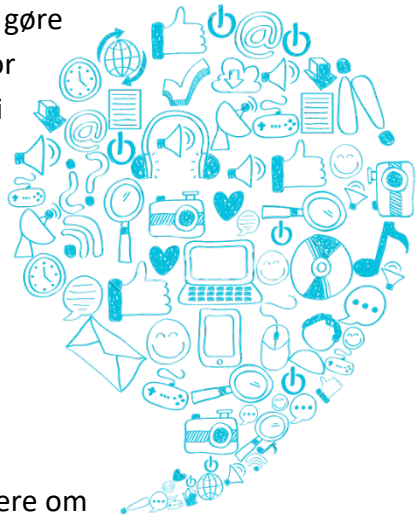
INDHOLDSFORTEGNELSE

Dette materiale er udarbejdet til brug for *Consumer PRO*, projektet, hvilket er et initiativ under det Europæiske Forbrugerprogram, finansieret af den Europæiske Kommissions finansieringsprogrammer. Den Europæiske Kommissions støtte indeholder ikke en godkendelse af indholdet af materialet. Materialet afspejler alene forfatternes synspunkter. Kommissionen kan ikke holdes ansvarlig for brug af indholdet heri.

INTRODUKTION TIL DET TEORETISKE BAGGRUNDSDOKUMENT

Kære Læser,

Dette teoretiske baggrundsdokument er en del af de træningsressourcer, der er blevet udarbejdet af Consumer Pro, et EU-initiativ, hvis mål er at gøre forbrugerorganisationer og andre aktører indenfor forbrugerrettigheder bedre klædt på til at beskytte forbrugerne i deres land.



Formålet med dette dokument er at give dig og dit team brugbar og relevant information om digitale rettigheder. Dets indhold er udarbejdet fra et EU-perspektiv af BEUC´s politiske eksperter i digitale rettigheder, og giver dig værktøjer til:

- Hurtigt at træne dit team af praktikere
- Hurtigt at finde relevant information
- Give dine ansatte bedre mulighed for at informere forbrugere om deres rettigheder, og
- øge dine nationale ministerier og myndigheders viden om digitale rettigheder

Dette teoretiske baggrundsdokument er en del af en række uddannelsesressourcer, der bliver tilpasset eventuelle nationale reguleringer. Der er supplerende teoretiske baggrundsdokumenter tilgængelig efter anmodning eller online, om emnerne forbruger rettigheder og kollektiv klageadgang, på engelsk såvel som på mange andre europæiske sprog.

Om Consumer PRO

Consumer PRO er et initiativ under EU Kommissionens forbrugerprogram og er implementeret af BEUC – den europæiske forbrugerorganisation. Formålet med initiativet er at opbygge viden hos de europæiske forbrugerorganisationer samt andre aktører inden for forbrugerpolitik gennem ikke-formel uddannelse. Projektet dækker EU-medlemsstaterne, samt Island og Norge.

For yderligere information, skriv venligst til Info@consumer-pro.eu.

1. DATABESKYTTELSE

1.1. Introduktion til databeskyttelsens forbrugerpolitik og udviklingen heraf

Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger er en grundlæggende rettighed i Den Europæiske Union. Artikel 8, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder og artikel 16, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde (TEUF) bestemmer, at enhver har ret til beskyttelse af personoplysninger, der vedrører ham/hende. Derudover fastslår artikel 7 i chartret om grundlæggende rettigheder, at enhver har ret til respekt for privatliv og familieliv, hjem og kommunikation.

Den generelle databeskyttelsesforordning (GDPR) regulerer behandlingen af personoplysninger i EU. Forordningen stiller krav om, at data behandlere, herunder både offentlige myndigheder og private virksomheder, anvender forbrugernes personoplysninger på en gennemsigtig og retfærdig måde. Databeskyttelsesforordningen styrker de registreredes rettigheder og gælder for alle organisationer, der behandler personoplysninger om personer der befinder sig i EU, uanset hvor databehandleren befinder sig eller er etableret.

Reglerne om databeskyttelse inden for elektronisk kommunikation (i øjeblikket ePrivacy-direktivet, som er under revision) beskytter fortroligheden af elektronisk kommunikation og indeholder en beskyttelse af forbrugerne bl.a. mod uønsket kommerciel kommunikation sendt via elektroniske kommunikationstjenester.

1.2. Hvorfor databeskyttelse er vigtig for forbrugerne

Selv om digitale informationsteknologier også er gavnlige for forbrugerne, udgør de sammen med fremkomsten af nye online-tjenester også en stor udfordring for de grundlæggende rettigheder til privatliv og beskyttelse af personoplysninger. De forretningsmodeller, der i øjeblikket dominerer den digitale verden, er baseret på at overvåge og analysere hver eneste af forbrugernes bevægelser. Virksomheder bruger den information, de indsamler til at opbygge brugerprofiler, som efterfølgende sælges online og herefter bruges til at levere adfærdsmålrettet annoncering. Brugerprofilerne kan også misbruges til at diskriminere forbrugere samt til at påvirke deres adfærd. Det er derfor vigtigt at sikre, at forbrugerne har kontrol over deres personlige data og at de kan drage fordel af innovative digitale produkter og tjenester uden at skulle give afkald på deres privatliv.

1.3. De primære udfordringer vedrørende databeskyttelsesforbrugerpolitik

I praksis er det er meget svært for forbrugerne at kunne kontrollere, hvad der sker med deres personoplysninger. Forbrugernes rettigheder bliver ofte ikke respekteret, hvorfor forbrugerne kan være tvunget til at acceptere at give afkald på deres privatliv, hvis de ønsker at bruge digitale produkter og tjenester.

Forbrugere er under konstant kommerciel overvågning, og deres personlige data udnyttes af et utal af virksomheder, hvoraf mange er nogen forbrugerne aldrig har hørt om. Privatlivspolitikker er vage, lange, komplekse og ofte meget svære at forstå, og forbrugeren har ofte intet andet valg end at acceptere dem. Forbrugerne bliver dermed givet en illusion af kontrol, men i de tilfælde, hvor de bliver bedt om at give deres samtykke, bliver dette blot en systematisk, meningsløs "tick the box''-øvelse fra forbrugerens side.

Databeskyttelsesforordningen var egentlig beregnet til at løse mange af disse problemer. Men næsten fire år efter, at den trådte i kraft, er der ikke sket væsentlige ændringer i praksis. Niveauet af overholdelse af databeskyttelsesforordningen er lavt på flere områder, og håndhævelsen af forordningen er samtidig ikke helt effektiv. Databeskyttelsesmyndighederne har svært ved at håndtere alle de klager de modtager, og håndhævelsen af forordningen, som er bygget op omkring samarbejde og ensartethed for at sikre en sammenhængende fortolkning og anvendelse af loven i hele EU, står over for flere udfordringer.

Et andet problem er, at ændringerne af e-privatlivsreglerne, som er beregnet til at supplere databeskyttelsesforordningen og yderligere beskytte kommunikationshemmeligheden, har været undervejs i mere end fem år, og der er stadig ingen aftale i sigte. (For mere information om e-databeskyttelsesforordningen se BEUC-faktaark).

1.4. De primære forbrugerrettigheder og -forpligtelser kort fortalt

Databeskyttelsesforordningen kræver at dataansvarlige, herunder både offentlige myndigheder og private virksomheder, behandler forbrugernes persondata på en gennemsigtig og retfærdig måde. Databeskyttelsesforordningen indeholder en række principper, der regulerer behandlingen af personoplysninger.

Databeskyttelsesforordningen giver også forbrugerne en række rettigheder for at sikre, at forbrugerne har kontrol over deres data. Forbrugere har blandt andet ret til, at:

- Blive informeret på en klar og letforståelig måde om, hvordan deres persondata bliver brugt. Det skal specificeres, hvilke data der bruges, af hvem og til hvilke formål.
- Få adgang til de data, som organisationer har om dem, og få en kopi af disse data.
- Ret til at få rettet data, hvis de er unøjagtige.
- Få organisationer til at slette deres data.
- Bede organisationer om at stoppe med at bruge deres data, enten midlertidigt eller permanent.
- Modtage deres data i et almindeligt format, så de kan tage dem med og bruge dem et andet sted.
- Bestride automatiserede beslutninger baseret på deres personlige data, hvis beslutningen påvirker dem på en væsentlig måde (f.eks. at blive nægtet et lån).

- Blive informeret, hvis deres data går tabt eller bliver stjålet.
- Indgive en klage til deres nationale databeskyttelsesmyndighed eller indbringe en virksomhed for domstolene

1.5. Love og reguleringer i EU og på nationalt niveau

- EU Charter of Fundamental Rights
- Forordning 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger
- Direktiv 2002/58/EC om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) – ændret ved Directive 2009/136/EC
- Guidelines, anbefalinger mv. fra det Europæiske Databeskyttelsesråd
- Opinions fra det Europæiske databeskyttelsestilsyn
- Eksempel på Code of Conduct: Federation of Direct Marketing
- Lov nr. 502 af 23/05/2018 Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)
- Datatilsynets vejledninger, anbefalinger og afgørelser

1.6. Retspraksis/afgørelser

Besøg: www.GDPRHub.eu for et udpluk af afgørelser fra EU databeskyttelsesmyndigheder og domstolsafgørelser samt artikler om databeskyttelsesforordningen.

På den officielle EU-lovportal: Eurlex findes tillige en side om Databeskyttelsesforordningen. Her er bl.a. en liste over EU-Domstolssager og foreløbige spørgsmål, der vedrører Databeskyttelsesforordningen: find listen over retspraksis under "d*okumentoplysninger*".

1.7. Hvad kan forbrugere gøre, hvis de har et problem?

Hvis forbrugerne vurderer, at deres rettigheder efter databeskyttelsesforordningen er blevet krænket, har de 2 muligheder:

- Klage til den nationale databeskyttelsesmyndighed. Du kan finde en liste over myndigheder her.
- Anlægge en sag direkte ved domstolene mod en virksomhed/myndighed. Dette forhindrer ikke forbrugeren i også at indgive en klage til de nationale databeskyttelsesmyndigheder, hvis de ønsker det.

Hvis forbrugeren mener, at databeskyttelsesmyndighederne ikke har behandlet deres klage korrekt, eller hvis forbrugeren ikke er tilfredse med databeskyttelsesmyndighedens svar, eller hvis databeskyttelsesmyndigheden ikke informerer forbrugeren om forløbet eller resultatet inden for 3 måneder fra den dag, hvor klagen blev indgivet, kan forbrugeren også anlægge en sag ved domstolene mod Datatilsynet.

Nationale myndigheder

- Justitsministeriet er ansvarlig for implementeringen af databeskyttelsesforordningen, og har i forbindelse med vedtagelsen af reglerne, udarbejdet betænkninger herom.

I tillæg til de nationale myndigheder, kan man også overveje følgende myndigheder:

På Europæisk niveau:

- Europa-Kommissionen, som er ansvarlig for at sikre, at medlemsstaterne implementerer databeskyttelsesforordningen korrekt og som også har beføjelse til at vedtage visse gennemførelsesretsakter i databeskyttelsesforordningen via tildelte beføjelser (f.eks. til oprettelse af standardiserede ''privatlivsikoner'').
- Det Europæiske Databeskyttelsesråd (EDPB), som samler alle de nationale databeskyttelsesmyndigheder. EDPB's hovedopgave er at sikre sammenhængen i anvendelsen og fortolkningen af GDPR.
- Den europæiske tilsynsførende for databeskyttelse (EDPS), som fører tilsyn med EU-institutionernes respekt for personers personoplysninger og rådgiver institutionerne om databeskyttelsesspørgsmål.

Alternativ konfliktløsning

Udenretslige procedurer og andre alternative konfliktløsninger til løsning af tvister mellem dataansvarlige og registrerede om behandling af personoplysninger, kan udarbejdes via adfærdskodekser vedtaget af brancheorganer (artikel 40 GDPR), uden at dette berører de registreredes rettigheder til at indgive klager til deres databeskyttelsesmyndighed eller adgangen til domstolsprøvelse.

1.8. Yderligere kilder – faktaark, publikationer, links mv. på engelsk

- European Commission website with information about GDPR
- European Commission GDPR Library - Infographics, factsheets and other materials aimed at citizens and businesses
- BEUC Factsheet – What does EU data protection law mean to you?
- BEUC Report – The long and winding road: A cross border data protection enforcement case from a consumer perspective
- AccessNow – User guide to data protection in the EU: Your rights and how to exercise them

- Fundamental Rights Agency – European Data Protection Handbook
- Guides og vejledninger udarbejdet af Datatilsynet (https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning)
- Factsheets Udgivet af the European Data Protection Supervisor (EDPS)
- The History of the GDPR and a Glossary (EDPS)

2. PLATFORME

2.1. Introduktion til platformes forbrugerpolitik og udviklingen heraf

Forbrugerne køber flere og flere tjenester og produkter online, især via platforme.

I de første år af e-handlen foregik sådanne køb hovedsageligt på websteder hos virksomheder, der også havde fysiske butikker. I dag er forbrugernes købsadfærd ved at ændre sig radikalt: flere og flere personer bestiller tjenesteydelser og produkter via online-markedspladser, som sendes direkte til europæiske forbrugere fra lande også uden for EU.

Købene foretages ikke kun via e-handelsplatforme som Amazon Marketplace, AliExpress, wish.com eller eBay, men også via sociale medier som Instagram.

For eksempel blev der i 2017 foretaget omkring 100 millioner salg fra Kina til Tyskland. Hvilket er 40 millioner flere end i 2016, ligesom der er rapporteret om store stigninger i andre europæiske lande.

I tillæg til dette, sker der en stigende svindel med webshops, hvor webshops bliver sat op i EU af sælgere, der udgiver sig for at være europæiske virksomheder, men som i virkeligheden bestiller produkter på platforme fra Kina og sælger disse til forbrugerne til en højere pris end på for eksempel på wish.com. Dette er bl.a. observeret i Danmark og Frankrig [1].

Der er en meget alvorlig bekymring for, at mange af disse produkter ikke overholder de europæiske love og tekniske standarder, som er indført for at beskytte forbrugernes rettigheder, sikkerhed, sundhed og miljøet.[2] Mens producenter og distributører beliggende i EU kan holdes ansvarlige for produktsikkerhed og skal overholde EU-regler, vil dette ofte ikke være tilfældet for producenter, der ikke er etableret i EU, da mellemmændene, dvs. e-handelsplatformene, nægter ansvaret for overholdelsen heraf.

Der er vigtige lovgivningsinitiativer under vedtagelse for at løse nogle af disse problemer, særligt forslaget til en lov om digitale tjenester[3] og forslaget om en generel produktsikkerhedsforordning.[4]

---

[1] http://www.leparisien.fr/economie/consommation/achats-en-ligne-attention-aux-derives-du-dropshipping-16-01-2020-8237226.php

[2] https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html

[3] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

2.2. Hvorfor platforme er vigtige for forbrugerne

At shoppe, komme i kontakt med venner og familie, dele oplevelser, se en film, lytte til musik, læse en bog, bestille en rejse, lave mad efter en ny opskrift, planlægge en aften i byen, finde rundt i en by, bede om naboens hjælp og søge oplysninger på nettet er blot nogle grundlæggende eksempler på aktiviteter, som millioner af forbrugere foretager hver dag online. For hver af disse aktiviteter findes der en eller flere onlineplatforme til formålet. Forbrugerne har taget platformøkonomien til sig, hvilket giver mange fordele, men også udfordringer for forbrugerbeskyttelsen.

2.3. De primære udfordringer ved platforme

Da e-handelsdirektivet blev vedtaget (i 2000), var platforme som Google, Amazon eller Booking.com i deres spæde start. Mange andre platforme fandtes ikke engang. For eksempel blev Facebook og Shopify først lanceret i 2004. Etsy blev grundlagt i 2005; Airbnb i 2008. Mens Instagram, Wish og AliExpress først blev lanceret i 2010.

I løbet af de seneste 20 år har forretningsmodellerne for nogle af disse og andre virksomheder ændret sig. Dynamikken i markedsmagten har ligeledes ændret sig.

Det europæiske digitale markedslandskab har oplevet en "dataficering" (omdannelse af informationer til data, hvilket er grundlaget for digitale forretningsmodeller); en mangedobling af platforme; en udbredelse af samarbejdsøkonomien og en diversificering af tjenesteudbydere med hensyn til funktioner, vertikal integration og størrelse. Men alle disse virksomheder skal fortsat følge reglerne. Forbrugerbeskyttelse afhænger ikke – og må ikke afhænge – af virksomhedens størrelse. Når alt kommer til alt, kan dagens nystartede virksomhed eller SMV blive morgendagens "Alibaba".

Forbrugerbeskyttelse afhænger ikke – og må ikke afhænge af – virksomhedens størrelse. Når alt kommer til alt, kan dagens nystartede virksomhed eller SMV blive morgendagens "Alibaba".

Mange platforme har genopfundet sig selv. Nogle af dem begrænser sig ikke længere til deres oprindelige rolle som informations- eller betroede mellemmænd (som f.eks. sammenlignings- eller anmeldelsesplatforme som Yelp), men gør det nu muligt også at indgå transaktioner på platformen. Dette er forretningsmodeller, der medvirker til, at platformen

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021PC0346&from=EN

nu falder ind under kategorien "onlinemarkedsplads"[5], hvilket flere forbrugerbeskyttelsesorganisationer i øjeblikket har fokus på.

Denne type af platform er defineret i EU's direktiv om "bedre håndhævelse og modernisering af EU-reglerne om forbrugerbeskyttelse"[6], som *"en tjenesteydelse, der gør brug af software, herunder et websted, en del af et websted eller en applikation, der drives af eller på vegne af den erhvervsdrivende, der giver forbrugere mulighed for at indgå fjernsalgsaftaler med andre erhvervsdrivende eller forbrugere."* Platformens rolle vil dog ofte ikke være begrænset til at gøre det muligt at indgå en aftale mellem sælgere og købere, men vil også kunne omfatte andre tjenester såsom betalingstjenester, returbehandling og klagebehandling[7].

Andre platforme har flere forskellige roller. Der findes "hybridplatforme", som kombinerer forskellige formidlingsfunktioner eller vertikalt integrerede platforme. Sidstnævnte fungerer ikke kun som mellemmænd, men konkurrerer også med de erhvervsdrivende, enten direkte eller via undervirksomheder. Amazon er f.eks. både sælger, online-markedsplads, cloud computing-virksomhed, videodelingsplatform, forlag, reklamevirksomhed, producent af internettilsluttede enheder og en kunstig intelligens-virksomhed.

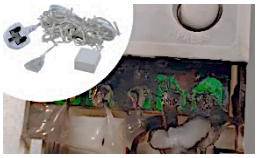
Forbrugerorganisationerne går ind for justeringer af lovgivningen for at imødegå denne nye markedsrealitet. Forslaget til en lov om digitale tjenester er et meget vigtigt initiativ i dette perspektiv. Kommissionen fremlagde forslaget til lov om digitale tjenester i december 2020. Forslaget er i øjeblikket i de sidste faser af lovgivningsprocessen. Forslaget forventes at blive vedtaget i 2022.

Specifikke udfordringer

Udfordring #1. Spredning af en lang række af ulovligt indhold

[5] Vzbv study, https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf, p. 17.
[6] Article 3(1)(n) of the Unfair commercial practices Directive, as amended by Directive 2019/2161", https://eur-lex.europa.eu/eli/dir/2019/2161/oj
[7] Vzbv study, https://www.vzbv.de/sites/default/files/downloads/2020/02/12/vzbv_gutachten_verbraucherrechtliche_plattformhaftung.pdf, p. 18.

Digitale tjenester er - til en vis grad - blevet et sted til udbredte overtrædelser af forbrugerlovgivningen; en indtægtskilde for salg af reklamer eller promovering af farlige, usikre, ulovlige produkter online. For eksempel[8]:

	BEUC's UK-medlem, fandt juletræskæder solgt online, som kunne bryde i brand eller giver forbrugeren stød[9].
	Det danske forbrugerråd, afslørede kosmetik på wish.com, som ikke overholdt EU-lovgivningen
	For nylig fandt seks BEUC-medlemmer ud af, at to tredjedele af 250 produkter købt online ikke levede op til sikkerhedstests hvilket kunne føre til elektrisk stød, brand eller kvælning.[10]

Udfordring #2. Forvirring mellem online markedspladsaktiviteter og andre platformsaktiviteter.

Den debat, der har været omkring ændring af direktivet om e-handel har i et vist omfang fokuseret på spørgsmål som hadefuldt indhold, terrorindhold, ophavsretligt beskyttet materiale, ytringsfrihed eller overvejelser om det indre marked. Selv om disse spørgsmål er vigtige, bør EU dog ikke glemme forbrugerbeskyttelsesproblemer. Det er nødvendigt at sikre forbrugere, der køber produkter eller tjenesteydelser via online markedspladser[11] fuld beskyttelse.

[8] Se for eksempel https://www.beuc.eu/publications/beuc-x-2019-072_new_evidence_from_beuc_member_organisations_regarding_dangerous_products_available_online.pdf

[9] https://www.which.co.uk/news/2019/12/these-christmas-tree-lights-bought-online-at-ebay-wish-and-aliexpress-could-catch-fire-or-electrocute-you/

[10] https://www.beuc.eu/publications/two-thirds-250-products-bought-online-marketplaces-fail-safety-tests-consumer-groups/html

[11] Defined by the EU Omnibus Directive as "*a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers*". Having said that, often the role of the platform is not limited to enabling the conclusion of a contract between sellers and buyers, but it also includes other services such as payment services, fulfilment services, returns processing and complaints handling.

Det er nødvendigt at skelne mellem salg af ulovlige produkter og andre aktiviteter, f.eks. at skrive kommentarer på sociale medier. Mens der i sidstnævnte tilfælde er klare hensyn til ytringsfriheden, er det i førstnævnte tilfælde langt fra ytringsfriheden, der er på spil, men snarere et spørgsmål om produktsikkerhed og forbrugerbeskyttelse.

Udfordring #3. Direktivet om e-handel "finder ikke anvendelse på tjenesteudbydere, der er etableret i et tredjeland"[12].

Nogle udbydere, der er etableret i tredjelande, udnytter direktivets territoriale begrænsninger - hvilket skaber uretfærdige og ulige konkurrencevilkår

Udfordring #4. Den måde, e-handelsdirektivet regulerer hosting-udbydere på, bruges af nogle platforme - herunder (men ikke kun) online markedspladser - til enten at beskytte sig selv mod ethvert ansvar eller til ikke at træffe nogen betydelige foranstaltninger af frygt for ansvar.

Udfordring #5. Den nuværende lovgivning har mangler med hensyn til regulering af onlinemarkedspladser. Der lægges kun lidt vægt på online-markedspladsers indtjening på ulovligt indhold.

Udfordring #6. De nye regler kan være en hindring for, at medlemsstaterne kan tage højde for mål af almen interesse på passende måde.

For eksempel slog EU-domstolen fast, i C-390/18[13], at Airbnb skal betragtes som en informationssamfundstjeneste (artikel 2, litra a), i direktivet om e-handel. Da Frankrig ikke havde underrettet Kommissionen om en lov, der krævede, at virksomheder som Airbnb skulle have en erhvervsmæssig tilladelse som ejendomsmægler, kunne Frankrig ikke pålægge Airbnb denne forpligtelse, da dette ville være i strid med artikel 3, stk. 4, litra b), i direktivet om e-handel. Denne sag viste, at direktivet om e-handel ved at sætte det indre marked øverst, først og fremmest skaber problemer for medlemsstaternes mulighed for at vedtage love og politikker der beskytter forbrugerne. Det er dog vigtigt at bemærke, at dommen ikke betyder, at medlemsstaterne ikke kan pålægge virksomheder som Airbnb sådanne foranstaltninger. EU-Domstolen var klar over, at anmeldelsespligten i e-handelsdirektivet *"ikke tager sigte på at forhindre en medlemsstats vedtagelse af foranstaltninger, der falder inden for dennes kompetenceområde og kan påvirke den frie udveksling af tjenesteydelser, men at forhindre, at en medlemsstat griber ind i den principielle kompetence, som tilkommer den medlemsstat, hvor udbyderen af den pågældende informationssamfundstjeneste er etableret*."

[12] E-handelsdirektivet præambel 58.
[13] http://curia.europa.eu/juris/documents.jsf?num=C-390/18

Udfordring #7. Manglende tilsyn og håndhævelse.

De digitale markeder udvikler sig hurtigt, og de kompetente myndigheder ser ikke ud til at kunne håndtere udviklingen, have den nødvendige ekspertise eller de nødvendige ressourcer til at overvåge og håndtere markedsproblemerne.

2.4. De primære forbrugerrettigheder og -forpligtelser

E-handelsdirektivet har længe været en af hjørnestenene for internettet. E-handelsdirektivet indførte bl.a. oprindelseslandsprincippet med nogle vigtige undtagelser (navnlig forbrugeraftaler), centrale oplysningsforpligtelser over for modtagerne af tjenesterne (f.eks. forbrugerne), ansvarsfritagelser og -begrænsninger for udbydere af onlineformidlingstjenester og andre bestemmelser.:

- **Artikel 1 – 3: Almindelige bestemmelser**
- **Artikel 4 – 15: Principper**

  Afdeling 1: Krav vedrørende etablering og oplysninger

  Afdeling 2: Kommerciel kommunikation

  Afdeling 3: Kontrakter, der er indgået elektronisk

  Afdeling 4: Formidleransvar for tjenesteydere
- **Artikel 16 – 20: Iværksættelse**
- **Artikel 21 – 24: Afsluttende bestemmelser**

Hvor kan man finde de vigtigste bestemmelser i e-handelsdirektivet?

- **Formål**: bidrage til et velfungerende indre marked ved at sikre fri bevægelighed for informations- og samfundstjenester mellem medlemsstaterne (Artikel 1).
- **Andre formål:** sikre " *retssikkerhed og forbrugernes tillid*" (præambel 7), sikre en høj grad af beskyttelse af almene hensyn og især beskyttelse af mindreårige
- (præambel 10)
- **Anvendelsesområde**: uden at det berører forbrugerbeskyttelsen (Artikel 1)
- **Definitioner** (Artikel 2)
- **Grundlæggende oplysninger** til forbrugere og andre brugere (Artikel 5, 6, 10)
- **Rettigheder ved online ordreafgivelse** (Artikel 11)
- **Formidleransvar for tjenesteydere** (Artikel 12-15). De vigtigste principper er:
  - Leverandører af informationssamfundstjenester er ikke ansvarlige for tredjepartsindhold, så længe de, når de får kendskab til det ulovlige indhold, hurtigt fjerner eller deaktiverer adgangen til det. (Artikel 14)
  - Forbud for medlemsstaterne mod at pålægge tjenesteyderne en generel overvågningsforpligtelse (Artikel 15)
- **Adfærdskodekser** (Artikel 16)
- **Udenretslig bilæggelse af tvister** (Artikel 17)

- **Søgsmålsadgang** " *for at bringe den påståede overtrædelse til ophør og hindre, at der opstår yderligere skade for de berørte interesser* " (Artikel 18)
- **Samarbejde mellem Medlemsstaterne** (Artikel 19)
- **Sanktioner** (Artikel 20)

Siden vedtagelsen af e-handelsdirektivet i 2000 har digitale tjenester udviklet sig og givet anledning til nye udfordringer. F.eks. giver safe harbor-princippet nogle platforme et frirum til ikke at blive holdt ansvarlige. Nogle udbydere af digitale tjenester påtager sig ikke et egentligt ansvar eller giver forbrugerne en ordentlig erstatning, hvis noget går galt. På samme måde har nogle frivillige initiativer forsinket meget nødvendige lovgivningsmæssige tiltag. Nogle af disse spørgsmål vil blive behandlet i den kommende lov om digitale tjenester.

Consumer PRO har udarbejdet to øvrige dokumenter om emnerne generel forbrugerlovgivning og kollektive klagemuligheder, som kan supplere kapitlet i dette dokument.

2.5. Perspektiv: Den kommende forordning om digitale tjenester

Den kommende forordning om digitale tjenester (DSA) vil regulere forpligtelserne for de digitale formidlingstjenester - navnlig onlineplatforme såsom sociale medier og markedspladser – som vil skulle træffe foranstaltninger til at beskytte deres brugere mod ulovlige varer, tjenester og indhold.

Den har til formål at sikre en bedre beskyttelse af forbrugerne og de grundlæggende rettigheder online, at etablere en effektiv gennemsigtigheds- og ansvarlighedsramme for onlineplatforme og dermed fremme mere retfærdige og åbne digitale markeder.

I modsætning til e-handelsdirektivet er DSA en forordning, så den vil harmonisere reglerne i hele EU og være direkte anvendelig. De nye regler skal sikre det samme beskyttelsesniveau for alle borgere i EU.

Forordningen om digitale tjenester, vil bl.a. indeholde[14]:

[14] Dette er en generel oversigt over nogle af de elementer, der forventes at indgå i den endelige tekst til forordningen, som stadig er under drøftelse.

- Foranstaltninger til bekæmpelse af ulovligt indhold online, for varer og tjenesteydelser, f.eks. ved en ordning, der gør det muligt for brugerne at "flagge" sådant indhold og for platforme at samarbejde med "trusted flaggers";
- Nye regler om forpligtelsen til at spore erhvervsdrivende skal skærpes (det såkaldte "kend din erhvervskunde "-princip) for erhvervsbrugere på online-markedspladser, hvilket har til formål at gøre det lettere at identificere sælgere af ulovlige varer;
- garantier for brugerne, herunder muligheden for at anfægte platformes beslutninger om moderering af indhold;
- yderligere gennemsigtighedsforanstaltninger for onlineplatforme, herunder om de algoritmer, der anvendes til anbefalinger, og målrettet reklame;
- Forpligtelser for meget store onlineplatforme til at forhindre misbrug af deres systemer, navnlig ved at imødegå systemiske risici bl.a. ved tilsyn gennem uafhængige revisioner af de foranstaltninger, de træffer;
- En ny tilsynsstruktur for at imødegå onlineområdets kompleksitet, hvor medlemsstaterne vil have den primære rolle, støttet af et nyt europæisk råd for digitale tjenester. For meget store onlineplatforme vil Kommissionen få en styrket tilsyns- og håndhævelsesrolle.

Selv om forordning om digitale tjenester vil medføre meget nødvendige forbedringer med hensyn til forbrugerbeskyttelse i forbindelse med digitale tjenester, er der et punkt, hvor der sandsynligvis ikke vil ske større ændringer, nemlig i ansvaret for online-markedspladser. DSA vil højst sandsynligt opretholde principperne for fritagelse for mellemmandsansvar i e-handelsdirektivet, om end med nogle præciseringer og små forbedringer

Love og reguleringer på EU-niveau

Forordning / Direktiv	Gennemførelses-dato	GENNEMGANG/EVALUERING: TYPE AF FORANSTALTNING	FORFALDSDATO	Kommentar
E-handelsdirektivet	17/01/2002 (gennemførelse)	EC re-examination rapport (Art. 21)	Før 17/07/2003, og derefter hvert andet år	Der har ikke været nogle officielle evalueringer siden 2012. Kommissionens sektorundersøgelser fra 2017, kan være interessant fra et konkurrencemæssigt perspektiv.
		Forordning om digitale tjenester (DSA)	Forslag fremlagt i december 2020 – Er i øjeblikket i den sidste fase af den fælles beslutningsprocedure. Forventes vedtaget i 2022.	DSA-forslaget blev fremlagt i december 2020 sammen med forordning om digitale markeder (DMA), som indeholder specifikke regler rettet mod gatekeeper-platforme.

				Centrale emner i DSA set fra et forbrugerperspektiv: ansvar for formidlere, navnlig online markedspladser; forpligtelser til at kende din erhvervskunde, procedurer for meddelelse og handling, gennemsigtighedskrav, håndhævelse og koordinering mellem medlemsstaterne, forpligtelser i forbindelse med målrettet reklame og brug af anbefalingssystemer.
Platform to Business Regulation (P2B Regulation)	12/07/2020	EU-Kommissionen vejledning om rangordning af gennemsigtighedskravet (Art. 5)	Publiceret 7. december 2020Publiceret 7. december 2020	
		EU-Kommissionen tilskynder til udarbejdelse af adfærdskodekser (Art. 17)	Ingen dato	En analyse af funktionen vil være en del af revisionen
		EU-Kommissionens evalueringsrapport (Art. 18)	13/01/2022 og hvert 3. år	
Omnibus Directive	28 november 2021 (gennemførelse) 28 May 2022 (anvendelse)	Artikel 7 – gennemførelse	Artikel 6 – Kommissionens rapportering samt evaluering. Rapport vil blive publiceret af kommissionen 28. Maj 2024, "DQ of food and doorstep selling measures".	

2.6. Retspraksis

- **Vedr.: Omnibus Directive**: ingen retspraksis endnu, da det først træder i kraft den 28. maj 2022. Se det teoretiske baggrundsdokument om den generelle forbrugerlovgivning for at finde oplysninger om retspraksis vedrørende andre forbrugerretlige instrumenter.
- **Vedr..: eCommerce Directive**: se retspraksis her

2.7. Hvad kan forbrugerne gøre, hvis de har et problem?

- Gå direkte til sælgeren/platformen (dette er ikke obligatorisk).
- Forsøge alternativ tvistbilæggelse (dette er ikke obligatorisk).
- Gå til medlemsstaternes kompetente myndigheder: Det varierer fra land til land og fra emne til emne.
- Klage til forbrugerklagenævnet, først via mæglingsteamet, se mere om processen her

2.8. Yderligere kilder - faktablade, publikationer, links mv.

- Europa-Kommissionens præsentation af de instrumenter og mål, der følges i e-handelsdirektivet (her)
- BEUC Redegørelse om sikring af forbrugerbeskyttelse i platformsøkonomien: (her)
- BEUC redegørelse om samarbejdsøkonomi (her)
- BEUC redegørelse om at få forordning om digitale tjenester til at være til gavn for forbrugerne (her)
- BEUC redegørelse om forslaget til forordning om digitale tjenester (her)
- BEUC faktablad: Den foreslåede forordning om digitale tjenester – bedre beskyttelse af forbrugere (her)
- Europa-Parlamentets orientering om forslaget til forordning om digitale tjenester (her)
- Europa Kommissionen – Q&A om forordning om digitale tjenester (her)

3. INTERNET OF THINGS (IOT)

3.1. Introduktion til IoT og udviklingen heraf

I løbet af de sidste par år er internetforbundene enheder blevet almindelige i mange forbrugeres liv. Hvor vi førhen normalt sad foran en computer for at få adgang til internettet, har vi nu smartphones med internetforbindelse med os overalt, hvor vi går. Samtidig bliver stadig flere og flere af de daglige enheder omkring os udstyret med sensorer og koblet til internettet. Fra internetforbundene kaffemaskiner og sikkerhedskameraer til biler og medicinsk udstyr er den stigende mængde af forbundne anordninger almindeligvis kendt som "internet of things", eller IoT.

3.2. Hvorfor IoT er vigtig for forbrugerne

I de seneste år er internetforbundene enheder, som nævnt, blevet almindelige i mange forbrugeres liv, og den stigende brug af internetforbundene enheder er ved at ændre den måde, vi lever vores liv på. Selv om digitaliseringen af enheder giver mange fordele for forbrugerne, er de risici og udfordringer, som den medfører, lige så vigtige, hvis ikke endnu større. Hvad sker der for eksempel, når tjenesteudbyderen af dit smart home-system beslutter sig for at lukke sine servere ned? Og hvem er ansvarlig, hvis dit smart-tv bliver hacket eller ubrugeligt på grund af manglende softwareopdateringer? Og hvad med indvirkningen på vores privatliv?

Det er derfor vigtigt at udvikle klare og fremsynede EU-regler og en retlig ramme, der sikrer, at forbrugernes rettigheder opretholdes i det internetforbundene miljø.

3.3. De primære udfordringer ved IoT

At forbinde store mængder af enheder til internettet skaber både muligheder og risici for forbrugerne. Den internetforbundene verden lover øget komfort, problemfri oplevelser og potentielt betydelige forbedringer af livskvaliteten. De samlede oplysninger fra IoT-enheder kan også føre til ny viden inden for områder som lægevidenskab, kunstig intelligens og byplanlægning.

F.eks. kan et smart hjem fyldt med internetforbundene enheder og sensorer lære ejerens vaner og præferencer og tilpasses hertil. Samtidig kan de enkelte enheder kommunikere med hinanden, så at f.eks. en lav hjerterytme, der registreres af et smart ur, genererer en hastebesked til det nærmeste hospital. Desuden kan muligheden for fjernbetjening af enhederne via internettet hjælpe personer, der har brug for hjælp, med at bevare deres uafhængighed, f.eks. ved at låse døre op på afstand uden fysisk at skulle gå hen til døren. I brancher som industrien og sundhedssektoren vil IoT kunne have stor betydning for effektivitet og informationsindsamling.

Men de udfordringer, som de internetforbundene enheder medfører, er meget forskellige set fra et forbrugerperspektiv. De vedrører en lang række politiske områder og spørgsmål: privatlivets fred og databeskyttelse, cybersikkerhed, forældelse af produkter, bæredygtighed og energiforbrug, konkurrence, sikkerhed, forbrugerrettigheder osv.

For eksempel vil internetforbundene enheder typisk indsamle store mængder data om brugerne og deres omgivelser. Den omfattende dataindsamling giver anledning til en række alvorlige problemer i forbindelse med databeskyttelse og privatlivets fred. Efterhånden som flere aspekter af vores liv i stigende grad integreres i et større netværk af sensorer og enheder, vokser også de potentielle risici samt omfanget af databrud og cyberangreb. Hver ny enhed, som vi forbinder til internettet, medfører endnu en potentiel angrebsmulighed, og rækken af enheder er ofte kun så stærk som dens svageste led. Fremkomsten og implementeringen af kunstig intelligens i IoT-teknologier skaber også udfordringer i forbindelse med retfærdighed, ansvarlighed mm.

Andre udfordringer, der opstår eller forstærkes af Internet of Things, omfatter kunstig nedsættelse af produktlivscyklusser, lock-in-effekter og produktansvar.

Desuden har internetforbundne enheder et øget energiforbrug på grund af de nødvendige netværkskomponenter. En stor del af dette energiforbrug skyldes, at enhederne konstant kobler op via netværket (idle mode). Friedli et al. (2016) forventer, at det globale standby tab vil stige fra 7,5 TWh i 2015 til 47 TWh i 2025, baseret på standbyforbruget af internetforbundne enheder, der er permanent tilsluttet elnettet.[15]

3.4. De primære forbrugerrettigheder og -forpligtelser

De forbrugerrettigheder, der gælder for ikke-internetforbundene enheder, gælder også for internetforbundene enheder. F.eks. gælder reglerne om juridisk garanti (direktivet om digitalt indhold, direktivet om salg af varer) for IoT-forbrugerprodukter. Reglerne om forbrugerinformation (direktivet om forbrugerrettigheder) på salgsstedet finder også anvendelse. Se det supplerende teoretiske baggrundsdokument om generel forbrugerlovgivning for at få mere at vide om direktivet om salg af varer og direktivet om forbrugerrettigheder. I et vist omfang gælder reglerne i produktsikkerhedslovgivningen også for IoT-udstyr.

På grund af disse enheders tilslutningsmuligheder gælder der dog også særlige forpligtelser:

1) For det første skal internetforbundene enheder, der indsamler personoplysninger om forbrugere, behandle disse oplysninger i overensstemmelse med reglerne i GDPR. Disse regler omfatter bl.a., princippene om dataminimering,

[15] https://nachhaltigwirtschaften.at/resources/iea_pdf/reports/iea_4e_edna_energy_efficiency_of_the_internet_of_things_technical_report.pdf

formålsbegrænsning og databeskyttelse gennem design samt forpligtelsen til at indhente brugerens samtykke afhængigt af formålene med databehandlingen.[16]

2) For det andet skal producenter af internetforbundene enheder i henhold til radioudstyrsdirektivet fra 2014 sikre, at deres enheder har et vist sikkerhedsniveau. Tiltagene i direktivet skal sikre, at enhederne i) ikke skader netværket og forårsager en forringelse af tjenesten, ii) indeholder sikkerhedsforanstaltninger, der sikrer, at brugerens og abonnentens personoplysninger og privatlivets fred beskyttes, og iii) understøtter visse funktioner, der sikrer beskyttelse mod svindel som f.eks. ransomware.
3) For det tredje følger det af direktivet om digitalt indhold at internetforbundene enheder skal leveres med opdateringer, herunder sikkerhedsopdateringer, i et tidsrum, som forbrugerne med rimelighed kan forvente. Længden af denne forpligtelse er knyttet til den lovbestemte reklamationsret, men kan også gå længere end denne. For Danmark gælder reklamationsretten i 2 år – se mere herom her

4) For det fjerde skal producenten af den pågældende internetforbundene enhed i henhold til forordning om cybersikkerhed, hvis der findes certificeringsordninger, som finder anvendelse på den internetforbundene enhed, informere forbrugeren om den periode, hvor der vil blive tilbudt sikkerhedssupport til slutbrugerne, navnlig med hensyn til tilgængeligheden af cybersikkerheds-relaterede opdateringer.

5) For det femte skal forbrugerne kunne forvente, at adgangen til internettjenester leveres på en neutral og ikke-diskriminerende måde i overensstemmelse med forordningen om det åbne internet. Internetudbydere skal behandle al internettrafik ens uden forskelsbehandling, begrænsning eller indblanding ("netneutralitet"). Det er vigtigt at holde internetadgangen åben og neutral, hvis vi skal kunne udøve vores grundlæggende frihedsrettigheder og demokratiske rettigheder til at deltage i nutidens online-samfund, der er koblet sammen. Det er også en forudsætning for at kunne drage fordel af Internet of Things. Forbrugerne har brug for et ubegrænset og neutralt internet for at kunne bruge deres internetforbundene enheder til at få adgang til nyheder og kulturelt indhold eller til at handle uden begrænsninger.

6) For det sjette - vedrørende regler om produktansvar, blev det relevante direktiv - produktansvarsdirektivet - udarbejdet tilbage i 1985, længe før man overhovedet overvejede brugen af internetforbundene enheder, og da slet ikke kunne forudse de hertil hørende udfordringer. Direktivet er ikke længere tilpasset til at håndtere udfordringerne i forbindelse med Internet Of Things og til at sikre erstatning til forbrugerne, når noget går galt. Processen med at revidere direktivet er i gang. I april 2020 fremsatte BEUC en række anbefalinger for at sikre, at EU's

[16] For uddybende information om databeskyttelse og databeskyttelsesforordningen (GDPR), se kapitel 1.

produktansvarsregler fortsat er tilpasset forbrugerne i den digitale tidsalder og til Internet of Things.[17]

3.5. Love og reguleringer i EU

- Direktiv 2014/53/EU af 16. april 2014 om harmonisering af medlemsstaternes love om tilgængeliggørelse af radioudstyr på markedet og om ophævelse af direktiv 1999/5/EF
- Forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed)
- Direktiv 2001/95/EC af 3. december 2001 om produktsikkerhed i almindelighed
- Direktiv (EU) 2019/770 af 20. maj 2019 om visse aspekter af aftaler om levering af digitalt indhold og digitale tjenester
- Forordning om åbent internet (Forordning (EU) 2015/2120) af 25. november 2015.
- Forordning (EU) 2015/2120 om foranstaltninger vedrørende adgang til det åbne internet og om ændring af direktiv 2002/22/EF om forsyningspligt og brugerrettigheder i forbindelse med elektroniske kommunikationsnet og -tjenester og forordning (EU) nr. 531/2012 om roaming på offentlige mobilkommunikationsnet i Unionen
- Europa kommissionens rapport om consumer Internet of Things sector inquiry

* Andre relevante love, der er omfattet af andre af andre retsområder, f.eks. GDPR og forbrugerrettighedsreglerne, er ikke nævnt her, men som forklaret ovenfor gælder de også i IoT-sammenhæng ligesom for andre produkter eller tjenester. Hvis en tilsluttet enhed f.eks. behandler personoplysninger, skal den overholde den generelle forordning om databeskyttelse.

3.6. Retspraksis

I relation til 'net neutralitet' (se afsnit 5 i kapitel 3.4), Har EU-domstolen, for nyligt afsagt dom i C-854/19, C-5/20 og C-34/20 der tilbyder at anvende en "nultarif"[18] på specifikke apps - og dermed de begrænsninger, der følger af aktiveringen af disse muligheder (om båndbredde, opkobling eller brug under roaming) - er i strid med artikel 3, stk. 3, i forordningen om det åbne internet og er derfor ulovlige efter EU-retten. Tjenesteudbyderne bør derfor revidere deres handelspraksis i overensstemmelse med denne fortolkning for at sikre, at de fuldt ud overholder EU's regler om netneutralitet. Domstolen kunne anvende et lignende ræsonnement på tjenesteudbydere, der tilbyder en "nultarif" for de apps, der er

[17] BEUC, *Product liability 2.0 - How to make EU rules fit for consumers in the digital age*, April 2020, www.beuc.eu/publications/product-liability-20-how-make-eu-rules-fit-consumers-digital-age/html

[18] 'Nultarif" er en handelspraksis, hvorefter en internetudbyder anvender en "nultarif" (eller en mere fordelagtig tarif) på hele eller en del af den datatrafik, der er forbundet med en applikation eller en kategori af specifikke applikationer, som tilbydes af internetudbyderens partnere.

forbundet med internetforbundene enheder (f.eks. tilbyder en internetudbyder i forbindelse med en markedsføringskampagne en fordelagtig takst, dvs. en nultarif, til den app, der bruges til at styre et smartkamera).

3.7. Hvad kan forbrugerne gøre, hvis de har et problem?

Flere love finder anvendelse for internetforbundene enheder. Afhængigt af den gældende regulering har forbrugerne forskellige muligheder, hvis der opstår et problem. Hvis spørgsmålet er relateret til forbrugerens personoplysninger (se afsnit 1) i kapitel 3.4), finder GDPR anvendelse.[19]

- I henhold til radioudstyrsdirektivet vil forbrugerne fra 2024 kunne underrette deres nationale markedsovervågningsmyndigheder (ofte telemyndighederne), hvis der er et problem med sikkerheden i deres udstyr (se afsnit 2 i kapitel 3.4), og disse skal derefter indlede en undersøgelse af det pågældende udstyr. Markedsovervågningsmyndighedens afgørelse kan gå så vidt som til at beordre tilbagetrækning af det pågældende produkt fra markedet.
- Hvis enheden ikke er blevet leveret som forventet af forbrugerne, for så vidt angår levering af sikkerhedsopdateringer (jf. punkt 3 i kapitel 3.4), har forbrugerne ret til at ophæve aftalen, få et forholdsmæssigt nedslag i prisen eller kræve, at enheden bringes i overensstemmelse med kravene (jf. direktivet om digitalt indhold).
- I henhold til "forordning om cybersikkerhed" skal forbrugerne kunne indgive en klage til et nationalt organ, hvis sikkerhedsopdateringer er mulige i kortere tid end meddelt af producenten (jf. afsnit 4 i kapitel 3.4). Hvis forbrugerne er utilfredse med den afgørelse, som det nationale organ har truffet, har de ret til effektiv domstolsprøvelse.
- Hvis netneutraliteten ikke overholdes (se afsnit 5 i kapitel 3.4), kan forbrugerne klage til deres telekommunikationstilsynsmyndighed, som skal reagere på klager.

3.8. Yderligere kilder - faktablade, publikationer, links mv.

Arbejdsdokument fra Europa-Kommissionens administration - Advancing the Internet of Things in Europe

Europa kommissionen Sector Inquiry into the consumer Internet of Things (IoT)

BEUC redegørelse: Protecting European consumers in the world of connected devices

BEUC faktaark: Ensuring cybersecure consumer products

AK EUROPA - Consumers' expectations of the Internet of Things

[19] Se forrige fodnote.